F.H. MƏMMƏDOV
M.Y. ORUCOVA

# "INFORMASİYA TƏHLÜKƏSİZLİYİ VƏ TƏMİNATI"

# KOMPÜTER ŞƏBƏKƏLƏRİNDƏ TƏHLÜKƏSİZLİYİN TƏŞKİLİ PRİNSİPLƏRİ

**MƏMMƏDOV F. H., ORUCOVA M.Y.**

# “INFORMASİYA TƏHLÜKƏSİZLİYİ VƏ TƏMİNATI” (KOMPÜTER ŞƏBƏKƏLƏRİNDƏ TƏHLÜKƏSİZLİYİN TƏŞKİLİ PRİNSİPLƏRİ)

*Ali məktəb tələbəldə təhsil alan magistrlər üçün dərs vəsaiti*

*Azərbaycan Texniki Universitetin*
*Elmi-metodik şurasının 11.02.2022-ci il*
*tarixli (3 saylı protokol) qərarı ilə*
*dərs vəsaiti kimi təsdiq edilmişdir*

**“ZƏNGƏZURDA”**
**ç a p e v i**
**BAKI – 2022**

**UMO 004**

**Rəyçilər:** AMEA İnformasia Texnologiyaları İnstitutunun şöbə müdiri dos., t.ü.f.d. ***F.T. Ağayev***

Azərbaycan Texniki Universitetin "Radiotexnika və telekommunikasiya" kafedrasının müdiri t.e.d., professor ***B.Q. İbrahimov***

Məmmədov F.H., Orucova M.Y. **"Informasiya təhlükəsizliyi və təminatı" (Kompüter şəbəkələrində təhlükəsizliyinin təşkili prinsipləri).**
Bakı: "Zəngəzurda" çap evi, 2022. – 175 səh.

Dərs vəsaitində müasir elmi-texniki inqilabın texnoloji hadisəsi olan və cəmiyyətin informasiyalaşdırılması ilə sıx bağlı olan kom-püter şəbəkələrində təhlükəsizliyin təmin edilməsi, onların model-ləri,sintezi,strukturlarının paylanma prinsipləri və informasi-yanın sızması yolları təhlili edilir. İnformasiya mühafizəsi sistemlərinin kriptoqrafik vasitələri, mexanizmləri və modelləri işıqlandırılır. Bağ-lı və açıq açarlı kriptoqrafiya texnologiyalarına aid geniş və məzmunlu material dərc edilir,onların azərbaycan əlifbası əsasında qurulmasının və alqoritmlərinin dolğun təhlili aparılır. Tam məxfi sistemlərə baxılır, bu sistemlərdə məlumatın əldə edilməsi, emalı, ötürülməsi və mühafizəsi, eləcə də şifrləmə, maneədavamlı kodlama və informasiyanın sıxılması məsələləri işıqlandırılır. VPN şəbəkələrinə və onlarda informasiya təhlükəsizliyinin təmin olunmasına aid geniş məlumatlar verilir, bu şəbəkələrin müxtəlif şəbəkə texnologiyaları bazasında qurulması və eləcə də onların qurulmasında istifadə olunan protokolların analizi verilir.

Dərs vəsaiti ali məktəblərdə 060632-"İnformasiya texnologiya-ları və sistemləri mühəndisliyi" ixtisası üzrə təhsil alan magistrlər və kompüter şəbəkələrinin təhlükəsizliyi ilə məşqul olan mühəndis-texniki işçilər üçün də faydalı ola bilər.

**DOI: https://doi.org/10.36719/2022/175**

## MÜNDƏRİCAT

**GİRİŞ ..... 6**
**I FƏSİL. İNFORMASİYA MÜHAFİZƏSİ VASİTƏLƏRİ VƏ METODLARI ..... 10**
1.1. İnformasiya mühafizəsi vasitələri ..... 10
1.2. İnformasiyanın mühafizə mexanizmləri ..... 13
1.3. Hücumların aşkarlanması sistemləri ..... 16
1.4. Şəbəkə daxilində girişin məhdudlaşdırılması ilə şəbəkələrin təhlükəsizliyinin yüksəldilməsi ..... 17
1.5. İnformasiya mühafizəsinin kriptoqrafik vasitələri ..... 22
1.5.1. Kriptoqrafik sisemlərin modelləri və şifrləmə metodları ..... 24
1.5.2. Sezar şifrləmə metodu ..... 27

**II FƏSİL. SİMMETRİK ŞİFRLƏMƏ TEXNOLOGIYALARI ..... 30**
2.1. Simmetrik şifrləmənin struktur sxemi ..... 30
2.2.Əvəzetmə metodu ..... 32
2.2.1.Birəlifbalı əvəzetmə. ..... 32
2.2.2. Rəqəm şəkilli informasiyanın şifrlənməsi ..... 36
2.2.3. Proporsional şifrləmə üsulu ..... 37
2.3. Çoxəlifbalı əvəzləmə üsulu. ..... 38
2.4. Qammalaşdırma üsulu ..... 46
2.5. Yer dəyişdirmə metodu ..... 51
2.6. Cədvəl üzrə yerdəyişmə ..... 53
2.7. Proqram və aparat yolu ilə reallaşdırılan yerdəyişmə ..... 55
2.8. Kompozisiya şifri anlayışı ..... 55
2.9. Simmetrik şifrləmənin blok alqoritmlərində istifadə olunan əməliyyatlar ..... 58
2.10. Cədvəl əvəzlənməsi ..... 60
2.11. Simmetrik şifrləmənin blok alqoritminin strukturu ..... 61
2.12. Bağlı açarlı blok şifrinin qurulma prinsipi ..... 61
2.13. DES və AES şifrləmə alqoritmləri ..... 63
2.13.1. Əsas məlumatlar ..... 63
2.13.2. İkiqat DES və "ortada görüş" hücumu ..... 68
2.13.3. Üçqat DES ..... 69
2.13.4. Reyndal alqoritmi ..... 70
2.14. DÜİST28147-89 –üzrə verilənlərin kriptoqrafik çevrilməsi alqoritmi ..... 74
2.14.1.Əsas məlumatlar ..... 74

2.14.2. DÜİST28147-89-un raundunun strukturası ..... 75
2.14.3 Şifrləmə və şifrin açılması əməliyyatları ..... 76
2.14.4. Şifrləmənin əsas rejimləri ..... 78
2.14.5. DÜİST 28147-89 və DES şifrləmə alqoritmləri arasındakı fərq ..... 79
2.15. Kriptoqrafik heş-funksiya ..... 80
2.15.1.Heş- funksiya anlayışı ..... 80
2.15.2. Heş-funksiyanı formalaşdırmaq üçün şifrləmənin blok alqoritmindən istifadə edilməsi ..... 82
2.16. Arakəsilməz şifr və saxta təsadüfi ədədlər generatoru ..... 84
2.16.1.Arakəsilməz şifr ..... 84
2.16.2. Arasıkəsilməz şirləmə zamanı saxtatəsadüfi ədədlər generatorlarının istifadə olunması prinsipi. ..... 87
2.16.3. Xətti konqruyent saxtatəsadüfi ədədlər generatoru ..... 88
2.17. Gecikmə ilə Fibonaççi metodu ..... 89
2.17.1.BBS alqoritmi əsasında saxtatəsadüfi ədədlər generatoru ..... 91
2.18. Əks əlaqəli sürüşmə registri əsasında saxta təsadüfi ədədlər generatoru. ..... 92
2.18.1. Saxta təsadüfi ədədlər almaq üçün OFB və CTR rejimlərindən istifadə olunması ..... 94
2.19. RC4-aqoritmi ..... 96
2.20. Məxfi açarın idarə olunması ..... 106

**III FƏSİL. AÇIQ AÇARLI KRİPTOQRAFİYA TEXNOLOGİ-YALARI ..... 110**
3.1. Açıq açarlı kriptoqrafiyaya giriş ..... 110
3.1.1. Birtərəfli funksiya ..... 111
3.2. Açıq açarlı alqoritm əsasında rəqəmli imza ..... 113
3.3. Asimmetrik alqoritmdən istifadə etməklə məxfi açarın formalaşdırılması ..... 118
3.3.1. Açıq açarlı şifrləmə alqoritminə tələblər ..... 120
3.4. Kombinasiya olunmuş şifrləmə kriptosistemi ..... 121
3.5. Elektron rəqəmli imza ..... 124
3.5.1.Elektron rəqəmli imza və heşləmə funksiyası ..... 124
3.5.2. Rəqəmli imzanın əsas prosedurları ..... 125
3.5.3. Rəqəmli imzanın formalaşdırılması proseduru ..... 126
3.5.4. Rəqəmli imzanın yoxlanılması proseduru ..... 127
3.5.5.Heşləmə funksiyası ..... 129

**IV FƏSİL. TAM MƏXFİ SİSTEMLƏR ..... 131**
4.1. Məlumatın əldə edilməsi, emalı, ötürülməsi və qorunması..... 131
4.2. Entropiya və qeyrimüəyyənlik ..... 133
4.3. Dil norması və məlumat artıqlığı ..... 135
4.3.1 Dilin mütləq norması ..... 135
4.3.2. Dilin artıqlığı ..... 136
4.4. Tam məxfi sistemlər anlayışı ..... 136
4.4.1.Təklik (yaxud nadirlik) məsafəsi ..... 138
4.5. Şifrləmə, maneəlovamlı kodlama və informasiyanın sıxılması ..... 140
4.5.1.Maneədavamlı kodlama ..... 142
4.5.2. Kod sözü ..... 143
4.6.Verilənlərin sıxılma prinsipləri ..... 147

**V FƏSİL. VPN TEXNOLOGİYASI BAZASINDA LOKAL KOMPÜTER ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA MÜHAFİZƏSİNİN TƏŞKİLİ ..... 152**
5.1. VPN texnologiyası bazasında Lokal kompüter şəbəkələrinin qurulması..... 152
5.2. Xüsusi tunel vasitəsilə ötürülən paketin bir nümunəsi ..... 156
5.3. Lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması ..... 157
5.4. VPN texnologiyası bazasında qurulmuş lokal kompüter şəbəkələrində verilənlərin mühafizə vasitələri ..... 159
5.5. Lokal kompüter şəbəkələrinin müxtəlif VPN texnologiyaları bazasında qurulması ..... 163
5.6. Lokal kompüter şəbəkələrinə uzaq daxilolmaların təmin olunması üçün istifadə olunan tunelləşmə protokolları ..... 166

**ƏDƏBIYYAT .....172**

# GİRİŞ

Hal-hazırda informasiyanın kompleks mühafizəsi probleminin həlli ilə yüksək ixtisaslı mütəxəssislər məşquldur. İnformasiya mühafizəsinin müxtəlif vasitələri arasında kriptoqrafik metodlar xüsusi yer tutur. Bir tərəfdən, bu onunla bağlıdır ki, kriptoqrafik metodlar insanlara çoxdan məlumdur və onları çoxdan istifadə edirlər.

Digər tərəfdən, kriptoqrafiyanın yeni nailiyyətləri nəinki, klassik məsələləri həll edir, həm də digər növ mühafizə vasitələrin həll edə bilmədiyi məsələləri həll etməyə imkan verir. Belə məsələlərə misal olaraq elektron sənədlərə rəqəmli imzanın formalaşdırılma-sını və elektron pulun istifadə olunması imkanını aid etmək olar. Kriptoqrafiyanın inkişafı uzun illər ləng inkişaf etmişdir, lakin XX əsrdə riyaziyyatda əldə olunan nailiyyətlər sayəsində kriptoqrafiya-ya sıçrayışla inkişaf etməyə başladı.

Tarixi bilinməsə də, "gizli yazı" mənasına görə də güman etmək olar ki, kriptoqrafiya yazı ilə bir vaxtda meydana gəlmişdir. *Krip-toqrafiya* informasiyanın kənar və ya qanunsuz istifadəçilərdən qo-runması məqsədi ilə çevrilməsi metodlarının işlənməsi haqqında elmdir.

Kriptoqrafiya yunan dilində və *γραφω* (gizli) və *kryptos* «yazı» sözlərindən yaranmışdır. Kriptoqrafiyada adətən kənar istifadəçi-lərin (əks kəşfiyyatın) rabitə kanalına tam nəzarət etməsi fərziyyəsi nəzərdə tutulur. Kriptoqrafiya məlumatların ötürülməsi faktını "giz-lətmir", onları həmin tərəflərin anlaması üçün mümkün olmayan şəklə çevirir. Kriptoqrafiyanin inkişaf dövrü XIV əsrin sonuna təsa-düf edir. Siyasətdə, diplomatiyada və hərbi işlərdə ənənəvi tətbiqi ilə yanaşı kriptoqrafiya intellektual mülkiyyətin qorunmasında və ya piratçılığın qarşısını almaqda və s. kimi işlərdə də istifadə olun-mağa başlandı.

**Kriptoqrafiyanın tarixindən məlumatlar.** XIX əsrin sonların-da hərbi akademiyalarda öyrənilməsinə başlanması kriptoqrafiyaya dəqiq elm əlamətləri verir. Bu akademiyaların birində "Sen-Sir xət-keşi"adlandırılan məxsusi hərbi-səhra şifrəsi hazırlanmışdır.Sen-Sir xətkeşinin ideyasında inkişaf hərəkət edən hissədə hərflərin ixti-yari ardıcılliqda düzülməsi ilə bağlıdır.

Elmi metodlar kriptoqrafiya üzrə ilk dəfə ərəb ölkələrində mey-dana gəlmişdir. Şifrə sözünün özü (ərəbcə "sıfra"(rəqəm)) ərəb mənşəlidir. İlk dəfə məhz ərəblər açıq mətni mühafizə etmək məq-sədilə hərfləri rəqəmlərlə əvəz etdilər. Xüsusi olaraq bir neçə şifrə-yə həsr olunan "İnsanların qədim yazıların sirlərini açmasına böyük cəhdləri haqqında kitab" adlandırılmış birinci kitab 855-ci ildə işıq üzü görmüşdür. İtaliyalı riyaziyyatçı və filosof Cerolamo Kardano bir hissəsi kriptoqrafiyaya həsr edilmiş "İncəliklər haqqında" kitab yazmışdır. Kardano açarların sayını nəzərə almaqla şifrələrin da-vamlığının "isbatını"vermiş, açıq mətni açar kimi istifadə etməklə ye-ni şifr- "Kardano qəfəsi" təklif etmişdir.

Kardano qəfəsi bərk maddədən hazırlanan lövhə üzərində fərqli intervallarla bir hərf hündürlüklü və müxtəlif uzunluğa malik düz-bucaqlı kəsiklər açmaqla təşkil edilir. Vərəq üzərinə bu qəfəsi qoy-maqla kəsiklərə məxfiləşdirilməli məlumat yazarlarmış. Qəfəs gö-türüldükdən sonra qalan sahələrə ixtiyari məzmunlu mətn elə yerləşdirilirdi ki, məxfiləşdirilmiş məlumat müxtəlif uzunluqlu kə-sik yerlərinə səpələnərək kriptomətnin tərkib hissəsinə çevrilirdi 4 (üzü yuxarı, üzü aşağı, şaquli və döndərilmiş) vəziyyətdə tutularaq yerləşdirilərək qəfəsin yerləşdirilməsinin mümkün sayı dörd dəfə artır. Ümumiyyətlə XIX əsr kriptoqrafiyaya bir neçə yeni ideya gə-tirmişdir.

Tomas Cefferson (Amerikanın birinci dövlət katibi, sonra isə prezdenti) kriptoqrafiya tarixində xüsusi yer tutan "diskli şifrə"- sistemi yaratmış, onu Cefferson şifrələyicisi-xüsusi qurğu ilə real-laşdırmışdır. Şifrələyicinin konstruksiyası qısa olaraq aşağıdakı ki-mi şərh edilir. Ağac silindir 36 (fərqli də ola bilər) dairəyə döğra-nır. Ayrıca olaraq sərbəst firladıla bilməklə onlar bir ox boyu yer-ləşdirilir. Kəsiklərin üz tərəfinə ingilis əlifbasının hərfləri ixtiyari ardıcıllıqda qeyd olunur. Silindirin səthi üzrə oxa paralel çubuq bərkidilir. Şifrələmə zamanı açiq mətn 36 hərf üzrə qruplaşdırılır. Mətni təşkil edən hərflər öz qrupunda durduğu sira nömrəsinə uyğun nömrəli dairədə çubuq üzrə düzülür. Şifrələnmiş mətn həmin çubuğa paralel istənilən sıradan seçilə bilir. Alınmış kriptomətn analoji şifrələyicidə dairələri fırlamaqla yığılır, açıq mətn isə ona paralel sıralar içindən seçilir.

1817-ci ildə Desius Uodsvort prinsip etibarı ilə yeni şifrələmə qurğusu konstruksiya etdi. Burada yenilik açıq mətnlə şifrələnmiş mətnin müxtəlif uzunluqlara malik olmasından ibarət olmuşdur. XIX əsrin 80-ci illərində Oqyust Kerkqoffs "Hərbi kriptoqrafiya" adlı kitab dərc etdirdi. Bu kitab cəmi 64 səhifədən ibarət olsa da, bu səhifələr onun kriptoqrafiya tarixində ölməzliyini təmin etmişdir. Həmin kitabda şifrə üzrə 6 əsas tələb irəli sürülmüşdür ki, onlar bu gündə aktualdır:

1. Sistemin fiziki, yoxsa riyazi belə üstü açılmamalı.
2. Sistemin gizli saxlanması tələb olunmasa da, onu kənar tərəflərin əldə etməsi rahatsızlıq yaratmamalı.
3. Açar sadə olmaqla, yadda kağıza (informasiya daşıyıcılarına) qeyd edilmədən saxlanaraq, müəllif tərəfindən asanlıqla dəyişilə bilən olmalı.
4. Sistem teleqrafla (rabitə sistemilə) ötürülə bilən məlumata yararlı olmalı;
5. Sistem asan daşına (köçürülə) bilinməklə onun işlənməsində bir neçə istifadəçinin (fərdin) iştirakı tələb edilməməlidir.
6. Nəhayət, müxtəlif şəraitlərdə tətbiq ediləcəyini nəzərə alaraq sistemdən dərin zəka və riayət edilməli çoxlu sayda qayda tələb etmədən asanlıqla istifadə oluna bilinməsi tələb olunur.

Bu tələblərdən ikincisi *Kerkqoffs prinsipi* kimi məhşurlaşmışdır. Onun mahiyyəti nə qədər az məxfi element saxlanarsa sistem bir o qədər təhlükəsiz hesab edilməsindən ibarətdir. Sistemin açıqlığı onun təhlükəsizliyinə təsir etməməlidir. Şennon bu prinsipi "Qarşı tərəf (düşmən) sistemi bilir" kimi ifadə etmişdir. Kerkqoffs prinsipi alqoritm və protokolların təhlükəsizliyinin onların məxfiliyindən asılı olmamasına istiqamətlənmişdir.

Kriptosistemlərin təşkili qaydası olaraq Kerkqoffs prinsipinə görə müəyyən işarələr ardıcıllığından ibarət alqoritmin açar adla-nan parametri yalnız gizlədilir.

1917-ci ildə amerikalı Edvard Xepbern tərəfindən "Eniqma" (tapmaca) rotor maşını icad olundu. "Eniqma"elektrik yazı maşının üzərində işləyirdi. Sonrada (1923-cü ildə) berlinli mühəndis Artur Şer-buis "Eniqma"–nın ayrıca sənaye versiyasını hazırlamışdır.

Statistik tədqiqatlara əsaslanaraq onun etibarlığına son dərəcə inamla Almaniya hökuməti onun üzərində hüquqlarını tam bərqərar edərək özünün hərbi qüvvələrinin ehtiyacları üçün istifadə etməyə başlamışdır.XX əsrin ikinci yarısında hesablama texnikasının inki-şafı nəticəsində elektron şifrləyicilər yaradıldı.

Bu gündə onlar etibarlıq və sürət tələblərini təmin edərək şifrələmə vasitələrinin böyük əksəriyyətini təşkil edərlər. XX əsrin yetmişinci illərində Kerkqoffsa prinsiplərini "leqallaşdıran" veri-lənləri şifrələmə standartı (DES) qəbul olunub dərc edildi. Amerika riyaziyyatçıları Uitfrid Diffi *(Diffie)* və Martin Hellman tərəfindən aparılan tədqiqatlar sayəsində "yeni kriptoqrafiya"-açıq açarlı kriptoqrafiya meydana gəlmişdir.

Beləliklə XX əsr şifrələmədə inqilablar əsri hesab olunur.

- Hilbert Vernam metodu (O, teletayp məlumatlarını şifrələmək üçün təsadüfi işarələrlə "qamma" perfolentinin istifadə olunmasını təklif etmişdir).
- XX əsrin 70-ci illərində ABŞ-da ilk dəfə informasiyanın kriptoqrafik mühafizəsi üzrə mülki standart (DES, Data Encryption Standard) qəbul olunmuşdur.
- 1976-cı ildə Uitfrid Diffi (Diffie) və Martin Hellman açıq açarlı kriptoqrafik inqilabi konsepsiya təklif etmişdirlər.
- Tətbiq sahələrinin genişlənməsi ilə əlaqədar olaraq kriptoqrafiyanin əhəmiyyəti daha da artır:

- Elektron imza;
- Autentifikasiya, əslliyin təsdiqi və elektron sənədlərin tamlığı (bütövlüyü);
- Elektron ticarətin təhlükəsizliyi;
- İnternet ilə mübadilə olunan informasiyanın mühafizəsi və s.

Elektron informasiya mübadiləsi vasitələrinin hər bir istifa-dəçisinin kriptoqrafiya ilə tanışlığı tələb olunur. Ona görə də İKT vərdişlərinə yiyələnmək üzrə **"**ikinci savad" ilə yanaşı kriptoqrafiya üçüncü savad hesab olunur.

# I FƏSİL. İNFORMASİYA MÜHAFİZƏSİ VASİTƏLƏRİ VƏ METODLARI

## 1.1. İnformasiya mühafizəsi vasitələri

İnformasiya mühafizəsi vasitələri dedikdə mühəndistexniki, elektrik,elektron və digər qurğular, aparatlar, eləcə də informasiya mühafizəsi üzrə müxtəlif məsələləri həll edən digər elementlər, o cümlədən sızmanın qarşısının alınmasını və mühafizə olunan informasiyanın təhlükəsizliyini təmin edən elementlər başa düşülür. İnformasiya mühafizəsinin təmin edən vasitələr reallaşdırılma üsullarına görə aşağıdakı qruplara bölünür [1,2]:

- texniki vasitələrə;
- aparat vasitələrinə;
- proqram vasitələrinə;
- qarışıq vasitələrə;
- təşkilati vasitələrə;
- kriptoqrafik vasitələrə.

**Texniki vasitələr** növlərinə görə mexaniki, elektromexaniki, elektron və s. olurlar. Bu vasitələr aparat vasitələrinin köməyi ilə informasiya mühafizəsi məsələlərini həll edirlər. Onlar informa-siyaya daxilolmanın, o cümlədən onun köməkliyi vasitəsilə mas-kalanmanın qarşısını alırlar. Texniki vasitələrin üstün cəhətlərinə onların etibarlığını, subyektiv faktorlardan asılı olmamalarını, mo-difikasiyaya yüksək dayanıqlıqlarını aid etmək olar. Çeviklikiynin zəif olması, nisbətən böyük həcmə və çəkiyə, eləcə də baha başa gəlmələri onların çatışmayan cəhətidir.

İnformasiya sistemlərinin perimetrlərinin mühafizəsi üçün aşa-ğıdakı informasiya sistemləri yaradılır [1,2]:

- mühafizə və yanğın siqnallaşması;
- rəqəmli video müşahidə sistemi;
- nəzarət və daxilolmanın idarə olunması sistemi(NDİS).

İnformasiyanın texniki rabitə kanalları ilə sızmadan mühafizəsi aşağıdakı vasitələr və tədbirlərlə təmin olunur:

- ekranlaşdırılmış kabeldən istifadə olunması;

- rabitə xəttinə yüksəktezlikli süzgəcin qoyulması;
- ekranlaşdırılmış binanın tikilməsi (“kapsul”);
- ekranlaşdırılmış avadanlığın istifadə olunması;
- nəzarət etmə zonanın yaradılması və s.

**Aparat vasitələri.** Aparat vasitələrinə aiddirlər: elektron, elektronmexaniki, elektron-optik qurğuları, küy generatoru, şəbəkə süzgəci və informasiya sızmasının potensial kanallarının mühafi-zəsini təmin edən yaxud onları aşkar etməyə imkan verən digər qurğular aiddirlər. Hal hazırda informasiya mühafizəsinin çoxlu sayda aparat vasitələri mövcuddur, lakin onlardan ən geniş yayıl-mışlar aşağıdakılardır [1,2]:

- mühafizə rekvizitlərinin saxlanılması üçün xüsusi registrlər: parollar, eyniləşdirici kodlar, qrif və yaxud məxfilik dərəcəsi;
- şəxsiyyətin tanınması məqsədilə, onun fərdi xarakteristikalarını ölçən qurğu (səsi, barmaq izlərini);
- periodik olaraq verilənlərin ötürülməsi adreslərinin yoxlanılması məqsədilə rabitə xəttində informasiya verilişinin kəsilməsi;
- informasiyanın şifrlənməsi qurğusu (kriptoqrafik üsullar).
- kompüterin etibarlı yüklənməsi modulu.

**Proqram vasitələri** istifadəçilərin eyniləşdirilməsi, daxilol-maya nəzarət, informasiyanın şifrlənməsi, müvəqqəti növlü qalıq fayllarının kənar edilməsi, mühafizə sistemlərinə testlə nəzarət edilməsi və s. üçün proqram vasitələrindən ibarətdir. Proqram vasitələrinin üstün cəhətlərinə, onların universallığı, çevikliyi, etibarlığı, qurulmasının sadəliyi, modifikasiyaya və inkişaf qabliyyətləri aiddir. Çatışmayan cəhətlərinə isə şəbəkə funksional-lığının məhdudluğu, resursların (fayl-serverin ) və işçi stansi-yaların bir hissəsinin istifadə olunması, təsadüfi və qəsdən edilən dəyişikliklərə həssaslığı, kompüterlərin növündən asılılığının mümkünlüyü aiddirlər.

Proqram vasitələrinə aşağıdakılar aiddirlər [1,2]:

- başqa qurğu daxilində qurulan mühafizə vasitələri;
- antivirus proqramı-bu, kompüter viruslarının aşkar edilməsi və yoluxdurulmuş faylların müalicə edilməsi, eləcə də yoluxmuş

faylların kənar edilməsi yaxud əməliyyat sistemlərinin ziyanverici kodlardan təmizlənməsi proqramıdır.

- şəbəkələrarası ekran (eləcə də brandmauer yaxud fayrvol–almanca, ingiliscə *firewall*-"yanğının qabağını alan divar").

Lokal və qlobal şəbəkələr arasında xüsusi aralıq serverlər yara-dılır. Bu serverlər onlardan keçən şəbəkə/nəqliyyat səviyyələ-rinin trafiklərinə nəzarət edir və süzgəcləyir. Bu korporotiv şəbə-kələrə kənardan icazəsiz daxilolmaları kəskin olaraq azaldır, lakin bu təhlükəni tam aradan qaldıra bilmir. Metodun daha çox müha-fizə olunmuş növü-maskarad növüdür. Burada lokal şəbəkəni görünməz etməklə, lokal şəbəkədən fireval-server adından bütün çıxış trafiki göndərilir [1,2].

- proxy-servers (proxy-etibarnamə, etibar edilən şəxs). Lokal və qlobal şəbəkələr arası şəbəkə/nəqliyyat səviyyələrinin bütün trafikləri tam qadağan edilir-marşrutlaşma olmur. Bu zaman lokal şəbəkədən qlobal şəbəkəyə müraciət xüsusi server vasitəsi ilə həyata keçirilir. Aşkardır ki, bu zaman qlobal şəbəkədən lokal şəbəkəyə prinsipcə müraciət mümkün olmur. Bu metod daha yüksək səviyyələrdə, məsələn, tətbiq səviyyəsində (viruslar, Java kodu və Java Script) hücumdan mühafizəni kifayət dərəcədə təmin edə bilmir.
- VPN (xüsusi virtual şəbəkə) şəbəkə üzərindən məxfi informasiyanın verilməsinə imkan yaradır. Bu metod şəbəkə üzrə məxfi informasiyanın verilməsi zamanı, onun kənar şəxslər tərəfindən eşidilməsinə imkan verir.

***Qarışıq* vasitələr** ayrı-ayrılıqda aparat və proqram vasitələrinin funksiyalarını yerinə yetirirlər və aralıq xüsusiyyətlərə malikdir-lər [1,2].

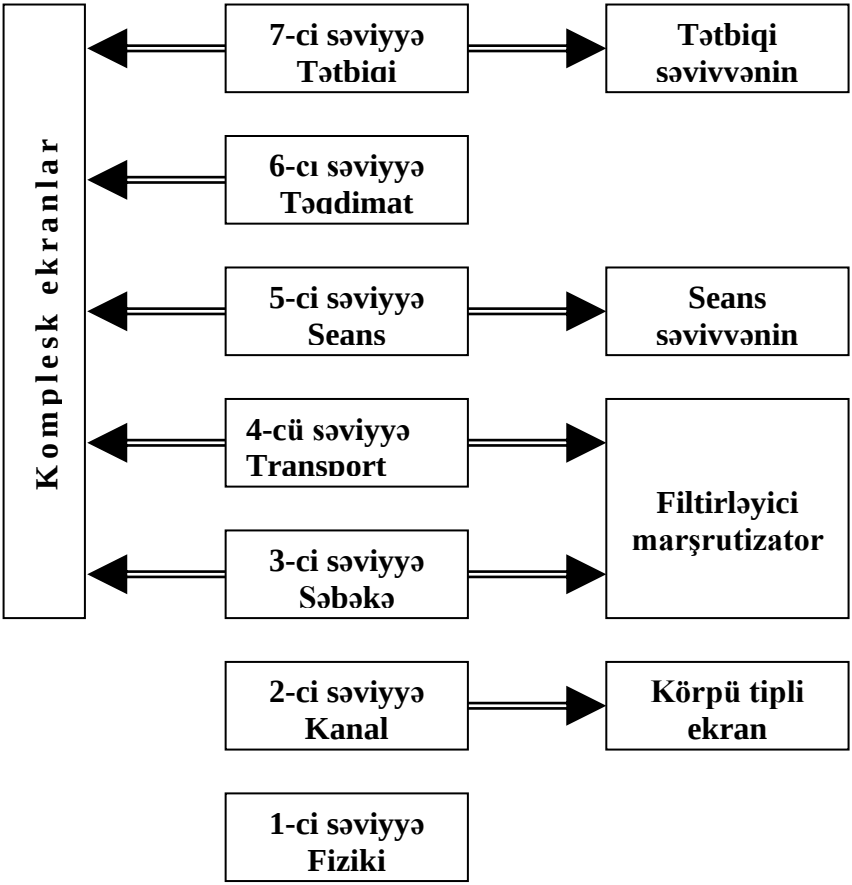
**Təşkilati vasitələr** təşkilati-texniki (binanın kompüterlə, daxilolmanın məhdudlaşdırılmasını nəzərə almaqla kabel sistemi ilə təhciz edilməsi və s.) və təşkilati-hüquqi (milli qanunvericilik və konkret müəssisənin rəhbərliyinin qoyduğu iş qaydası) vasitə-lərin cəmindən ibarətdir [1,2]. Bu vasitələrin üstün cəhəti ondan ibarət-dir ki, onlar müxtəlif məsələlərin həll olunmasına imkan verir, sadə reallaşdırılır, şəbəkədə arzuolunmaz hərəkətlərə tez reaksiya verir, sonsuz

modifikasiya və inkişaf imkanlarına malikdir. Çatış-mayan cəhətlərinə isə subyektiv faktorlardan asılı olması, konkret bölmələrdə işin ümumi təşkili aiddir.

### 1.2. İnformasiyanın mühafizə mexanizmləri

**Şəbəkələrarası ekran**. İnformasiya təhlükəsizliyinin proqram-aparat vasitələri haqda danışarkən qəbul etmək lazımdır ki, lokal şəbəkələrin obyektlərinin açıq şəbəkələrin (məsələn, İnternet şəbə-kəsinin) təsirlərindən mühafizə etmək üçün ən effektiv üsul, onla-rın arasında hər-hansı bir elementin yerləşdirilməsi üsuludur. Bu element ondan keçən şəbəkə paketlərinin verilən qaydaya uyğun olaraq nəzarət edir və süzgəcləyir. Bu element şəbəkələrarası ek-ran yaxud fayrvol, brandmuer(“firewall”) adını almışdır. Qorunan korporativ şəbəkənin resurslarına girişin məhdudlaşdırılması və bu şəbəkə ilə xarici şəbəkələr arasında, elecə də şəbəkənin seq-mentləri arasında informasiya axınlarının nəzarət edilməsi üçün qorunma vasitələrinin şəbəkələrarası qoruyucu ekranların isti-fadəsi zəruridir. Şəbəkələr arası ekran (ŞAE)-korporativ kompü-ter şəbəkələrində avtomatlaşdırılmış informasiya sistemlərinə da-xil olan və ya onlardan çıxan informasiya axınına nəzarəti həyata keçirən lokal və ya funksional baxımdan paylanmış proqram (pro-qram-aparat) vasitələridir (şək.1.1). Korporativ kompüter şəbəkə-lərində şəbəkə ekranın qoşulma sxeminin aşağıdakı təsnifatını ver-mək olar [1,2] (şək. 1.2):

- körpü tipli ekranlar (OSİ modelinin 2-ci səviyyəsi);
- filtirləyici marşutizatorlar (OSİ modelinin 3-cü və 4-cü səviyyəsi);
- seans səviyyəsinin şlüzləri (OSİ modelinin 5 ci səviyyəsi);
- tətbiqi səviyyənin şlüzləri (OSİ modelinin 7 ci səviyyəsi);
- kompleks ekranlar (OSİ modelinin 3-7-ci səviyyələri);




**Şək.1.2.** ŞE-nin OSİ modelinin müxtəlif səviyyələrində reallaşdırılması

Şəbəkələrarası ekran OSİ modelinin aşağıdakı səviyyələrində işləyə bilər [1,2]:

1. Şəbəkə səviyyəsində.
2. Seans səviyyəsində.
3. Tətbiqi səviyyədə.

**Şəbəkə səviyyəsində süzgəcləmə.** Bu səviyyədə giriş və çıxış paketlərinin süzgəclənməsi TCP və İP paketlərinin başlıqlarındakı

informasiyalar əsasında həyata keçirilir: göndəricinin İP-ünvanın-da; alıcının İP-ünvanında; göndəricinin portunda; alıcının portun-da.

Bu növ süzgəcləmənin aşağıdakı üstün cəhətləri var [1,2]:

- dəyərinin nisbətən aşağı olması;
- süzgəclənmə qaydasının təyin olunmasında çevikliyi;
- paketlərin keçməsində kiçik gecikmənin olması.

Çatışmayan cəhətləri:

- fraqmentləşdirilmiş paketləri toplaya bilməməsi;
- paketlərarası qarşılıqlı əlaqəyə nəzarət edə bilməməsi.

**Seans səviyyəsində süzgəcləmə.** Bu səviyyədə aşağıdakı növ süzgəcləmə həyata keçirilir [1,2]:

- sadə süzgəcləmə. Bu növ süzgəcləmə cari birləşməni nəzarət etmir, statistik qaydalara əsasən yalnız verilənlər axınını süzgəcləyir;
- konteksti nəzərə almaqla süzgəcləmə. Bu növ süzgəcləmə yalnız uyğun protokolların və tətbiqlərin məntiqini və iş alqoritmlərini təmin edən cari birləşməni nəzarət edir.
- Bu növ süzgəcləmənin aşağıdakı üstün cəhətləri var [1/2]:
- paketlərin tutumunun analizinin aparılması;
- 7-ci səviyyənin protokollarının işi haqqında informasiyanın tələb olunmaması.

Çatışmayan cəhətləri təybiqlərin səviyyələrində verilənlərin analizinin mürəkkəbliyi.

**Tətbiqi səviyyədə süzgəcləmə.**Paketlərin süzgəclənməsinə xas olan zəif yerləri mühafizə etmək üçün şəbəkələrarası ekran Telnet, HTTP, FTP protokollarından istifadə etməlidir.

Üstün cəhətləri [1,2]:

- süzgəclənmənin sadə qaydası;
- çoxlu sayda yoxlamaların təşkil olunması;
- tətbiqlərin verilənlərinin analiz edilməsi qabliyyətinin olması

Çatışmayan cəhətləri [1,2]:

- məhsuldarlığının aşağı olması;
- məlum olmayan protokollardan istifadə oluna bilməməsi;
- mürəkkəb əməliyyat sistemlərinə malik olması

ŞE-nin qeyd olunan təsnifatından əlavə aşağıdakı növləri mü-əyyən olunur:

Ekspert səviyyəli ŞE-OSİ modelinin üç (şəbəkə, seans, tətbiqi) səviyyəsində qəbul olunan paketlərin məzmununu yoxlayır.

Fərdi ŞE-hansı növ sistem funksiyaların və ya proseslərin şəbə-

kənin resurslarına giriş imkanı və hüquqlarına malik olmasına gö-rə idarəetmə prinsiplərinə əsaslanaraq gələcəkdə qorunmanı genişləndirməyə imkan verir. Bu növ ŞE trafikin icarəyə verilməsi və ya rədd edilməsi üçün müxtəlif siqnatura və şərtləri istifadə edə bilərlər. Dinamik ŞE-yuxarıda qeyd olunan standart ŞE-ləri və şə-bəkəyə soxulmaların aşkarlanması üsullarını birləşdirir, bunun kö-məyilə müəyyən siqnaturalara uyğun gələn və həmin porta digər mənbələrdən qoşulmalara icazə verən şəbəkə qoşulmalarının ani olaraq bloklanmasını təmin edir. Məsələn, normal fəaliyyəti poz-madan şəbəkə qurdlarının fəaliyyətini dayandırmaq olar.

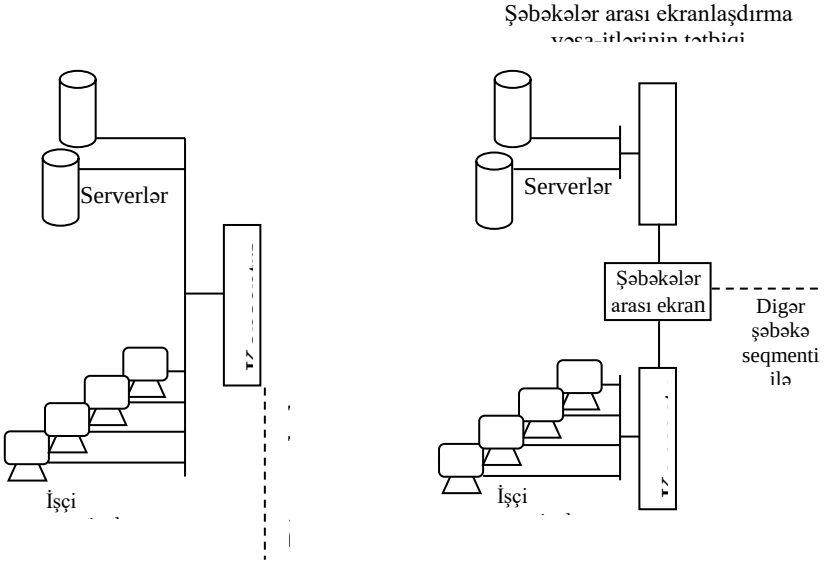
### 1.3. Hücumların aşkarlanması sistemləri

Korporativ informasiya sistemlərinin normal fəaliyyətinin təmin edilməsi üçün vacib olan standart qoruma vasitələri (məsələn, ŞE, ehtiyat sürətin saxlanılması sistemi, antivirus proqramları) ilə yanaşı hücumların aşkarlanması sistemlərinin (HAS) istifadəsinə zərurət yaranır. HAS şəbəkə hücumları ilə mübarizə üçün əsas vasitədir. Hazırda HAS korporativ kompüter şəbəkələrinin təhlükəsizliyinin təmin edilməsi üçün getdikcə daha çox istifadə olunur. HAS-ın tipik arxitekturasına, bir qayda olaraq aşağıdakılar daxil edilir [1,2]:

- sensor (informasiya toplama vasitələri);
- analizator (toplanmış informasiyanın təhlili vasitələri);
- reaksiya vermə vasitələri;
- idarə etmə vasitələri;

Aydındır ki, HAS-ın qeyd olunan bütün komponentləri bir kompüterdə və ya bir proqram əlavəsi çərçivəsində fəaliyyət göstərə bilər. Lakin onların ərazicə və funksional baxımdan korporativ şəbəkənin hissələri üzrə paylanması daha məqsədə-uyğundur. HAS – ın analizator və idarə etmə vasitələrinin ŞE-dən sonra xarici şəbəkədə

yerləşdirilməsi çox təhlükəlidir. Belə ki, əgər bu vasitələr sındırılarsa, onda bədniyyətli (cinayətkar) şəxs HAS-da istifadə olunan baza qaydalarını təhlil etəmklə qorunan daxili şəbəkənin strukturu haqqında məlumatlara giriş əldə edə bilər. HAS-ın nü-munəvi arxitekturası, başqa sözlə, onun komponentlərinin yerləş-dirilməsi sxemi şək.1.3-də göstərilmişdir.




**Şək.1.3.** HAS-ın nümunəvi strukturu 1.4. Şəbəkə daxilində girişin məhdudlaşdırılması ilə şəbəkələrin təhlükəsizliyinin yüksəldilməsi

## 1.4. Şəbəkə daxilində girişin məhdudlaşdırılması ilə şəbəkələrin təhlükəsizliyinin yüksəldilməsi

Müasir korporativ kompüter şəbəkələrinin qeyri-bircinsliliyi və miqyasının sürətli artımı nəinki xarici, eləcə də daxili şəbəkə ser-vislərində də həddən artıq zəif yerlərin çoxalmasına gətirib çıxarır.

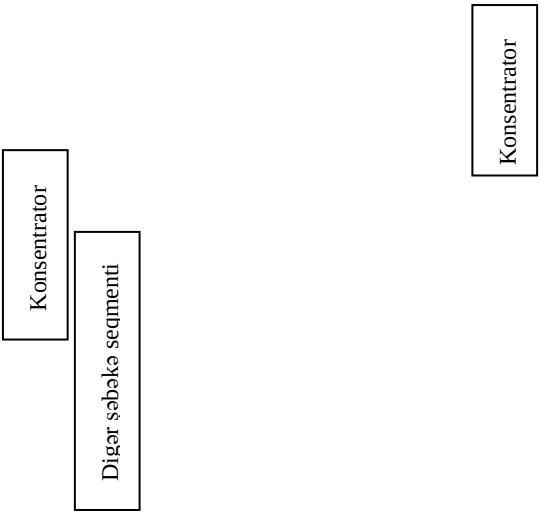
Şəbəkə nə qədər böyük olarsa, administrator tərəfindən onun təhlükəsizliyinin etibarlı təmin edilməsi bir o qədər çətin olar. Nə-zərə almaq lazımdır ki, şəbəkədə icazəsiz girişə yalnız işçi stan-siyalar, serverlər və ya rabitə xətləri deyil, həmçinin məlumat axınlarının

şəbəkədaxili marşrutlaşdırma funksiyalarını yerinə yetirən xüsusiləşdirilmiş qurğular da məruz qala bilər. Müasir korporativ kompüter şəbəkələrində müxtəlif növ qeyri bircins proqram-texniki təminat istifadə olunur. Bununla əlaqədar olaraq, korporativ şəbəkənin mürəkkəbliyi əhəmiyyətli dərəcədə artır. Belə şəraitdə korporativ şəbəkənin ümumi resurslarına onun daxili istifadəçiləri tərəfindən icazəsiz giriş təhlükələri də güclənir. Bu vəziyyətdən çıxış yolu kimi korporativ şəbəkənin ümumi resurs-larının qorunmasını şəbəkə daxili girişin məhdudlaşdırılması sə-viyyəsini idarə etməklə gücləndirmək olar. Bunu isə Firewall və ya brandmauer adlanan şəbəkələrarası ekranlaşdırma vasitələrinin köməyi ilə reallaşdırmaq mümkündür. İcazəsiz girişə qarşı müba-rizə aparmaq üçün brandmauer şəbəkədaxili informasiya axınla-rının sərhəd yerlərində yerləşdirilməlidir. Beləki, korporativ şəbə-kənin ayrı-ayrı seqmentləri, eləcə də istifadəçiləri (müştə-riləri) və daha vacib şəbəkə servisləri arasında qarşılıqlı əlaqə yalnız şəbə-kələrarası ekran vasitəsilə həyata keçirilməlidir (şək.1.4).

Şəbəkələrarası ekran simmetrik deyildir. Onun üçün bir şəbəkə seqmentindən digərinə və əksinə keçidi məhdudlaşdıran qaydalar verilir. Ümumi halda, şəbəkələrarası ekranın işi iki qrup funksiya-nın dinamik yerinə yetirilməsinə əsaslanır [1,2]:

- ondan keçən informasiya selinin süzgəclənməsi;
- şəbəkələrarası qarşılıqlı əlaqələrin reallaşdırılması zamanı vasitəçilik etmə.

İnformasiya selinin təhlili üçün kriteriya qismində aşağıdakı parametrlərdən istifadə edilə bilər [1,2]:




**Şək.1.4.** Korporativ kompüter şəbəkəsinin fraqmentləri
(şəbəkələr arası ekran qoşulmamışdan əvvəl və sonra)

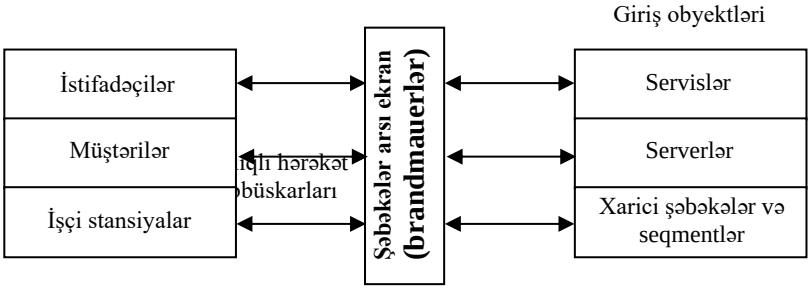
- şəbəkə ünvanını, identifikatorları, interfeyslərin ünvanlarını, portların nömrələrini, və digər əhəmiyyətli məlumatları özündə saxlayan məlumat paketlərinin xidməti sahələri;
- məlumat paketlərinin yoxlanılan (məsələn, kompüter virusunun mövcudluğunun) məzmunu;
- informasiya selinin xarici xarakteristikaları, məsələn, zaman, tezlik xarakteristikaları, verilənlərin həcmi və s.

Şəbəkələrarası qarşılıqlı əlaqələrin reallaşdırılması zamanı vasitəçilik prosesində ekranlaşdırıcı agentlər məlumatlar selinin şəffaf ötürülməsini bloklaşdıraraq aşağıdakı funksiyaları yerinə yetirə bilərlər [1,2]:

- istifadəçilərin identifikasiyası və antentifikasiyası;
- ötürülən məlumatların həqiqiliyinin yoxlanılması;
- qorunan şəbəkə seqmentinin resurslarına girişin məhdudlaşdırılması;

- məlumat selinin süzgəclənməsi və çevrilməsi, məsələn, virusların dinamik axtarışı və informasiyanın şəffaf şifrlənməsi;
- çıxan məlumat paketləri üçün daxili qovşaq ünvanlarının translyasiyası;
- hadisələrin qeydiyyata alınması, verilən hadisələrə reaksiya verilməsi, qeydiyyata alınmış informasiyanın təhlili və hesabatların hazırlanması;
- soruşulan məlumatların keş yaddaşda saxlanılması.

Şəbəkənin təhlükəsizliyini effektiv təmin etmək üçün kompleks brandmauer ondan keçən bütün seli idarə etməli və öz vəziyyətini izləməlidir (şək.1.5).




**Şək.1.5.** Məlumat paketlərinin nəzarət edilməsi sxemi

Şəbəkələrarası qarşılıqlı əlaqəni effektiv qorumaq üçün Firew all sistemi düzgün quraşdırılmalı və konfiqurasiya edilməlidir. Bu proses aşağıdakı mərhələləri ardıcıl yerinə yetirməklə həyata keçi-rilir [1,2]:

- şəbəkələrarası qarşılıqlı əlaqə siyasətinin işlənilməsi;
- qoşulma sxemlərinin, eləcə də bilavasitə şəbəkələrarası ekran-
- ların qoşulması sxemlərinin müəyyən edilməsi;
- brandmauerlərin fəaliyyət göstərməsi üçün parametrlərinin köklənməsi.

Şəbəkələrarası qarşılıqlı əlaqə siyasəti təşkilatın təhlükəsizlik siyasətinin onun xarici mühitlə informasiya mübadiləsinin təhlükəsizliyi üçün tələbləri müəyyən edən hissəsi olub aşağıdakı iki aspekti müəyyən edir [1,2]:

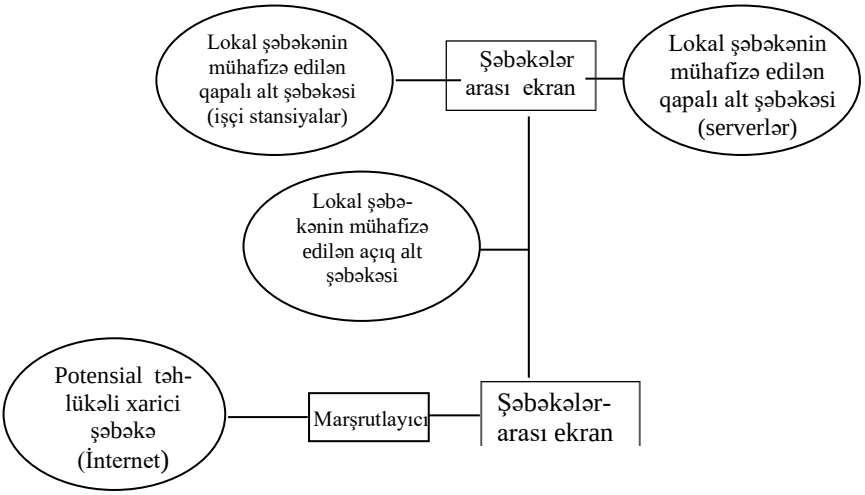
- şəbəkə servislərinə giriş siyasəti;

- şəbəkələrarası ekranın iş siyasəti.

Şəbəkələrarası ekranın iş siyasəti brandmauerin fəaliyyətinin əsasını təşkil edən şəbəkələrarası qarşılıqlı əlaqənin idarə edilmə-sinin baza prinsiplərini müəyyən edir. Burada iki prinsipial yanaş-ma nəzərdə tutulur [1,2]:

- açıq icazə verilməyən hər şey qadağan edilmişdir.
- açıq qadağa qoyulmayan hər şeyə icazə verilmişdir.

Şəbəkələrarası ekranların qoşulması üçün müxtəlif sxemlərdən istifadə oluna bilər. Bu sxemlər fəaliyyət göstərmə şəraitindən və brandmauerin şəbəkə interfeyslərinin sayından asılıdır. Böyük ol-mayan korporativ şəbəkələr üçün iki şəbəkələrarası ekranın istifa-dəsi kifayətdir (şək.1.6).




**Şək.1.6.** Şəbəkələrarası ekranların qoşulmasının nümunəsi

Burada mühafizə olunan açıq alt şəbəkə ekranlaşdırıcı alt şəbəkə qismində çıxış edir.

Həmişə olduğu kimi ekranlaşdırıcı alt şəbəkə elə zahiri görünüş olunur ki, alt şəbəkənin kompyüterlərinə daxilolma, potensial olaraq, həm düş-mən xarici şəbəkəsindən, həm də lokal şəbəkənin bağlı alt şə-bəkələrində daxil olma təmin edilsin.

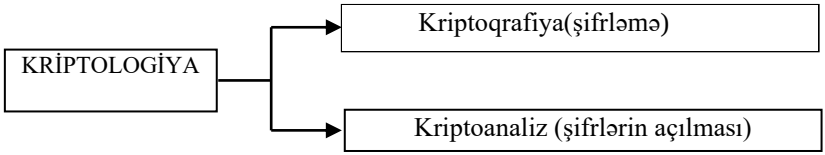
Habelə xarici şəbəkə və bağlı alt şəbəkələr arasında birbaşa informasiya mübadiləsi mümkün deyildir. Ekranlaşdırıcı alt şəbə-kəsi olan sistemə hücum etmək üçün heç olmasa iki asılı olmayan qoruma sədləri dəf edilməlidir ki, bu da çox çətin məsələdir. Belə olduqda, şəbəkələrarası ekranların vəziyyətlərini monitorinqi vasi-tələri belə cəhdləri, praktiki olaraq, aşkar edəcək və sistemin administratoru isə icazəsiz girişin qarşısını almaq üçün zəruri tədbirlər görəcəkdir.

### 1.5. İnformasiya mühafizəsinin kriptoqrafik vasitələri

Telekommunikasiya şəbəkələri və sistemlərində informasiya-nın bilavasitə mühafizəsi üçün daha çox kriptoqrafiya (şifrələmə) üsullarından istifadə olunur [3,4]. Şifrələmə vasitələri informasiyanın mahiyyətinin gizlədilməsi ilə yanaşı, informasiyanın tamlığını tə-min edilməsi, imzalanması, informasiya sahibinin həqiqiliyinin təsdiq olunması, mühafizə olunmuş istiqamətli kanalların təşkili və digər vacib məsələləri həll etməyə kömək edir.

Kriptoqrafiya dedikdə istənilən formada olan, o cümlədən yad-daş qurğularında saxlanılan və ya kompüterdə emal olunan, eləcə də rabitə kanalları vasitəsilə ötürülən informasiyanın mənasının gizlədilməsi başa düşülür. Kriptoqrafiya, həmçinin, proqram təmi-natının qorunması üçün də tətbiq oluna bilər. Yuxarıda qeyd olun-duğu kimi, informasiya təhlükəsizliyinin əsas istiqamətləri məxfi-liyin, tamlığın və əldə olunması imkanlarının təmin edilməsidir. Kriptoqrafik üsullar hər üç istiqamətdə təhlükəsizliyin təmin edil-məsi üçün tətbiq edilir. Beləki, bu üsulların köməyi ilə informa-siyanı şifrələmək və icazəsi olmayan şəxslər tərəfindən onun isti-fadəsinin qarşısını almaq yolu ilə informasiyanın gizliliyini təmin etmək olur.Şəbəkə vasitəsilə ötürülən məlumatın təhrif olunmadan ünvana çatmasının təmin edilməsi ilə yanaşı onun məhz müəllif tərəfindən göndərildiyinin müəyyən edilməsi böyük əhəmiyyət kəsb edir. Beləki, çox vaxt bir adam özünü başqasının adı altında təqdim edir, onun adından məlumatlar göndərir, qəbul edir və s. Bu mənada informasiyanın, istifadəçinin, sistemin və şəbəkənin həqiqiliyinin yoxlanması, audentifikasiyası zəruridir və bu məq-sədlə, əsasən, kriptoqrafik üsullar tətbiq edilir. İnformasiya müha-fizəsi

üsullarının hazırlanması haqqında elm *kriptologiya* adlanır (şək.1.7). Kriptologiya bir-birini tamamlayan iki istiqaməti əhatə edir.




**Şək.1.7.** Kriptologiya

*Kriptoqrafiya* məlumatın məxfiliyinin necə təmin olunmasını öyrənən elmdir [3,4]. Kriptoqrafiya informasiyanın çevriləməsinə elə imkan verir ki, onun oxunması (bərpası) müəyyən açarın (parolun) məlumluğu halında mümkün olur.

*Kriptoanaliz* üzrə isə şifrlərin açılması metodları öyrənilir [3,4]. Deməli, kriptpologiya üzrə məlumatların şifrlənməsi və şifrələrin açılması metodları öyrənilir. Şifrləmə yə və deşifrə-ləməyə məruz qalan informasiya dedikdə müəyyən *əlifba* əsasında tərtib olun-muş *mətn* nəzərdə tutulur. Şifrləmə proseduru adətən müəyyən kriptoqrafik alqoritmin və açarın (*key*, K) istifadə olunmasını nə-zərdə tutur. *Açar* mətnin maneəsiz (sərbəst olaraq) şifrələnməsi və deşifrələnməsi üçün tələb olunan informasiyadır. Yalnız bu acarı bilərək deşifrləmənin yerinə yetirilməsi təmin edilir. Şifrləmə və deşifrələmə proseslərində istifadə olunan üsul (qayda) *kriptoal-qoritm* adlanır. *Kriptoqrafik alqoritm* şifrələnmə/deşifrələnmə üçün məlumatların çevrilmə üsulu olub *şifr* (*cipher*) və ya *krip-toalqoritm* adlanır. Kriptoqrafiya terminologiyasında adi sənədlər *açıq mətn* (*Plaintext*, P və ya *cleartext*) hesab olunur. Məzmunu qalmaqla ilkin mətnin dəyişdirilməsi çevirmə prosesi olub *şifrələmə* (*encryption*, E), şifrlənmiş məlumat isə *şifrmətn* (*cipher-text*, C) və ya *kriptoqram* adlanır. Şifrmətndən açıq mətnin bər-pası, əks proses olub *deşifrələmə* (*decryption*, D)-adlandırılır. Şifrə dedikdə verilmiş açar və kriptoqrafik çevirmə alqoritmi vasitəsi ilə açıq məlumat toplusunu şifrələnmiş məlumat toplusuna çevirən dönümlü (biektiv, yəni bərpa qabiliyyətinə malik olan və ya ilk vəziyyətinə qayıtmaq qabiliyyətinə malik olan) çeviricilər məcmuusu başa düşülür [3,4]. Deşifrlənmə açarı (şək.1.8) məxfi məlu-matı alana məlum

olmalıdır ki, açıq mətni bərpa etsin. Müasir kriptoqrafiyada şifrmətnin məxfiliyi bu açarın vasitəsi ilə təmin edilir.

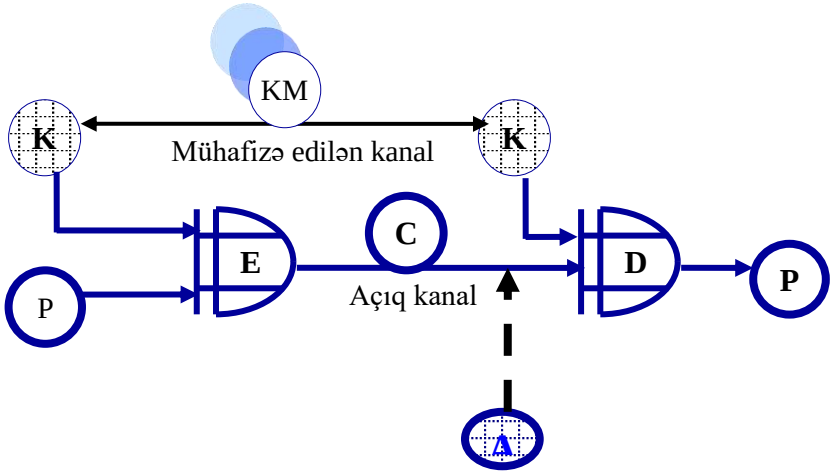
**Şək.1.8.** Deşifrlənmə açarı

Aydındır ki, belə sistemin təhlükəsiz fəaliyyəti üçün həmin açar məxfi saxlanılmalıdır, ona görə də belə sistemlər *məxfi açarlı kriptosistemlər* adını almışlar.

### 1.5.1. Kriptoqrafik sisemlərin modelləri və şifrləmə metodları

Məlumatın müəllifi tərəfindən təqdim edilmiş açıq mətn (P), informasiya mənbəyində (KM) hasil olunan açar (K) vasitəsi ilə şifrələnib (E) şifrmətnə (C) çevrilərək açıq kanalla ötürülür (şək. 1.9) [3,4]. Müəllif tərəfdə məxfiləşdirilmiş bu mətn deşifrləmə (D) üçün təyin olunmuş açar vasitəsilə açıq mətnini əvvəlki vəziy-yətinə qaytarılır.

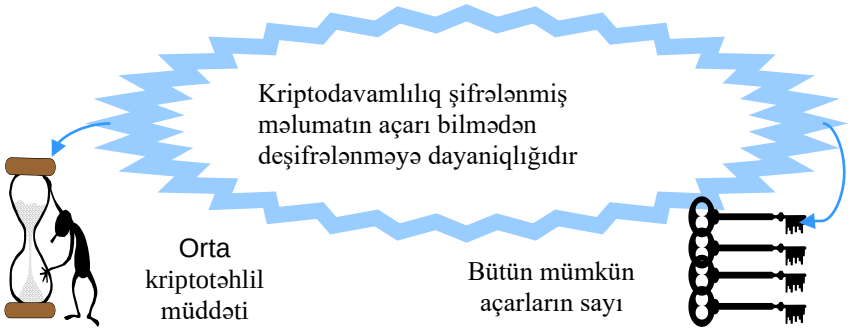
Məxfi açarlı kriptoqrafik sistemin modelinin vacib hissəsi açar ötürülən təhlükəsiz kanaldır. Bu kanal yüksək etibarliğa və məx-filiyə malik olmalıdır. Bir sözlə məxfi açar istifadə olunan siste-min bütün elementləri mühafizə olunmalıdır. Şifrələnmiş məlu-matı göndərən üçün onun deşiflənməyə davamlığı vacibdir. Şifrin davamlığı kənar



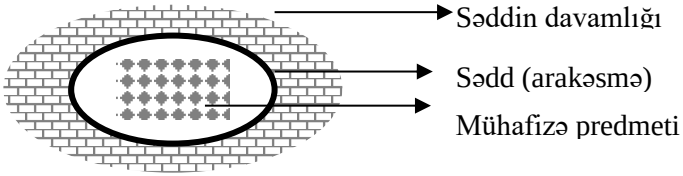

**Şək.1.9.** Şifrələnmə/deşifrələnmə sxemi

davamlığı kənar şəxslər tərəfindən ələ keçirilmiş şifrmətn üzrə açıq mətni deşifrələmək cəhdinə dayanıqlığı qəbul olunur. Bu cəhdi kriptoanalitiklər (A) əvvəl şifrin (kriptoqramın) qurulması prinsipini, sonra isə deşifrələmə üçün açarı müəyyən etməyə çalışırlar. Şifrin bu xarakteristikası kriptodavamlıq adlanır. Şifr-lərin müqayisəli dayanıqlığı, hesablama texnikasının müasir vasitələri ilə təchiz edilmiş və istənilən üsulla məlumatı deşifrələməyə cəhd göstərən qarşı (maraqlı) tərəfə vacib olan vaxtı nəzərə almaqla qiymətləndirilir. Açarın nə qədər çox variantı olarsa, mətni deşifrələmək (uzun vaxt sərf edilməsinə görə) bir o qədər çətin olacaqdır (şək. 1.10) [3,4]. Təhlükəsizlik modelinə görə səddin davamlığı o vaxt kafi hesab olunur ki, ziyankarlar tərəfindən onun aradan qaldırılmasına sərf olunan vaxt informasiya mühafizə predmetinin aktuallıq dövründən artıq olsun. Bu müddət mühafizə predmetini nəzərə almaqla informasiyanın elementar təhlükəsizlik modelinə əsasən müəyyən olunmalıdır (şək.1.11) [3,4]. K.Şennon açıq məlumatın şifrələnməsini riyazi olaraq $C = F_i P$ modeli

ilə təsvir etmişdir. Burada ($i$) indeksi konkret açara istinadı, $F_i$ isə cevirmə funksiyasını gös-



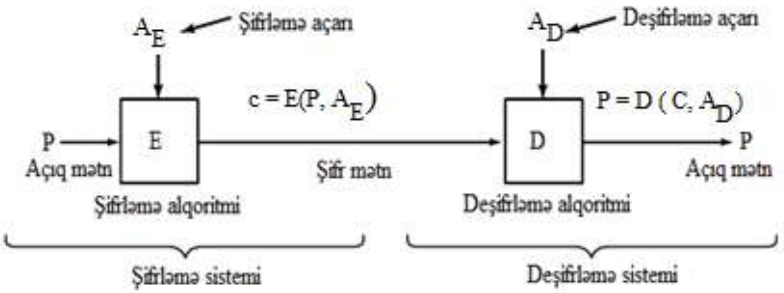

**Şək. 1.10.** Kriptodavamlılıq modeli




**Şəkil.1.11.** Informasiyanın elementar mühafizə modeli tərir. Deşifrələnmənin birqiymətliliyinin mümkünlüyü üçün onun tərs funksiyası $(F_i^{-1})$ mövcud olmalıdır: $P = F_i^{-1}C$

**Şennonun şifrləmə/deşifrələmə modeli.** Aşağıdakı sxemdə məxfi açarlı kriptosistemlərin Şennon modeli göstəril-mişdir (şək.1.12) [3,4].

İlk kriptosistemlər artıq bizim eranın əvvəlində meydana çıx-mışdır. Məsələn, məşhur Roma sərkərdəsi Yuli Sezar (e.ə. 100-cü




**Şək.1.12.** Şifrələnmə/deşifrələnmə modeli

### 1.5.2. Sezar şifrləmə metodu

illər) öz yazışmalarında indi onun adını daşıyan şifrdən istifadə edirdi. Adi əlifba (məs.azərbaycan) yazılırdı, sonra onun altında həmin əlifba, lakin sola üç hərf dövri sürüşmə ilə yazılırdı [4]:

A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z

Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z A B C

Şifrləmə zamanı A hərfi Ç hərfi ilə, B hərfi D ilə və s. əvəz olunurdu. Şifrlənmiş məlumatı alan hərfləri ikinci sətirdə axtarırdı və onların üstündəki hərflərə görə ilkin mətni bərpa edirdi. Sezar şifrində açar əlifbanın ikinci sətrindəki sürüşmənin qiymətidir. Sezar alqoritminin bir neçə modifikasiyası mövcuddur. Onlardan biri Vijiner kvadratıdır (şək.1.13).

Tutaq ki, kvadratda göstərilən açıq mətn "LEMON" açar ilə şifrələnməlidir. Məlumatın müəllifi açarın mətnini dövrü olaraq təkrarlamaqla məlumatın uzunğu ilə aşağıdakı kimi eyniləşdirir [4]:

Açıq mətn: A L M A G Ö Z Ə L D İ R (1.1)

Açar: L E M O N L E M O N L E

Mətni təşkil edən hərflərin Vijiner cədvəlində durduğu sütunla açarın simvolları yerləşən sətrin kəsişməsindəki işarələr ardıcıl-lığından şifrmətn alınır [4]:

Şifrmətn: L P D O U Ə D S E R Y Ü

Deşifrələmə üçün əvvəlcə açar üst sətirdə yazılır, onun altında isə şifrmətn yerləşdirilir,yəni

Açar:L E M O N L E M O N L E

Şifrmətn: L P D O U Ə D S E R Y Ü

Vijiner cədvəlində açar işarələrinin yerləşdiyi sətirdə şifrmət-nin müvafiq hərfini tapıb, həmin hərfin yerləşdiyi sütunla cədvə-lin yuxarı başında yerləşdirilmiş əlfbanın hərfinin kəsişmə nöqtə-sindəki hərfi tapırıq, elə bu hərf də açıq mətnin birinci hərfi ola-caq. Məsələn, axırıncı yazılışda açarın birinci hərfi L-dir, Vijiner cədvəlində onun yerləşdiyi sətrdə şifrmətnin birinci hərfi olan L

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

hərfini tapırıq. Sonra bu hərfin yerləşdiyi sütunla yuxarı qalxıb cədvəlin yuxarı başında yerləşən əlifbanın hərfinə dək irəliləyib kəsişmə nöqtəsində yerləşən hərfi tapırıq. Bu hərf əlifbanın A hərfidir, elə bu hərf də açıq mətnin birinci hərfi olacaq. Açıq mət-nin digər hərfləridə bu qayda ilə tapılır. Beləliklə, bu qaydadan istifadə edərək biz aşağıdakı açıq mətni tapırıq:

Açıq mətn: A L M A G Ö Z Ə L D İ R

Digər bir misala baxaq. Tutaq ki, şifrləmə üçün "YAŞA M A Q G Ö Z Ə L D İ R" sözünü "B Ə L İ" açarı ilə şifrləmək tələb olunur. Bu sözü şifrləmək üçün, onu birinci sətrdə yazırıq, onun alt sətrində isə açarın mətnini dövrü olaraq təkrarlamaqla məlumatın uzunluğu ilə aşağıdakı kimi eyniləşdiririk, yəni:

Açıq mətn: Y A Ş A M A Q G Ö Z Ə L D İ R

Açar: B Ə L İ B Ə L İ B Ə L İ B Ə L

Yuxarıda göstərilən qaydanı tətbiq edərək aşağıdakı şifrmətni alarıq:

Şifrmətn: Z Ə H İ N Ə B P P E R Y E N G

Deşifrələmək üçün əvvəlcə açarın mətnini dövrü olaraq təkrarlamaqla birinci sətrdə yazırıq, ikinci sətrdə isə şifrmətni yerləşdiririk,yəni

Açar:B Ə L İ B Ə L İ B Ə L İ B Ə L

Şifrmətn: Z Ə H İ N Ə B P P E R Y E N G

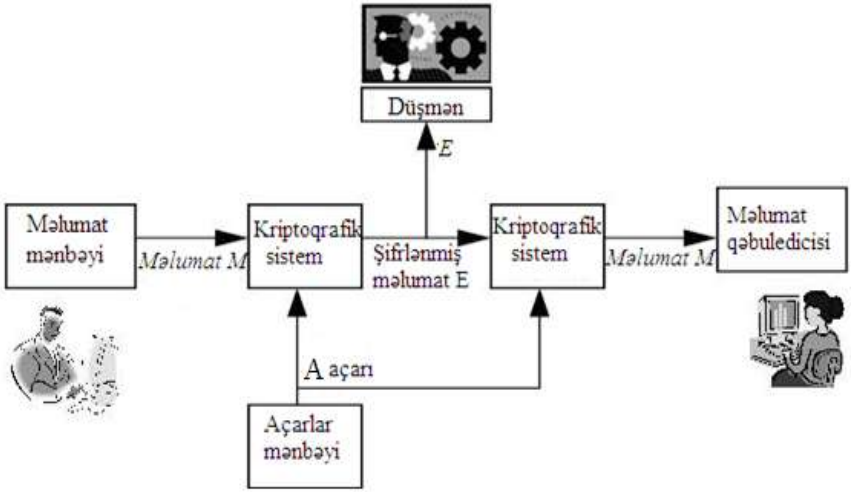
Beləliklə, yuxarıdakı qaydadan istifadə edərək biz aşağıdakı açıq mətni tapırıq:

Açıq mətn: Y A Ş A M A Q G Ö Z Ə L D İ R

# II FƏSİL. SİMMETRİK ŞİFRLƏMƏ TEXNOLOGIYALARI

## 2.1. Simmetrik şifrləmənin struktur sxemi

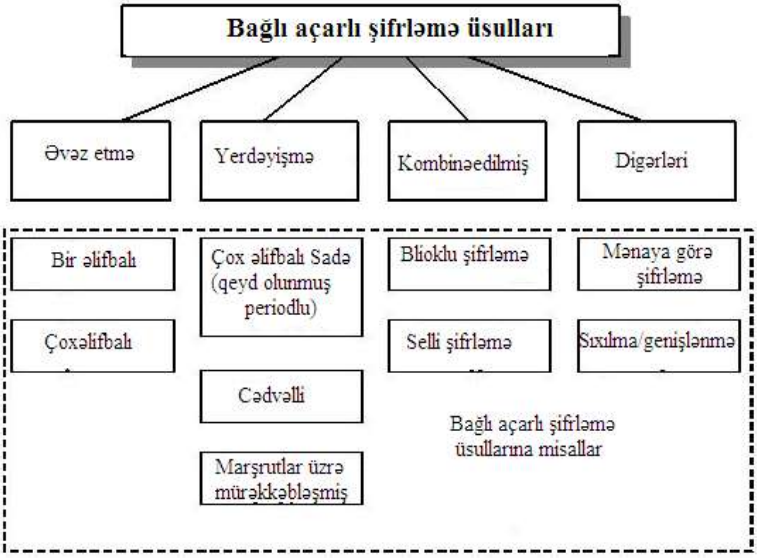
Klassik yaxud biraçarlı kriptoqrafiya simmetrik şifrləmə alqoritmlərinə əsaslanır. Belə texnologiyada şifrləmə və deşifrləmə yal-nız yerinə yetirilmə qaydalarına və bəzi addım istiqamətlərinə görə fərqlənirlər. Bu texnologiyada eyni bir məxfi element (açar) istifa-də edirlər və deşifrləmə əməliyyatı şifrləmənin sadə çevirməsidir. Ona görə də mübadilə iştirakçılarından hər biri məlumatı həm şifr-ləyə, həm də deşifrləyə bilər. Simmetrik şifrləmənin struktur sxemi şək.2.1-də verilib [3,4].




**Şək.2.1.** Simmetrik şifrləmənin struktur sxemi

Şifr dedikdə ilkin məlumatın mühafizəsi üçün əvvəlcədən şərtləşdirilmiş çevirmə üsullarının məcmuu başa düşülür. Açar-məlumatların şifrlənməsi və deşifrlənməsi üçün vacib olan informasiyadır.Verici tərəfdə məlumat mənbəyi və açarlar mənbəyi var. Açarlar mənbəyi bütün mümkün olan açarlar sırasından konkret "A" açarını seçir. Bu "A" açarı hər hansı bir üsulla qəbuledici tərə-fə verilir, hərçənd güman edilir ki, onu ələ keçirmək olmaz, məsə-lən, bu açar xüsusi

kuryer vasitəsilə verilir (ona görə simmetrik şifrləmə bağlı açarlı şifrləmə adlanır). Məlumat mənbəyi hər hansı bir M məlumatı hasil edir, sonra bu məlumat seçilmiş açarı istifadə etməklə şifrlənir. Şifrləmə prosedurunun nəticəsində kriptoqramma adlanan şifrlənmiş E məlumatı alınır. Sonra E kriptoqramı rabitə kanalı üzrə verilir. Rabitə kanalı (radiokanal, yaxud kompüter şəbə-kəsi) açıq və mühafizə olunmamış olduğundan verilən informasiya düşmən tərəfindən tutulub saxlanıla bilər. Qəbul tərəfdə E kriptoq-ramını açar vasitəsilə deşifrələyib ilkin M məlumatı alırlar. Əgər M məlumatdırsa, A-açardırsa, E şifrlənmiş məlumatdırsa, onda yaz-maq olar: E=f(M,A), yəni şifrlənmiş E məlumatı ilkin M məlu-matından və A açarından asılı olan hər hansı bir funksiyadır. Krip-toqrafik sistemdə istifadə olunan şifrləmə üsulları və alqoritmləri yuxarıda göstərilən ifadədə f funksiyasını təyin edir [3,4]. Bağlı açarla şifrələmənin müxtəlif üsulları mövcuddur (şək.2.2).




**Şək.2.2.** Bağlı açarlı şifrləmə üsulları

Praktikada yer dəyişmə, əvəz etmə, eləcə də kombinasiya edil-miş alqoritmlərdən tez-tez istifadə olunur [3,4].

## 2.2.Əvəzetmə metodu

Əvəzetmə (yerdəyişmə) şifrləmə metodları ilkin mətnin bir qay-da olaraq bloklara ayrılmış və bir əlifbada yazılmış işarələri, çevir-mələrin qəbul olunmuş qaydalarına uyğun olaraq digər əlifbanın bir yaxud bir neçə işarələri ilə əvəz edilirlər. *Əlifba* informasiyanın kodlaşdırılması üçün sonlu sayda işarələr çoxluğudur. *Mətn* isə bu əlifbanın elementlərindən təşkil olunmuş ardıcıllıqdır.

### 2.2.1.Birəlifbalı əvəzetmə

Əsas əvəzetmə metodlarından biri birəlifbalı əvəzetmə meto-dudur. Bu metodda A məlumatının ilkin əlifbasının hər bir $a_i$ işa-rəsi ilə şifrlənmiş E mətninin uyğun $e_i$ işarəsi arasında birmənalı uyğunluq yaranır. Birəlifbalı əvəzetmə ən sadə əvəzetmə şifri oldu-ğundan bəzən sadə əvəzetmə adlanır. Birəlifbalı əvəzetməyə misal olaraq ən sadə şifrləmə sistemlərindən biri olan və "Yuliy Sezar şifri" adını daşıyan şifrləmə sistemini göstərmək olar. Belə fərziyə var ki, bizim erayadək 1-ci əsrdə yaşayan məhşur roma imperatoru Yuliy Sezar öz sərkərdələri ilə məktublaşmada bu şifri istifadə edir-miş. Sezarın şifri azərbaycan dilinə tətbiq edildikdə aşağıdakılardan ibarət olur. Azərbaycan əlifbasında məlumatın hər bir hərfi ilkin hərfdən üç işarə sağda olan hərflə əvəz edilir. Beləliklə, A hərf**i** Ç-yə, B hərfi D-yə və s. bu proses Ü-yə dək davam etdirilir, sonra V hərfi A-ya, Y hərfi B-yə və nəhayət Z hərfi C hərfi ilə əvəz edilir.

**Misal 1.** Azərbaycan əlifbası ilə belə bir ilkin əlifba verilir. A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z. Bu əlifbaya əsasən "ƏV Ə Z LƏ M Ə" açıq mətnini şifrləsək aşağı-dakı şifrmətni alarıq.

Həlli:"ƏV Ə Z LƏ M Ə"- şifrləmə →"ĞAĞCOĞÖĞ"-şifrmətn.

Sezar şifrləmə metoduna əsasən burada Ə hərfi Ğ hərfinə, V hərfi A–ya, Ə hərfi Ğ-yə, Z hərfi C-yə, L hərfi O-ya, Ə hərfi Ğ-yə, M-hərfi Ö-yə, Ə hərf Ğ -yə əvəz edilir.

Beləliklə, "ƏV Ə Z LƏ M Ə"sözü Sezar şifrləmə metoduna əsa-sən"ĞAĞCO ĞÖĞ" sözünə çevrilir.

Şifrmətnin deşifrlənməsi zamanı şifrlənmiş mətnin hər bir hərfi sola doğru olan üçüncü hərflə əvəz edilir. Məsələn yuxarıda gös-tərilən şifrmətni deşifrələsək aşağıdakı açıq mətni alarıq

"ĞAĞCO ĞÖĞ" - deşifrləmə → "Ə V Ə Z L Ə M Ə"- deşifr-lənmiş mətn.

Bu metod çox çətin metod deyil, xüsusən ona görə ki, bir neçə sözdən ibarət məlumatın şifrlənməsi zamanı ilkin mətnin neçə söz-dən ibarət olması dərhal aydın olur. Bundan başqa, şirlənmiş məlu-matda hərflərin təkrarlanması üzrə hər hansı məlumatı almaq olar. Məsələn, şifrlənmiş "ĞAĞCOĞÖĞ" sözündə hərflərdən birinin Ğ hərfi dörd dəfə təkrar olunması aydın olur.

Buna baxmayaraq, Sezar kriptoqrafiya tarixinə düşdü, "Yuliy Sezar şifri" isə ilk şifləmə sistemlərindən biri kimi qiymətləndirilir.

"ĞAĞCOĞÖĞ"sözünün şifrini açmaq üçün yalnız şifrləmə al-qoritminin özünü bilmək vacibdir. Şifrləmə üsulunu bilən istənilən adam, məxfi məlumatın şifrəsini asanlıqla aça bilər. Beləliklə, bu metodda açar alqoritmin özüdür.

Bu primitiv alqoritmin kriptodavamlığını qismən artırmaq üçün 3-5-7 açarından da istifadə etmək olar. İşarələrin yerdəyişməsi əv-vəlcə 3, sonra 5 və 7 hərfdən bir baş verəcək və bu proses mətnin sonuna qədər təkrarlanacaqdır. Bu halda açarı təşkil edən işarələr ardıcıllığı *açar sözü*, bir neçə sözdən ibarət olduqda isə *açar cüm-ləsi* adlanır. Müxtəlif məlumatların şifrələnməsində dəfələrlə isti-fadə olunan eyni bir açar *statik*, hər bir məlumatın şifrələnməsi üçün istifadə olunan yeni açar isə *dinamik* açar adlanır. Burada birinci sətr ilkin əlifba, ikinci (dövrü olaraq k qədər sürüşmə ilə sola) isə əvəz etmə vektoru adlanır.

Birəlifbalı şifrləmə metodunda əvəzləmə cədvəlindən də istifadə etmək olar. Bunu aşağıdakı cədvəlin timsalında göstərək (cədvəl 2.1). Bu cədvəldə iki cədvəl birləşdirilib. Onlardan birində (şifr 1) ilkin mətnin azərbaycan əlifbasının digər hərfləri ilə əvəzlənməsini, digəri isə (şifr 2) xüsusi işarələrlə əvəzlənməsi göstərilib. Hər iki şifr üçün ilkin mətn azərbaycan əlifbasının hərfləri olacaq. Bu cəd vələ əsasən əvəzləmə aşağıdakı kimi aparılır.

***Cədvəl 2.1***

| Açıq mətn | Şifr 1 | Çifr 2 | Açıq mətn | Şifr 1 | Şifr 2 | Açıq mətn | Şifr 1 | Şifr 2 |
|---|---|---|---|---|---|---|---|---|
| A | G | ^ | X | B | № | P | D | ∑ |
| B | X | @ | I | Ü | # | R | Y | ∇ |
| C | O | ) | İ | Ğ | - | S | Ö | ϒ |
| Ç | P | + | J | V | = | Ş | J | ℵ |
| D | S | < | K | Ə | ( | T | L | ⊕ |
| E | Ç | > | Q | E | ? | U | M | × |
| Ə | K | ∀ | L | T | % | Ü | I | ⊗ |
| F | N | ♦ | M | U | ⊗ | V | H | $ |
| G | Z | * | N | F | ! | Y | Q | Δ |
| Ğ | Boşluq | ♥ | O | İ | № | Boşluq | | ∞ |
| H | R | ♠ | Ö | Ş | ® | Z | A | ^ |

Monoəlifba əvəzlən-məsində istənilən şifrlərlə şifrlənmiş məlumat aşağıdakı kimi alınır. İlkin məlumatdan növbəti işarə götürülür. Əvəzləmə cədvəlinin "Açıq mətn" sütununda onun mövqeyi təyin edilir. Şifrlənmiş mə-lumata əvəzləmə cədvəlinin bu sətrindən şiflənmiş işarə qoyulur.

Misal:Azərbaycan əlifbası ilə verilmiş "GÜCLƏNDİRMƏ GÖN DƏRİN" məlumatın bu iki şifrini istifadə etməklə şifrlənməsinə baxaq (cədvəl.2.2).

***Cədvəl 2.2***

| Açıq mətn | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| G | Ü | C | L | Ə | N | D | İ | R | M | Ə | | G | Ö | N | D | Ə | R | İ | N |
| Şifr 1-i istifadə etməklə şifrlənmiş məlumat | | | | | | | | | | | | | | | | | | |
| Z | I | O | T | K | F | S | Ğ | Y | U | K | | Z | Ş | F | S | K | Y | Ğ | F |
| Şifr 2-ni istifadə etməklə şifrlənmiş məlumat | | | | | | | | | | | | | | | | | | |
| * | ⊕ | ) | % | ∀ | ! | < | - | ∇ | ⊗ | ∀ | | × | ® | ! | ∑ | ∀ | ∇ | - | ! |

Bunun üçün ilkin məlumatın birinci hərfi “G”-nı götürürük. Cədvəl 2.1-də “Şifr1” sütununda “G” hərfi üçün əvəzləmə işarəsini tapırıq. Bu “Z” hərfidir. Cədvəl 2.2-də “Z” hərfini “G” hərfinin altında yazırıq. Sonra cədvəl 1-in ilkin məlumatın ikinci işarəsi olan “Ü” hərfinə baxırıq. Həmin cədvəldə“Şifr1” sütununundan “Açıq mətn”in “Ü” hərfinin qarşısında duran hərfi tapırıq. Bu “I” hərfidir. Beləliklə, şifrlənmiş məlumatın ikinci hərfi olan “I” hərfini alırıq. Bu hərfi cədvəl 2-də Ü hərfinin altında yazırıq. Analoji ola-raq davam etməklə bütün ilkin məlumatı şifrələyirik. Bu şifrələmə-nin nəticəsi cədvəl. 2.2-də yazılıb.Bu şəkildə alınan mətn nisbətən aşağı mühafizə səviyyəsinə malikdir, çünki, həm ilkin və həm də şifrlənmiş məlumat eyni statistik qanunauyğunluğa malikdir. Bu zaman əvəzləmə üçün hansı işarələrin (ilkin mətnin yerdəyişən işarələrinin yaxud əsrarəngiz surətdə görünən işarələrin) istifadə olunması əhəmiyyət kəsb etmir. Kriptoqrafiyada qəbul olunub ki, düşmən şifrləmə alqoritmini, məlumatın xarakterini və şifrmətni bilə bilər, lakin məxfi açarı bilə bilməz. Bu üsul Kerkxoffs prinsipi adlanır. Kerkxoffs qaydasını istifadə etməklə Sezar şifrini təkmil-ləşdirək. Fərz edək ki, hərflər sağa üç hərf deyil n qədər sürüşür ($0<n< 32$). Burada n sürüşmə parametridir. Tutaq ki, FÜZCİKA şifrmətni tutulub saxlanılır. Düşmənə aydındır ki, sürüşmə para-metri n 1-dən 32-yə kimi qiymət alır. Məxfi açarı tapmaq üçün biz şifrmətnə baxırıq. Bütün mümkün olan açarların ardıcıl seçilmə metoduna baxaq. Hər bir hərfin 32 işarə sağa sürüşməsi ilə alınan bütün variantları 32 sətrdə yazaq:

A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z

“FÜZCKA”

| | | | |
|---|---|---|---|
| 1. | G V A Ç Q B | 7. J Ç Ə Ğ P F | 13. O Ğ I K Ü İ |
| 2. | Ğ Y B D L C | 8. K D F H R G | 14. Ö H İ Q V J |
| 3. | H Z C E M Ç | 9. Q E G X S Ğ | 15. P X J L Y J |
| 4. | X A Ç Ə N D | 10. L Ə Ğ I Ş H | 16. R I K M Z Q |
| 5. | I B D F O E | 11.M F H İ T X | 17. S İ Q N A L |
| 6. | İ C E G Ö Ə | 12. N G X J U I | |

Buradan görürük ki, vahid məna daşıyan söz "SİQNAL" sözü-dür. Bu söz 17-ci mövqedə yerləşir. Beləliklə, şifrlənmiş mətnin hər bir hərfini, məsələn F hərfini onun yuxarısında yazılmış azər-baycan əlifbası üzrə 32 hərf sürüşdürərək ona uyğun hərfi tapırıq. Bu hərf G hərfidir. Bu qayda ilə şifrlənmiş mətnin digər FÜZCKA hərflərinə uyğun hərflər tapıb 1-ci sütuna yazırıq. Sonra 1-ci sütun-da aldığımız hərfləri əlifba üzrə 32 hərf sürüşdürərək onlara uyğun hərfləri tapıb ikinci sütuna yazırıq. Digər sürüşmələridə bu qayda ilə apararaq 17–ci mövqedə açıq mətni , yəni "SİQNAL" sözünü tapırıq. Alınan açıq mətni, deşifrə edib şifrmətni tapmaq üçün əlifbanın hərflərinin sayından açıq mətnin yerləşdiyi mövqeni çıxırıq, yəni 32-17=15. Bununla belə "SİQNAL" sözünün hər bir hərfini 15 işarə sağa sürüşdürməklə şifrmətni, yəni "FÜZCKA" sözünü alırıq.

### 2.2.2. Rəqəm şəkilli informasiyanın şifrlənməsi

Əgər ilkin məlumat rəqəmlərdən ibarətdirsə vahid həlli tapmaq çox çətindir. Məsələn, tutaq ki, ilkin məlumat ərəb rəqəmlərindən ibarətdir, yəni aşağıdakı şəkil alır: 0123456789

Abonentlərdən biri digərinə beş ədəddən, yəni 12345-dən ibarət olan kod göndərməyi arzulayır. Göndərici və alıcı əvvəlcədən şifr-ləmə açarının n = 3 olması haqqında razılığa gəlirlər. Göndərici se-çilən açarla 12345 ilkin məlumatı şifrləyir və 45678 ədədini alıb, onu öz abonentinə göndərir. Düşmənin bu kriptoqramı alması mümkündür və onu açmağa çalışır. İlkin məlumat 10 işarədən ibarət olduğu üçün, açarın qiyməti 1-dən 9-a dək diapazonda yerləşə bilər. Əvvəl olduğu kimi tutulub saxlanılan məlumatın işarələri uyğun olaraq 1,2,3,...,9-dək işarə sürüşməsindən alınan bütün variantları yazaq (cədvəl 2.3).

Görünür ki, alınan bütün variantlar eyni qiymətlidir və cina-yətkar hansı kombinasiyanın həqiqi olduğunu başa düşmür. Şifr-mətni analiz edərək, o məxfi açarın qiymətini tapa bilmir.

### 2.2.3. Proporsional şifrləmə üsulu

Birəlifbalı əvəz etmə metoduna proporsional yaxud monofonik şifrlər aiddirlər. Bu şifrlərdə tezlik analizinin köməyi ilə açmadan mühafizə üçün şifrlənmiş işarələrin tezliyi hamarlanır. Tez-tez təkrarlanan işarələr üçün nisbətən çoxlu sayda mümkün olan ekviva-lentlər istifadə olunur. Az istifadə olunan ilkin işarələr üçün bir ya-xud iki ekvivalentin olması kifayətdir. Şifrləmə zamanı əvəzləmə ya təsadüfi, ya da müəyyən şəkildə (sıra qaydasında) seçilir.

**Cədvə 2.3. Qıfılın şifrlənmiş kodunu açmaq üçün variantların seçiməsi**

| Tutulub saxlanılan kriptoqram 45678 | |
|---|---|
| 1 | 56789 |
| 2 | 67890 |
| 3 | 78901 |
| 4 | 89012 |
| 5 | 90123 |
| 6 | 01234 |
| 7 | 12345 |
| 8 | 23456 |
| 9 | 34567 |

Proporsional şifrin istifadə olunması zamanı işarələrə əvəz ha-lında adətən ədəd seçilir.

Məsələn, azərbaycan dili hərflərinə uyğun olaraq üç işarəli ədəd götürük (cədvəl 2.4-ə bax).

**Misal:** B Ö Y Ü K D A Y A Q

101 545 216 750 134 129 760 104 128 800

Beləliklə, biz 101 545 216 750 134 129 760 104 128 800 şifrlənmiş mətni aldıq. Bu misalda təkrar olan hərflər üçün əvəz va-riantı sıra qaydasında seçilir. Proporsional şifrləmə üsulu sadə bir əlifbalı əvəzləmə üsuluna nisbətən daha mürəkkəbdir. Lakin, əgər heç olmasa

bir ”açıq mətn – şifrmətn” cütü olsa, onda açma adi olardı. Əgər yalnız şifrmətn olarsa, onda açarın açılması çox zəhmətli olardı.

**Cədvəl. 2.4. Proporsional şifrləmə üçün əvəzləmə cədvəli**

| İşarə | Əvəz-ləmə variantı | İşarə | Əvəz-ləmə variantı | İşarə | Əvəz-ləmə variantı | İşarə | Əvəz-ləmə variantı |
|---|---|---|---|---|---|---|---|
| A | 760, 128 350 201 | G | 762 211 | Q | 800 767 105 | S | 752 561 |
| B | 101 | Ğ | 754 764 | L | 759 135 214 | Ş | 561 |
| C | 210 106 | H | 132 354 | M | 544 | T | 136 |
| Ç | 351 | X | 755 742 | N | 560 | U | 562 |
| D | 129 | I | 763 756 | O | 768 | Ü | 750 |
| E | 761 130 802 | İ | 757 213 | Ö | 545 | V | 570 |
| Ə | 102 | J | 743 766 | P | 215 | Y | 216 104 |
| F | 753 | K | 134 532 | R | 103 | Z | 751 769 |

## 2.3. Çoxəlifbalı əvəzləmə üsulu

İlkin dilin təbii tezlik statistikasını maskalamaq üçün çoxəlif-balı əvəzləmə istifadə olunur. Çoxəlifbalı əvəzləmədə ilkin mətnin işarələrini əvəzləmək üçün bir deyil bir neçə əlifbadan istifadə olu-nur. Adətən əlifba əvəzləmə üçün ilkin əlifbanın digər qaydada ya-zılmış işarələrindən yaradılır.

Çoxəlifbalı əvəzləməyə misal olaraq Vijiner cədvəlinə əsaslanan sxemi göstərmək olar. Bu metod artıq XVI əsrdə, 1585-ci ildə fransız Blez Vijiner tərəfindən yazılmış "şifr haqqında elmi əsər"-dən məlumdur. Bu metodda şifrləmə üçün özündə elementlərinin sayı NxN olan kvadratik matrisanı əks etdirən cədvəl istifadə olu-nur, burada N əlifbadakı işarələrin sayıdır. Matrisanın birinci sətrində ilkin əlifbanın növbəlik qaydasında hərfləri yazılır, ikinci sətrində hərflərin həmin ardıcıllığı saxlanılır, lakin dövri olaraq bir işarə, üçüncüdə isəiki işarə sola sürüşdürülür və s. Bunu cədvəl 2.5-dən aydın görmək olar.

***Cədvəl 2.5***

A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z

B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z A

C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z A B

Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z A B C

D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z A B C Ç

E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z A B C Ç D

Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y Z A B C Ç D E

.....

.

Y Z A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V

Z A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y

Mətnin şifrlənməsi üçün özündə ilkin əlifbanın bəzi sözlərini yaxud işarələr yığımını əks etdirən açar seçilir. Daha sonra tam matrisadan (cədvəl 2.5-dən) seçilən açarın baş hərflərinə uyğun olan sətrlərdən ibarət olan alt matrisa reallaşdırılırar(cədvəl 2.6-ya bax). Misal üçün açar halında ixtiyari olaraq "BƏYAZ" sözündən ibarət olan açarı seçək. Göründüyü kimi açarın tərkibində A, B, Ə, Y və Z hərfləri mövcuddur. Tam matrisadan (cədvəl 2.5-dən) bu açarın tərkibində olan A, B, Ə, Y və Z hərflərinə uyğun olan sətrləri seçib alt-alta yazmaqla altmatrisa reallaşdırılır (cədvəl 2.6-yə bax). Bu cədvəl ilkin mətnin şifrlənməsinə imkan verir. Cədvələ əsasən ilkin mətnin şifrlənməsi aşağıdakı qaydada həyata keçirilir.

***Cədvəl 2.6***

A B C Ç **D** E Ə F G Ğ H X I İ J K Q L **M** N **O** Ö P R S Ş T U Ü V Y Z

B C Ç D E Ə F G Ğ H X I İ J K Q L M **N** O Ö P R S Ş T U **Ü** V Y **Z** A

Ə F G Ğ H **X** I İ J K Q L M **N** O Ö P R S Ş T U Ü V Y Z A B C Ç D E

Y Z A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O **Ö** P **R** **S** Ş T U Ü V

Z A B C **Ç** D **E** Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T U Ü V Y

Bu məqsədlə aşağıda göstərildiyi kimi birinci sətrdə ilkin mətn olan "YERDƏYİŞMƏ METODU" yazılır, onun altında isə təkrar -təkrar olaraq "BƏYAZ" açarı yazılır, yəni:

İlkin mətn: Y E R D Ə Y İ Ş M Ə M E T O D U

Açar: B Ə Y A Z B Ə Y A Z B Ə Y A Z B

Bundan sonra cədvəl 3.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin birinci hərfi olan Y hərfini tapırıq, sonra hə-min cədvəlin açarın birinci hərfi B ilə başlayan ikinci sətrinin sıra-sı üzrə sağ tərəfə ilkin mətnin Y hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın ikinci sətrində qalın qara rənglə qeyd edilmiş Z hərfidir. Elə bu hərf də şifrmətnin birinci hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin ikinci hərfi olan E hərfini tapırıq, sonra həmin cədvəlin açа-rın ikinci hərfi Ə ilə başlayan üçüncü sətrinin sırası üzrə sağ tərəfə ilkin mətnin E hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, Bu hərf cədvəl 2.6-ın üçüncü sətrində qalın qara rənglə qeyd edilmiş X hərfidir. Bu hərf şifrmətnin ikinci hərfi olacaq.

Daha sonra cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin üçüncü hərfi olan R hərfini tapırıq, sonra hə-min cədvəlin açarın üçüncü hərfi Y ilə başlayan dördüncü sətrinin sırası üzrə sağ tərəfə ilkin mətnin R hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın dördüncü sətrində qalın qara rənglə qeyd edilmiş Ö hərfidir. Bu hərf şifrmətnin üçüncü hərfi olacaq.

Sonra cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sıra-sında ilkin mətnin dördüncü hərfi olan D hərfini tapırıq, sonra həmin cədvəlin açarın dördüncü hərfi A ilə başlayan birinci sırası üzrə sağ tərəfə ilkin mətnin D hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın birinci sətrində qalın qara rənglə qeyd edilmiş D hərfidir. Bu hərf şifrmətnin dördüncü hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin beşinci hərfi olan Ə hərfini tapırıq, sonra həmin cədvəlin açarın beşinci Z hərfi ilə başlayan beşinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin Ə hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın beşinci sətrində qalın qara rənglə qeyd edilmiş E hərfidir. Bu hərf şifrmətnin beşin-ci hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin altıncı hərfi olan Y hərfini tapırıq, sonra həmin cədvəlin açarın

altıncı B hərfi ilə başlayan ikinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin Y hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın ikinci sətrində qalın qara rənglə qeyd edilmiş Z hərfidir. Bu hərf şifrmətnin altıncı hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin yeddinci hərfi olan İ hərfini tapırıq, sonra həmin cədvəlin açarın yeddinci Ə hərfi ilə başlayan sətrinin üçüncü sırası üzrə sağ tərəfə ilkin mətnin İ hərfi ilə kəsişmə nöqtəsinə dək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın üçüncü sətrində qalın qara rənglə qeyd edilmiş N hərfidir. Bu hərf şifrmətnin yed-dinci hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin səkkizinci hərfi olan Ş hərfini tapırıq, sonra həmin cədvəlin açarın səkkizinci Y hərfi ilə başlayan dördüncü sətrinin sırası üzrə sağ tərəfə ilkin mətnin Ş hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın dördüncü sətrində qalın qara rənglə qeyd edilmiş R hərfidir. Bu hərf şifrmət-nin səkkizinci hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin doqquzuncu hərfi olan M hərfini tapırıq, sonra həmin cəd-vəlin açarın doqquzuncu A hərfi ilə başlayan birinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin M hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın birinci sətrində qalın qara rənglə qeyd edilmiş M hərfidir. Bu hərf şifrmətnin doqquzuncu hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin onuncu hərfi olan Ə hərfini tapırıq, sonra həmin cədvəlin açarın onuncu Z hərfi ilə başlayan beşinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin Ə hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın beşinci sətrində qalın qara rənglə qeyd edilmiş E hərfidir. Bu hərf şifrmətnin onun-cu hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin onbirinci hərfi olan M hərfini tapırıq, sonra həmin cədvəlin açarın onbirinci B hərfi ilə başlayan ikinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin M hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə

yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın ikinci sətrində qalın qara rənglə qeyd edilmiş N hərfidir. Bu hərf şifrmətnin on-birinci hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin onikinci hərfi olan E hərfini tapırıq, sonra həmin cədvəlin açarın onikinci Ə hərfi ilə başlayan üçüncü sətrinin sırası üzrə sağ tərəfə ilkin mətnin E hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın üçüncü sətrində qalın qara rənglə qeyd edilmiş X hərfidir. Bu hərf şifrmətnin oni-kinci hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin-mətnin onüçüncü hərfi olan T hərfini tapırıq, sonra həmin cəd-vəlin açarın onüçüncü Y hərfi ilə başlayan dördüncü sətrinin sırası üzrə sağ tərəfə ilkin mətnin E hərfi ilə kəsişmə nöqtəsinədək irəli-ləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın dör-düncü sətrində qalın qara rənglə qeyd edilmiş S hərfidir. Bu hərf şifrmətnin onüçüncü hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin ondördüncü hərfi olan O hərfini tapırıq, sonra həmin cədvə-lin açarın ondördüncü A hərfi ilə başlayan birinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin O hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın birinci sətrində qalın qara rənglə qeyd edilmiş O hərfidir. Bu hərf şifrmətnin ondördüncü hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin onbeşinci hərfi olan D hərfini tapırıq, sonra həmin cədvəlin açarın onbeşinci Z hərfi ilə başlayan beşinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin D hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərf cədvəl 2.6-ın beşinci sətrində qalın qara rənglə qeyd edilmiş Ç hərfidir. Bu hərf şifrmətnin on-beşinci hərfi olacaq.

Cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin onaltıncı hərfi olan U hərfini tapırıq, sonra həmin cədvəlin açarın onaltıncı B hərfi ilə başlayan ikinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin U hərfi ilə kəsişmə nöqtəsinə dək irəliləyib bu nöqtədə yerləşən

hərfi tapırıq, bu hərf cədvəl 2.6-ın ikinci sətrində qalın qara rənglə qeyd edilmiş Ü hərfidir. Bu hərf şifrmətnin onaltıncı hərfi olacaq.

Beləliklə, biz nəticədə "Z X Ö D E Z N R M E N X S O Ç Ü" şəklində şifrlənmiş mətni alırıq.

Məlumatın şifrinin açılması (deşifrlənməsi) prosesini Vijiner metodu timsalında nəzərdən keçirək. Fərz edək ki, "BƏYAZ" açа-rının köməyi ilə şifrlənmiş "Z X Ö D E Z N R M E N X S O Ç Ü" şifrmətni mövcuddur (şifrlənmə zamanı boşluq buraxılıb). Mətnin deşifrə olunması aşağıdakı ardıcıllıqla həyata keçirilir.

Şifrmətni deşifrləmək üçün əvvəlcə açarın hərfləri tələb olunan sayda təkrarlanaraq ardıcıl olaraq birinci sətrdə yazılır, onun altında isə aşağıda göstərildiyi kimi şifrmətn yazılır, yəni:

B Ə Y A Z B Ə Y A Z B Ə Y A Z B
Z X Ö D E Z N R M E N X S O Ç Ü

Bundan sonra cədvəl 2.6-ın B hərfi ilə başlayan ikinci sətri üzrə sağa doğtu irəliləyərək şifrmətnin birinci hərfi olan Z hərfini tapırıq, bu hərfdən başlayaraq həmin cədvəlin A hərfi ilə başlayan birinci sətrinə doğru yuxarı gedərək onların kəsişmə nöqtəsindəki hərfi tapırıq. Bu hərif Y hərfidir, elə bu hərfdə açıq mətnin birinci hərfi olacaq. Açıq mətnin digər hərfləridə bu qayda ilə tapılır. Bu qaydaya əsasən aşağıdakı açaıq mətn alınır:

Y E R D Ə Y İ Ş M Ə M E T O D U

Beləliklə, şifrlənmiş mətnin deşifrə edilməsinin nəticəsi cədvəl 2.7-də aydın göstərilib.

***Cədvəl 2.7***

Cədvəl 2.7. Şifrənin açılması mexanizmi

| | |
|---|---|
| Açar | B Ə Y A Z B Ə Y A Z B Ə Y A Z B |
| Şifrlənmiş mətn | Z X Ö D E Z N R M E N X S O Ç Ü |
| Şifrəsi açılmış mətn | Y E R D Ə Y İ Ş M Ə M E T O D U |

İlkin mətn Y E R D Ə Y İ Ş M Ə M E T O D U

Fransız diplomatı Bleyz Vijiner demək olar ki, yarım əsr bundan əvvəl ən gözəl şifrlərdən birini kəşf etdi. Onun metodu özünə yunan kvadratını və sürüşmə şifrini birləşdirir. O bundan ibarətdir ki, ilkin mətnin hər bir hərfi açar sözə yaxud koda əsasən müxtəlif cür şifrlənir. Bu üsulu araşdırmaq üçün cədvəl 2.8-ə baxaq:

a b c ç d e ə f g ğ h x ı i j k q l m n o ö p r s ş t u ü v y z
1 b c ç d e ə f g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a
2 c ç d e ə f g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b
3 ç d e ə f g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b c
4 d e ə f g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b c ç
5 e ə f g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b c ç d
6 ə f g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b c ç d e
7 f g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b c ç d e ə
8 g ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b c ç d e ə f
9 ğ h x i i j k q l m n o ö p r s ş t u ü v y z a b c ç d e ə f g

Göründüyü kimi açıq mətnin işarələri sütunların adı ilə göstəri-lib, sürdürülmüş əvəzləmə əlifbası isə ikinci sətrdən başlayır.

Misal üçün tutaq ki, "a z a d l ı q" sözünü şifrləmək lazımdır. Açar kodu halında 345 ədədini götürürük.

Bu kodu ilkin mətnin altında lazımi qədər təkrar olunmaqla yazaq:

İlkin mətn: a z a d l ı q
Açar kodu:3 4 5 3 4 5 3

Burada Cədvəl 8-in birinci sətrində yerləşən əsas əlifbanın birinci hərfi olan"a" hərfi ilə həmin cədvəlin 3-ə uyğun olan sətrinin kəsişməsində olan hərfi tapırıq. Bu hərf "ç" hərfidir, elə bu hərf də şifrmətnin birinci hərfi olacaq.

Əsas əlifbanın ikinci "z" hərfi ilə 4-ə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərf "ç" hərfidir, bu hərf şifrmətnin ikinci hərfi olacaq.

Əsas əlifbanın üçüncü "a" hərfi ilə 5-ə uyğun olan sətrin kəsişməsində olan hərfi tapırıq, Bu hərf "e" hərfidir, bu hərf şifr mətnin üçüncü hərfi olacaq. Əsas əlifbanın dördüncü "d" hərfi ilə 3-ə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərf "f" hərfidir, bu hərf şifr-mətnin 4-cü hərfi olacaq. Əsas əlifbanın beşin-ci "l" hərfi ilə 4-ə uyğun

sətrinin kəsişməsində olan hərfi tapırıq. Bu hərf "ö" hərfidir, bu hərf şifrmətnin 5-ci hərfi olacaq. Əsas əlif-banın altıncı hərfi "ı" ilə 5-ə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərf "l" hərfidir, bu hərf şifrmətnin 6-cı hərfi olacaq.

Həhayət, əsas əlifbanın yeddinci "q" hərfi ilə 3-ə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərf "n" hərfidir, bu hərf də şifrmətnin 7-ci hərfi olacaq.

Beləliklə, biz nəticəvi şifrmətni alırıq: "ç ç e f ö l n".

Deşifrlənmə prosesində aşağıda göstərildiyi kimi birinci sətrdə açar kodu, onun altında isə əsas əlifba yazılır, yəni

Açar kodu 3 4 5 3 4 5 3

Şifrmətn ç ç e f ö l n

Deşifrlənmə məqsədilə 3-ə uyğun sətrdə olan "ç" hərfini tapıb əsas əlifba istiqamətində yüxarı qalxaraq onların kəsişmə nöqtəsindəki hərfi tapırıq. Bu hərf "a" hərfdir, elə bu hərf də şifrlənmiş mətnin birinci hərfi olacaq. İlkin mətnin digər hərfləri də ardıcıl olaraq bu qayda ilə tapılır.

Beləliklə, şifrmətni deşifrələyərək aşağıdakı ilkin mətni alırıq:

"a z a d l ı q".

## 2.4. Qammalaşdırma üsulu

Çoxəlifbalı əvəzləmənin xüsusi üsullarından bri də qamma-laşdırma üsuludur. Bu üsulda şifləmə ilkin mətnin işarələrinin açarın işarələri ilə iki modulu üzrə toplanması vasitəsilə yerinə yetirilir. Əgər ilkin əlifbada 32 işarə varsa, onda toplama 32 modulu üzrə həyata keçirilir. İlkin mətnin və açarın belə toplama prosesi kripto-qrafiyada qammaların üst-üstə qoyulması adlanır.

Fərz edək ki, ilkin əlifbanın işarələri 0 (A)-dan 32 (Z)-ə qədər olan aralıqda dəyişir. Əgər ilkin mətnin işarələrnə uyğun gələn ədədləri x-la, açarın işarələrini isə a ilə işarə etsək, onda qamma-laşma qaydasını aşağıdakı kimi yazmaq olar:

$$z = x + a \pmod{N},$$

burada z – kodlaşdırılmış işarə, N- əlifbadakı işarələrin sayıdır.

Bu zaman N modulu üzrə toplama əməliyyatı adi toplamaya oxşardır, fərq yalnız ondadır ki, əgər adi toplama N-ə bərabər yaxud

ondan böyük nəticə verirsə, onda toplamanın qiyməti onun N-ə bölünməsindən alınan qalıq hesab olunur.

Praktikada ən çox ikili qammalaşdırmadan istifadə olunur. Bu zaman ikili əlifbadan istifadə olunur, toplama isə iki modulu üzrə həyata keçirilir. İki modulu üzrə toplama tez-tez $\oplus$ -ilə işarə olu-nur, onda yazmaq olar:

$$z = x + a(mod2) = x \oplus a$$

İki modulu üzrə toplama əməliyyatı məntiqi cəbrdə "istisna" yaxud ingiliscə XOR adlanır.

**Misal.** Fərz edək ki, bizdən14 onluq ədədini 12 açarını istifadə etməklə qammalaşdırma metodu ilə şifrləmək tələb olunur. Bunun üçün əvvəlcə ilkin ədədi və açarı (qammanı) ikili formaya çevir-mək vacibdir: $14_{(10)} = 1110_{(2)}$, $12_{(10)} = 1100_{(2)}$. Sonra alınan ikili işarələri biri-birinin altında yazmaq və hər bir cüt işarələri iki modulu üzrə toplamaq lazımdır. İki ikili işarələri modul iki üzrə toplayan zaman "0" alınır, əgər ilkin ikili ədədlər eynidirsə, yox əgər müxtəlifdirsə, onda 1 alınır, yəni:

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

Iki 1110 və 1100 ikili ədədləri modul iki üzrə toplayaq:

| | |
|---|---|
| İlkin ədəd | 1 1 1 0 |
| Qamma | 1 1 0 0 |
| Şifrmətn | 0 0 1 0 |

Toplama nəticəsində 0010 şəklində ikili şifrmətni aldıq. Əgər onu onluq ədədə çevirsək 2 ədədini alarıq. Beləliklə, nəticədə 14 ədədinə 12 açarla qammalaşdırma əməliyyatını istifadə etməklə onluq hesablama sistemində 2 ədədi şəklində şifrmətni alırıq.

Bəs hansı şəkildə şifrin açılması yerinə yetirilir? Şifrin açılması üçün onluq hesablama sistemində alınan 2 ədədini 0 0 1 0 ikili şəkildə yazaraq ikili şəkildə şifrmətni alıb, onu yenidən açarla iki modulu üzrə toplayırıq, yəni:

| | |
|---|---|
| Şifrlənmiş məlumat | 0 0 1 0 |
| Qamma: | 1 1 0 0 |

Ilkin məlumt: 1 1 1 0

Alınan ikili ədədi, yəni 1110-ı onluq ədədinə çevirsək ilkin ədədi-14-ü alırıq. Beləliklə, iki modulu üzrə qammalaşdırma zama-nı həm şifrləmə və həm də şifrin açılması üçün eyni əməliyyat apa-rmaq lazımdır. Bu həm şifrləmə və həm də şifrin açılması üçün proqram reallaşdırılması zamanı eyni bir alqoritm və uyğun olaraq eyni bir proqramı istifadə etməyə imkan verir. İki modulu üzrə top-lama əməliyyatı digər hesablama əməliyyatlarına nisbətən kompü-terdə tez yerinə yetirilir, ona görə də hətta çox böyük açıq mətnin hesablanması praktiki olaraq dərhal yerinə yetirilir. Göstərilən üstün-lük sayəsində qammalaşdırma metodu müasir texniki sistemlərdə geniş istifadə olunur. Ümumi halda 2 modulu üzrə qammalaşdır-manın necə yerinə yetirildiyini göstərək:

**Misal:** Tutaq ki, onaltılıq işarəlik şəklində verilmiş 83 AO AC AC A8 EO AE A2 AO AD A8 A5 ilkin məlumatı 82 A5 E1 AD AO açarı ilə qammalaşdırma metodu ilə şifrləmək tələb olunur. Bu misalda ilkin məlumatın uzunluğu 12 bayt, açarın uzunluğu isə 5 bayta bərabərdir. Buna görə də, şifrləmə zamanı qamma iki dəfə tam və hələ bir dəfə də natamam təkrar olunmalıdır. Şifrləmə məq-sədlə ilkin məlumatı və açarı ayrı-ayrılıqda ikili şəkildə yazırıq. Onda 8-1000, 3-0011, A-1010, O-0000, A-1010, C-1100, A-1010, C-1100, A-1010, 8-1000, E-1110, O-0000, A-1010, E-1110, A-1010, 2-0010, A-1010, O-0000, A-1010, D-1101, A-1010, 8-1000,

A-1010, 5-0101şəklini alacaq. İndi də 82 A5 E1 AD AO açarını ikili şəkildə yazaq. Bu zaman 8-1000, 2-0010, A-1010, 5-0101, E-1110, 1-0001, A-1010, D-1101, A-1010, O-0000 olacaq.

İlkin mətni qammalaşdırma metodu ilə şifrləmək üçün əvvəlcə onun ilk onaltılıq şəkildə olan 83 AO AC-nin 1000 0011 1010 0000 1010 1100 ikili şəkildə təsvirini birinci blokun birinci sətrinə sıra ilə ardıcıl yazırıq, onun altında onaltılıq sistemdə verilmiş 82 A5 E1 açarının ikili təsvirlərini 1000 0010 1010 0101 1110 0001 yerləşdirib birinci bloku formalaşdırırıq, sonra ikinci blokun birinci sətrində ilkin mətnin növbəti AC A8 EO-un uyğun olaraq 1010, 1100, 1010, 1000, 1110, 0000 ikili təsvirlərini ardıcıl sıra ilə yazıb, onun altında açarın onaltılıq AD AO

82-in uyğun olaraq1010, 1101, 1010, 0000, 1000, 0010 ikili təsvirini sıra ilə ardıcıl olaraq yazırıq, bundan sonra ilkin mətnin onaltılıq şəkildə olan AE A2 AO işarələrinin 1010,1110, 1010, 0010, 1010, 0000 ikili təsvirini üçüncü blokun birinci sətrinə yazıb, onun altında açarın A5 E1 AD onaltılıq işarələrinin uyğun 1010 0101 1110 0001 1010 1101 ikili təsvirlərini yazırıq, nəhayət ilkin mətnin axırıncı AD A8 A5 onaltılıq işarələrinin1010, 1101, 1010, 1000, 1010, 0101 ikili təsvi-rini dördüncü blokun birinci sətrinə sıra ilə ardıcıl yazıb, onun altında açarın onaltılıq şəkildə verilmiş birinci üç AD A8 A5 işarəsinin uyğun 1000, 0010, 1010, 0101, 1110,0001 ikili işarələ-rini yazıb blokları ayrı-ayrılıqda 2 modulu üzrə toplayıb:

1-ci. İlkin bitlər: 1000 0011 1010 0000 1010 1100
Qamma(açar): 1000 0010 1010 0101 1110 0001
Nəticə: 0000 0001 0000 0101 0100 1101
2-ci blok. İlkin bitlər: 1010 1100 1010 1000 1110 0000
Qamma (açar): 1010 1101 1010 0000 1000 0010
Nəticə: 0000 0001 0000 1000 0110 0010
3-cü blok. İlkin bitlər:1010 1110 1010 0010 1010 0000
Qamma (açar):1010 0101 1110 0001 1010 1101
Nəticə: 0000 1011 0100 0011 0000 1101
4-cüblok.İlkin bitlər:1010 1101 1010 1000 1010 0101
Qamma (açar):1000 0010 1010 0101 1110 0001
Nəticə: 0010 1111 0000 1101 0100 0100

Şifrmətni almaq üçün birinci blokun nəticəsini ayrı-ayrlıqda onaltılıq işarələrə çeviririk. Onda nəticədə olan birinci cütlük "0000 və 0001"-01-ə; ikinci cütlük "0000 və 0101" cütlük-05-ə; üçüncü cütlük "0100 və 1101"-4D-yə çevrilir.

İkinci blokun nəticəsini də ayrı-ayrılıqda onaltılıq sistemə çevir-sək birinci cütlük "0000 və 0001"- 01-ə; ikinci cütlük "0000 və 1000"- 08-ə; üçüncü cütlük "0110 və 0010"-62-yə.

Üçüncü blokda alınan nəticəni onaltılıq işarəyə çevirsək, onun nəticəsində alınan birinci cütlük "0000 və 1011"- 0B-yə" ikinci cütlük "0100 və 0011"- 43-ə üçüncü cütlük "0000 və 1101"- 0D-yə çevrilir.

Nəhayət dördüncü blokun nəticəsindəki birinci cütlük “0010 və 1111” – 2F; ikinci cütlük “0000 və 1101”-0D; üçüncü cütlük “ 010 0 və 0100”- 44-ə çevriləcək.

Bundan sonra ayrı-ayrı blokların nəticələrində alınan onaltılıq işarələri uyğun olaraq ardıcıl olaraq bir sətrdə yazaraq aşağıdakı onaltılıq sistemdə şifrlənmiş mətni alırıq:

Şifrmətn: 01 05 4D 01 08 62 0B 43 0D 2F 0D 44

İndi də qammalaşdırma nəticəsində alınan şifrlənmiş mətnin deşifrlənməsi prosesinə baxaq. Bu məqsədlə birinci sətrdə onaltılıq işarə ilə şifrmətn, onun altlında isə onaltılıq işarə ilə açar yazılır yəni:

Şifrlənmiş mətn: 01 05 4D 01 08 62 OB 43 OD 2F OD 45

Açar: 82 A5 E1 AD AO

Şifrləmədə olduğu kimi burada da ilkin məlumatın uzunluğu 12 bayt, açarın uzunluğu isə 5 bayta bərabərdir. Buna görə də, deşifr-ləmə zamanı qamma iki dəfə tam və hələ bir dəfə də natamam şəkildə təkrar olunmalıdır. Deşifrlənmiş mətnin və açarın onaltılıq işarələri yuxarıda göstərildiyi kimi ayrı-ayrılıqda ikili kod şəklində yazılır və biri o birinin altında yazılır və 2 modulu üzrə toplanır.

I blok.Şifr mətn: 0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 1 0 1 0 0 1 1 0 1

Qamma: 1 0 0 0 0 0 1 0 1 0 1 0 0 1 0 1 1 1 1 0 0 0 0 1

Nəticə: 1 0 0 0 0 0 1 1 1 0 1 0 0 0 0 1 0 1 0 1 1 0 0

II blok.Şifr mətn 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 1 0 0 0 1 0

Qamma:1 0 1 0 1 1 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 1 0

Nəticə:1 0 1 0 1 1 0 0 1 0 1 0 1 0 0 0 1 1 1 0 0 0 0 0

III blok.Şifrmətn: 0 0 0 0 1 0 1 1 0 1 0 0 0 0 1 1 0 0 0 0 1 1 0 1

Qamma: 1 0 1 0 0 1 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 1 0 1

Nəticə: 1 0 1 0 1 1 1 0 1 0 1 0 0 0 1 0 1 0 1 0 0 0 0 0

lV blok. Şifr mətn:0 0 1 0 1 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 0 1 0 0

Qamma: 1 0 0 0 0 0 1 0 1 0 1 0 0 1 0 1 1 1 1 0 0 0 0 1

Nəticə:1 0 1 0 1 1 0 1 1 0 1 0 1 0 0 0 1 0 1 0 0 1 0 1

Deşifrləmə üçün birinci blokun nəticəsini ayrı-ayrılıqda onaltılıq işarələrə çeviririk. Onda nəticədə olan birinci cütlük “1 0 0 0 və 0 0 11” - 83-ə; ikinci cütlük “1 0 1 0 və 0 0 0 0”-A0-ya; üçüncü cütlük “1 0 1 0 və 1 1 0 0”- AC-yə çevrilir.

İkinci blokun nəticəcini də ayrı-ayrılıqda onaltılıq işarəyə çevir-sək birinci cütlük “1 0 1 0 və 1 1 0 0”-AC-yə; ikinci cütlük “1 0 1 0 və 1 0 0 0”-A8-ə; üçüncü cütlük “1 1 1 0 və 0 0 0 0”-EO-ya çevrilir.

Üçüncü blokda alınan nəticəni onaltılıq işarəyə çevirsək, onun nəticəsində alınan birinci cütlük “1 0 1 0 və1 1 1 0”- AE-yə; ikinci cütlük “1 0 1 0 və 0 0 1 0”-A2-yə; üçüncü cütlük “1 0 1 0 və 0 0 0 0”- A0-ya çevriləcək.

Nəhayət, dördüncü blokun nəticəsindəki birinci cütlük “1 0 1 0 və 1 1 0 1”- AD-yə; ikinci cütlük “1 0 1 0 və 1 0 0 0”- A8-ə; üçüncü cütlük “1 0 1 0 və 0 1 0 1”-A5-ə çevriləcək.

Bundan sonra ayrı-ayrı blokların nəticələrində alınan onaltılıq işarələri uyğun olaraq ardıcıl olaraq bir sətrdə yazaraq aşağıdakı onaltılıq sistemdə ilkin məlumatı alırıq:

İlkin mətn: 83 A0 AC AC A8 EO AE A2 AO AD A8 A5

Açar uzun olduqca qammalaşdırma metodu ilə şifrləmənin də etibarlığı artıq olur. Praktikada açarın uzunluğu verilənlərin müba-diləsi aparatının imkanları ilə və hesablama texnikasının, eləcə də açara ayrılan yaddaşın həcmilə məhdudlaşır.

Açarın istifadə olunması üçün əvvəlcə hər-hansı bir etibarlı üsulla onu hər informasiya mübadiləsi aparan iki tərəfə çatdırmaq vacibdir.

Bu açarların paylanması problemlərinin yaranmasına səbəb olur. Bu problemin həlli açarın uzunluğunun artması və şəbəkədə abonentlərin sayının artması ilə daha da artır.

## 2.5. Yer dəyişdirmə metodu

Bu metodun istifadə olunması zamanı ilkin mətn seli bloklara bölünür. Bu blokların hər birində işarələrin yerdəyişməsi baş verir. Klassik “kompüter” kriptoqrafiyasınadək yerdəyişmə ilkin mətnin yazılması və şifrlənmiş mətnin həndəsi fiqurlar üzrə müxtəlif yol-larla oxunması nəticəsində alınırdı.

Yerdəyişməyə sadə misal olaraq qeyd edilmiş d periodlu yerdə-yişməni göstərmək olar. Bu metodda məlumat d işalərindən ibarət bloklara bölünürlər və hər bir blokda eyni bir yerdəyişmə baş verir. Yerdəyişmənin baş vermə qaydası açarla tənzimlənir və natural ədədlərin hər hansı birinci d yerdəyişməsi ilə verilə bilər. Nəticədə məlumatın

hərflərinin özləri dəyişmirlər, lakin digər qaydada veri-lirlər. Məsələn, d = 6 olduqda yerdəyişmə açarı kimi 436215-i gö-türmək olar. Bu onu göstərir ki, 6 işarədən ibarət olan hər bir blokda dördüncü işarə birinci yerdə, üçüncü –ikinci yerdə, altıncı- üçüncü yerdə durur və s.

**Misal:** Tutaq ki, azərbaycan dilində verilən aşağıdakı mətnin şifrlənməsi tələb olunur:

BU_MƏTN_ŞİFRLƏMƏ_ÜÇÜNDÜR

İlkin mətndə işarələrin sayı 24-dür, buna görə məlumatı 4 bloka bölmək vacibdir. 436215 açarının köməyi ilə yerdəyişmənin nəticə-sində şifrlənmiş məlumat aşağıdakı kimi olacaq:

M_TUBƏİŞR_NFƏMÜƏL_DNRÜÇÜ

Deşifrləmə də açar vasitəsilə aparılır. Bu məqsədlə aşağıda göstərildiyi kimi əvvəlcə birinci sətrdə açar təkrar olunmaqla yazılır, onun altında isə şifrmətn yerləşdirilir, yəni

4 3 6 2 1 5 4 3 6 2 1 5 4 3 6 2 1 5 4 3 6 2 1 5
M _ T U B Ə İ Ş R _ N F Ə M Ü Ə L _ D N R Ü Ç Ü

Deşifrləmə nəticəsində 1 rəqəminin altında duran ədəd açıq mətnin birinci hərfi, 2 rəqəminin altında olan ədəd açıq mətnin ikinci hərfi və s., açıq mətnin digər hərfləri də bu qayda ilə tapılaraq açıq mətn aşağıdakı kimi alınır:

BU_MƏTN_ŞİFRLƏMƏ_ÜÇÜNDÜR

Beləliklə, biz şifrmətni deşifrələməklə açıq mətni aldıq.

Nəzəri olaraq, əgər blok d işarələrdən ibarətdirsə, onda müm-kün olan yerdəyişmələr d!= 1*2...*(d-1)*d olacaq. Axırıncı misalda d=6-dır, buna görə də yerdəyişmələrin sayı 6!= 1*2*3*4*5*6= 720 olacaq. Beləliklə, əgər düşmən baxılan misaldakı şifrlənmiş məlumatı tutarsa, ona ilkin məlumatı açmaq üçün 720 cəhd lazım gələcək (əgər düşmənə blokun ölçüsü məlumdursa). Kriptodayanıqlığı artırmaq üçün şifrlənəcək məlumatda müxtəlif periodlarla ardıcıl olaraq iki yaxud daha çox yerdəyişmələr aparmaq lazımdır.

## 2.6. Cədvəl üzrə yerdəyişmə

Yerdəyişmə metoduna digər misal olaraq cədvəl üzrə yerdə-yişməni göstərmək olar. Bu metodda ilkin məlumatın bəzi cəd-vəllərin sətrlərinə yazılması və onu elə bu cədvəlin də sütunları üzrə oxunması həyata keçirilir. Sətrin doldurulması ardıcıllığı və sütunların oxunması istənilən kimi açarla verilir.

**Misal.** Fərz edək ki, kodlama cədvəlində 4 sütun və 3 sətr var (blokun ölçüsü 3*4 =12-dir). bu mətni cədvəl üzrə şifrləmək tələb olunr.

Aşağıda göstərildiyi kimi ilkin məlumatda işarələrin sayı 24-ə bərabərdir, yəni

BU_MƏTN_ŞİFRLƏMƏ_ÜÇÜNDÜR

Buna görə də, məlumatı 2 bloka bölmək lazımdır (yəni 24:12= =2). Hər bloku sətrlər üzrə öz cədvəlinə yazaq (cədvəl 3.8).

Sonra cədvəldən hər bloku ardıcıl olaraq sütünlar üzrə oxuyub yazmaqla aşağıdakı şifrlənmiş mətni alaceyik:

BƏŞ UTİ _NFMM_RL_NƏÜD MÇU ƏÜD

Sütunları ardıcıl olmayaraq da oxumaq olar.Bu halda oxunma qaydası açarla olacaq. Əgər məlumatın ölçüsü blokun uzunluğuna

bərabər olmayacaqsa, onda məlumatı mənaya xələl gətirməyən hər-

***Cədvəl 2.8.***

| Cədvəl 2.8. Cədvəl üzrə yerdəyişmə metodu ilə şifrləmə | | | |
|---|---|---|---|
| **1-ci blok** | | | |
| B | U | _ | M |
| Ə | T | N | _ |
| Ş | İ | F | R |
| **2 –ci blok** | | | |
| L | Ə | M | Ə |
| _ | Ü | Ç | Ü |
| N | D | Ü | D |

hansı əlavə işarələrlə doldurmaq olar, məsələn, boşluqlarla. Lakin bunu etmək tövsiyyə edilmir, çünki, bu, düşmənə informasiyanın kriptoqramını tutduğu zaman istifadə olunan yerdəyişmə cədvəlinin ölçüsü (blokun uzunluğu) haqda informasiya əldə etməyə imkan verər. Blokun uzunluğunu tapdıqdan sonra düşmən blokun uzunlu-ğunun bölücüləri arasından açarın uzunluğunu tapa bilər.

Ölçüsü yerdəyişmə cədvəlinin ölçüsündən az olan məlumatın şifrlənməsi və onun şifrinin açılmasına baxaq. Aşağıda verilmiş sö-

zü şifrləyək:

DƏYİŞMƏLİ

İlkin məlumatda işarələrin sayı 9-a bərabərdir. Məlumatı sətrlər üzrə cədvələ yazaq (cədvəl.2.9), axırıncı üç oyucuğu boş qoyaq. Sonra cədvəldən ardıcıl olaraq sütunlar üzrə oxuyaceyik, nəticədə aşağıdakı şifrmətni alırıq:

DŞİƏMYƏİL

***Cədvəl 2.9***

Cədvəl 2.9. Yerdəyişmə cədvəli üzrə natamam blokun şifrlənməsi

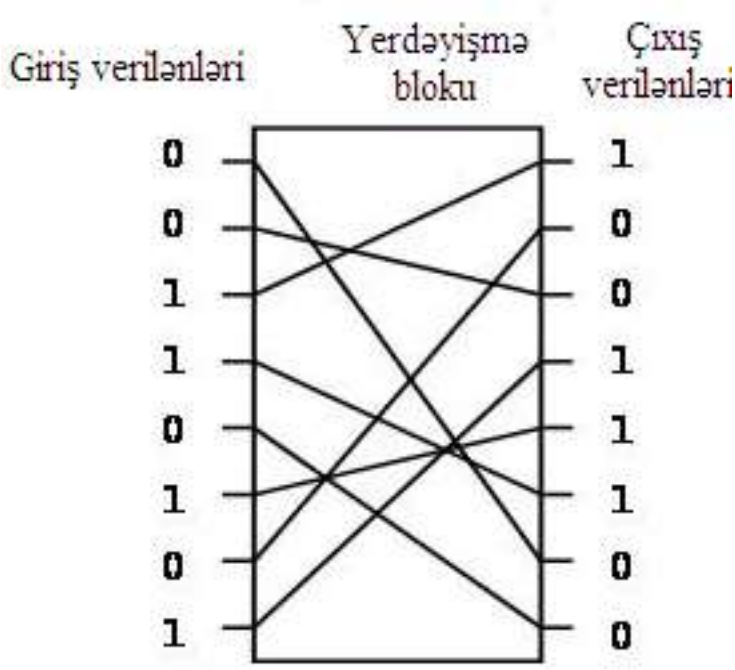
| | | | |
|---|---|---|---|
| D | Ə | Y | İ |
| Ş | M | Ə | L |
| İ | | | |

Şifri açmaq üçün əvvəlcə tam sütunların sayı təyin edilir, yəni axırıncı sətrdəki işarələrin sayını (bizim misalda 1-dir). Bunun üçün məlumatın ölçüsünü (bizim misalda 9-dur) sütunların sayına bölürlər yaxud açarın ölçüsünə (bizim misalda 4-dür). Buna görə də bizim misalda 1 tam və üç qısa sütun var. İndi məlumatın hərflə-rini öz yerinə yazıb məlumatın şifrini açmaq olar. Şifrləmə zamanı açar 1234 (sütunları ardıcıl oxumaqla) olduğu üçün, şifrin açılması zamanı birinci üç işarəni (DŞİ) yerdəyişmə cədvəlinin birinci sütu-na yazılır, növbəti iki işarə (ƏM) ikinci sütuna, növbəti iki işarə (YƏ)-üçüncü sütuna və axırıncı iki işarə (İL) isə dördüncü sütuna yazılır. Cədvəl dolduqdan sonra sətrləri oxuyuruq və ilkin məluma-tı alırıq:

DƏYİŞMƏLİ

## 2.7. Proqram və aparat yolu ilə reallaşdırılan yerdəyişmə

Proqram və aparat yolu ilə reallaşdırıla bilən digər yerdəyişmə üsulları mövcuddur. Məsələn, ikili şəkildə yazılan verilənlərin ötürülməsi zamanı, aparat blokunu istifadə etmək əlverişlidir, hansı ki, uyğun elektrik montajın köməyi ilə işarəli məlumatı müəyyən qaydada qarışdırır. Əgər blokun uzunluğunu səkkiz bitə bərabər qəbul etsək şək.2.3-də verilmiş yerdəyişmə blokunu istifadə etmək olar. Şifrin açılması üçün qəbul tərəfdə dövrənin qaydasını bərpa edən blok qoyulur [4]. Bu metod praktikada geniş istifadə olunur.




**Şək.2.3.** Aparatlı yerdəyişmə bloku

## 2.8. Kompozisiya şifri anlayışı

Bir neçə dalbadal istifadə edilən sadə şifrlər kombinasiyası (məsələn, əvəzetmə) nəticədə kombinasiya edilmiş (kompozisiya) adlanır və çox çətin çevirmə verir. Bu şifr ayrı-ayrı əvəzetmələrə nisbə-tən daha

güclü kriptoqrafik imkanlara malikdir.Bunu aşağıdakı misalın timsalında göstərək. Fərz edək ki, əvəzləmə periodu d = 6-dır, açar isə A = 436215-dir. Bu o deməkdir ki, hər blokda altı işa-rədən dördüncusü- birinci yerdə, üçüncü işarə- ikinci yerdə, altıncı işarə - üçüncü yerdə və s. dururlar.

Seçilən A= 436215 açarla "SİQNAL" sözünü şifrləyək. Nəticə-də alırıq:

$$\text{SİQNAL} \xrightarrow{A = 436215} \text{NQLİSA}$$

Fərz edək ki, düşmənə şifrləmə metodu məlumdur, lakin açar məlum deyil. Əgər düşmən NQLİSA məlumatını tutarsa, ona 720-dən az olmayan cəhd lazım gələcək. 720 variantları öyrənmək üçün elədə çox vaxt aparmır. Fərz edək ki, hər bir variantı öyrənmək üçün düşmən 1 saniyə itirir. Onda 720 cəhdə 12 dəqiqə vaxt tələb olunur. Beləliklə, 12 dəqiqədən çox olmayan bir vaxtda düşmən bizim açarımızı öyrənir və həmin bağlı açarla da bütün məlumatın şifrini aça bilir. Əgər düşmən tərəfindən axtarış kompüterlə apa-rılırsa, NQLİSA məlumatının şifrəsinin açılmasına daha az vaxt sərf olunur.

Bu zaman belə bir sual yaranır, bizim şifrin kriptoanlizini necə mürəkkəbləşdirmək olar?

Əvəzləmə periodunun ölçüsünü artırmaq olar, məsələn, minədək işarə qoyulur. Lakin, bu zaman açarın ölçüsü də artır. Belə açarı yadda saxlamaq və istifadə etmək çox çətindir. Başqa yolla get-məyə cəhd edək və altı işarədən ibarət blokda əvəzləmədən qabaq Sezar metodu ilə sadə əvəzləmə istifadə edək. Sezar metodunda açarı $a_1$ ($1<=a_1<=31$)-lə, əvəzləmə zamanı isə açarı $a_2$ ilə işarə edək. Onda ümumi açar $A= (a_1,a_2)$ olar. Beləliklə, əgər A= (5; 436215)-dirsə, bu onu göstərir ki, əvvəlcə şifrlənən işarələr Sezar metodu üzrə 5 açarı ilə şifrlənir, sonra isə altı işarədən ibarət olan hər bir blokda əvəzləmə 436215 açarı ilə həyata keçirilir.

SİQNAL sözünün şifrlənməsini iki mərhələdə yerinə yetirək. Bu məqsədlə əvvəlcə azərbaycan əlifbasını yazaq:

A B C Ç D E Ə F G Ğ H X I İ J K Q L M N O Ö P R S Ş T UÜV Y Z

Birinci mərhələdə beş açarı ilə şifrləmə zamanı hər bir hərf özündən sağ tərəfə beş işarə sağa sürüşdürülür, ikinci mərhələdə isə yerdəyişmə üsulundan istifadə olunur. Bu zaman SİQNAL sözü-nün şifrlənməsi hər iki mərhələdə aşağıdakı qaydada aparılır:

a1=5

I Mərhələ (əvəzetmə):SİQNAL → VMÖSEP

k2= 436215

II Mərhələ(yerdəyişmə): VMÖSEP → SÖPMVE

Belə də yazmaq olar:

A=(5,436215)

SİQNAL → SÖPMVE

Sezar şifrində mümkün olan açarların sayı 31-dir, ona görə də mümkün olan açarların variantlarının ümumi sayı 31x720=22320-yə bərabərdir. Beləliklə, həqiqətən alınan kompozisiya şifr ayrı-ayrı yerinə yetirilmiş əvəzləmə və yerdəyişmədən kifayət dərəcədə güc-lüdür.

Statistik üsulla kriptoanalizi mürəkkəbləşdirmək üçün eyni bir açarla kompozisiya şifrini iki dəfə istifadə etmək olar:

I şifrləmə dövrü a1=5

I Mərhələ (əvəzetmə): SİQNAL → VMÖSEP

a2= 436215

II Mərhələ(yerdəyişmə): VMÖSEP → SÖPMVE

İkinci şifrləmə dövrü a1=5

I Mərhələ (əvəzetmə): SÖPMVE → VTURCH

a2= 436215

II Mərhələ (yerdəyişmə): VTURCH → RUHTVC

Dalbadal iki yerinə yetirirlən şifrləmə dövrünün nəticəsində SİQNAL sözü RUHTVC sözünə çevrildi. Bu zaman şifrin açarlar məkanı dəyişmədi, lakin ikiqat şifrəmətnin hesabına ilkin mətnin statistik qanuna uyğunluğu güclü olaraq maskalanmışdır.

Deşifrləmə aşağıdakı qaydada aparılır:

Birinci mərhələ

a2=436215

I Mərhələ: RUHTVC → VTURCH

a1=5

II Mərhələ: VTURCH → SÖPMVE

İkinci mərhələ

a2= 436215

I Mərhələ: SÖPMVE → VMÖSEP

a1=5

II Mərhələ: VMÖSEP → SİQNAL

Simmetrik alqoritmlər ilkin mətni bloklarla və sellərlə emal edə bilirlər. Buna görə də simmetrik şifrləmə alqoritmləri blok və sel alqoritmlərinə bölünürlər. Mətnin blokuna mənfi olmayan tam ədəd kimi baxılır. Blokun uzunluğu həmişə 64,128,256 bitə bərabər götürülür.

Real şifrlərdə zəncirvari yaxud bloklarla verilən işarələr üzərin-də bir neçə sadə əməliyyatlar istifadə olunur. Kriptodayanıqlığı artırmaq üçün bu əməliyyatlar raundlar yaxud addımlar yarat-maqla dövrü olaraq bir neçə dəfə yerinə yetirilir. Şifrin dayanıq-lığına blokun ölçüsü, açarın ölçüsü, şifrləmə raundlarının sayı kimi faktorlar təsir göstərir. Bağlı açarlı müasir şifrlər yalnız ikili veri-lənləri emal edirlər, ona görə də onlarda adi əvəzləmədən və yerdə-yişmədən başqa ikili ədədlərə xas olan bir sıra digər əməliyyatlar da istifadə olunur.

## 2.9. Simmetrik şifrləmənin blok alqoritmlərində istifadə olunan əməliyyatlar

Bu alqoritmlərdə əməliyyatlar ikili verilənlərə tətbiq edilirlər. İstənilən informasiya, məsələn, təsvir yaxud mətn ikili şəkildə ifadə edilə bilər. Bunun sayəsində şifrləmə zamanı verilən informasiya-nın mənası haqda düşünmək lazım gəlmir. Tez-tez istifadə olunan əməliyyatlardan biri-2modulu üzrə bitlərin toplanması əməliyyatı-dır. 2 modulu üzrə toplama zamanı operandlar işarələr üzrə emal olunurlar. Əgər operandlarda cüt olmayan işarələr varsa, onda həmin işarələrə vahid, cüt işarələrə isə sıfır verilir. Məsələn, 2 mo-dulu üzrə 16-işarəli ədədləri toplayaq [3]:

| İşarələr: | 15 | 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Operand 1: | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| Operand 2: | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |

2 modulu: 1 1 0 1 1 0 0 1 1 0 0 1 1 0 0 1

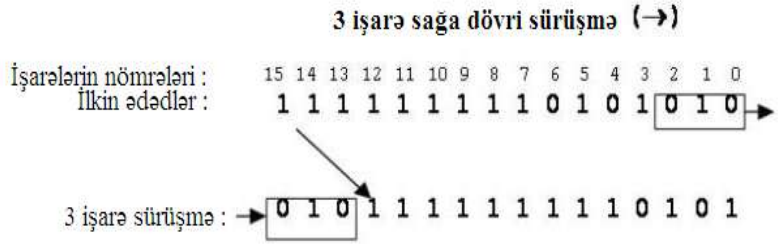
Bu əməliyyat çox əlverişli xassəyə malikdir:iki modulu üzrə çıxma elə toplama əməliyyatı kimidir, ona görə də operandlardan biri cəmə digər operadumu əlavə etməklə alına bilər.

***Dövrü sürüşmə*** bit zəncirlərini bir neçə işarə sola yaxud sağa sürüşdürür. Sola dövrü sürüşmə zamanı, soldan işarələr torundan çıxan bitlər, sağdan azad olan yerlərə yazılır (şək.2.4). Sağa dövrü sürüşmə zamanı bütün bitlər zəncirvari olaraq sağa hərəkət edirlər, hansılarınakı yer çatmır, onlar zəncirin quyruğuna keçirilir. Məsə-lən, ikili işarələri üç işarə sola sürüşdürək. Bunun üçün onları aşa-ğıda göstərildiyi kimi hər dəfə 1 işarə sola sürüşdürərək və on-beşinci işarədən kənara çıxan işarələri sıfırıncı yerə gətirməklə ikili işarələri 3 dəfə təzədən yazaceyik.

Analoji olaraq sağa dövri sürüşmə yerinə yetirilir (şək. 2.5). Göstərildiyi kimi sağa 3 işarə sürüşmə zamanı, ilkin ədədlərin sıfı-rıncı, birinci və ikinci bitləri işarələr torundan kənara çıxır [3]:


**Şək.2.4**. 3 İşarə sola doğru sürüşmə

və yadda saxlanılırlar, yerdə qalan bitlər 3 işarə sağa sürüşdürülür-lər, sonra yadda saxlanılan bitlər 13-cü, 14-cü və 15-ci yerlərə yazılırlar.




**Şək.2.5.** 3 işarə sağa doğru sürüşmə [3]

## 2.10. Cədvəl əvəzlənməsi

Cədvəl əvəzlənməsi zamanı bit qrupları bitlərin digər qrupu ilə əvəz edilir. Bu əməliyyat zamanı bir ikili verilənlər bloku müəy-yən qayda yaxud cədvəl üzrə digər blokla əvəz edilir (cədvəl 2.10). Məsələn, 3 işarədən ibarət olan blokların hər birini aşağıdakı cəd-vəl üzrə digər 3 işarədən ibarət olan blokla əvəz etmək olar.

Əgər "Giriş" və "Çıxış" sütunlarında yazılmış hər bir qiyməti ikili şəkildə deyil, onluq şəkildə yazarıqsa, onda həmin cədvəli aşa-

ğıdakı kimi qısa yazmaq olar, yəni:

0->3, 1->5, 2->0, 3->7, 4->2, 5->6, 6->1, 7->4

Bu yazılışın birinci ədədləri girişdəki ədədləri, ikincilər isə çıxış

***Cədvəl 2.10.***

| G i r i ş | | Ç ı x ı ş | |
|---|---|---|---|
| İkili sistemdə | onluq sistemdə | İkili sistemdə | onluq sistemdə |
| 000 | 0 | 011 | 3 |
| 001 | 1 | 101 | 5 |
| 010 | 2 | 000 | 0 |
| 011 | 3 | 111 | 7 |
| 100 | 4 | 010 | 2 |
| 101 | 5 | 110 | 6 |
| 110 | 6 | 001 | 1 |
| 111 | 7 | 100 | 4 |

qaydada nizama salınıbsa, onda ümumiyyətlə birinci ədədləri yaz mamaq, ancaq onlara uyğun çıxış ədədlərini yazmaq olar yəni:

3,5,0,7, 2, 6,1, 4.

Yəni 3- bitli blok üçün əvəz halında əvəz cədvəlindən sıra nöm-rəsilə, əvəzlənən blokun qiymətinə bərabər element götürülür.

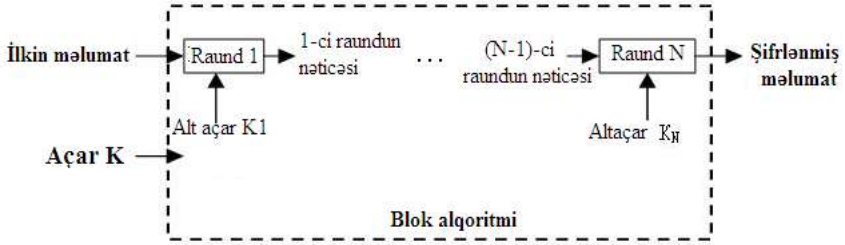
Əgər 4 ikili ədəddən ibarət qrupu əvəzləmək vacibdirsə, onda əvəzləmə cədvəli 16 ədəddən ibarət olacaq. Ümumi halda n bitli blok üçün əvəzləmə cədvəli $2^n$ elementdən ibarət olmalıdır.

Cədvəl əvəzlənməsini ədəbiyyatlarda bəzən S-blokun istifadə olunması ilə əvəzləmə adlandırırlar (S hərfi ingilis sözündən götü-rülüb substitution-əvəzləmə). Sürüşmə əməliyyatının köməyi ilə məlumatın bitləri yenidən qaydaya salınır. Sürüşmə həm də P-blokla adlanır.

## 2.11. Simmetrik şifrləmənin blok alqoritminin strukturu

Simmetrik şifrləmə alqoritmində tez-tez 2 modulu üzrə toplama, $2^{16}$ modulu üzrə toplama, $2^{32}$ modulu üzrə toplama, dövri sürüşmə, əvəzləmə və yerdəyişmə əməliyyatları işlənilir. Bu əməliyyatlar al-qoritmdə raund yaxud addım ilə dövrü olaraq N dəfə təkrar olunur. Hər bir raund üçün ilkin verilənlər əvvəlki raundun çıxışı və müəy-yən alqoritm üzrə ümumi şifrləmə açarı K-dan alınan açar olur.

Raundun açarı alt açar adlanır və $K_i$ ilə işarə edilir [3,4] (şək.2.6).



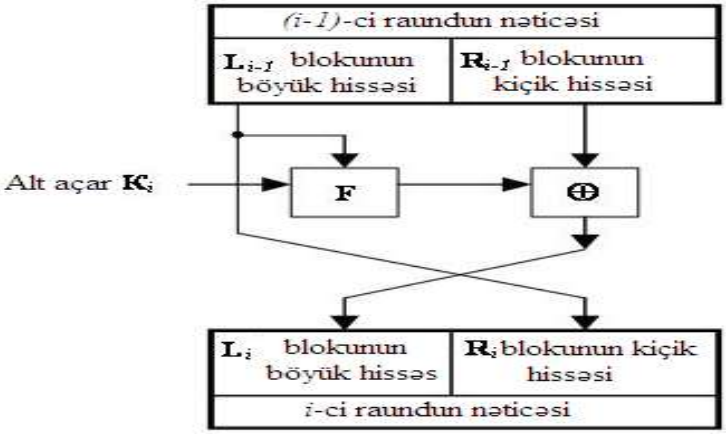

**Şək. 2.6.** Simmetrik şifrləmənin blok alqoritminin strukturası

Şifrləmənin blok alqoritmi ikili verilənlərə tətbiq olunur. Ümu-mi halda blok şifrləmə əməliyyatı açıq mətnin n-bitli blokunu şifr-lənmiş mətnin k-bitli blokuna çevirir. n uzunluqlu blokun uzunlu-ğu $2^n$-ə bərabərdir. Çevirmənin ilk vəziyyətinə qayıtmaq qabiliy-yətinə malik olması üçün, bu bloklardan hər biri şifrlənmiş mətnin öz nadir blokuna çevrilməlidir. Blokun uzunluğu həmişə 2-in dərə-cəsinə n-ə bərabər seçilir, məsələn 64, 128, 256.

## 2.12. Bağlı açarlı blok şifrinin qurulma prinsipi

**Feystel şəbəkəsi.** Şifrləmənin blok alqoritminin ümumi struktu-ru şək.2.7-da verilib. Aşkardır ki, verilənlərin çevrilməsinin özü raundlarda yaxud addımlarda yerinə yetirilir [3,5].

Bir raunda hansı əməliyyatları etmək lazımdır ki, bütün alqoritmlərin yerinə yetirilməsi nəticəsində etibarlı şifrlənmiş mətn alınsın. Blok şifrlərinin işlənmə prinsiplərinin tədqiqində amerika alimi Horst Feystelin böyük əməyi olmuşdur. O, hal-hazırda Feystel şəbəkəsi adlanan struktur təklif etmişdir. Feystel şəbəkəsi bir tərəfdən simmetrik şifrləmənin bütün tələblərini ödəyir, digər tərəfdən, kifayət dərəcədə sadədir və istifadə olunmada əlverişlidir. Feystel şəbəkəsi üzrə




**Şək.2.7.** Feystel şəbəkəsinin i-ci raundu

yaradılan Raund aşağıdakı struktura malikdir. Giriş bloku bərabər uzunluqlu bir neçə hissələrə bölünür. Bu hissələr bu-daq adlanırlar. Məsələn, blokun uzunluğu 64 bit-ə bərabərdirsə, on-da hər birinin uzunluğu 32 bitə bərabər olan iki budaq istifadə olu-nur. Budaqlar ayrı-ayrılıqda emal olunurlar, bundan sonra bütün budaqların sola dövri sürüşmələri həyata keçirir. İki budaqlı halda hər bir raund aşağıdakı struktura malikdir . F funk-siyası yaradıcı funksiya adlanır. Hər bir raund bir budaq üçün F funksiyasının hesablanmasından və F funksiyasının nəticələrini digər budaqla "2 modulu üzrə toplama" əməliyyatının yerinə yetirilməsindən ibarətdir. Bundan sonra budaqlar yerlərini dəyi-şirlər. Raundların sayı müxtəlif alqoritmlər üçün müxtəlif ola bilir. Bəzi alqoritmlərdə 8-dən 32-yə dək, digər alqoritmlərdə isə daha çox olur. Raundların sayı artdıqca alqoritm dəyişmədən onun

kriptodayanığı artır. Elə bu səbəbdən də Feystel şəbəkəsi praktika-da geniş yayılmışdır. Son zamanlar raundların sayı qeyd olunmur, yalnız tövsiyyə olunan sədd göstərilir. Praktikada Feystel şəbəkəsinin 4-budaqlı 128 bitli blok üçün müxtəlif növləri istifadə olunur.

## 2.13. DES və AES şifrləmə alqoritmləri

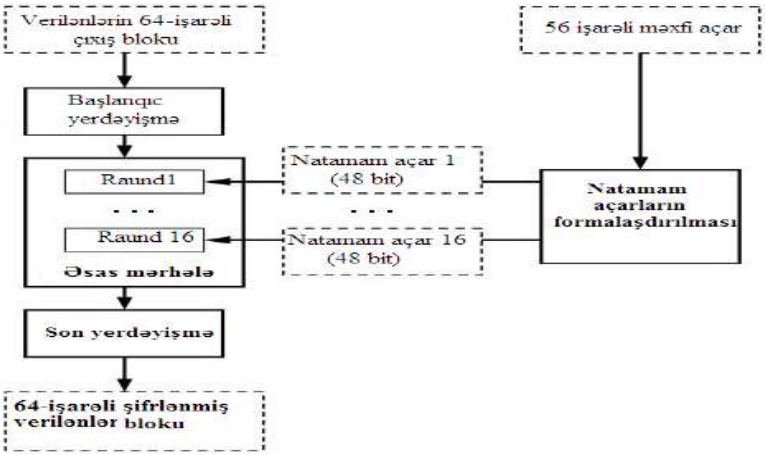
### 2.13.1. Əsas məlumatlar

Bağlı açarlı kriptoqrafik sistemlərdən ən məhşur olanlardan biri DES (*Data Encryption Standard)* alqoritmidir [3,5]. Bu sistem verilən-lərin şifrlənməsi sahəsində ilk dövlət standartı adını almışdır. DES alqoritmi İBM firmasının mütəxəssisləri tərəfindən işlənib hazırlan-mışdır və 1977-ci ildən ABŞ-da fəaliyyət göstərir. Bu alqoritm müxtəlif hesablama sistemləri arasında verilənlərin mühafizə edilməsində və ötürülməsində; poçt sistemlərində, cizgilərin elektron sistemlərində və kommersiya informasiyasının elektron mübadiləsində geniş istifadə olunur. DES standartı həm aparat və həm də proqram şəklində reallaşdırılmışdır. Baxmayaraq ki bu standart bir neçə ildir ki, dövlət standartı adını daşımır, lakin əvvəlki kimi bağlı açarlı şifrləmə sisteminin öyrənilməsində geniş istifadə olunmaqdadır. Açarın uzunluğu DES alqoritmində 56 bit-dir. Müxtəlif hücumlara nisbətən müqavimət göstərmək mübahisəsi məhz bu faktla bağlıdır. Məlum olduğu kimi, istənilən bağlı blok şifrini açarların mümkün olan kombinasiyasını seçməklə sındırmaq olar. Açarın uzunluğu 56 bit olan zaman $2^{56}$ müxtəlif açarlar mümkündür. Əgər kompüter saniyyədə 1 000 000 açar (təqribən $2^{20}$–yə bərabər) açar seçə bilir-sə, onda bütün $2^{56}$ açarların seçilməsinə $2^{36}$ saniyə yaxud iki ildən bir qədər çox vaxt tələb olunur, bu əlbətdəki düşmənə qəbul olunan deyil. Lakin personal kompüterlərdən başqa daha bahalı və cəld işləyən hesablama sistemləri mümkündür. Məsələn, əgər milyon prosessorları birləş-dirməklə paralel hesablamaları aparmaq imkanına malik olmaqla açarların seçilməsinə sərf olunan maksimum vaxt təqribən 18 saata qədər azalar. Bu vaxt bir o qədər çox deyil və kriptoanalitik bu bahalı texnikaya malik olarsa, onda DES-lə şifrlənmiş məlumatın şifrini aça bilər. Bununla bərabər DES sistemini az qiymətə malik olan verilənlərin şifrlənməsi üçün kiçik

və orta həcmli sistemlərdə istifadə etmək olar. Dövlət əhəmiyyətli yaxud böyük kommersiya qiymətli verilənlərin şifrlənməsi üçün DES sistemindən hal-hazırda istifadə etmək olmaz. 2001-ci ildə xüsusi elan olunmuş müsabiqə-dən sonra ABŞ-da belgiya mütəxəssislərinin işləyib hazırladıqları Reyndal şifri adını almış yeni AES (Advanced Encryption Stan-dard) standart qəbul olundu. Bu standartın öyərənilməsinə bir qədər sonra başılayaceyik. DES-in əsas parametrləri: blokun uzunluğu 64 bit, açarın uzunluğu 56 bit, raundun sayı-16-dır. DES iki budaqlı klassik Feystel şəbəkəsidir. Bu alqoritm bir neçə raund ərzində 64- bitli giriş verilənlər blokunu 64–bitli çıxış blokuna çevirir. DES standartı yerdəyişmə, əvəzləmə və qammalaşdırma şifrləmə metod-larının kombinasiya edilməsi əsasında qurulmuşdur. Şifrlənən verilənlər ikili şəkildə olmalıdır.

**Şifrləmə.** DES alqoritminin ümumi sxemi şək.2.8-də göstərilib. İlkin mətnin hər bir 64-bitli blokunun şifrlənmə prosesini üç mərhələyə bölmək olar [3,5]:

1. Verilənlər blokunun başlanqıc hazırlığı;
2. "Əsas dövrün" 16 raundları;
3. Verilənlər blokunun son emalı.

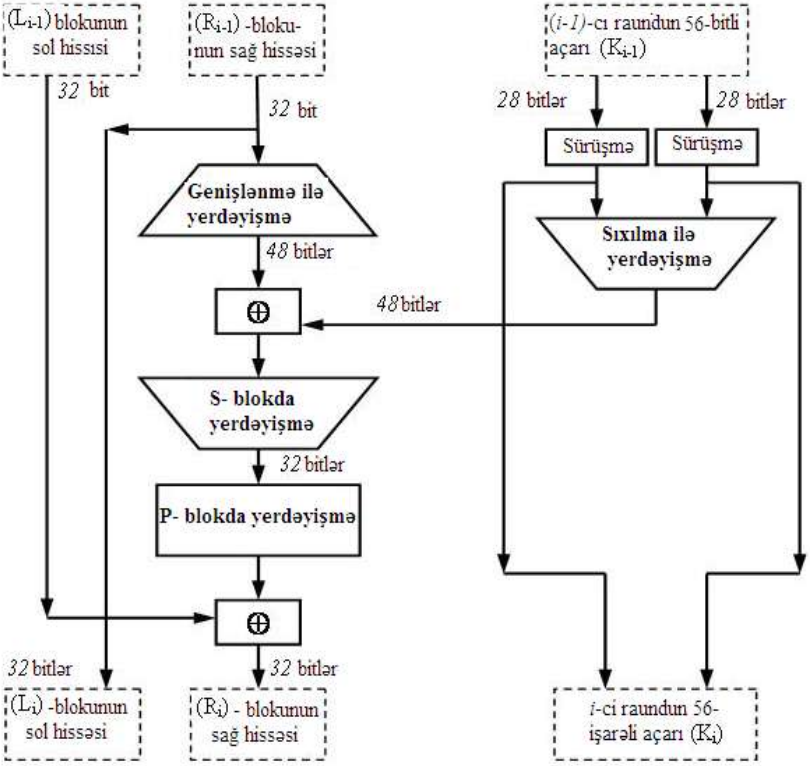



**Şək. 2.8.** DES-in ümumi sxemi

Birinci mərhələdə mətnin 64-bitli çıxış blokunun ilk yerdəyiş-məsi yerinə yetirilir, bu zaman ərzində bitlər müəyyən qaydada yenidən qaydaya salınır.

Növbəti (əsas) mərhələdə blok hər birinin ölçüsü 32 bit olan iki hissəyə (budağa) bölünür. Sağ budaq bəzi F funksiyasının istifadə olunması ilə və açarların xüsusi çevirmə alqoritmləri üzrə əsas şifr-ləmə açarından alınan tezlik açarına uyğun olaraq çevrilir. Sonra blokun sol və sağ budaqları arasında verilənlərin mübadiləsi həyata keçirilir. Bu, dövr 16 dəfə təkrar olunur.

Nəhayət, üçüncü mərhələdə əsas dövrün 16-cı addımından sonra alınan nəticənin yerdəyişməsi yerinə yetirilir. Bu yerdəyişmə ilkin yerdəyişməyə əksdir. DES standartı üzrə kriptoqrafik çevirmələrin bütün mərhələlərinə təfsilatı ilə baxaq. Birinci mərhələdə ilkin verilənlərin 64–işarəli bloku başlanqıc yerdəyişməyə məruz qalır. Başlanqıc yerdəyişmə zamanı verilənlər blokunun bitləri müəyyən şəkildə yenidən nizama salınır. Bu əməliyyat ilkin məlumata bir qədər xaotiklik verir və bununla da statistik metodla kriptoanalizin istifadə olunma imkanını azaldır. Eyni zamanda verilənlər bloku-nun başlanqıc yerdəyişməsilə 56 bitli açarın başlanqıc yerdəyişməsi yerinə yetirilir. Şəkil 2.8-dən görünür ki, raundların hər birində 48- bitli uyğun natamam $K_i$ açarı istifadə olunur. $K_i$ açarı başlanqıc açarın hər bir bitindən bir neçə dəfə istifadə etməsi müəyyən al-qoritm ilə alınır. Raundların hər birində 56-bitli açar 28-bitdən iba-rət iki hissəyə bölünür. Sonra bu hissələr raundun nömrəsindən asılı olaraq bir yaxud iki bit sola sürüşürlər. Sürüşmədən sonra müəyyən qaydada 56 bitdən 48-i seçilir. Bu zaman nəin ki, bitlər çoxluğu se-çilir, həm də onların nizamları dəyişdirilir. Bu əməliyyat "sıxılma ilə yerdəyişmə" adlanır. Onun nəticəsi 48 bit komplektidir. Orta he-sabla ilkin 56-bitli açarın hər bir biti 16 alt açardan 14-ündə istifadə olunur, bəzən də bitlərin hamısı eyni sayda istifadə olunmurlar. Da-ha sonra Feystel şəbəkəsi üzrə təşkil olunmuş və eyni cür olan 16 raundlardan ibarət çevirmənin əsas dövri yerinə yetirilir. Bu zaman hər bir raunddan (şək.2.9) sonra növbəti raunda emal olunan 64-bitli aralıq qiymət alınır [3,5].




**Şək.2.9.** DES-in bir raundunun strukturu

Hər bir aralıq qiymətin L və R ilə işarə edilən sol və sağ budaq- ları 32-bitli qiymət kimi ayrıca emal edilirlər. Əvvəlcə blokun sağ hissəsi $R_i$ yerdəyişmə plyus 16 işarə genişlənmə cədvəlindən istifa-də edərək 48 bitlərə dək genişləndirilir. Bu əməliyyat sağ yarının ölçüsünü XOR (2 modulu üzarə toplama) əməliyyatının yerinə yetirilməsi üçün açarın ölçüsü ilə uyğunlaşdırır. Bu əməliyyatın yerinə yetirilməsi hesabına nəticənin bütün bitlərinin ilkin verilən-lərin və açarın bitlərindən asılılığı tez artır (bu "sel effekti" adla-nır). Bu və ya digər alqoritmin istifadə olunması zamanı "sel ef-fekti" özünü nə qədər güclü göstərsə, bir o qədər yaxşıdır. 48-bitli qiymət üçün genişlənmə ilə yerdəyişmə yerinə yetrildikdən sonra 48- bitli $K_i$ açaraltı ilə XOR əməliyyatı yerinə

yetirilir. Sonra 48-bitli qiymət, nəticəsi 32- bit olan S yerdəyişmə blokunun girişinə verilir. Yerdəyişmə səkkiz yerdəyiş-mə blokunda yaxud səkkiz S-blokunda yerinə yetirilir. Bu əməliyyatın yerinə yetirilməsi zamanı 48 bit verilənlər 6-bitli 8 altbloka bölünürlər. Bu altblokların hər biri öz əvəzləmə cədvəli üzrə dörd bitlə əvəzlənir. S-bloku ilə yer-dəyişmə DES-in vacib mərhələlərindən biridir. Bu əməliyyat üçün əvəzləmə cədvəli mütəxəssislər tərəfindən elə layihələndirilib ki, maksimum təhlükəsizlik təmin olunsun. Bu mərhələnin yerinə yetirilməsi nəticəsində səkkiz 4-bitli blok alınır ki, onlar yenidən vahid 32-bitli qiymətə birləşirlər.

Daha sonra alınan 32-bitli qiymət istifadə olunan açardan asılı olmayan P yerdəyişməsinin köməyi ilə emal olunur. Yerdəyiş-mənin məqsədi bitlərin yenidən nizamlanma-sını elə maksimum qiymətə çatdırılmalıdır ki, şifrləmənin növbəti raundunda hər bir bit böyük ehtimalla digər S-blokunda emal olunsun. Nəhayət, yerdəyişmənin nəticəsi XOR əməliyyatının kö-məyi ilə 64-bitli ilkin verilənlər blokunun sol yarısı ilə birləşir. Sonra sol və sağ yarımlar yerlərini dəyişirlər və növbəti raund başlayır. Şifrləmənin 16 raundundan sonra nəticənin son yerdəyiş-məsi yerinə yetirilir.

Bu yerdəyişmə başlanqıc yerdəyişməyə əksdir. Bütün addımlar yerinə yetirildikdən sonra verilənlər bloku tam şifrlənmiş sayılır və növbəti ilkin məlumatın şifrlənməsinə keçmək olar. DES alqoritmi hal hazırda həm aparat və həm də proqram variantında həyata keçirirlir.

**Şifrin açılması.** Məlumdur ki, kriptoqrafik sistem məlumatı həm şifrlənməsinə və həm də onun şifrinin açılmasına imkan verməlidir. Gözləmək olardı ki, DES üzrə şifrin açılması prosesi olduqca dolaşdırılmışdır. Lakin işləyicilər standartın müxtəlif kom-ponentlərini elə seçiblər ki, məlumatın şifrlənməsi və onun şifrinin açılması üçün eyni bir alqoritmdən istifadə edilsin. Şifrin açılması zamanı alqoritmin girişinə şifrlənmiş mətn verilir. Bircə fərq natamam $K_i$ açarlarlarının əks qaydada istifadə olunmasıdır. $K_{16}$ birinci raundda, $K_1$ axırıncı raundda istifadə olunur. Şifrin açılması prosesinin axırıncı raundundan sonra çıxışın iki yarımın yerləri elə dəyişirlər ki, son yerdəyişmənin girişi $R_{16}$ və $L_{16}$ -dan tərtib edilsin. Bu dövrün çıxışı şifrlənməmiş mətndir.

### 2.13.2. İkiqat DES və “ortada görüş” hücumu

Hazırkı zamanda DES-in çatışmayan cəhəti açarın kiçik uzunlu-ğa malik olmasıdır. Kriptoanaliz prosesinin mürəkkəbləşdirilməsi-nin ən sadə üsulu müxtəlif açarlı eyni bir alqoritmin köməyi ilə ikiqat şifrlənmənin istifadə olunmasıdır. Əgər M-məlumatdırsa, $K_1$,

$K_2$-açardırsa, f- DES üzrə şifrləmə prosesidirsə, E isə şifrlənmiş məlumatdırsa, onda belə yazmaq olar [3,5] :

$$E=f(f(M,K_1),K_2),$$

yəni blok əvvəlcə bir açarla şifrlənir, sonra alınan şifrmətn ikinci açarla şifrlənir. Şifrin açılması əks qaydada aparılır ( $f^{-1}$-*DES* üzrə şifrin açılması) [3,5]:

$$E=f^{-1}(f^{-1}(E,K_2),K_1)$$

Bu halda açarın uzunluğu 56*2 = 112 bit olur, ona görə də blo-kun şifrləndiyi ikiqat açarı müəyyən etmək üçün ümumi halda $2^{112}$ cəhd tələb olunur. Bu problemi tədqiq edərək, amerika alimləri Merkl və Xellman açıq mətnə hücum aparılması üsulunu təklif et-dilər. Bu üsul əvvəlkindən fərqli olaraq $2^{112}$ deyil $2^{57}$ cəhd tələb edir. Bu hücum variantı “ortada görüş” hücumu adlanır. Bu hücum alqoritmin aşağıdakı xüsusiyyətinə əsaslanır. Yuxarıda göstərildiyi kimi bizə məlumdur [3,5]:

$$E=f(f(M,K_1),K_2)$$

burada M-məlumat, $K_1$, $K_2$-açar, f-DES üzrə şifrləmə, E-şifrlənmiş məlumat. Onda yaza bilərik [3,5]:

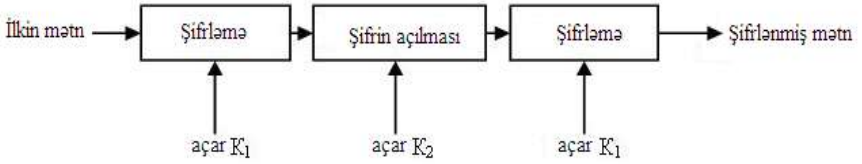
$$X=f(M,K_1)=f^{-1}(E,K_2).$$

Hücum aşağıdakından ibarətdir. Tələb olunur ki, hücumçu bir neçə cüt “şifrlənməmiş mətn ona uyğun şifrlənmiş mətni” (M, E) bilsin. Bu halda əvvəlcə $K_1$-in bütün mümkün olan $2^{56}$ qiyməti üçün M şifrlənir. Bu nəticə EHM-in yaddaşında yadda saxlanılır. Yadda saxlanılan verilənlər X qiymətinə görə nizama salınır. Növbəti ad-dım $K_2$-in bütün mümkün olan $2^{56}$ qiymətlərini istifadə etməklə E-in deşifrlənməsindən ibarətdir. Yerinə yetirilən hər bir deşifrləmə üçün birinci cədvəldə ona bərabər qiymət axtarılır. Əgər belə qiy-mət tapılırsa, onda hesab olunur ki, bu açarlar həqiqidir və onlar növbəti məlum “şifrlənməmiş mətn, şifrlənmiş mətn” cütə yoxlanı-lırlar.

Şifrləməyə mümkün olan maksimum cəhdi $2*2^n$ yaxud $2^{n+1}$-ə bərabər götürürük (burada n- şifrləmə mərhələlərinin hər birində olan açarların uzunluğu; DES üçün n= 56). Hücuma "Ortada görüş" adı ona görə verilib ki, bir tərəfdən şifrləmə, digər tərəfdən şifrin açılması yerinə yetirilir və ortada alınan nəticə müqaisə edilir. "Orada görüş" hücumunu həyata keçirmək üçün böyük yaddaş həcmi tələb olunur: $2^n$ blok ( burada n-açarın uzunluğudur). 56 bitli açar istifadə olunan DES üçün $2^{56}$ 64- işarəli yaddaş bloku tələb olunur. Bu $2^{62}$ bayt yaxud $2^{22}$ bayt təşkil edir. Belə yaddaş həcmini təsəvvür etmək çətindir, bundan başqa, belə böyük massivdə axtarış əməliyyatının aparılması üçün uyğun vaxt tələb olunur. Buna bax-mayaraq, ikiqat DES şifrləməsi praktiki olaraq heç vaxt istifadə olunmayıb.

### 2.13.3. Üçqat DES

"Ortada görüş" hücumunun əksinə olaraq iki açarlı ikiqat şifrləmənin istifadə olunması təklif olunmuşdur [3] (şək. 2.10).




**Şək.2.10.** İki açarlı üçqat DES şifrləməsi

Bu halda şifrləmə - şifrin açılması – şifrləmə ardıcıllığı yerinə yetirilir ( *EDE* – ingiliscə. *Encrypt – Decrypt -Encrypt* ). Bu prosesi simvolik olaraq aşağıdakı kimi yazmaq olar [3,5]:

$$E=f(f^{-1}(f(M,K_1),K_2),K_1)$$

Göndərici əvvəlcə birinci açarla məlumatı şifrələyir, sonra ikinci açarla onun şifrini açır və nəhayət son olaraq birinci açarla şifrələyir. Alıcı əvvəlcə birinci açarla şifrəni açır, sonra ikinci ilə şifrələyir və yenidən birinci ilə şifrəni açır. Bu zaman açarın uzunluğu iki dəfə artır və 112 bit təşkil edir. Etibarlı alternativ olaraq üç müxtəlif açar istifadə edən (hər mərhələnin öz açarı) üçqat şifrələmə təklif olunur. Bu metodda açarın ümumi uzunluğu (112+56=168 ) -ə dək artır, lakin bir neçə on

biti yadda saxlamaq problem olmur. Üçqat DES kifayət dərəcədə *DES-ə* məhşur alternativdir və ANSI X9.17 və ISO 8732 standartlarında açarların idarə olunmasında istifadə olunur. Bir sıra kriptoanalitiklər hələ daha çox etibarlı şifrləmə üçün üç yaxud beş açarlı beşqat DES-in istifadə olunmasını təklif edirlər.

### 2.13.4. Reyndal alqoritmi

Reyndal alqoritmini belçika mütəxəssisləri Joan Daemen (*Proton* World *International*) və Vincent Rijmen (Katholieke Universiteit Leuven) işləyib hazırlamışdılar [3,5]. Bu alqoritmlər ABŞ Milli Startlarlar və Texnika İnstitutunun (*NIST*) ANS (*Advanced Encryption Standard*) standartı üzrə keçirdiyi konkursda qalib gəlmişdir. Reyndal alqoritmini təsvir etmək çox mürəkkəb oldu-ğundan, burada onun yalnız qurulmasının əsas aspektlərinə və şifrin istifadə olunması xüsusiyyətlərinə baxaceyik. Bu alqoritm ilə tövsiyyə olunan Reyndal şifri/AES blokunun uzunluğu 128 bit, açarın uzunluğu 128,192 yaxud 256 bit və raundlarının sayı açarın uzunluğundan asılı olaraq 10, 12 yaxud 14 ilə xarakterizə olunur. Prinsipcə, Reyndal alqoritminin strukturunu 32-yə tam qalıqsız bölünən istənilən blokun və açarın uzunluğuna uyğunlaşdırmaq olar, eləcə də raundların sayını da dəyişdirmək mümkündür. DES və DÜİST(Dövlət Ümumitdifaq Standartı) 28147-89 alqoritmləri ilə tövsiyyə olunan şifrlərdən fərqli olaraq Reyndal alqoritminin əsasını Feystel şəbəkəsi deyil, xətti əvəzləmə adlanan əvəzləmə təşkil edir. Reyndal alqoritminin istifadə olunması ilə emal olunan verilənlər bloku, baytlar massivinə bölünür və şifrləmənin hər bir əməliyyatı bayt yönümlü hesab olunurlar. Hər bir raund qat adlanan müxtəlif bərpa olunan çevirmədən ibarərdir. Bu qatlar aşa-ğıdakılardan ibarətdir [3,5]:

1. Qeyri xətti qat. Bu qatda baytların əvəzlənməsi yerinə yetirilir. Bu qat optimal qeyrixətliliyə malik olan S-blokların vasitəsilə reallaşdırılır və differensial, xətti və digər müasir kriptoanaliz metodlarının istifadə olunması imkanlarının qarşısını alır.
2. Xətti qarışdırma təbəqəsi. Bu qat statistik əlaqələrin maskalan-ması üçün blok işarələrinin yüksək səviyyədə birləşməsini təmin

edir. Bu qatdakı bir düzbucaqlı baytlar massivində baytların sətirlərinin sürüşməsi və sütunlarının yerdəyişməsi yerinə yetirilir.

3. İki modulu üzrə toplama qatı. Bu qatda altaçarla şifrələmə bilavasitə yerinə yetirilir.

*Şifr* açarla toplama ilə başlayır və qurtarır. Bu, məlum mətnə hücum zamanı birinci raundun girişini bağlamağa və kriptoqrafik cəhətdən əhəmiyyətli nəticə olan axrıncı raundu əldə etməyə imkan verir. Alqoritmdə cədvəl hesablamaları geniş şəkildə istifadə olunur və bütün lazımi cədvəllər sabit olaraq verilir, yəni nə açardan, nə də məlumatdan asılı deyil.

Qeyd etmək lazımdır ki, Feystel şəbəkəsi üzərində qurulmuş şifrələmədən fərqli olaraq, bu alqoritmdə şifrələmə və deşifrələmə əməliyyatları başqa prinsipdə qurulurlar. Reyndal alqoritmi həm proqram və həm də aparat variantlarında yaxşı reallaşdırıla bilir. Reyndal alqoritmində yaddaşa ciddi tələblər qoyulmur, bu da onu məhdud resurslu sistemlər üçün əlverişli edir. Reyndal alqoritminin etibarlığı mütəxəssislər tərəfindən yüksək qiymətləndirilir.

**Blok alqoritmlərinin iş rejimləri.** Blok alqoritmləri müxtəlif məsələlərin yerinə yetirilməsi üçün istifadə edilə bilər. Ona görə də istənilən simmitrik blok alqoritmlərinin istifadəsi üçün bir neçə rejim müəyyən edilib. Rejimlərdən hər biri öz xüsusiyyətlərinə və istifadə olunma sahələrinə malikdirlər. Fərz edək ki, ilkin X veri-lənlər blokunu A açarı vasitəsilə Y şifrlənmiş bloka f çevirməsini yerinə yetirən hər hansı blok şifri mövcuddur, yəni [3,5]:

$$Y = f ( X, K ).$$

f çevirməsini yerinə yetirən hər hansı mümkün olan rejimləri nəzərdən keçirək.

Ən sadə rejim sadə bloklu əvəzləmə rejimidir. Mütəxəssislər bu rejimi ECB-Electronic CodeBook rejimi adlandırırlar ki, bu da azərbaycan dilinə "elektron kod kitabı" kimi tərcümə olunur. Bu rejimdə ilkin verilənlərin hər bir bloku eyni bir şifrləmə açarını isti-fadə etməklə digər yerdə qalan bloklardan asılı olmayaraq şifr-lənir. Əgər məlumatın uzunluğu uyğun alqoritmin blokunun uzun-luğundan böyükdürsə, onda

həmin məlumatın uzunluğu uyğun uzunluqlu $X_1$, $X_2$,..., X n bloklara bölünür, bu zaman son blok lazım olduğu təqdirdə sabit qiymətlərlə əlavə olunur. Hər bir blok, blok şifri ilə şifrlənir:

$$Y = f(X_i, K) \quad \text{bütün i bloku üçün 1-dən n-ə dək.}$$

İlkin Xi verilənlərinin bütün bloklarının şifrləmə nəticəsində aşağıdakı şifrələnmiş məlumat alınır [3,5]:

$$Y=Y1, Y2,..., Yn$$

Alınmış məlumatın deşifrələnməsi aşağıdakı qaydada yerinə yetirilir [3,5]:

$$X = f^{-1}(Y_i, K) \text{ bütün i üçün 1-dən n-ə dək.}$$

ESB anlayışından belə çıxır ki, məlumatın deşifrələnməsini şifr-mətnin bloklarını təsadüfi qaydada seçməklə yerinə yetirmək olar. Bu rejim çoxlu real hallar üçün əlverişlidir, xüsusilə təsadüfi daxil olan faylların emal edilməsi üçün. Məsələn, ESB rejimində hər bir yazılışın özündə ayrı bir verilənlər blokunu əks etdirməsi və digər bloklardan ayrılıqda şifrələnməsi şərtində şifrələnmiş verilənlər bazası ilə işləmək olar.

Bu rejimin çatışmayan cəhəti ilkin mətnin eyni bloklarının eyni şifrmətnə çevrilməsidir. Əksər real şifrəli verilənlər dəstləri təkrar-lanan elementlərə malikdirlər. Məlumat yüksək artıqlığa, təkrarla-nan başlıqlara yaxud uzun seriyalı sıfırlara yaxud boşluqlara malik ola bilər. Beləliklə, cinayətkar tezlik kriptoanalizi üçün verilənləri öz himayəsinə ala bilər. Baxılan rejimin daha ciddi problemi cina-yətkarın, alıcını aldatmaq məqsədilə şifrələnmiş məlumatı dəyişdirə bilməsi və əvəz etmə imkanına malik olmasıdır.

Ümumiyyətlə, bu rejim vahid qısa məlumatların göndərilməsi üçün tövsiyə olunur (məsələn, kriptoqrafik açarın). Verilənlərin bir neçə blokunun ötürülməsi zamanı ESB rejiminin çatışmayan cəhət-lərini aradan qaldırmaq üçün CBC (şifrin bloklarının zəncirlən-məsi) rejimini istifadə etmək olar.

CBC rejimində çevirmə aşağıdakı kimi yerinə yetirilir: açıq mət-nin hər bir bloku əvvəlki blokun şifrələnməsinin nəticəsi ilə 2 mo-dulu ilə toplanır. Beləliklə, əvvəlki blokun şifrələnməsinin nəticəsi növbəti

blokun şifrlənməsinə təsir göstərir. CBC rejimində şifrləmə əməliyyatı riyazi şəkildə aşağıdakı kimi yazılır [3,5]:

$$Y = f((X_i \oplus Y_{i-1}), K) \quad \text{bütün } i \text{ üçün 1-dən n-ə dək.}$$

Yəni açıq mətn üzərində növbəti blokun şifrələnməsindən və növbəti blokun şifrələnməsinin nəticəsindən qabaq "2 modulu üzrə toplama" əməliyyatı yerinə yetirilir. Açıq mətnin bloku şifrələn-dikdə, o əks əlaqəli registr qurğusunda saxlanılır. Şifrlənmədən qabaq verilənlərin növbəti bloku, o əks əlaqəli registrlə birlikdə "2 modulu üzrə toplama" əməliyyatına məruz qalır və yalnız bundan sonra şifrlənir. Alınan şifrələnmiş blok yenidən əks əlaqəli registr qurğusunda saxlanılır və məlumatın sonuna qədər giriş verilənlə-rinin növbəti blokunun şifrlənməsi üçün istifadə olunur. $Y_0$ bloku giriş verilənlərinin birinci blokunun şifrlənməsindən qabaq forma-laşmalıdır. O başlanğıc vektoru adlanır və giriş verilənlərinin birin-ci bloku ilə 2 modulu üzrə toplanmaq üçün istifadə olunur. Əks əlaqəli registr qurğusundan istifadə olunması nəticəsində hər bir blokun şifrlənməsi bütün əvvəlki bloklardan asılıdır. Şifrələnmiş məlumatı riyazi olaraq aşağıdakı kimi deşifrələmək olarq [3,5]:

$$Y = Y_{i-1} \oplus f^{-1}(Y_i, K) \quad \text{bütün } i \text{ üçün 1-dən n-ə dək.}$$

Şifrlənmiş mətnin bloku əvvəlcə əks əlaqəli registr qurğusunda saxlanılır, sonra adi qaydada deşifrələnir. Sonra növbəti blok deşif-rələnir və məlumatın sonuna qədər əks əlaqəli registrlə "2 modulu üzrə toplamaya" məruz qalır. Hətta bütün Xi ilkin verilənlərin bü-tün blokları eyni olsa belə, şifrələnmiş mətn Y-in müxtəlif blok-larından ibarət olacaq. Bu rejim ölçüsü blokun ölçüsündən artıq olan məlumatların şifrlənməsi zamanı daha geniş istifadə olunur. Bununla belə iki eyni məlumat eyni şifrlənəcək. Bunun qarşısını almaq üçün, hər şifrləmə zamanı müxtəlif başlatma vektorlarını istifadə etmək vacibdir. Başlatma vektorları həm də verilənlərin deşifrlənməsi üçün vacibdir, ona görə də onları şifrlənmiş məlu-matla birlikdə ya ünvançıya göndərmək lazımdır, ya da hər hansı bir yalançı təsadüfi başlatma vektorlarının birgə formalaşması barədə razılığa gəlinməlidir. CBC rejimində şifrələnmiş məlu-matın deşifrələnməsini yalnız ardıcıl olaraq ilk blokdan başlamaqla təmin etmək olar.

## 2.14. DÜİST28147-89 –üzrə verilənlərin kriptoqrafik çevrilməsi alqoritmi

### 2.14.1.Əsas məlumatlar

Bağlı açarlı blok şifrləmə alqoritmi DÜİST 28147-89 1989-cu ildə rusiyada standart halında qəbul olunmuşdur [3,5]. Bu standart verilənlərin kriptoqrafik mühafizəsi üçün tövsiyə olunmuşdur. Bu standartla təklif olunan şifr amerika DES-in prinsipində qurul-muşdur. Rusiya DES-in amerikanın 16 raundlu DES-ti ilə mü-qaisədə proqram reallaşdırılması üçün çox əlverişlidir, uzunluğu 256 bitə bərabər olan daha uzun açara və 32 şifrləmə raunduna malikdir. Beləliklə, rusiya standartının əsas parametrləri aşağıdakı-lardır: blokun ölçüsü 64 bit, açarın uzunluğu 256 bit və raundların sayı 32-dir. Alqoritm özündə Feyştel şəbəkəsini əks etdirir. Şifr-lənən verilənlər bloku iki eyni cür hissəyə ayrılır: sağ R və sol L-ə.

Sağ hissə raundun altaçarı ilə toplanır və bəzi alqoritmlərlə sol hissəni şifrələyir. Növbəti raund qabağı sol və sağ hissələr yerlərini dəyişirlər. Belə struktur şifrələmə və deşifrələmə üçün eyni bir alqoritmin istifadə olunmasına imkan verir.

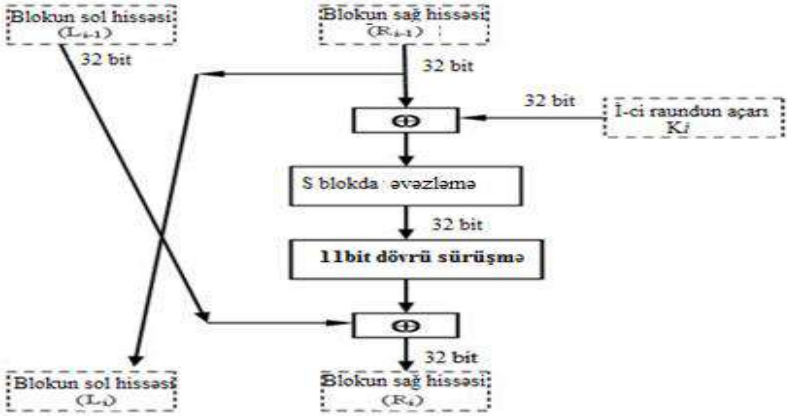
DES şifrləmə alqoritmində aşağıdakı əməliyyatlar istifadə olu-nur [3,5]:

- sözü $2^{32}$ modulu üzrə toplama;
- sözü göstərilən bit sayda dövri olaraq sola sürüşdürmək;
- 2 modulu ilə bit üzrə toplama;
- cədvəl üzrə əvəzləmə.

Bu standartın alqoritmlərinin müxtəlif addımlarında verilənlər müxtəlif şəkildə təsvir olunur və istifadə olunur. Bir sıra hallarda verilənlərin elementləri asılı olmayan bitlər massivi kimi, digər hallarda nişansız tam ədəd kimi, üçüncüdə isə bir neçə daha sadə elementlərdən ibarət olan mürəkkəb element kimi istifadə olunur.

### 2.14.2. DÜİST28147-89-un raundunun strukturası

Bu alqoritmin bir raundunun strukturası şək.2.11-də verilib.




Şifrlənən verilənlər bloku iki hissəyə bölünür, hansılar ki, sonra ayrıca nişansız 32-bitli tam ədəd kimi emal olunur. Əvvəlcə blokun sağ tərəfi və raundun altaçarı $2^{32}$ modulu üzrə toplanırlar. Sonra bloklar üzrə əvəzləmə həyata keçirilir.Əvvəlki addımda alınan 32-bitli qiymət (onu S-lə işarə edək) kodun səkkiz 4-bitli bloklar

massivi kimi təsvir olunur [3,5]:

$$S=(S_0,S_1,S_2,S_3,S_4,S_5,S_6,S_7).$$

Daha sonra səkkiz bloklardan hər birinin qiyməti yenisinə, hansı ki, əvəzləmə cədvəlindən aşağıdakı kimi seçilir: $S_i$ blokunun qiy-məti əvəzləmə cədvəlinin $S_i$-ci sətrinə (nömrələmə sırası "0"-dan başlamaqla) əvəzlənir. Başqa sözlə, blokun qiyməti üçün əvəz kimi əvəzlənən blokun nömrəsinə bərabər sətrin nömrəsilə və əvəzlənən blokun qiymətinə 4-bitli mənfi olmayan tam ədəd kimi sütunun nömrəsilə element seçilir.

Əvəzləmə cədvəlinin hər sətrində şəkildə təkrar olunmadan sərbəst qaydada "0"-dan 15-ə qədər ədəd yazılır [3,5]. Əvəzləmə cədvəlinin elementlərinin qiyməti "0"-dan 15-ə qədər götürülüb, çünki, əvəzləməyə məruz qalan 4 bitdə, 0-dan 15-ə dək diapazonda nişansız

tam ədəd yazıla bilər. Məsələn, S-blokun birinci sətri belə qiymətlərə malik ola bilər: 5, 8, 1, 13, 10, 3, 4, 2, 14, 15, 12, 7, 6, 0, 9, 11. Bu halda $S_0$ blokunun qiyməti (32-işarəli S ədədinin 4 kiçik biti) nömrəsi əvəzlənən blokun qiymətinə bərabər olan mövqedə duran ədədə əvəz olunur.

Əgər $S_0 = 0$, onda o 5-ə əvəz olunur, əgər $S_0 = 1$, onda o 8-ə əvəz olunur və s. Əvəzləmə yerinə yetirildikdən sonra bütün 4-bitli blok yenidən vahid 32-bitli sözə birləşir, hansı ki, sonra dövri olaraq 11 bit sola sürüşür. Nəhayət, bitlər üzrə "2 modulu toplama" əməliyyatının köməyi ilə nəticə sol yarımla birləşəcək, bunun nəticəsində yeni $R_i$ sağ yarım alınacaq. Yeni $L_i$ sol yarım çevrilən blokun kiçik hissəsinə bərabər götürülür: $L_i = R_{i-1}$. Çevrilən blokun alınan qiymətinə şifrləmə alqoritminin bir raundunun yerinə yetirilməsinin nəticəsi kimi baxılır.

### 2.14.3 Şifrləmə və şifrin açılması əməliyyatları

DÜİST 28147-89 blok şifridir, ona görə də verilənlərin çevril-məsi *baza dövri* adlanan bloklarla həyata keçirilir [3,5]. Baza dövri verilənlər bloku üçün əsas raundun çoxdəfəli yerinə yetirilməsidir. Hər bir raund da səkkiz mümkün olan 32-işarəli altaçarlardan biri istifadə olunur. Raundların altaçarlarının yaranması prosesinə baxaq. DÜİST 281 47-89-da bu proses çox sadədir, xüsusilə DES-lə müqaisədə. 256-bitli açar K səkkiz 32-bitli altaçarlara bölünür və $K_0$, $K_1$, $K_2$,$K_3$, $K_4$, $K_5$, $K_6$, $K_7$ ilə işarə olunurlar. Alqoritm 32 raunddan ibarətdir, ona görə də hər bir altaçar şifrləmə zamanı cədvəl 2.10-da verilən ardıcıllıqla dörd raundda istifadə olunur. Şifrin açılması eyni ilə şifrləmə alqoritmi ilə yerinə yetirilir. Yegənə fərq $K_i$ altaçarının istifadə qaydasındadır. Şifrin açılması zamanı altaçarlar cədvəl 2.11-də göstərildiyi kimi əks qaydada istifadə olunmalıdır.

**Cədvəl 2.10.** Şifrləmə zamanı altaçarların istifadə olunması ardıcıl-lığı

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Raund | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Altaçar | $K_0$ | $K_1$ | $K_2$ | $K_3$ | $K_4$ | $K_5$ | $K_6$ | $K_7$ |
| Raund | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Altaçar | $K_0$ | $K_1$ | $K_2$ | $K_3$ | $K_4$ | $K_5$ | $K_6$ | $K_7$ |
| Raund | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| Altaçar | $K_0$ | $K_1$ | $K_2$ | $K_3$ | $K_4$ | $K_5$ | $K_6$ | $K_7$ |
| Raund | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| Altaçar | $K_7$ | $K_6$ | $K_5$ | $K_4$ | $K_3$ | $K_2$ | $K_1$ | $K_0$ |

DÜİST28147-89 verilənlərin şifrlənməsinin aşağıdakı rejimləri mövcuddur: sadə əvəzləmə,qammallaşdırma, əks əlaqəli qamma-laş dırma və "imitasiya" adlanan bir əlavə rejim.

**Cədvəl 2.11.** Şifrin açılması zamanı altaçarların istifadə olunması qaydası

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Raund | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Altaçar | $K_7$ | $K_6$ | $K_5$ | $K_4$ | $K_3$ | $K_2$ | $K_1$ | $K_0$ |
| Raund | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Altaçar | $K_7$ | $K_6$ | $K_5$ | $K_4$ | $K_3$ | $K_2$ | $K_1$ | $K_0$ |
| Raund | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| Altaçar | $K_7$ | $K_6$ | $K_5$ | $K_4$ | $K_3$ | $K_2$ | $K_1$ | $K_0$ |
| Raund | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| Altaçar | $K_7$ | $K_6$ | $K_5$ | $K_4$ | $K_3$ | $K_2$ | $K_1$ | $K_0$ |

### 2.14.4. Şifrələmənin əsas rejimləri

Bu rejimlərdən hər birində verilənlər, üzərlərinə şifrələnən mas-siv ayrılan 64 bitlik bloklarla emal edilir, məhz ona görə də DÜİST 28147-89 blok şifrələrinə aiddir.

*Sadə əvəzləmə rejimi.* Bu rejimdə ilkin verilənlərin hər bir blo-ku eyni bir şifrələmə açarının istifadə olunması ilə digər bloklardan asılıolmayaraq şifrlənir. Bu rejiminin xüsusiyyəti ondan ibarətdir ki, ilkin mətnin eyni blokları eyni şifrmətnə çevrilir. Ona görə də DÜİST 28147-89 sadə şifrləmə rejimini yalnız açarların şifrlənməsi üçün istifadə etməyi tövsiyyə edir [3,5] .

*Qammalaşdırma rejimində* ölçüsü 8 baytdan az olan natamam blokun emal olunması imkanı var [3,5].

Qammalaşdırma və əks əlaqəli qammalaşdırma rejimləri ixtiyari ölçülü verilənlərin şifrlənməsi üşün istifadə oluna bilərlər.

Qammalaşdırma rejimində ilkin mətnin bitləri 2 modulu üzrə DÜİST 28147-89 –un şifrləmə alqoritmi ilə hasil edilən qamma ilə toplanır. Yəni DÜİST 28147-89 üzrə şifrləmə alqoritmi bu rejimdə 64-işarəli qamma bloklarının generatoru kimi istifadə edilir. Əks əlaqəli qammalaşdırma rejiminə oxşardır və ondan qammaların hasil olunması üsulu ilə fərqlənir.

DÜİST 28147-89–un şifrlənmiş massivində təhriflərin aşkar olunması üçün kriptoqrafik çevirmənin əlavə rejimi olan "imita-siya"nın hasil olunması nəzərdə tutulub. "İmitasiya" –bu açıq mətndən və informasiyanın məxfi açarından asılı olan nəzarət kombinasiyasıdır. "İmitasiya"nın istifadə olunmasında məqsəd informasiya massivində bütün təsadüfi və qəsdən törədilən dəyişik-likləri aşkar etməkdir. "İmitasiya"nın hasil olunması rejimində giriş mətn aşağıdakı şəkildə bloklarla emal olunur [3,5]:

$$Y = f((X_{ii-1}), K) \quad \text{bütün } i \text{ üçün 1-dən n-ə dək}$$

burada $f$ – DÜİST 28147-89 üzrə baza dövri; $X_{ii}$ – ilkin mətnin 64-işarəli bloku; K – açar.

"İmitasiya" kimi çıxışda alınan, onun adi 32 kiçik biti $Y_n$ blokun-bir hissəsi götürülür. Beləliklə, cinayətkar, şifrləmə açarına malik olmadan informasiyanın verilən açıq massivi üçün "İmitasiya"nı tapa bilməz, eləcə də verilən "İmitasiya"ya uyğun açıq verilənləri seçə bilməz.

### 2.14.5. DÜİST 28147-89 və DES şifrləmə alqoritmləri arasındakı fərq

Baxmayaraq ki, DÜİST28147-89-la verilən alqoritm kifayət dərəcədə çoxdan layihə olunub, ona etibarlıq üzrə kifayət dərə-cədə çox böyük ehtiyat var [3,5]. Bu hər şeydən əvvəl şifrləmə açarının böyük uzunluğu ilə bağlıdır. Məlum olduğu kimi, müasir kripto-sistem işləyənlər şifrlənmiş məlumatın məxfiliyi açarın məxfiliyi ilə təyin olunmalıdır prinsipinə tərəfdardırlar. Bu o deməkdir ki, əgər şifrləmə alqoritminin özü kriptoanalitikə məlumdursa, o buna baxmayaraq uyğun açara malik deyilsə məlumatın şifrinin açılması imkanına malik olmamalıdır. Klassik blok şifrinin hamısı, o cüm-lədən DES və DÜİST28147-89, bu prinsipə uyğundur və bu şəkildə layihələndirilib ki, onları daha effektiv üsullarla açmaq olmasın. Aşkardır ki, belə şifrlərin dayanıqlığı onlarda istifadə olunan açarın ölçüsü ilə təyin olunur. DÜİST 28147-89-da reallaşdırılan şifrdə 256-bitli açar istifadə olunur və açar məkanının həcmi $2^{256}$-dır . Hətta əgər, "DES və AES alqoritmlərində"olduğu kimi, güman edilir ki, şifrin sındır-ılmasına hesablama kompleksinin $10^{12}$ (bu təxminən $2^{40}$-ə bərabər-dir) seçim imkanı ilə bütün gücü sərf edilirsə, onda bütün $2^{256}$ açar-ların tam seçiminə saniyə vaxt tələb olunur (by vaxt milyard ildən çox vaxt edir). DES və DÜİST 28147-89 alqoritmlərinin arasında olan fərqə daha bir fərq əlavə etmək olar. DES-in əsas raunda ilkin məlumatın müntəzəm olmayan yerdəyişməsi istifadə olunur, DÜİST 28147-89-da isə sola 11-bitli dövri sürüşmə istifadə olunur. Axırıncı əmə-liyyat proqram reallaşdırılması üçün daha əlverişlidir. Lakin DES yerdəyişməsi sel effektini artırır. DÜİ ST 28147-89-da bir giriş bitinin dəyişməsinə 8 raund, DES-də isə 5 raund sərf olunur. DES-dən fərqli olaraq DÜİST 28147-89-da əvəzləmə cədvəli 512-bitli açara əlavədir.

## 2.15. Kriptoqrafik heş-funksiya

### 2.15.1. Heş- funksiya anlayışı

İxtiyari uzunluqlu sətr üçün bəzi tam ədədi yaxud qeyd olun-muş uzunluqlu digər sətri hesablayan funksiyaya riyazi heş-fun-

ksiya deyilir. Riyazi olaraq bunu aşağıdakı kimi yaza bilərik [3,5] :

$$H = H(M),$$

burada M – ilk məlumat, h –heş-funksiyasının qiyməti (başqa sözlə heş-kodu yaxud məlumat daycesti).

Heş–funksiyasının məqsədi ilk məlumatın xarakterik əlamətlə-rininin heş-funksiyasının qiymətinin təyin olunmasıdır. Bu funksi-ya adətən sabit ölçüyə malik olur, məsələn, 64 yaxud 128 bit. Heş-funksiyası daha sonralar hər-hansı bir məsələ üçün istifadə edilə bi-lər. Məsələn, heşləmə verilənlərinin müqaisə edilməsi üçün istifadə oluna bilər. Əgər iki verilənlərin heş-kodu müxtəlifdirsə, onda mas-sivlər müxtəlifdr, yox əgər onların heş-kodu eynidirsə çox ehtimal ki, massivlər də eynidirlər.

Ümumi halda ilkin verilənlər və heş-kod arasında birmənalı uy-ğunluq yoxdur, çünki, heş-funksiyasının qiymətlərinin sayı həmişə giriş verilənlərinin variantlarının sayına nisbətən azdır. Buna görə də, eyni heş-kodlarını verən giriş məlumatlar çoxluğu mövcuddur (belə vəziyyət *toqquşma* adlanır). Toqquşmanın yaranma ehtimalı heş-funksiyanın keyfiyyətinin qiymətlndirilməsində az rol oynamır. Heş- funksiya müasir kriptoqrafiyada geniş istifadə olunur.

Adi heş-funksiyası "2 modulu üzrə toplama" əməliyyatının isti-fadə olunması ilə aşağıdakı kimi yaradıla bilər: giriş sətrini alırıq, bütün baytları 2 modulu üzrə toplayırıq və nəticəni heş-funksiya-sının qiyməti kimi qaytarırırıq.

Heş-funksiyasının uzunluğunun qiyməti bu halda giriş məluma-tının ölçüsündən asılı olmayaraq 8 bit olur.

Məsələn, rəqəm şəklinə gətirilən çıxış məlumatı, aşağıdakı kimi-dir (onaltılıq formada) : 3E 54 A0 1F B4

Bu məlumatı ikili şəklə çevirək, baytları biri-birinin altında yazaq və bitləri hər sütunda 2 modulu üzrə toplayaq [3,5]:

0011 1110

0101 0100
1010 0000
0001 1111
1011 0100
---
0110 0101

Alınan nəticə ($0110\ 0101_{(2)}$ yaxud $65_{(16)}$ ) heş funksiyasının qiyməti olacaq. Lakin belə heş-funksiyasını kriptoqrafik məqsədlər üçün istifadə etmək olmaz, məsələn, elektron imzanı formalaş-dırmaq üçün, nəzarət cəminin qiymətini dəyişmədən imzalanan mə-lumatın məzmununu dəyişmək kifayətdir. Ona görə də baxılan heş-funksiyanın kriptoqrafiyada tətbiq olunması yaramır. Əgər bərabər qiymətli heş-funksiyalı iki başlanqıc verilənləri çətin yaratmaq olarsa, eləcə də əgər funksiyanın çıxışında girişdən açıqdan-açığa asılılıq yoxdursa, onda kriptoqrafiyada heş-funksiyası yaxşı hesab olunur. Kriptoqrafik heş-funksiyaya aşağıdakı tələblər qoyulur [3]:

- heş-funksiya istənilən ölçüdə məlumata tətbiq olunmalıdır;
- funksiyanın qiymətinin hesablanması kifayət dərəcədə tez yerinə yetirilməlidir;
- heş-funksiyasının məlum qiymətində əlverişli ilkin məlumatı M tapmaq çətin olmalıdır (praktiki olaraq mümkün olmamalıdır);
- məlum məlumat M zamanı, heş funksiyasının qiyməti ilkin mə-lumatda olan heş-funksiyanın qiymətinə bərabər olan digər məlumatın M tapılması çətin olmalıdır;
- hər-hansı bir eyni qiymətli heş-funksiyalı təsadüfi müxtəlif məlumat cütlüyünün tapılması çətin olmalıdır.

Bütün bu sadalanan tələbləri ödəyən heş-funksiyasını yaratmaq sadə məsələ deyil. Yada salmaq vacibdir ki, verilənlər funksiyanın girişinə ixtiyari ölçüdə daxil olur, heş-nəticə isə bu müxtəlif ölçülər üçün eyni alınmamalıdır.

Hal-hazırda praktikada heş-funksiyası halında məlumatı blok dalınca blok emal edən və $M_i$ giriş məlumatın hər bir bloku üçün aşağıda verilmiş asılılıq üzrə heş-qiymətini hesablayan funksiya istifadə olunur [3,5]:

$$h_i=H(M_i,h_{i-1}),$$

burada $h_{i-1}$ –əvvəlki giriş verilənləri üçüm heş-funksiyasının hesablanması zamanı alınan nəticədir.

Nəticədə heş-funksiyasının çıxışı $h_n$ giriş məlumatının bütün n blokunun funksiyasıdır.

### 2.15.2. Heş-funksiyanı formalaşdırmaq üçün şifrləmənin blok alqoritmindən istifadə edilməsi

Heş-funksiyası halında simmetrik şifrləmənin blok alqoritmini istifadə etmək olar. Əgər istifadə olunan blok alqoritmi dayanıq-lıdırsa, onda onun əsasında heş-funksiya da etibarlı olacaq. Heş-kodunun alınması üçün blok alqoritminin istifadə olunmasının sadə üsulu məlumatın CBC rejimində şifrlənməsidir. Bu halda məlu-mat, uzunluğu şifrləmə alqoritminin blokunun uzunluğuna bərabər olan bloklar ardıcıllığı şəklində təsvir olunur. Vacib olduğu zaman axırıncı blok lazımi uzunluqlu blokun alınması üçün sağdan sıfırlarla doldurulur. Heş-qiyməti mətnin axırıncı şifrlənmiş bloku olacaq. Şifrləmənin etibarlı blok alqoritminin istifadə olunması zamanı alınan heş-qiymət aşağıdakı xüsusiyyətlərə malik olacaq [3,5]:

- verilən açıq informasiya massivi üçün heş-qiymətinin hesablanması şifrləmə açarını bilmədən praktiki olaraq mümkün deyil;
- heş-funksiyasının verilən qiyməti üçün açıq verilənlərin seçilməsi şifrləmə açarını bilmədən praktiki olaraq qeyri mümkündür.

Bu şəkildə formalaşdırılan heş-qiyməti “imutasiya” yaxud autentifikator adlanır və məlumatın bütövlüyünü yoxlamaq üçün istifadə olunur. Beləliklə, “imitasiya”– bu, açıq verilənlərdən və informasiyanın məxfi açarından asılı olan nəzarət kombinasiyasıdır. “İmitasiya”nın istifadə olunmasının məqsədi informasiya masivin-də bütün təsadüfi yaxud qəsdən törədilən dəyişiklikləri aşkar etməkdir. Giriş məlumatının emalı zamanı heş-funksiyasının alınan qiyməti məlumata, məlumatın korreksiyalı olması məlum olduğu anda birləşir.

Alıcı alınan məlumatın “imitasiya”sının hesablanması və onu alınan heş-kodla müqaisə etmək yolu ilə məlumatın bütövlüyünü yoxlayır.

Belə təhlükəsiz üsullardan biri "imitasiya"nın göndəri-cinin bağlı açarı ilə şifrlənməsi, yəni imzanın yaradılması ola bilər. Əgər göndərici və alıcı simmetrik şifrləmənin ümumi açarına ma-likdirlərsə, onda alınan heş-kodun simmetrik şifrləmə alqoritmi ilə də şifrlənməsi mümkündür.

Heş-kodun hasil olunması üçün blok şifrinin istifadə olunma-sının digər mümkün olan üsullardan biri aşağıdakından ibarətdir. Çıxış məlumatı ardıcıl bloklarla emal olunr. Axırıncı blok vacib olduqda sıfırlarla doldurulur, bəzən axırıncı bloka ikili ədədlər şəklində məlumatın uzunluğunu əlavə edirlər. Hər bir mərhələdə açar halında məlumatın cari blokunu götürərək əvvəlki mərhələdə alınan heş-qiymətini şifrləyirik. Axırıncı alınan şifrlənmiş qiymət son heş-nəticə olacaq. Beləliklə, əgər məlumatın M adi şifrləmə sxemini K açarında blok şifrinin köməyi ilə biz E=f(M,K) kimi yazdıq, onda heş-kodunun h alınması sxemi yuxarıda yazılan alqo-ritm ilə aşağıdakı kimi yazmaq olar [3,5]:

$$h_i=f(h_{i-1},M)$$

Başlanqıc heş-kodunu $h_0$ hər hansı bir sabit ədəd götürürlər. Şifrləmə sadə əvəzləmə rejimində yerinə yetirilir. Göstərilən üsulu istifadə edən zaman blokun uzunluğu açarın uzunluğu ilə üst-üstə düşür və heş-qiymətinin ölçüsü blokun uzunluğu olacaq. Sadə əvəzləmə rejimində blok şifrinin istifadə olunmasının digər üsulu da mümkündür: məlumatın elementləri əvvəlki mərhələdə alınan heş-qiyməti ilə şifrlənir, yəni [3,5]:

$$h_i=f(M,h_{i-1})$$

Heş-funksiyasının formalaşdırılması üçün blok şifrlənməsinin bir sıra sxemləri də mümkündür. Fərz edək ki, $M_i$ – çıxış məlu-matının blokudur, $h_i$ – i-ci mərhələdə heş-funksiyasının qiymətidir, f-sadə əvəzləmə rejimində istifadə olunan şifrləmənin blok alqoritmidir, $\oplus$ - 2 modulu üzrə toplama əməliyyatıdır. Onda heş -funksiyasının formalaşmasının aşağıdakı sxemi mümkündür [3,5]:

$h_i=f(M_i h_{i-1})\oplus M_i$, $h_i=f(M_i,h_{i-1})\oplus h_{i-1}\oplus M_i h_i$,

$h_i=f(h_{i-1},M_i)\oplus h_{i,}$ $h_i=f(h_{i-1}\oplus M_i,M_i)\oplus h_i$

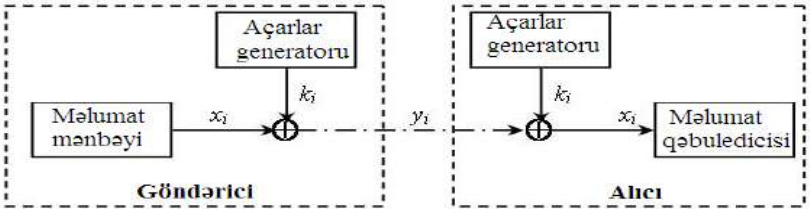
Bu sxemlərin hamısında formalaşdırılan heş-qiymətinin uzun-luğu şifrləmə zamanı blokun uzunluğuna bərabərdir. Blok alqorit-minin

əsasında layihələndirilən heş-funksiyasının çatışmayan cəhə-ti, nisbətən alçaq iş sürətidir. Vacib kriptodayanıqlığı giriş verilən-ləri üzərində kiçik sayda əməliyyatlar aparmaqla təmin etmək olar. Heşləmənin kriptodayanıqlıq baxımından müstəqil olaraq sıfırdan layihələndirilən daha sürətli alqoritmləri mövcuddur. Onlardan ən geniş yayılmışları MD5, SHA-1, SHA-2 və DÜİST P34.11-94 alqoritmləridir.

## 2.16. Arakəsilməz şifr və saxta təsadüfi ədədlər generatoru

### 2.16.1. Arakəsilməz şifr

Blok alqoritmi müəyyən uzunluqlu blokun şifrlənməsi üçündür. Lakin verilənlərin şifrlənməsi bloklarla deyil, işarələr üzrə də şifr-lənə bilir. Arakəsilməz şifr giriş məlumatının bir bit (yaxud bayt) üzrə çevrilməsi əməliyyatını həyata keçirir. Arakəsilməz şifrləmə alqoritmi məlumatın kifayət dərəcəli böyük uzunluqlu tam ədədlə-rə bölünməsini aradan qaldırır, buna görədə, o real zamanda işləyə bilər. Beləliklə, əgər işarələr seli verilirsə, onda hər bir işarə dərhal şifrlənər və ötürülə bilər. Tipik arakəsilməz şifrin işi şək.2.12-də təsvir edilib [3,5].




**Şək.2.12.** Arakəsilməz şifrin iş prinsipi

Açarlar generatoru qamma kimi istifadə olunan $k_i$ bitlər selini verir. Məlumat mənbəyi $k_i$ qamma ilə 2 modulu üzrə toplanan açıq mətnin $x_i$ bitlərini generasiya edir, nəticədə şifrlənmiş məlumat $y_i$ alınır [3,5]:

$$y_i = x_i \oplus k_i, \quad i = 1, 2, \ldots, n$$

$y_1, y_2, \ldots, y_n$ şifrmətndən $x_1, x_2, \ldots, x_n$ məlumatlarını bərpa etmək üçün şifrləmədə olduğu kimi eyni ilə $k_1, y_k, \ldots, k_n$ açar ardıcıllığını generasiya etmək vacibdir və şifrin açılması üçün olan ifadəni aşa-ğıdakı kimi yazmaq olar [3,5]:

$$x_i = y_i \oplus k_i, \quad i = 1, 2, \ldots, n$$

Adi çıxış məlumatı və açar ardıcıllığı özündə asılı olmayan bit selini əks etdirir. Beləliklə, şifrləyən (və şifri açan) çevirmələr bütün arakəsilməz şifrlər üçün eyni olduğu üçün, onlar açarlar generatorunun qurulması üsuluna görə fərqlənməlidirlər. Buradan aydın olur ki, sistemin təhlükəsizliyi açarlar seli generatorunun xüsusiyyətindən asılıdır [3,5]. Əgər açarlar seli generatoru yalnız sıfırlardan (yaxud sırf vahidlərdən) ibarət ardıcıllıq verirsə, onda şifrlənmiş məlumat dəqiqliklə çıxış bit selləri kimi olacaq (vahidli açarlar halında şifrlənmiş məlumat çıxış məlumatının çevrilməsi olacaq).

Əgər qamma halında səkkiz bitlə təsvir edilən bir işarə istifadə edilərsə, onda şifrlənmiş məlumat xaricən çıxış məlumatından fərqlənəcək və sistemin təhlükəsizliyi çox aşağı olacaq [3,5]. Bu halda bütün mətnin uzunluğu boyu açar kodunun çoxdəfəli təkrarlanması zama-nı onun statistik metodla şifrinin açılması təhlükəsi mövcud olur. Bunu qammalaşdırma metodu ilə qısa rəqəmli kodlu açarla bağlı sadə rəqəmli mətnin timsalında izah edək.

**Misal**. Fərz edək ki, çıxış məlumatı özündə ikili-onluq ədədi əks etdirir, yəni 0...9 onluq ədədlərinin ikili şəklə çevrilməsindən alınan hər tedradanı (dörd biti). Şifrlənmiş Y məlumatının 24 biti tutulub, yəni altı $Y_1$, $Y_2$, $Y_3$, $Y_4$, $Y_5$, $Y_6$ tedrada, məhz 1100 1101 1110 1111 0000 0001 işarələri. Məlumdur ki, şifrləmə açarı dörd bitdən ibarət idi, hansı ki, həm də özündə birmənalı onluq ədədləri əks etdirirlər, yəni çıxış məlumatının hər bir dörd bitini şifrləmək üçün $0 \le K \le 9$ eyni bir qiyməti istifadə olunub. Beləliklə, K açarı ilə $X_1$, $X_2$, $X_3$, $X_4$, $X_5$, $X_6$ ədədlərini şifrlənməsini tənlik sistemi şəklində aşağıdakı kimi yazmaq olar:

$X_1 \oplus K = 1100$, $X_2 \oplus K = 1101$, $X_3 \oplus K = 1110$,

$X_4 \oplus K = 1111$, $X_5 \oplus K = 0000$, $X_5 \oplus K = 0001$.

$X_i$ -nin 0-dan 9-a dək onluq ədədlər qiymətini aldığını nəzərə alsaq, məlum olmayan K-nı axtarmaq üçün 2 modulu üzrə cəmi 11 00 nəticəsinə gətirən bütün mümükün olan qiymətləri $X_1'$ və K-nı, hansıların ki, modul 2 üzrə cəmi 1100-a gətirir:

K = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001

$Y_1$ = 1100 1100 1100 1100 1100 1100 1100 1100 1100 1100

$X_1'$ = 1100 1101 1110 1111 1000 1001 1010 1011 0100 0101

Çıxış qiymətləri 0-dan 9-a dək olduğundan,baxılan qiymətlərdən açarın 0000, 0001, 0010, 0011, 0110, 0111 bu qiymətlərini çıxar-maq olar, çünki, onlarla toplama zamanı qiymət 9 ekvivalentindən çox qiymət alır. Belə qiymət açıq mətndə iştirak edə bilməzdilər. Beləliklə, analizin birinci mərhələsi mümkün olan açarların sayını ondan dördə endirməyə imkan verdi.

Məlum olmayan K-ın sonrakı axtarışı üçün bütün mümkün olan $X_2'$ qiymətini təyin edək və açarın qalan variantlarını tapaq, hansıların ki, modul 2 üzrə cəmi $Y_2 = 1101$ nəticəsinə gətirir:

$$K = 0100\ 0101\ 1000\ 1001$$
$$\underline{Y_2 = 1101\ 1101\ 1101\ 1101}$$
$$X_2' = 1001\ 1000\ 0101\ 0100$$

Görünür ki, bu mərhələ açarın qalan variantlarından heç birinin atılmasına imkan vermədi. Buna $Y_3$=1110 –ı istifadə etməklə cəhd edək:

$$K = 0100\ 0101\ 1000\ 1001$$
$$\underline{Y_3 = 1110\ 1110\ 1110\ 1110}$$
$$X_2' = 1010\ 1011\ 0110\ 0111$$

Bu mərhələni yerinə yetirdikdən sonra aydın olur ki, 0100 və 0101 qiymətləri açar ola bilməzlər. Açarın iki mümkün olan varian-tı qalır:

$$1000_{(2)}=8_{(10)} \text{ и } 1001_{(2)}=9_{(10)}.$$

Təəssüflər olsun ki bu metodika ilə sonrakı analiz, açarın alınan iki variantlarından hansının şifrləmə zamanı istifadə olunmasını birmənalı göstərməyə imkan vermir. Lakin onu uğur saymaq olar ki, mümkün olan açarların sayı 10-dan 2-yə dək azaldı. Bundan sonra tapılan iki açardan hər birini məlumatın deşifrlənməsi üçün yoxlamaq və alınan açıq məlumatın mənasını analiz etmək qalır. Real halda, ilkin məlumatın yalnız bir ədədlərdən deyil, həm də digər işarələrdən tərtib edilibsə, onda statistik analizdən istifadə olunması, məxfi verilənlər selini bağlayan açarın qısa uzunluğu za-manı açarı və ilkin məlumatı tez və dəqiq bərpa etməyə imkan verir.

### 2.16.2. Arasıkəsilməz şirləmə zamanı saxtatəsadüfi ədədlər genera-torlarının istifadə olunması prinsipi

Müasir informatika müxtəlif tətbiqlərdə saxta təsadüfi ədədləri riyazi statistika metodlarından və imitasiya modelləşdirilməsindən tutmuş kriptoqrafiyayadək geniş istifadə edir [3,5]. Bu zaman alınan nəticələrin keyfiyyəti istifadə olunana saxta təsadüfi ədədlər gene-ratorlarının (STƏG) keyfiyyətindən bilavasitə asılıdır. STƏG arası-kəsilməz şifrdə açarlar generatoru kimi istifadə oluna bilər. STƏG-in istifadə olunmasının məqsədi nisbətən kiçik uzunluqlu açara malik olmaqla "sonsuz"açar sözlərinin alınmasıdır. Saxta təsadüfi ədədlər generatorları təsadüfə oxşar bitlər ardıcıllığı yaradır [3,5]. Belə ardıcıllıqlar müəyyən qayda ilə hesablanır və təsadüfi olmurlar, ona görədə onlar həm verici, həm də qəbuledici tərəflərdə tam dəqiq-liklə yenidən hasil edilirlər. Şifrləmədə istifadə olunan açar işarələr ardıcıllığı, yalnız lazımınca uzun olmalıdırlar. Əgər açarlar genera-toru hər qoşulmada eyni bitlər ardıcıllığı yaradırsa, onda belə sistemi sındırmaq mümkündür. Buna görə də, açarlar seli genera-torunun çıxışı açarın funksiyası olmalıdır. Bu halda məlumatı şifrləmək və oxumaq yalnız şifrləmə zamanı istifadə olunan həmin açarın özünün istifadə olunması ilə olacaq. Saxta təsadüfi ədədlər generatorları kriptoqrafik məqsədlərlə istifadə olunmaq üçün aşağı-dakı xüsusiyyətlərə malik olmalıdır [3,5]:

1. Ardıcıllıq periodu çox böyük olmalıdır;
2. Yaradılan ardıcıllıq təsadüfdən "təxminən" fərqlənməməlidir;
3. Müxtəlif qiymətlərin yaranma ehtimallıqları dəqiq bərabər olmalıdır;
4. Qanuni alıcının məlumatın şifrəsini açа bilməsi üçün, açar bitləri selinin $k_i$ alınması zamanı bəzi məxfi açarı istifadə etmək və nəzərə almaq lazımdır, bununla belə $k_{i+1}$ ədədinin əvvəlki məlum element ardıcıllığı ilə hesablanması açarı bilmədən mürəkkəb məsələ olmalıdır.

Bu göstərilən xüsusiyyət zamanı saxta təsadüfi ədədlər ardıcıllı-ğı arası kəsilməz şirləmədə istifadə oluna bilər.

### 2.16.3. Xətti konqruyent saxta təsadüfi ədədlər generatoru

Saxta təsadüfi ədədlər generatorları müxtəlif alqoritmlərlə işlə-yə bilərlər. Sadə generatorlardan biri xətti konqruyent saxtatəsadüfi ədədlər generatorudur. Bu generator növbəti $k_i$ ədədləri hesablayan zaman aşağıdakı ifadəni istifadə edir [3,5]:

$$k_i=(a*k_{i-1}+b)\text{mod } c,$$

burada a, b, c-hər hansı sabit kəmiyyətdirlər, $k_{i-1}$ -əvvəlki saxtatəsadüfi ədəddir. $k_1$ –in alınması üçün $k_0$ başlanqıc qiymət verilir. **Misal:** a = 5, b = 3, c = 11 götürək və qoy $k_0$= 1 olsun.

Bu halda biz yuxarıda göstərilən ifadə ilə 0-dan 10-a dək qiy-mətləri ala bilərik (c=11 olduğu üçün). Ardıcıllığın bir neçə ele-mentlərini hesablayaq: 0-dan 10-a dək (c = 11olduqdq).

$$k_1 = (5 * 1 + 3) \text{ mod } 11 = 8;$$
$$k_2 = (5 * 8 + 3) \text{ mod } 11 = 10;$$
$$k_3 = (5 * 10 + 3) \text{ mod } 11 = 9;$$
$$k_4 = (5 * 9 + 3) \text{ mod } 11 = 4;$$
$$k_5 = (5 * 4 + 3) \text{ mod } 11 = 1.$$

Alınan qiymətlərin (8, 10, 9, 4, 1) təsadüfi qiymətlərə oxşaması görünür. Lakin növvbəti $k_6$ işarəsi yenidən 8 olacaq [3,5]:

$$k_6 = (5 * 1 + 3) \text{ mod } 11 = 8,$$

$k_7$ və $k_8$ içarələri uyğun olaraq 10 və 9 –a bərabər olacaq [3,5]:

$$k_7 = (5 * 8 + 3) \text{ mod } 11 = 10;$$
$$k_8= (5 * 10 + 3) \text{ mod } 11 = 9.$$

Belə çıxır ki, bizim saxtatəsadüfi ədədlər generatoru 8, 10, 9, 4, 1 periodik ədədləri yaradaraq təkrarlanır. Təəssüflər olsun ki, bu xüsusiyyət bütün xətti konqruyent genaratorlara aiddir. Əsas parametrləri a, b və c dəyişməklə periodun uzunluğuna və hasil edilmiş qiymətlərin özlərinə $k_i$ ilə təsir göstərmək olar. Məsələn, ümumi halda c-in artması periodun artmasına gətirib çıxarır. Əgər a, b və c parametrləri düzgün seçilibsə, onda generator, c-yə bərabər olan maksimum periodlu təsadüfi ədədlər hasil edəcək.

Proqram reallaşdırılması zamanı c-in qiyməti $2^{b-1}$ yaxud $2^b$ kimi təyin edilir, burada b-EHM sözünün uzunluğu, bitlərlə təyin olunur.

Xətti konqruyent saxtatəsadüfi ədədlər generatorunun üstün cə-həti onların sadəliyi və saxtatəsadüfi ədədlərin yüksək sürətə malik olmasıdır. Xətti konqruyent saxtatəsadüfi ədədlər generatorlar modelləşmə və riyazi statistikada tətbiq olunurlar, lakin kriptoqrafik məqsədlərdə onları istifadə olunmağa tövsiyə etmək olmaz, çünki, kriptoanaliz mütəxəssisləri saxtatəsadüfi ədədlər ardıcıllığını bir neçə qiymətlər üzrə bərpa etməyə öyrəniblər. Məsələn, fərz edək ki, düşmən $k_0$, $k_1$, $k_2$, $k_3$ qiymətlərini təyin edə bilər: $k_1 = (a*k_0+b) \bmod c$

$$k_2 = (a*k_1+b) \bmod c$$

$$k_3 = (a*k_2+b) \bmod c$$

Bu üç tənlikdən sistemi həll edib, a, b və c-ni tapa bilərik. Saxta təsadüfi ədədləri almaq üçün həm də kvadratik və kubik generatorlardan istifadə etmək təklif olunur [3,5]:

$$k_i=(a_1^2*k_{i-1}+a_2*k_{i-1}+b) \bmod c$$

$$k_i=(a_1^3*k_{i-1}+a_2^2*k_{i-1}+a_3*k_{i-1}+b) \bmod c$$

Lakin belə generatorlar da yuxarıda göstərilən səbəbə görə kriptoqrafik məqsədlər üçün yaramırlar.

## 2.17 Gecikmə ilə Fibonaççi metodu

Saxta təsadüfi ədədlərin alınması üçün digər metodlar da məlumdur. Bu metod saxta təsadüfi ədədlərin generasiya olunması metodlarından biridir. Bu metod saxta təsadüfi ədədlərin yüksək keyfiyyətini təmin etməyə imkan yaradır. Fibonaççi vericiləri real ədədli cəbri əməliyyatların yerinə yetirilməsi sürətinin, tam ədədli cəbri əməliyyatların aparılması sürəti ilə müqaisə olunan andan məhşurlaşmağa başladı, Fibonaççiyev vericiləri təbii olaraq real hesabda reallaşır. Gecikmə ilə Fibonaççi metodunun istifadə olunmasının müxtəlif sxemləri mövcuddur. Ən geniş yayılmış Fibonaççi vericiləriləri aşağıdakı rekurent ifadəyə əsaslanır [3]:

$$k_i = \begin{cases} k_{i-a} - k_{i-b}, & \text{əgər } k_{i-a} \geq k_{i-b} \\ k_{i-a} - k_{i-b} + 1, & \text{əgər } k_{i-a} < k_{i-b} \end{cases}$$

burada $k_i$ - [0,1] diapazonundan real ədəddir, a, b-müsbət tam ədəd-dir, generatorun parametridir. Fibonaççiyev vericilərinin işi üçün əvvəlki

max{a,b} təsadüfi ədədləri bilmək tələb olunur. Proqram reallaşdırılması zamanı bu təsadüfi ədədlərin saxlanılması üçün a və b parametrlərindən asılı olan bəzi yaddaş həcmi tələb olunur.

**Misal**. Birinci on ədədlərdən gecikmə ilə Fibonaççi metodu ilə generasiya olunan ardıcıllığı $k_5$- dən başlayaraq aşağıdakı başlanqıc veriənləri istifadə etməklə hesablayaq: a = 4, b = 1, $k_0$=0.1; $k_1$=0.7; $k_2$=0.3; $k_3$=0.9; $k_4$=0.5:

$k_5 = k_1 - k_4 = 0.7 - 0.5 = 0.2$; $k_6 = k_2 - k_5 = 0.3 - 0.2 = 0.1$;
$k_7 = k_3 - k_6 = 0.9 - 0.1 = 0.8$; $k_8 = k_4 - k_7 + 1 = 0.5 - 0.8 + 1 = 0.7$; $k_9 = k_5 - k_8 + 1 = 0.2 - 0.7 + 1 = 0.5$; $k_{10} = k_6 - k_9 + 1 = 0.1 - 0.5 + 1 = 0.6$;
$k_{11} = k_7 - k_{10} = 0.8 - 0.6 = 0.2$; $k_{12} = k_8 - k_{11} = 0.7 - 0.2 = 0.5$;
$k_{13} = k_9 - k_{12} + 1 = 0.5 - 0.5 + 1 = 1$; $k_{14} = k_{10} - k_{13} + 1 = 0.6 - 1 + 1 = 0.6$.

Görürük ki, hasil olunan ədəd ardıcıllığı təsadüf ardıcıllığa ox-şardır. Həqiqətən, tədqiqat təsdiqləyir ki, alınan təsadüfi ədədlər yaxşı statistik xüsusiyyətə malikdirlər. Fibonaççi metodu üzrə qurulan generatorlar üçün, tövsiyə olunan a və b parametrləri mövcuddur. Məsələn, tədqiqatçılar bu işarələri təklif edirlər [3]:

(a,b) = (55, 24), (17, 5) yaxud (97,33).

Alınan təsadüfi ədədlərin keyfiyyəti sabit a-ədədindən asılıdır. Bu ədəd nə qədər böyük olarsa, təsadüfi vektorların bərabərliyinin saxlanıldığı ölçü məkanının ölçüsü bir o qədər çox olar. Eyni za-manda a-sabit ədədinin artması ilə alqoritmi ilə istifadə olunan yad-daşın həcmi də artır. Nəticədə (a,b) = (17,5) sadə tətbiqlər üçün tövsiyə olunur. (a,b) = (55,24) ədədləri əksər kriptoqrafik alqorit-mlər üçün qənaətbəxş ədədlər almağa imkan verir. (a,b) = (97,33) qiymətləri çox keyfiyyətli təsadüfi ədədlər almağa imkan verir və yüksək ölçülü təsadüfi vektorlarla işləyən alqoritmlərdə istifadə olunurlar. Gecikmə ilə olan Fibonaççi metoduna əsaslanan saxtatə-sadüfi ədədlər generatoru kriptoqrafik məqsədlər üçün istifadə olunmuşdur. Bundan başqa, onlar riyazi və statistik hesablama-larda, eləcə də təsadüfi proseslərin modelləşdirilməsində istifadə olunurlar [3]. Gecikmə ilə olan Fibonaççi metoduna əsaslanan saxta-təsadüfi ədədlər generatoru məşhur Matlab sistemində istifadə olunmuşdur.

### 2.17.1.BBS alqoritmi əsasında saxtatəsadüfi ədədlər generatoru

Saxtatəsadüfi ədədlər hasil edən BBS (müəlliflərin familiyala-rından L. Blum, M. Blum, M. Shub) yaxud kvadratik qalıqlı adla-nan alqoritm geniş yayılmışdır. Kriptoqrafik məqsədlər üçün bu metod 1986-cı ildə təklif olunmuşdur. O aşağıdakılardan ibarətdir. Əvvəlcə iki böyük sadə ədədlər p və q seçilir. p və q ədədləri modul 4 üzrə 3-lə müqaisə olunmalıdır, yəni p və q ədədlərinin 4-ə bölün-məsi zamanı eyni 3 qalığı alınmalıdır. Daha sonra Blyuma tam ədədi adlanan M = p* q ədədi hesablanır. Sonra digər sadə M-lə qarşılıqlı olaraq təsadüfi tam x-ədədi seçilir. x0= $x^2$mod M-i hesa-blayaq. $x_0$ generatorun start ədədi adlanır. Generatorun hər bir n-addımında $x_{n+1}= x_n^2$ mod M hesablanır. n-ci addımın nəticəsi bir (adətən kiçik) bit $x_{n+1}$. ədədidir. Bəzən nəticə halında cütlük biti qəbul olunur, yəni elementin ikili təsvirində vahidlərin sayı götürü-lür. Əgər yazılışda vahidlərin sayı cütdürsə -bit cütlüyü "0"-a bərabər götürülür, əgər cüt deyilsə, onda bit cütlüyü 1 götürülür.

**Misal.** Verilir p = 11, q = 19 (inanırıq ki, 11 mod 4 = 3, 19 mod 4 = 3). Onda M = p* q = 11*19=209. Sadə M-lə qarşılıqlı x-ı seçirik M: tutaq ki, x = 3. Generatorun start ədədi $x_0$ -ı hesablayaq.

$x_0 = x^2 \bmod M = 3^2 \bmod 209 = 9 \bmod 209 = 9$.

BBS alqoritmi üzrə birinci on ədədi $x_i$ hesablayaq (cədvəl 2.12-yə bax). Təsadüfi bit halında ədədlərin ikili yazılışında $x_i$ kiçik biti götürəceyik [3]:

***Cədvəl. 2.12***

| | | |
|---|---|---|
| $x_1=9^2 \bmod 209= 81 \bmod 209= 81$ | Kiçik bit: | 1 |
| $x_2=81^2 \bmod 209= 6561 \bmod 209= 82$ | Kiçik bit : | 0 |
| $x_3=82^2 \bmod 209= 6724 \bmod 209= 36$ | Kiçik bit : | 0 |
| $x_4=36^2 \bmod 209= 1296 \bmod 209= 42$ | Kiçik bit: | 0 |
| $x_5=42^2 \bmod 209= 1764 \bmod 209= 92$ | Kiçik bit : | 0 |
| $x_6=92^2 \bmod 209= 8464 \bmod 209= 104$ | Kiçik bit : | 0 |
| $x_7=104^2 \bmod 209= 10816 \bmod 209= 157$ | Kiçik bit : | 1 |

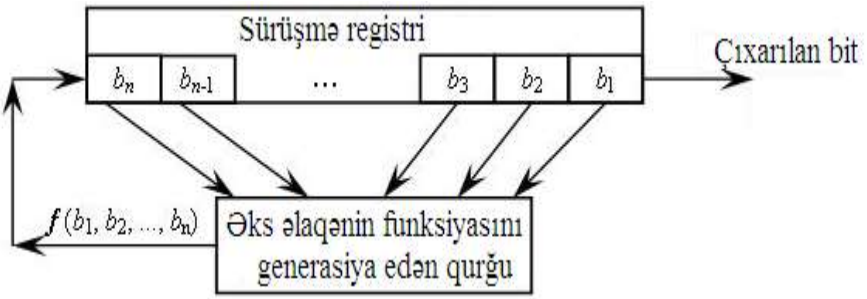
| | | |
|---|---|---|
| $x_8=157^2$ mod 209= 24649 mod 209= 196 | Kiçik bit : | 0 |
| $x_9=196^2$ mod 209= 38416 mod 209= 169 | Kiçik bit : | 1 |
| $x_{10}=169^2$ mod 209= 28561 mod 209= 137 | Kiçik bit : | 1 |

Praktiki olaraq bu metodun maraqlı xüsusiyyəti ardıcıllığın n-ci ədədini almaq üçün $x_i$ ədədinin bütün əvvəlki n ədədlərini hesab-lamaq lazım deyil. $x_n$ ədədini dərhal aşağıdakı ifadə üzrə almaq olar [3]:

$$x_n = x_0^{2^n mod((p-1)(q-1)} \text{ modM}$$

## 2.18. Əks əlaqəli sürüşmə registri əsasında saxta təsadüfi ədədlər generatoru

Kodlama və kriptoqrafiya nəzəriyyələrində əks ələqəli sürüşmə registrindən geniş istifadə olunur [3]. Bu növ registrdən saxtatəsadüfi ədədlər selinin alnması üçün istifadə oluna bilər. Əks əlaqəli sürüş-mə registri iki hissədən ibarətdir: n-bitli sürüşmə registrindən və əks əlaqəli qurğudan (şək.2.13).

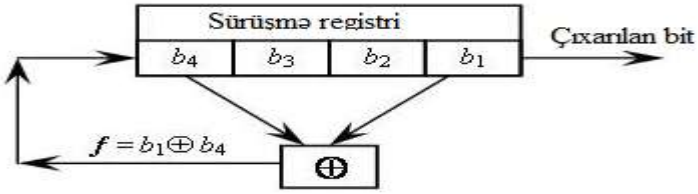



**Şək. 2.13**. Əks əlaqəli sürüşmə registri

Sürüşmə registrindən bitlərin çıxarılması yalnız bir-bir olur.Əgər növbəti biti çıxarmaq lazımdırsa, registrin bütün bitləri 1 işarə sağa sürüşdürülür. Bu zaman registrin girişinə soldan təzə bit daxil olur, hansı ki, əks əlaqəli qurğu ilə formalaşır və sürüşmə registrinin bütün yerdə qalan bitlərindən asılıdır. Bunun sayəsində registrin bitləri müəyyən qanun üzrə dəyişir, hansı ki, saxta təsadüfi ədədlə-rin (ST Ə) alınması

sxemini müəyyənləşdirir. Aşkardır ki, registrin bir neçə takt işindən sonra bitlər ardıcıllığı təkrar olunmağa başlayacaq. Alınan ardıcıllığın uzunluğu onun təkrar olunmasına başlayanadək sürüşmə registrinin *periodu* adlanır. Sürüşmə registri-nin istifadə olunması ilə arasıkəsilməz şifrlər praktikada kifayət dərəcədə çox istifadə olunmuşdurlar. Bu onunla bağl idi ki, onlar rəqəmli aparatların köməyi ilə çox yaxşı reallaşdırılırdılar.

Əks əlaqəli sürüşmə registrinin sadə növü əks əlaqəli xətti sür-üşmə registridir. Bu qurğuda əks əlaqə sadəcə olaraq registrin büt- ün (yaxud bir sıra) bitlərinin 2 modulu üzrə toplanması kimi real-laşdırılır. Əks əlaqədə iştirak edən bitlər, budaq ardıcıllığı yara-dırlar. Əks əlaqəli xətti sürüşmə registrləri yaxud onların modifi-kasiyaları kriptoqrafiyada tez-tez istifadə olunurlar. Əks əlaqəli sürüşmə registrinin necə işləməsinə aydınlıq gətirmək üçün 4-bitli xətti sürüşmə registrinin nümunəsini nəzərdən keçirək (şək.2.14).




**Şək.2.14.** 16-bitli xətti sürüşmə registrinin nümunəsi

Şəkildə təsvir olunmuş registrə başlanqıc qiyməti 1011-i yazaq. Registrin daxili vəziyyətinin ardıcıllığını 2.13-də təsvir olunmuş cədvəllə hesablayaq.

**Cədvəl 2.13.** Xətti sürüşmə registrinin iş ardıcıllığı

| Vəziyyərin nömrəsi | Registrin daxili vəziyyəti $b_4$, $b_3$, $b_2$, $b_1$ | Əks əlaqə funksiyasının hesablanmasının nəticəsi $f = b_1 \oplus b_4$ | Çıxarılan bit ( $b_1$ ) |
|---|---|---|---|
| 0 | 1 0 1 1 | 0 | 1 |
| 1 | 0 1 0 1 | 1 | 1 |

| | | | |
|---|---|---|---|
| 2 | 1 0 1 0 | 1 | 0 |
| 3 | 1 1 0 1 | 0 | 1 |
| 4 | 0 1 1 0 | 0 | 0 |
| 5 | 0 0 1 1 | 1 | 1 |
| 6 | 1 0 0 1 | 0 | 1 |
| 7 | 0 1 0 0 | 0 | 0 |
| 8 | 0 0 1 0 | 0 | 0 |

Cədvəldə registrin birinci doqquz vəziyyəti əks olunub. Hər bir addımda registrin bütün içindəkilər bir işarə sağa sürüşürlər. Bu zaman nəticə halında 1bit almaq olar. Solda boşalmış yerə əks əlaqə funksiyasının $f = b_1 \oplus b_4$ hesablanmasından alınan nəticəyə bərabər bit daxil olur. Generatorun çıxış saxta təsadüfi bit ardıcıllığı cədvəlin axırıncı sütununu yaradır (çıxarılan bitlər).

Ölçüsü n bit olan xətti sürüşmə registri $2^n$-1vəziyyətlərdən birin-də ola bilər. Ona görə də belə registr nəzəri olaraq maksimum $2^n$-1periodlu saxta təsadüfi ardıcıllıq hasil edə bilər. Əks əlaqəli xətti sürüşmə registri bitlərin maksimum periodlu dövri ardıcıllığını, yalnız budaq ardıcıllığı halında müəyyən bitlərin seçilməsi zamanı hasil edə bilər. Əks əlaqəli xətti sürüşmə registri əksər vaxtlar arasıkəsilməz verilənlərin şifrlənməsində istifadə olunmuşdur və indi də olunmaqdadır.

Saxta təsadüfi ədədlər generatorunun çatışmayan cəhəti proqram reallaşdırılmasının mürəkkəb olmasıdır [3]. Sürüşmə və bit əməliy-yatları elektron aparatlarda çox tez yerinə yetirilir, ona görə də müxtəlif ölkələrdə əks əlaqəli sürüşmə registrinin bazasında mikro-sxemlər və arası kəsilməz şifrləmə üçün qurğular buraxılır.

### 2.18.1. Saxta təsadüfi ədədlər almaq üçün OFB və CTR rejimlə-rindən istifadə olunması

İnformasiyanın arasıkısilməz şifrlənməsi üçün istənilən blok al-qoritmindən, məsələn, OFB və CTR rejimlərindən istifadə etməklə AES yaxud QOST 28147-89-dan istifadə etmək olar [3].

OFB rejiminin adı "*çıxış üzrə əks rabitə*" kimi tərcümə olunur. Fərz edək ki, veriliş üçün isrifadə olunan verilənlər bloku j bit-lərdən ibarətdir; adətən j=8 götürülür (yəni ötürülən verilənlərin porsiyası 1 baytdır). OFB rejimində blok şifri f, məxfi açar K və hər hansı bir $Y_0$ qiyməti əsasında j- bitli $z_1,z_2,...,z_k$ -dan ibarət j- bitli saxta təsadüfi ədədlər formalaşdırır, hansılar ki, sonralar mə-lumatın şifrələnməsi üçün qamma kimi istifadə oluna bilərlər. Şifr-ləmənin nəticəsi ilkin məlumatın növbəti blokunun şifrləmə əmə-liyyatının girişi sayılır. Şifrləmənin hər mərhələsində şifrlənmiş blok $Y_i$-dən j-kiçik bitlər seçilir. Beləliklə, saxta təsadüfi ədədlər almaq üçün aşağıdakı sxem istifadə olunur [3]:

$$Y_i=f(Y_{i-1},K),\ z_i=j \text{ kiçik bit } Y_i,\ 1<=i<=k$$

Əgər şifrin blokunun ölçüsü N-ə bərabərdirsə, onda j parametri 1-dən N-ə dək qiymət ala bilər. $Y_0$ qiymətini *təşşəbüsləndirici vek-tor* adlandırırlar. $z_i$ ədədlər ardıcıllığını $z_i$ işarələrdən ibarət ilkin verilənlərin şifrlənməsi üçün qamma kimi istifadə etmək olar [3]:

$$y_i = x_i \oplus z_i$$

Bunun nəticəsində $y_i$ işarələrinin şifrlənmiş seli alınır. $y_i$ qiymə-tinin açıq mətn – $x_i$ -dən asılı olmadığı üçün, onda hər dəfə, eyni bir K və $Y_0$ parametrlərini istifadə etməklə, biz eyni bir qamma $z_i$ ardıcıllığını alarıq. Ona görə də hər bir yeni məlumatın verilməsi üçün açarın K qiymətinin dəyişdirilməsi tövsiyə olunur. Bu rejim üçün məlumatın şifrinin açılması yalnız ardıcıllığın başlanqıcından ola bilər, çünki, əvvəlkiləri hesablamadan $z_i$ ardıcıllıqlı ixtiyari ele-ment almaq mümkün deyil. OFB rejiminin əsəs üstün cəhəti məlumat sellərinin alınması anında, onları tez şifrləmək yaxud şifrlərini açmaq üçün z ardıcıllığının əvvəlcədən formalaşdırılma-sıdır. Bu real zaman miqyasında verilənlərin emal olunması siste mləri üçün aktual ola bilər.

OFB rejiminin digər üstün cəhəti ondan ibarətdir ki, əgər veri-lənlərin ötürülməsi zamanı səhv baş verirsə o növbəti şifrlənmiş bloka keçmir, bununla da sonrakı blokların şifrinin açılması imkanı saxlanılır. Məsələn, küylü rabitə kanalı üzrə veriliş zamanı $y_i$ blo-kunda səhv bit yaranırsa, onda o yalnız bu blokun şifrinin açılma-sının qeyri mümkün olmasına və ilkin məlumatın $x_i$ bir blokunun alınmasına gətirib çıxarır.

*CTR rejiminin adı* "CounTeR"- "sayğac" sözündən yaranmışdır. Bu rejim OFB rejiminin modifikasiyasıdır. OFB-dən bir fərqi ondan ibarətdir ki,CTR rejimində şifrin əvvəlki çıxışı deyil, hər addımda 1vahid artan sayğac şifrlənir. Sayğacın ən birinci qiyməti hər hansı bir $Y_0$ təşəbbüsçü qiymətlə təyin olunur. Ümumi ifadə

aşağıdakı kimidir [3]:

$$Y_i = f(Y_{i-1}+1,K),\ Y_i \text{ - böyük biti } z_i=j$$

CTR rejiminin üstün cahəti z - ardıcıllığının istənilən elementi-nin bilavasitə hesablana bilməsidir. bu fakt $Y_i$ –in hər addımda 1 vahid artması ilə bağlıdır. Ona görədə, əgər bizə i- addımının nömrəsi məlumdursa, onda $Y_i$ qiymətini $Y_0$ və i-ni bilməklə bilavasitə aşağıdakı ifadə ilə hesablamaq olar [3]:

$$Y_i=f(Y_0+i,K),$$

Bu məlumatın istənilən fraqmentlərini biri-birindən asılı olma-yaraq şifrləməyə və deşifrləməyə imkan verir.

## 2.19. RC4-aqoritmi

Bu alqoritm saxta təsadüfi ədədlərin generasiya olunması alqo-ritmidir. Bu alqoritm R.Rivest tərəfindən dəyişən uzunluqlu açarlı informasiya seli üçün xüsusilə işlənmişdir. Bu alqoritmin köməyi ilə qurulan saxta təsadüfi ədədlər generatoru, bir qayda olaraq, blok şifrinə əsaslanan generatorlardan xeyli sürətlidir. RC4 alqoritmi arasıkəliməz şifrləmə zamanı açarların generasiya olunması üçün istifadə olunur [3,5]. Bu alqoritm çox sadədir. Onun iş prinsipinə baxaq.

Bu alqoritm RC4-blokun yaxud sözün ölçüsü ilə - n parametri ilə təyin olunan alqoritmlər sinfinə mənsubdur. Adətən n = 8, lakin digər ölçülərdə də istifadə etmək olar. Alqoritmin analizini sadələşdirmək üçün n=4 götürək. RC4-ün daxili vəziyyəti $2^n$ ölçülü söz massivindən və hər birinin ölçüsü 1 sözdən ibarət olan sayğac-dan ibarətdir [3,5]. Hər ikisi n=4 olan zaman, onları i və ji ilə işarə edək. Bütün hsablamalar $2^n$ modulu üzrə aparılır. Massiv, *S-boks* adlanan əvəzləmə cədvəli kimi istifadə olunur və daha sonra S ilə işarə olunacaq. Zamanın hər bir anında S cədvəli qarışdırılmış şəkildə bütün mümükün olan n-bitdən (bizim halda 4-bitli) ibarətdir. Qiy-mətlərin konkret yer dəyişməsi açarla

təyin olunur. Cədvəlin hər bir elementinin “0”-dan 15-ə dək aralığında qiymət aldığı üçün, onda onu iki cür yazmaq olar: ya ədəd kimi, yaxud da cədvəldə digər elementin nömrəsi kimi.

RC4 alqoritmi iki mərhələdən ibarətdir [3,5]. Birinci, hazırlıq mərhələsində S əvəzləmə cədvəlinin təşəbbüslənməsi yerinə yeti-rilir. Ikinci, əsas mərhələdə saxta təsadüfi ədədlər hesablanır.

S cədvəlinin necə təşəbbüslənməsinə baxaq. Əvvəlcə o “0”-dan 15-ə dək ədədlərlə ardıcıl olaraq doldurulur. Açar 4-bitli söz ardı-cıllığı şəklində təsvir olunur və onunla S kimi eyni ölçüyə malik olan digər K massivi doldurulur. Əgər açar lazım olandan qısadırsa, o lazım olan dəfə təkrarlanır. Sonra növbəti fəaliyyət başlayır (*al-qoritm 1*) [3,5]:

1. j = 0; i =0; 2. j = (j + $S_i$ + $K_i$) mod 16; 3.$S_i$ və $S_j$. –in yerlərini də-yişmək; 4. i = i +1; 5. əgər i <16, onda 2-ci bəndə keçək.

Bu alqoritmin yerinə yetirilməsi nəticəsində S əvəzləmə cəd-vəlinin ilk doldurulması aparılır, bununla belə qiymətlərin bu ilkin qarışdırılması məxfi açardan asılı olaraq yerinə yetirilir. S-cədvəli hazırlanandan sonra n-bitli sözləri hasil etmək olar. Bunu üçün i və j sayğaclarına başlanqıc “0” işarəsi verilir. Sonra hər yeni $z_i$ qiy-mətini aldıqdan sonra sonrakı fəaliyyət başlayır (alqortitm 2) [3,5]:

i = (i + 1) mod 16; j = (j + $S_i$) mod 16; $S_i$ $S_j$ -in yerlərini dəyişmək;

a = ($S_i$ + $S_j$) mod 16; $z_i$ = $S_a$.

Alınan 4- işarəli $z_i$ qiyməti, növbəti giriş verilənlər selinin 4-bitli blokunu şifrləmək üçün açar kimi istifadə edilə bilər. Məsələn, fərz edək ki, məxfi açar 4-bitli altı qiymətdən ibarətdir (onları onluq ədəd şəklində göstərək): 1,2,3,4,5,6.

RC 4 alqoritmi üzrə ədəd ardıcıllığını generasiya edək. S cəd-vəlini “0”-dan 15-ə dək ədəd ardıcıllığı ilə dolduraq.

***S cədvəli***

| Elementin nömrəsi | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Qiymətlər | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

Sonra K cədvəlini, ona lazımi sayda açar yazmaqla hazırlayaq:

***K-cədvəli [3]***

| Elementin nömrəsi | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Qiymətlər | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 1 | 2 | 3 | 4 |

Sonra S cədvəlinin içindəkiləri yazaq. Bunun üçün yuxarıda göstərilən alqoritm 1-i istifadə edəceyik. Yerinə yetirilən prosesi isti-qamət göstərən cədvələ yazaq (cədvəl 2.14). Hasablanma 16 modu-lu üzrə aparılır.

**Cədvəl 2.14.** RC4 alqoritmin hazırlıq mərhələsi (əvəzləmə cədvəlinin təşəbbüşlənməsi)

| Alqoritmin bəndlərinin nömrələri | Fəaliyyətin yerinə yetirilməsi (16 mod üzrə) | i-in yeni qiymət | j –in yeni qiyməti |
|---|---|---|---|
| 1 | j = 0; i =0 | 0 | |
| 2 | $j = j + S_i + K_i = 0 + 0 + 1 = 1$ | | 1 |
| 3 | $S_i$ və $S_j$yerlərinin dəyişdirilməsi , yəni$S_0$ və $S_1$ -in | | |
| 4 | i = i +1 | 1 | |
| 5 | i < 16, ona görə 2-ci bəndə (b.2) keşmək | | |
| 2 | $j = j + S_i + K_i = 1 + 0+ 2 = 3$ | | 3 |

| | | | |
|---|---|---|---|
| 3 | $S_i$ və $S_j$yerlərinin dəyişdirilməsi, $S_1$ və $S_3$-ün | | |
| 4 | i = i +1 | 2 | |
| 5 | i < 16, onagörə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (3 + 2 + 3) mod 16 = 8 | | 8 |
| 3 | $S_i$ və $S_j$ yerlərini dəyişdirmək, yəni $S_2$ və $S_8$ -in | | |
| 4 | i = i +1 | 3 | |
| 5 | i < 16, ona görə b. 2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (8 + 0 + 4) mod 16 = 12 | | 12 |
| 3 | $S_i$ və $S_j$ yerlərini dəyişmək, - yəni $S_3$ və $S_{12}$ in | | |
| 4 | i = i +1 | 4 | |
| 5 | i < 16, ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (12 + 4 + 5) mod 16 = 5 | | 5 |

| | | | |
|---|---|---|---|
| 3 | $S_i$ и $S_j$ yerlərini dəyişmək, yəni $S_4$ və $S_5$ -in | | |
| 4 | i = i +1 | 5 | |
| 5 | i < 16, ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (5 + 4 + 6) mod 16 = 15 | | 15 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , - yəni $S_5$ və $S_{15}$ -in | | |
| 4 | i = i +1 | 6 | |
| 5 | i < 16,ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (15 + 6 + 1) mod 16 = 6 | | 6 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_6$ və $S_6$ | | |
| 4 | i = i +1 | 7 | |
| 5 | i < 16, ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (6 + 7 + 2) mod 16 = 15 | | 15 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_7$ və $S_{15}$ | | |

| | | | |
|---|---|---|---|
| 4 | i = i +1 | 8 | |
| 5 | i < 16, a görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (15 + 2 + 3) mod 16 = 4 | | 4 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_8$ və $S_4$ | | |
| 4 | i = i +1 | 9 | |
| 5 | i < 16, ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (4 + 9 + 4) mod 16 = 1 | | 1 |
| 3 | Yelərini dəyişmək $S_i$ və $S_j$ , yəni $S_9$ və $S_1$ | | |
| 4 | i = i +1 | 10 | |
| 5 | i < 16, ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (1 + 10 + 5) mod 16 = 0 | | 0 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_{10}$ və $S_0$ | | |
| 4 | i = i +1 | 11 | |
| 5 | i < 16, ona görə b.2-yə keçmək | | |

| | | | |
|---|---|---|---|
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (0 + 11 + 6) mod 16 = 1 | | 1 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_{11}$ və $S_1$ | | |
| 4 | i = i +1 | 12 | |
| 5 | i < 16, ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (1 + 0 + 1) mod 16 = 2 | | 2 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_{12}$ və $S_2$ | | |
| 4 | i = i +1 | 13 | |
| 5 | i < 16, ona görə d.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (2 + 13 + 2) mod 16 = 1 | | 1 |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni S13və S1 | | |
| 4 | i = i +1 | 14 | |
| 5 | i < 16,ona görə b.2-yə keçmək | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (1 + 14 + 3) mod 16 = 2 | | 2 |

| | | | | |
|---|---|---|---|---|
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_{14}$ və $S_2$ | | | |
| 4 | i = i +1 | 15 | | |
| 5 | i < 16 , ona görə b.2-yə keçmək | | | |
| 2 | j = (j + $S_i$ + $K_i$ ) mod 16= (2 + 7 + 4) mod 16 = 13 | | 13 | |
| 3 | Yerlərini dəyişmək $S_i$ və $S_j$ , yəni $S_{15}$ və $S_{13}$ | | | |
| 4 | i = i +1 | 16 | | |
| 5 | i < 16 – yanlış, ona görə qurtarmaq | | | |

Alqoritmi 1-i yetirdikdən sonra biz əsas mərhələ üçün cədvəl S başlanılıb və hazırlanacaq

| Elementin nömrəsi | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Qiymətlər | 10 | 13 | 14 | 12 | 2 | 15 | 6 | 4 | 5 | 3 | 1 | 9 | 8 | 7 | 0 | 11 |

S cədvəli hazırlandıqdan sonra, 4-bitli təsadüfi sözün generasi-yasına başlamaq olar. Alqoritm 2-ni istifadə etməklə birinci 5 saxta təsadüfi ədədlər ardıcıllığını hesablayaq. Ədədlər ardıcıllığının hes-ablamasının nəticələrini birinci beş qiymət aşağıdakı kimi olanda: 2, 4, 10, 15, 3 cədvəl 2.15-ə yazaq.

**Cədvəl 2.15.** RC alqoritminin əsas mərhələsi (saxta təsadüfi ardıcıllığın elementlərinin hesablanması)

| | İşin yerinə yetirilməsi (16 modulu üzrə) | i-in yeni qiyməti | j-in yeni qiyməi | A-ın yeni qiyməti |
|---|---|---|---|---|
| $z_1$ -in hesablanması | 1. i = (i + 1) =0+1=1 | 1 | | |
| | 2. j = (j + $S_i$) mod 16=(0+13) mod 16=13 | | 13 | |
| | 3. yerlərini dəyişmək $S_1$ və$S_{13}$ | | | |
| | 4. a = ($S_i$ + $S_j$ )mod 16=(7+13)mod 16=4 | | | 4 |
| | 5. $z_1$ = $S_4$ =2 | | | |
| $z_2$ -hesablanması | 1. i = (i + 1) =1+1=2 | 2 | | |
| | 2. j = (j + $S_i$) mod 16=(13+14) mod 16=11 | | 11 | |
| | 3. yerlərini dəyişmək $S_2$ və $S_{11}$ | | | |
| | 4. a = ($S_i$ + $S_j$ )mod 16=(9+14)mod 16=7 | | | 7 |
| | 5. $z_2$ = $S_7$=4 | | | |
| $z_3$-ün hesablanması | 1. i = (i + 1) =2+1=3 | 3 | | |
| | 2. j = (j + $S_i$) mod 16=(11+12) mod 16=7 | | 7 | |

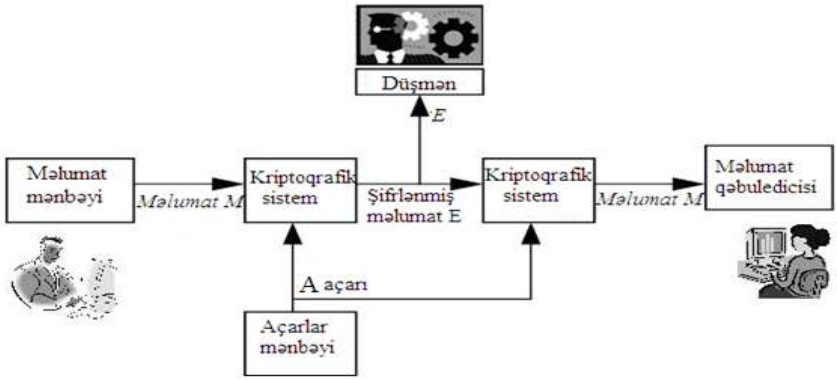
| | | | | |
|---|---|---|---|---|
| | 3. yerlərini dəyişmək $S_3$ və $S_7$ | | | |
| | 4. $a = (S_i + S_j) \bmod 16 = (4+12) \bmod 16 = 0$ | | | 0 |
| | 5. $z_3 = S_0 = 10$ | | | |
| $z_4$ -ün hesablanması | 1. $i = (i + 1) = 3+1 = 4$ | 4 | | |
| | 2. $j = (j + S_i) \bmod 16 = (7+2) \bmod 16 = 9$ | | 9 | |
| | 3. yerlərini dəyişmək $S_4$ və $S_9$ | | | |
| | 4. $a = (S_i + S_j) \bmod 16 = (3+2) \bmod 16 = 5$ | | | 5 |
| | 5. $z_4 = S_5 = 15$ | | | |
| $z_5$ -in hesablanması | 1. $i = (i + 1) = 4+1 = 5$ | 5 | | |
| | 2. $j = (j + S_i) \bmod 16 = (9+15) \bmod 16 = 8$ | | 8 | |
| | 3. yerlərini dəyişmək $S_5$ və $S_8$ | | | |
| | 4. $a = (S_i + S_j) \bmod 16 = (5+15) \bmod 16 = 4$ | | | 4 |
| | 5. $z_5 = S_4 = 3$ | | | |

Vacib olduqda böyük sayda təsadüfi ədədlər almaq üçün hesablamanı davam etdirmək lazımdır. n=4 olan zaman generasiya

olunan ədədlər 4 bit ölçüyə malik olacaqlar, yəni 0-dan 15-ə dək.Baxılan misalda alqoritm sözünün yaxud blokunun ölçüsü 4-ə bərabər götürülmüşdür. Bu qymətin yerinə başqa qiymət də götürmək olar, məsələn 8 yaxud 16. n = 8 olan halda əvəzləmə cədvəli S $2^8$ = 256, əvəzləmə cədvəlinin elementləri isə 0-dan 255-ə dək olmalıdır. i və j sayğaclarının ölçüsü də 8-bitə dək dəyiş-məlidir (maksimum qiymət - 255-dir). Bundan başqa, n=8 olduqda bütün hesablamaları 256 modulu üzrə aparmaq vacibdir. Alqo-ritmidə analoji dəyişikliyi n-in digər qiymətlərinə də aparmaq vacibdir.

## 2.20. Məxfi açarın idarə olunması

Belə sistemin struktur sxemi şək.2.15-də göstərilib. Özündə məlumat mənbəyini əks etdirən göndərici və alıcı (şifrlənmiş məlumatın




**Şək.2.15**. Simmetrik şifrləməni istifadə edən məxfi sisemin ümumi strukturası

qəbuledicisi) qəbul oluna bilən şifrin və açarın seçilməsi haq-qında razılığa gəlirlər [3,4]. Sonra göndərici öz seçilmiş məlumatını şifr-ləmə alqoritmini istifadə etməklə şifrələyir və alınan şifrəmətni (açıq) rabitə kanalı üzrə alıcıya göndərir. Alıcı açarı istifadə etməklə onun şifrini açır. Düşmən, hər şeydən əvvəl, məlumatın açıq kanal ilə verildiyi üçün şifrlənmiş məlumatı tuta bilər. Bu halda düşmənin kriptoanalitiki şifromətni açmağa cəhd edə bilər. Güman edəceyik ki, göndərici və alıcı

kifayət dərəcədə etibarlı şifr istifadə edirlər və onun şifrinin açılması ehtimalı yüksək deyil.

Bu halda şifrləmənin təhlükəsizliyi açarın təhlükəsizliyindən asılıdır. Açarın açılması ötürülən verilənlərin şifrinin açılmasına gətirib çıxarır. Beləliklə, açar verilənlərin bağlanmasınadək məxfilikdə saxlanılmalıdır. Ona görə də açarların ilkin paylanması üçün etibarlı rabitə kanalı vacibdir. Beləliklə, məxfi danışanlara açarın verilməsi kanalının etibarlığı prinsipial məsələlərdən biridir. Açarların ilkin paylanma-sının ən etibarlı üsulu verilənlərin ötürülməsi şəbəkəsinin abonent-lərinin şəxsi görüşü zamanı açar mübadiləsinin həyata keçirilmə-sidir. Açarların etibarlı çatdırılması üçün həm də xüsusi kuryerdən istifadə etmək olar. Əgər məxfi məlumatın mübadiləsi zamanı kiçik sayda tərəflərin iştirakı planlaşdırılırsa, məsələn, iki yaxud üç, onda hər iki üsulu tam yol veriləndir. Əgər qarşılıqlı əlaqədə olan abo-nentlərin sayı çoxdursa, onda açarların paylanması məsələsi problemə çevrilir. Məxfi açarın istifadə olunması zamanı digər çətinliklərdə mövcuddur. Məsələn, açarlar vaxtaşırı dəyişdirilmə-lidir. Bu, onunla bağlıdır ki, çox istifadə olunan açarın açılması ehtimalının böyük olması ilə bağlıdır [3,4]. Açar nə qədər çox istifadə olunursa, onun açılma-sından yaranan itgi də bir o qədər böyük olur, çünki, açarın alınması zamanı cinayətkar daha çox məlumatı açа bilər [3,4]. Hətta açar açılmayacaqsa, kriptoanaliz düşmənə, eyni bir açarla şifrlənmiş öz ixtiyarında olan lazımi sayda məlumatları ötürür. Şifrlənmiş məlumatın hər bir mübadilə seansı üçün *seans açarı* adlanan nadir açardan istifadə olunması optimal sayılr [3,4]. Lakin böyük telekommunikasiya şəbəkəsi üçün bu qədər sayda açarı hardan almaq və onları necə paylama?

Beləliklə, çoxlu sayda qarşılıqlı əlaqəli tərəflərin olması zamanı əvvəlcədən çoxlu sayda açarların göndərilməsi, eləcə də onların sonrakı saxlanılması və vacib olduqda dəyişdirilmə tələb olunur.

Fərz edək ki, lokal şəbəkədə 100 istifadəçi var. Bu istifadəçilər biri-birləri ilə "biri-hər biri" prinsipində məxfi verilənləri mübadilə etmək istəyirlər. Bu halda hər bir cüt abonent üçün məlumatın şifrlənməsi üçün özünün məxfi açarı olmalıdır. Yüz abonent üçün 100x99/2=4950 cüt açar tərtib etmək olar, ona görə də, verilənlərin ötürülməsi sistemində

4950 müxtəlif məxfi açar istifadə olunacaq. Bütün bu açarlar generasiya olunmalıdır və etibarlı şəkildə paylan-malıdır. Bundan başqa, yüz istifadəçilərin hər biri 99 müxtəlif açarı yadda saxlamalıdır. Əgər mübadilədə 100 deyil, 1000 adam iştirak edirsə, onda açarların paylanması məsələsi daha da mürəkkəbləşir.

Göstərilən çətinliklərlə əlaqadar praktikada açarların paylan-masının xüsusi avtomatlaşdırılmış idarə sistemləri istifadə olunur [3,4]. Belə sistemlər açarların generasiya olunmasına, onların saxlanılmasına və arxivləşirilməsinə, itirilmiş açarların bərpa olunmasına, dəyişrilməsinə yaxud köhnə və lazımsız açarları istismardan çıxarmağa imkan yaradır. Açarların idarə olunması sisteminin vacib hissəsi açarların paylanma mərkəzidir (Key Distribution Center-KD C). Bu mərkəzin fuksiyası açarların generasiyası, paylanması və ötürülməsidir. Mütəxəssislər xüsusi prosedurlar (yaxud protokol-lar) işləyib hazırlamışlar ki, onların vasitəsilə açarların paylanması mərkəzi istifadəçilərə, müstəqil rabitə seansı aparmaq üçün açar (*seans açarı*) çatdırır. Təssüflər olsun ki, simmetrik şifrləmə protokollarının hamısı bu və ya digər çatışmayan cəhətlərə malikdirlər.

Mümkün olan açarların mübadiləsi protokollarından birini nəzərdən keçirək.

Fərz edək ki, verilənlərin mübadiləsi şəbəkəsinin istifadəçilər cəmiyyətinə qoşulan zaman açarların paylanması mərkəzilə bütün yeni abonentlərə fərdi məxfi açar verilir. Baxaq görək açarların paylanması mərkəzilə (mərkəz) şəbəkənin iki abonenti arasında seansın aparılması üçün məxfi açarların paylanması proseduru necə görünür [3,4]:

1. Abonent A mərkəzinə müraciət edir və B abonenti ilə rabitə üçün seans açarı istəyir. Mərkəzdə təsadüfi seans açarı yaradılır. Bu seans açarının iki surəti şifrələnir-şifrlənmiş açarlardan biri A abonenti üçün, digəri isə B abonenti üçün. Sonra şifrlənmiş hər iki açar mərkəzdən A abonentinə göndərilir.
2. A abonenti öz seans açarının surətinin şifrəsini açır və ikinci şifrlənmiş surətini B abonentinə göndərir.
3. B abonenti də özünün şifrlənmiş seans açarının surətinin şifrini açır.

4. A və B abonentləri alınan sean açarlarını məxfi infomasiya mübadiləsi üçün istifadə edirlər.

Bu protokol olduqca sədədir və verilənlərin ötürülməsi proqramı ilə avtomatlaşdırıla bilər. Lakin seans açarlarının paylanmasının bu prosedurası bir sıra aşkar çatışmayan cəhətlərə malikdir.

Birinci çatışmayan cəhəti odur ki, mərkəz bütün mübadilələrdə iştirak edir. Bu zaman mərkəzdə baş verən nasazlıq bütün sistemin işini poza bilər. İkinci çatışmayan cəhət odur ki, açarların pay-lanması mərkəzi hərhansı bir şəkildə şəbəkənin bütün abonentlə-rinin məxfi açarlarını saxlamalıdır. Əgər cinayətkar sistemin istifa-dəçilərinin məxfi açarına daxilolma imkanına malik olarsa (sistemi "sındırar" administratoru bəxşiş və s. ilə ələ ala bilər), onda o verilən bütün məlumatı oxuyar və dəyişdirə bilər. Nəhayət, istifa-dəçinin şəbəkəya daxil olması zamanı məxfi açarın ilk başlanqıc paylanması problemi qalır. İlk başlanqıc məxfi açar mütləq etibarlı rabitə kanalı üzrə çatdırılmalıdır, başqa cür bütün protokol özünün hər cür mənasını itirir. Yaxşı olar ki, ilk başlanqıc açar yeni abonentin şəxsən özünə verilsin, lakin bəzi hallarda bu mümkün olmur, məsələn, verilənlər şəbəkəsinin territorial paylanması zamanı. Simmetrik şifrləmə alqoritmlərinin bu və ya digər çatışmayan cəhətləri asimmetrik şifrləmə alqoritmlərinin vasitəsilə aradan qaldırıla bilər.

# III FƏSİL. AÇIQ AÇARLI KRİPTOQRAFİYA TEXNOLOGİYALARI

## 3.1. Açıq açarlı kriptoqrafiyaya giriş

Bağlı açarlı şifrləmədə iki ciddi problem yaranır. Birinci prob-lem məxfi açarın hazırlanması və onların istifadəçilərə çatdırılması. İstifadəçilərin sayı çox olduqda və onların ərazi üzrə paylanması zamanı açarın təhlükəsizliyinə və onun əsilliyinə zəmanət vermək çox çətin olur [3,4].İkinci problem elektron mübadiləsi zamanı partnyor-ların əssilliyinin təmin edilməsidir [3,4].

İşgüzar yazışmalar və elektron kommersiya hər-hansı partn-yorun dəyişməməsini təmin edən metodlar tələb edirlər. Məktub alıcısı bu məktubun əsilliyinə inanmaq imkanına malik olmalıdır, elektron sənədin yaradıcısı isə özünün müəllifliyini alıcıya yaxud üçüncü tərəfə sübut etmək vəziyyətində olmalıdır. Ona görə də elektron sənəd adi imzanın analoqu olmalıdır.

Əksər kriptoqraflar bu problemlərin həll olunması üzərində işlə-dilər, bunun nəticəsində XX əsrin 70-ci illərininin ikinci yarısında prinsipial olaraq bu problemlərin həll olunmasına imkan verən yeni yanaşmalar işlənilib hazırlandı.

Bu yanaşmaların əsası *asimmetrik kriptoalqoritmlər yaxud me-todlar* oldu [3]. Bu alqoritmlər və yaxud metodlarda düz və əks kripto-çevirmələr müxtəlif açarlarda yerinə yetirilir və öz aralarında bir açarın digərini təyin etməyə imkan verən heç bir əlaqə yoxdur. Asimmetrik alqoritmlər simmetrik şifrləməyə nisbətən riyazi funksiyalara əsəslanır. Şifrləmənin asimmetrik alqoritmləri həm də açıq açarlı alqoritmlər adlanır. Şifrləmə və şifrin açılması üçün eyni bir açardan istifadə olunan simmetrik şifrləmə alqoritmlərdən (bağlı açarlı şifrləmə alqoritmilərdən) fərqli olaraq assimmetrik alqoritmlərdə bir açar şifrləmə üçün, birincidən fərqli olan digər açar isə şifrin açılması üçün istifadə olunur. Alqoritm asimmetrik adlanır, çünki, şifrləmə və şifrin açılması açarları müxtəlifdir, əsas kriptoqrafik proseslərin simmetriyası olmur. İki açarlardan biri *açıq* olur və hamıya bildirilə bilər, ikinci açar isə *bağlı* olur və məxfi saxla-nımalıdır. Açarlardan hansının, açıq yaxud bağlı, şifrləmə üçün istifadə

olunması, hansının isə şifrin açılması üçün istifadə edilməsi kriptoqrafik sistemin təyinatından asılıdır. Hazırkı dövrdə asimme-trik alqoritmlər praktikada geniş istifadə olunurlar, məsələn, tele-kommunikasiya şəbəkələrinin informasiya təhlükəsizliyini təmin etmək üçün, eləcə də mürəkkəb topologiyaya malik olan şəbəkələrin; qlobal İnternet şəbəkəsinin informasiya təhlükəsizliyinin təmin olunması üçün; müxtəlif bank və ödəmə sistemlərində.

Açıq açarlı şifrləmə alqoritmlərini minumum üç məsələnin həl-lində istifadə etmək olar [3,4]:

1. İcazəsiz daxilolmadan mühafizə məqsədilə ötürülən və saxlanı-lan verilənlərin şifrlənməsi üçün.
2. Elektron sənədin altında rəqəmli imzanın formalaşdırılması üçün.
3. Sonralar sənədlərin simmetrik metodla şifrlənməsi zamanı isti-fadə olunan məxfi açarların paylanması üçün.

### 3.1.1. Birtərəfli funksiya

Açıq açarlı şifrləmə alqoritmlərinin hamısı bir tərəfli funksiya-yanın istifadə olunmasına əsaslanırlar. Nisbətən asan hesablanan, lakin arqumentin qiymətinə uyğun olan funksiyanın qiyməti üzrə tapılması çətin olan riyazi funksiyaya bir tərəfli funksiya deyi-lir.Yəni, x- bilərək f(x) funksiası asan həll olunur, lakin məlum f(x) üzrə x-in uyğun gələn qiymətini tapmaq çətin olur. "Çətin hesab-lamaq" dedikdə bunun üçün EHM-i istifadə etməklə bir ildən çox vaxt tələb olunur. Birtərəfli funksiya kriptoqrafiyada heş funksiyası kimi istifadə olunur. Mühafizə məqsədilə məlumatın şifrlənməsi üçün birtərəfli funksiyanın istifadə olunması mənasızdır, çünki, əks olaraq şifrlənmiş məlumatın şifrəsini açmaq artıq mümkün olma-yacaq. Şifrləmə üçün xüsusi birtərəfli funksia istifadə olunur- məx-fi birtərəfli funksiya. Bu funksiya birtərəfli funksiyaların xüsusi növüdür ki, funksiyanın əks qiymətinin tez hesablanmasına imkan veririr.

Məxfi bir tərəfli funksiya üçün aşağıdakı müddəalar doğrudur [3,4]:

1. x-i bilərək, f(x) –i asanlıqla hesablamaq olar;
2. Məlum f(x) funksiyası üzrə x-i tapmaq çətindir;

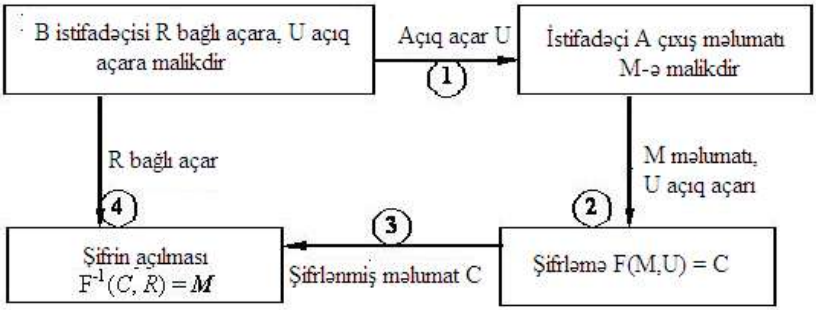
3. Bəzi əlavə məxfi informasiyaları bilərək, x-i asanlıqla hesablamaq olar.

Şifrləmə üçün asimmetrik alqoritmlərin istifadə olunması. XX əsrin 70-ci illərində amerika alimləri Diffi və Helman iki müxtəlif açarın istifadə olunmasına əsaslanan şifrləmə prinsipini təklif etdi-lər. Bu açarlar öz aralarında əlaqəli olmalarına baxmayaraq elə qu-rulublar ki, biri ilə (açıq) digərini (bağlı) açmaq praktiki olaraq mümkün deyil. Bu prinsip istifadəçiləri şifrləmə/şifrin açılması açarları ilə təmin etmək problemini həll etmək üçün istifadə edilə bilər, dəqiqliklə desək bu problemi aradan qaldırmaq üçün. Diffiyə və Helmana görə qabaqcadan paylanan bağlı açarlar şifrləmə üçün istifadə olunmamalıdır (çünki, məxfilik birdən çox adama nəlum-dursa bu artıq məxfi deyil). Bağlı açar yalnız bir şəxsə, yəni onun mülkiyyətçisinə məlum olmalıdır. Asimmetrik alqoritmlərin istifa-də olunmasının bu prinsipi açıq şifrləmə yaxud açıq açarlı şifrləmə adını almışdır. Bu prinsipə əsasən, istənilən arzu edən şəxslər məlu-matı açıq açarla şifrləyə bilərlər. Məlumatın şifrəsinin açılmasını yalnız bağlı açarın mülkiyyətçisi edə bilər.

Fərz edək ki, elektron məlumatla mübadilə aparan A və B istifadəçiləri, açıq şifrləmə sxemini istifadə edirlər. Tutaq ki, A istifa-dəçisi B istifadəçisinə məxfi məlumatı elə verməlidir ki, onu heç kim oxuya bilməsin. Bunun üçün aşağıdakı hərəkətləri yerinə yetir-mək vacibdir [3,4]:

1. İstifadəçi B özünün U açıq açarını istənilən rabitə kanalı üzrə A istifadəçisinə göndərir (məsələn, elektron poçtu üzrə).
2. İstifadəçi A açıq U açarı ilə alınan özünün M məlumatını şifrləyir və şifrlənmiş C məlumatını alır.
3. Şifrlənmiş C məlumatı istifadəçi B-yə göndərilir.
4. İstifadəçi B özünün bağlı R açarı ilə alınan C məlumatınının şifrəsini açır.

Əgər şifrləmə əməliyyatını F-lə, şifrin açılması əməliyyatını isə $F^{-1}$ işarə etsək, onda istifadəçilər arasında informasiya mübadiləsi protokolunun sxemini aşağıdakı kimi təsvir edə bilərik (şək.4.1).




**Şək.3.1.** Açıq şifrləmə sxemi

Açıq şifrləmənin istifadə olunması açarların paylanması proble-mini aradan qaldırır. Əvvəllər istifadəçilər şifrlənmiş verilənlərlə mübadilədən qabaq hər-hansı bir şəkildə bağlı rabitə kanalı üzrə istifadə olunan məxfi açarı razılaşdırmalı idilər. Bunun üçün onlar şəxsən görüşməli yaxud kuryerdən istifadə etməli idilər. Əgər istifadəçilərdən biri açarı dəyişməyi lazım hesab etsəydi, o yeni açarı öz abonentinə verməli idi. Açıq açarlı kriptoqrafiya bütün bunları sadələşdirir. İndi abonentlər məxfi açarı etibardan salma qayğısına qalmamalıdırlar. Rabitə sisteminin istifadəçiləri tamamilə sərbəst açıq açarla və özlərinin şifrlədiyi məlumatlarla mübadilə apara bilərlər. Əgər istifadəçi öz bağlı açarını etibarlı saxlaya bilirsə, heç kim verilən məlumatı oxuya bilməz. Məlumat verilişi şəbəkəsində mübadilə prosesini sadələşdirmək üçün adətən bütün istifadəçilərin açıq açarların saxlandığı verilənlər bazası istifadə olunur. Vacib olduqda sistemin istənilən istifadəçisi bazadan digər adamın açıq açarını sorğu edə bilər və alınan açarı məlumatın şifrlənməsi üçün istifadə edə bilər.

### 3.2. Açıq açarlı alqoritm əsasında rəqəmli imza

Bütün insanlar kimi verilənlərin ötürülməsi şəbəkəsinin istifadəçilərində biri-birlərinə etibar etməyə bilərlər yaxud özlərini şərəf-siz adam kimi apara bilərlər. Onlar özgə məlumatlarını saxtalaşdıra bilərlər, özlərinin müəllifliyindən imtina edərlər yaxud özlərini di-gər şəxs kimi təqdim edə bilərlər. Bu problemlər elektron kommersiyanın inkişafı və

ödənişlərin İnternet vasitəsilə aparılması ilə xüsusilə aktuallaşır. Ona görə də, əksər rabitə sistemlərində korrespondensiyanın alıcısında sənədin əsilliyinə əminlik olmalıdır, elektron müraciətnamənin yaradıcısı isə alıcıya yaxud üçüncü tərəfə özünün müəllifliyini sübut etməyə qadir olmalıdır. Buna görə də, elektron sənədlər adi fiziki imzaya oxşar olmalıdır. Bu zaman imza aşağı-dakı xüsusiyyətə malik olmalıdır [3,4]:

1. İmza yalnız bir şəxslə yaradılır, onun əsilliyiyinin təsdiq edilməsi isə çoxları ilə ola bilər;
2. İmza ayrılmaz surətdə verilən məlumatla bağlıdır və heç bir digər məlumata köçürülə bilməz;
3. Sənəd imzalandıqdan sonra onu dəyişmək mümkün deyil;
4. Qoyulmuş imzadan imtina etmək mümkün deyil, yəni sənədi imzalayan şəxs sonra təsdiq edə bilməz ki, imzanı o qoymayıb.

Asimmetrik şifrləmə alqoritmi rəqəmli (elektron) imzanın formalaşdırılmasında istifadə oluna bilər.

Rəqəmli (elektron) imza dedikdə verilən informasiyaya, onun müəllifliyini yoxlamaq üçün nadir rəqəmli əlavədir.

Elektron (rəqəmli) imza özündə sabit uzunluqlu bit ardıcıllığını əks etdirir ki, bu da imzalanan informasiyanın içindəkilərini məxfi açarın köməkliyi ilə müəyyən qaydada hesablamağa imkan verir.

Rəqəmli imzanın formalaşdırılması zamanı xüsusi şəkildə ya bütün məlumatlar bütövlükdə, ya da məlumatdan heş-funksiyanın hesablanmasının nəticəsi şifrlənir. Axırıncı üsul adətən daha yaxşı üsul hesab olunur, çünki, imzalanan sənəd müxtəlif ölçüyə malik ola bilər, bəzən daha böyük, heş-kod isə daimi çox böyük olmayan uzunluğa malik olur.

Elektron rəqəmli imzanın hər iki variantına təfsilatı ilə baxaq.

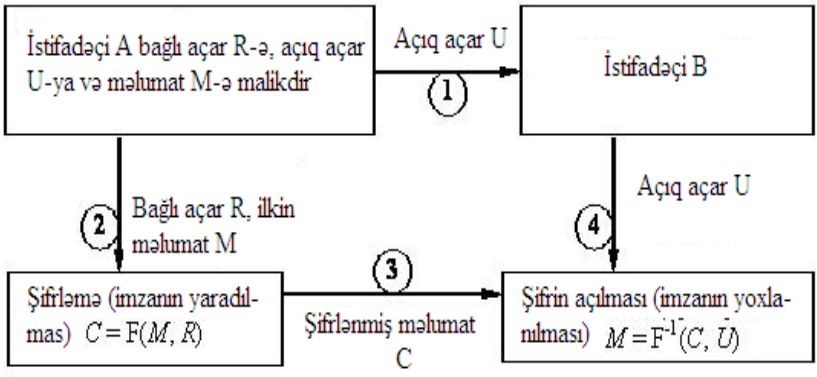
Ən sadə üsul açıq şifrləmədə olduğu kimi öz aralarında əlaqəli olan açarların istifadə olunmasına əsaslanır (açıq və bağlı açarlara). Lakin bağlı və açıq açarların rolu dəyişirlər- imzalanma açarı məxfi açar, yoxlama açarı isə açıq açar sayılır.

Əgər bu zaman xüsusiyyət saxlanılırsa, açıq açarla bağlı açarı tapmaq praktiki olaraq mümkün deyil, onda imza halında məxfi açarla şifrlənən məlumatın özü ola bilər. Beləliklə, məlumatı imza-layan yalnız bağlı

açarın mülkiyyətçisi ola bilər, lakin onun açıq açarına malik olan hər kəs, imzanı yoxlaya bilər. Məsələn, isti-fadəçi A istifadəçi B-yə imzalanan məktub göndərən zaman im-zanın yaranması və yoxlanması aşağıdakı addımlardan ibarət olur [3,4]:

1. İstifadəçi A istifadəçi B-yə istənilən rabitə kanalı üzrə özünün açıq açarını U göndərir, məsələn, elektron poçtu üzrə.
2. İstifadəçi A özünün bağlı açarı R ilə məlumatı M şifrələyir və şifrlənmiş məlumat C alır.
3. Şifrlənmiş məlumatı istifadəçi B-yə göndərir
4. İstifadəçi B istifadəçi A-ın açıq açarını istifadə edərək alınan məlumatın C şifrəsini açır.

Əgər məlumatın şifrəsi açılırsa, deməli, o istifadəçi A tərəfin-dən imzalanıb. Bu protokolun təsviri aşağıdakı sxemdə verilib (şək. 3.2).




**Şək. 3.2.** Rəqəmli imzanın yaranması və yoxlanılması sxeminin birinci variantı

İndiyədək, istifadəçi A öz açarını etibarlı saxlayır, onun imzası doğrudur. Bundan başqa, istifadəçi A-ın bağlı açarına daxil olmağa malik olmadan məlumatı dəyişmək mümkün deyil; bununla da verilənlərin audentikliyi və bütövlüyü təmin olunur. Açar cütlü-yünün fiziki təsviri elektron rəqəmli imzanın (ERİ) istifadə olun-masını dəstəkləyən konkret sistemdən asılıdır. Əksər vaxtlar açar fayla yazılır, hansı ki, açarın özünə əlavədə malik ola bilər, məsə-lən, istifadəçi haqda

məlumata- açarın mülkiyyətçisi haqda, açarın istifadə müddəti haqda, eləcə də konkret sistemin işi üçün nə isə bir verilənlər komplektinə.

Açarın mülkiyyətçisi haqda məlumatlar ERİ-ın digər vacib funksiyasını reallaşdırmağa, məsələn, müəllifliyin müəyyən edil-məsinə imkan verir, çünki, imzanın yoxlanılması zamanı bu və ya digər məlumatın kim tərəfindən imzalanması dərhal məlum olur. Adətən ERİ-ın yoxlanılmasını həyata keçirən, proqram məhsulu, elə köklənir ki, icranın nəticəsi imza qoyan istifadəçini göstərməklə başa düşülən şəkildə ekranda görünsün, məsələn belə:

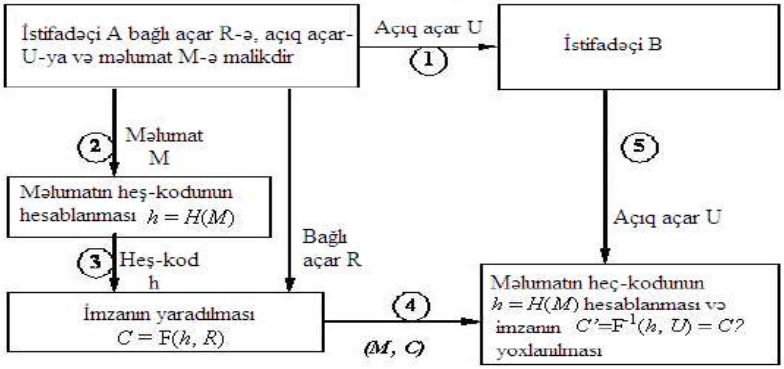
"Faylın imzası əmr.doc doğrudur (Müəllif: Həsənov M.H.)"

Sənədin bərpası ilə rəqəmli imza özündə imzalanan sənədi saxlayır [3,4]: imzanın yoxlanılması prosesində həm də sənədin məzmunu yekunlaşdırılır. Əgər şifrin açılması zamanı məlumat düzgün bərpa olunursa,deməli, imza doğru olub. Sənədin bərpası ilə rəqəmli imza formalaşdırıcı ERİ-in ən məhşur alqoritmlərdən biri –RSA ilə reallaşdırıla bilər [3,4].

Sənədin bərpası ilə rəqəmli imzanın istifadə olunması halında bütün məlumat bütövlükdə imzalanır, yəni şifrlənir. Hal hazırda praktikada adətən belə də edilir. Açıq açarlı şifrləmə alqoritmi kifayət dərəcə də ləngdir, bundan başqa, məlumatın bütövlüyünü təsdiq etmək üçün çox yaddaş tələb olunur. Praktiki olaraq ERİ-ın hesablanmasının bütün alqoritmləri məlumatın hesablanması üçün əvvəlcədən verilmiş standart uzunluğu istifadə edirlər. Məsələn, rəqəmli imzanı formalaşdırmaq üçün istifadə olunan DÜİST P34. 10-94 rusiya alqoritmində bu ölçü 32 bayta bərabərdir. Ona görə də vaxta və hesablama resurslarına qənaət, eləcə də işin əlverişliliyi üçün asimmetrik alqoritm hər hansı bir birtərəfli heş-funksiyası ilə bir yerdə istifadə olunurlar. Bu halda əvvəlcə heş–funksiyasının köməyi ilə ixtiyari uzunluqlu məlumatdan lazımi ölçüdə heş-kod hesablanır, sonra isə ERİ-in hesablanması üçün əvvəlki mərhələdə məlumatdan alınan heş-kodun şifrlənməsi aparılır. Sənədin heş-kodu üzrə hesablanan ERİ, rəqəmli imza ilə qoşma rəqəmli imza adlanır. Belə rəqəmli imza özündə imzalanan sənədə qoşmaq üçün vacib olan bəzi rəqəm kodlarını əks etdirir. Məlumatın özü bu zaman şifrlənmir və göndəricinin rəqəmli imzası ilə birlikdə açıq şəkildə

göndərilir. Əgər istifadəçi A istifadəçi B-yə qoşma rəqəmli imza əlavə edilmiş məlumat M göndərmək istəyirsə, onda imzanın yaradılması və yoxlanılması proseduru aşağıdakı addımlardan ibarət olur [3,4]:

1. İstifadəçi A istifadəçi B-yə istənilən rabitə kanalı ilə, məsələn, elektron poçtu üzrə özünün açıq açarını U göndərir.
2. İstifadəçi A bəzi etibarlı heş-funksiyanın H köməyi ilə öz məlumatının heş-kodunu h = H(M) hesablayır.
3. Sonra istifadəçi A özünün bağlı açarı R ilə məlumatın heş-kodunu h şifrləyir və rəqəmli imza C alır.
4. Çıxış məlumatı M rəqəmli imza C ilə bir yerdə istifadəçi B-yə göndərilir.
5. İstifadəçi B alınan məlumatın M heş-kodunu hesablayır, sonra isə istifadəçi A-ın açıq açarını istifadə etməklə rəqəmli imzanı C yoxlayır. Bu protokol aşağıdakı şəkildə göstərilib (şək.3.3).




**Şək.3.3.** Rəqəmli imzanın yaradılması və yoxlanılmasının ikinci variantı

Heş-funksiya ERİ-ın alqoritminin bir hissəsi deyil, ona görə də sxemdə istənilən etibatlı heş-funksiya istifadə oluna bilər [3,4]. İmzanın təsvir edilmiş bu prosesi məxfiliyi təmin etmir. Yəni bu şəkildə göndərilən məlumatı, dəyişmək mümkün deyil, lakin onu oxumaq olar. Hətta heş-funksiyanı istifadə etmədən, məlumatı bütövlükdə şifrləməklə də məxfilik təmin olunmur, belə ki, istənilən şəxs göndəricinin açıq açarını istifadə etməklə məlumatın şifrəsini aça bilər. Əksər hallarda

rəqəmli imzanın yaradılması və istifadə olunmasının gətirilmiş sxemi tamamilə kifayətdir. Lakin hallar ola bilər ki, istifadəçi B fırıldaqçılıq edə bilər [3,4]. Tutaq ki, göndərilən sənəddə istifadəçi A tərəfdən, məsələn, xidmətin göstə-rilməsinə görə qoyul-muş qəbz olub. İstifadəçi B inandırırdı ki, ondakı rəqəmli imza doğrudur və pulu götürmək üçün onu istifadə etdi. İstifadəçi B-yə imzalanmış sənədin bir yaxud bir neçə nüsxəsini götürməyə heç kim mane ola biməz (ona görə ki, sənəd elektrondur) və periodik olaraq kiçik intervallarla pulu götürmək üçün qəbzi banka təqdim edər. Belə fırıldaqçılığın qarşısını almaq üçün rəqəmli imzaya əksər vaxtlarda *vaxt nişanı* qoyurlar [3,4]. Sənədin imzalanması tarixi və vaxtı məlumata əlavə olunur və bütün sənədlərlə bir yerdə imzalanır. Çekin ödənilməsi zamanı vaxt nişanı bankla qeyd oluna bilər və verilənlər bazasına yerləşdirilər. Təkrar təqdim olunma cəhdi zama-nı bank bunu aşkar edər və uyğun ölçü götürər.

Rəqəmli imzanın növlərindən biri *inkar edilməyən rəqəmli im-zadır* [3/4]. Adi rəqəmli imza kimi, inkar edilməyən rəqəmli imza da imzalanan sənəddən və müəllifin bağlı açarından asılıdır. Adi ERİ-dən fərqi ondan ibarətdir ki, inkar edilməyən imza imzalayanın ica-zəsi olmadan yoxlanıla bilməz. Beləliklə, korrespondensiya alıcısı məlumatı imzalayan şəxsin icazəsi olmadan imzanı göstərə bilməz (yaxud imzanın doğruluğunu sübut edə bilməz).

### 3.3. Asimmetrik alqoritmdən istifadə etməklə məxfi açarın formalaşdirilması

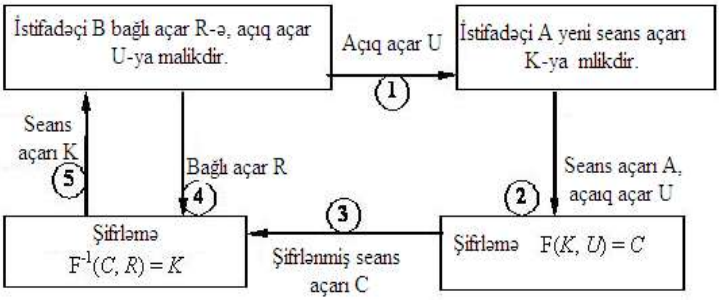
Açıq açarlı alqoritmlər praktikada məlumatın bilavasitə şifr-lənməsi üçün nadir hallarda istifadə olunur [3/4]. Buna böyük həcmli verilənlərin şifrləmə və şifrin açılması zamanı asimmetrik alqorit-mlərin nisbətən alçaq sürətinin olması mane olur. Bu faktor onunla bağlıdır ki, açıq açarlı sistemlərdə əsas əməliyyatlar böyük modullar üzrə 500-1000 bit ədədlərin dərəcəyə yüksəldilməsidir, bu da proqramın reallaşdırılması zamanı, bu həcmidə verilənlərin klassik simmetrik şifrləməyə nisbətən olduqca yavaş aparılmasına gətirib çıxarır [3,4]. Lakin qısa verilənlər blokunun emalı zamanı, məsələn, müəyyən uzunluqlu açarların açıq açarlı şifrləmə alqorit-mləri əhəmiyyətli dərəcə də effektiv isifadə olunur. Ona görə də əksər vaxtlarda aşağıdakı

kombinasiya edilmiş sxemi istifadə edirlər: asimmetrik alqoritm sessiya açarının razılaşdırılması üçün istifadə olunur, sonra isə bu açar simmetrik alqoritm ilə məlumatın şifrlənməsi üçün məxfi açar rolunu oynayır. Sessiyanın məxfi açarının formalaşdırılması protokolu aşağıdakı kimi görünə bilər [3,4]:

1. İstifadəçi A açarların paylanma mərkəzindən, yaxud bilavasitə B istifadəçisinin özündən B istifadəçisinin açıq açarını alır.
2. İstifadəçi A təsadüfi seans açarı generasiya edir və onu alınan açıq açarla şifrləyir.
3. Şifrlənmiş seans açarını istifadəçi B –yə göndərir.
4. İstifadəçi B alınan paketin öz bağlı açarı ilə şifrəsini açır.
5. İstifadəçi A və B şifrlənmiş məlumat mübadiləsi üçün razılaşdırılmış seans açarını istifadə edirlər.

A və B istifadəçi cütünə şifrləmə -şifrin açılması üçün ümumi məxfi açarının K formalaşdırılması sxemi aşağıdakı şəkildə verilib (şək.3.4).

Bu sxemdə ölçüsünə görə böyük olmayan seans açarı istifadə olunur, hansı ki, sonralar simmetrik alqoritmi ilə şifrləmədə isti-fadə olunacaq. Ölçüsünə görə böyük olmayan verilənlər blokunun




**Şək.3.4.** Ümumi sekret açarının formalaşdırılması sxemi

şifrlənməsi kifayət dərəcədə tez yerinə yetirilir və telekommuni-kasiya proseslərini ləngitmir, hətta sistemdə 1000-lərlə istifadəçi olduqda belə. Açarların paylanmasının daha mürəkkəb protokol-ları mövcuddur. Belə protokollar rabitə seansının iştirakçılarının əsilliyini təsdiq edir, sorğu-cavab mexanizmi ilə seansın doğrulu-ğunu yaxud digər tələbləri təmin edir.

### 3.3.1. Açıq açarlı şifrləmə alqoritminə tələblər

Açıq açarlı şifrləmə alqoritminə aşağıdakı tələblər qoyulur [3,4]:

1. Hesabi olaraq açar cütlüyünü asanlıqla yaratmaq olar (açıq açar, bağlı açar).
2. Hesabi olaraq məlumatı açıq açarla şifrləmək olar.
3. Hesabi olaraq məlumatı bağlı açarı istifadə etməklə şifrləmək olar.
4. Hesabi olaraq açıq açarı bilməklə uyğun bağlı açarı təyin etmək mümkün deyil.
5. Hesabi olaraq, yalnız açıq açarı və şifrlənmiş məlumatı bilməklə, ilkin məlumatı bərpa etmək olmaz.

Hal-hazırda çoxlu sayda açıq açarlı şifrləmə alqoritmləri mövcuddur. Biz onlardan dörd açıq açarlı alqoritmi nəzərdən keçirək. Onlardan üçü çoxdandır ki. praktikada istifadə olunur, dördüncü növ alqoritmlər isə lap yaxın zamanlarda informasiya mühafizəsi sistemlərində istifadə olunmağa başlamışdır. Bu alqoritmlər adətən müxtəlif məqsədlər üçün istifadə olunur və aşağıdakı cədvəldə əks olunmuşlar (cədvəl 3.1).

***Cədvəl 3.1.***

| Alqoritmin adları | İstifadə olunma imkanları | | |
|---|---|---|---|
| | Şifrləm /şifrin açılması | Rəqəmli imza | Açarın razılaşdırılması yaxud formalaşdırılması |
| RSA | Hə | Hə | Hə |
| Diffi- Helman alqoritmi | Yox | Yox | Hə |
| ƏL-Qamal alqoritmi | Hə | Hə | Hə |

| | | | |
|---|---|---|---|
| Elleptik əyrilərin istifadə olunması alqoritmi | Hə | Hə | Hə |

### 3.4. Kombinasiya olunmuş şifrləmə kriptosistemi

Simmetrik və asimmetrik kriptoqrafik sistemlərin yuxarıda göstərilən xüsusiyyətləri göstərir ki, onların birgə istifadədə olunması zamanı, onlar çatışmayan cəhətlərini kompensasiya etməklə biri-birlərini effektiv tamamlayırlar. Həqiqətən, açıq açarlı asimmetrik kriptosistemlərin üstün cəhəti yüksək potensial təhlükəsizliyidir, la-

kin onların sürəti yüzlərlə (və daha çox) dəfə məxfi açarlı sim-metrik kriptosistemlərin sürətindən azdır [6]. Öz növbəsində, yüksək sürətli simmetrik kriptosistemlərin də çatışmayan cəhətləri var: simmetrik kriptosistemlərin yenilənən məxfi açarı müntəzəm ola-raq informasiya mübadiləsi üzrə partnyora verilməlidir və bu veri-lişlər zamanı məxfi açarın düşmən tərəfindən açılması təhlükəsi var. Bu kriptosistemlərin birgə istifadə olunması, informasiyanın məxfiliyinin təmin olunması üçün, ona kriptoqrafik istehkam kimi mühafizə funksiyası bazası yaradır. Simmetrik və asimmetrik kriptosistemlərin kombinasiya edilmiş şəkildə istifadə olunması hər iki metoda xas olan çatışmayan cəhətləri aradan qaldırır və açıq açarlı asimmetrik kriptosistemlərin təqdim etdiyi yüksək məxfiliyi, məxfi açarlı simmetrik kriptosistemlərin yüksək sürəti ilə uyğunlaşdırmağa imkan verir. Simmetrik və asimmetrik şifrləmənin kombinasiya olunması metodunun mahiyyəti aşağıda-kılardan ibarətdir. Simmetrik kriptosistemi ilkin açıq mətnin şifr-lənməsi üçün istifadə edirlər, açıq açarlı asimmetrik kriptosistemi isə yalnız simmetrik kriptosistemin sekret açarını şifrləmək üşün istifadə edirlər. Nəticədə açıq açarlı asimmetrik kriptosistem sekret açarlı simmetrik kriptosistemi əvəz etmir, yalnız onu tamamlayır, bununla da verilən informasiyanın bütövlükdə mühafizəsini artırmağa imkan verir. Belə yanaşma bəzən elektron "rəqəmli konvert" adlanır [6]. Fərz edək ki, istifadəçi A istifadəçi B-yə müha-fizə olunmuş məlumat M verilişi

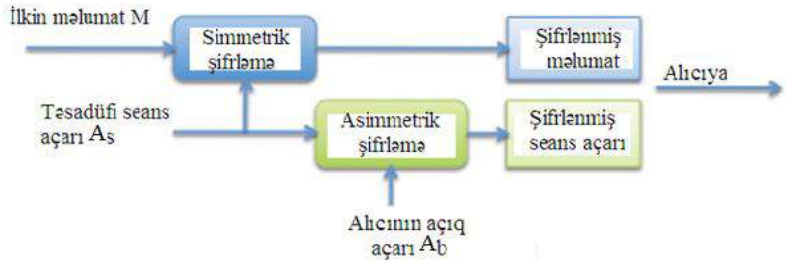
üçün kominasiya edilmiş şifrləmə metodunu istifadə etmək istəyir. Onda A və B istifa-dəçilərinin hərəkət ardıcıllığı aşağıdakı kimi olacaq.

**A istifadəçisinin hərəkəti [6]:**

1. O, seans məxfi açarını $A_s$ yaradır (məsələn, təsadüfi şəkildə generasiya edir). Bu açar konkret məlumatın yaxud zəncirvari məlumatın şifrlənməsi üçün simmetrik şifrləmə alqoritmində istifadə olunacaq.
2. Simmetrik alqoritmi ilə seans məxfi açarı $A_s$ uzərində məlumatı M şifrləyir.
3. Asimmetrik alqoritmi ilə istifadəçi B-in (məlumat alıcısının) açıq açarı üzərində $A_b$ seans sekret açarını $A_s$ şifrləyir.
4. Açıq rabitə kanalı üzrə istifadəçi B-in adresinə şifrlənmiş seans açarı $A_s$ -lə birlikdə şifrlənmiş məlumatı M göndərir.

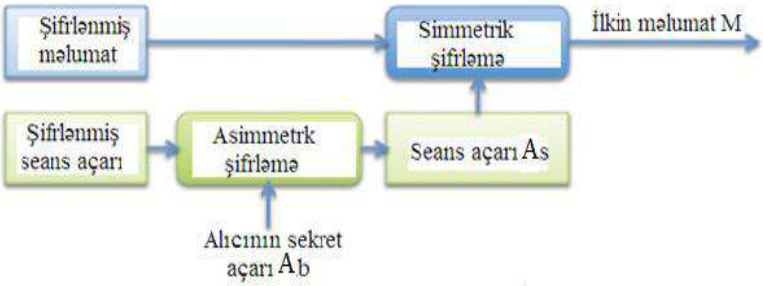
A istifadəçisinin hərəkəti aşağıdakı şəkilin üzərində təsvir olunmuşdur (şək. 3.5).

**İstifadəçi B-in hərəkəti** (elektron "rəqəmli konvert"in alınması zamanı şifrlənmiş məlumatın M və şifrlənmiş seans açarının $A_s$ alınması zamanı) [6]:




**Şək.3.5.** Kombinasiya olunmuş metodla məlumatın şifrlənməsi sxemi

1. Özünün məxfi açarı $A_b$ –in köməyi ilə seans açarı $A_s$ –in şifrəsini asimmetrik alqoritm ilə açır.
2. Alınan seans açarı $A_s$–in köməyi ilə qəbul olunan məlumat M-in simmetrik alqoritmlə şifrəsini açır. B istifadəçisinin hərəkəti aşağıdakı şəkilin üzərində təsvir olunmuşdur (şək.3.6).




**Şək.3.6.** Kombinasiya olunmuş metodla məlumatın şifrəsinin açılması sxemi

Alınan elektron "rəqəmli konvert"i yalnız qanuni alıcı–istifadə-çi B açа bilər.Yalnız şəxsi məxfi açarına $k_b$ malik olan istifadəçi B, sekret seans açarınının $A_s$ şifrəsini düzgün açа bilər və sonra bu açarın köməyi ilə alınan məlumatın M şifrəsini açar və oxuya bilər.

"Rəqəmli konvert" metodu zamanı simmetrik və asimmetrik kriptoalqoritmin çatışmayan cəhətləri aşağıdakı şəkildə kompen-sasiya olunur [6]:

- simmetrik kriptoalqoritmin açarlarının paylanması problemi onunla aradan qaldırılır ki, üzərində məhz məlumatın şifrləndiyi seans açarı As şifrlənmiş şəkildə açıq rabitə kanalı üzrə verilir; As açarının şifrlənməsi üçün asimmetrik kriptoalqoritm istifadə olunur;
- bu halda asimmetrik şifrləmənin yavaş sürəti praktiki olaraq yaranmır, çünki, asimmetrik kriptoalqoritm ilə yalnız qısa açar As şifrlənir, bütün verilənlər isə sürətli simmetrik alqoritm ilə şifrlənir.

Nəticədə sürətli şifrləmə ilə birlikdə açarların əlverişli paylan-masını alırlar.

Tərəflərin biri-birinə etibar etmədikləri protokolların qarşılıqlı əlaqəsinin reallaşdırılması zamanı, aşağıdakı qarşılıqlı əlaqə meto-du istifadə olunur. Hər bir məlumat üçün təsadüfi parametrlər əsa-sında simmetrik şifrləmənin ayrıca sekret açarı generasiya olunur, hansı ki, bu açarla şiflənmiş məlumatla birlikdə verilməsi üçün asimmetrik sistemlə

şifrlənir. Bu halda simmetrik şifrləmənin açа-rının hamıya yayılmasının mənası yoxdur, çünki, növbəti məluma-tın şifrlənməsi üçün digər təsadüfi məxfi açar istifadə olunacaq [6].

Kombinasiya edilmiş metod zamanı həm simmetrik, həm də asimmetrik kriptosistemlərin kriptoqrafik açarları istifadə olunur. Aşkardır ki, hər bir növ kriptosistem üçün açarların uzunluğunun seçilməsi elə şəkildə həyata keçirilir ki, kombinasiya edilmiş kriptosistemin istənilən mühafizə mexanizminə, cinayətkarın hücumu eyni cür çətin olsun.

## 3.5. Elektron rəqəmli imza

### 3.5.1.Elektron rəqəmli imza və heşləmə funksiyası

Elektron rəqəmli imza telekommunikasiya kanalları üzrə veri-lən mətnin audentifikasiyası üçün istifadə olunur [7,8,9]. Belə müba-dilə zamanı sənədlərin emalına və saxlanılmasına sərf olunan xərc aza-lır, onların axtarışı tezləşir. Lakin elektron sənədin müəllifinin və sənədin özünün audentifikasiyası problemi yaranır, yəni müəllifin əsilliyinin müəyyən edilməsi və alınmış elektron sənəddə dəyişikliyin olmaması.

Elektron sənədlərin audentifikasiyanın məqsədi onların mümkün olan pis niyyətlə edilən hərəkətlərdən mühafizəsidir. Belə pis niy-yətlərə aiddirlər [7,8,9]:

- aktiv tutma-şəbəkəyə qoşulan pozucu, sənədləri (faylları) tutub saxlayır və onları dəyişdirir;
- maskarad-abonent C abonent A-ın adından abonent B-yə sənəd göndərir;
- xainlik- abonent A abonent B-yə sənəd göndərmədiyini bildirir, amma iş ondadır ki, göndərib;
- dəyişmə-abonent B sənədi dəyişdirir yaxud yeni sənəd formalaşdırıb və sənədi abonent A-dan aldığını bildirir;
- təkrar –abonent C əvvəl göndərdiyi sənədi təkrar edir, hansı ki, abonent A abonent B-yə göndərmişdir;

Bu pis niyyətli hərəkətlər bank və kommersiya strukturlarına, dövlət müəssisələrinə və təşkilatlarına, öz fəaliyyətlərində infor-masiya texnologiyalarından istifadə edən xüsusi şəxslərə böyük ziyan verə bilər.

Məlumatın bütövlüyünün və onun müəllifinin əsilliyinin yoxlanılması problemini elektron rəqəmli imza metodologiyası effektiv həll etməyə imkan verir [7,8,9].

### 3.5.2. Rəqəmli imzanın əsas prosedurları

Adi əl imzasına analoji olan rəqəmli imza funksional olaraq aşağıdakı əsas üstün cəhətlər malikdir [7,8,9]:

- imzalanan sənəd imza qoyan şəxsdən çıxdığına inandırır;
- bu şəxsin özünə imzalanan sənədlə bağlı olan öhdəlikdən imtina eməyə imkan vermir;
- imzalanan sənədin bütövlüyünə zəmanət verir.

Elektron rəqəmli imza (ERİ) özündə imzalanan sənədlə bir yerdə verilən, nisbətən kiçik həcmli əlavə rəqəmli informasiyanı əks etdirir. ERİ asimmetrik şifrləmənin ilk vəziyyətinə qayıtma qabliyyətinə, eləcə də məlumatın içindəkilərin qarşılıqlı əlaqəsinə, imzanın özünə və açar cütlüyünə əsaslanır. Bu elementlərdən heç olmasa birinin dəyişməsi rəqəmli imzanın əsilliyinin tanınmasını mümkünsüz edir. ERİ asimmetrik şifrləmə alqoritminin və heş-funksiyasının köməkliyi ilə reallaşır [7,8,9]. ERİ sisteminin istifadə olunması texnologiyası şəbəkənin biri-birlərinə imzalanan sənədlərini göndərən abonentlərin olmasını ehtimal edir. Hər bir abonent üçün bir cüt açar generasiya olunur: məxfi və açıq.

Abonent məxfi açarı gizli saxlayır və onu ERİ-ni formalaşdır-maq üçün istifadə edir. Açıq açar isə bütün digər abonentlərə mə-lumdur və elektron sənəd alıcısının ERİ-ni yoxlaması üçün istifadə

edilir.

ERİ sistemi iki əsas prosedura malikdir [7,8,9]:

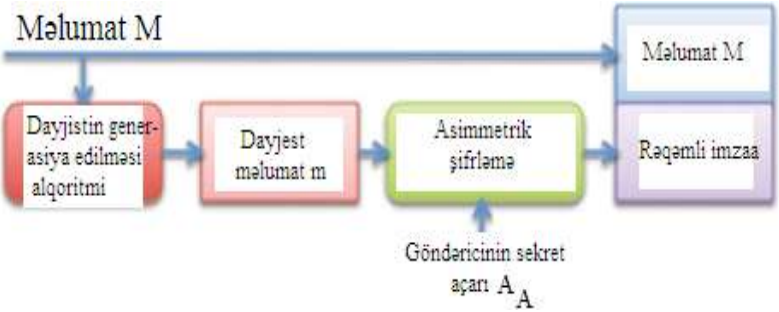
- rəqəmli imzanı formalaşdırmaq;
- rəqəmli imzanı yoxlamaq.

Rəqəmli imzanın formalaşdırılması prosedrunda məlumatı göndərənin məxfi açarı, rəqəmli imzanın yoxlanılması prosedrunda – göndəricinin açıq açarı isifadə olunur.

### 3.5.3. Rəqəmli imzanın formalaşdırılması prosedru

Bu prosedrun hazırlıq mərhələsində abonent A (məlumat göndəricisi) bir cüt açar generasiya edir[7,8,9]: məxfi açar $a_A$ və açıq $A_A$ açar. Açıq açar $A_A$ ona cüt olan sekret açar $a_A$ – dan hesablanıb tapılır. Açıq açar imzanın yoxlanılması məqsədilə şəbəkənin digər abonentlərinə göndərilir.

Rəqəmli imzanın formalaşdırılması üçün göndərici A hər şeydən əvvəl imzalanan mətnin M heş- funksiyasının qiymətini hesablayır (şək.3.7) [7,8,9].




**Şək.3.7.** Elektron rəqəmli imzanın formalaşdırılması sxemi

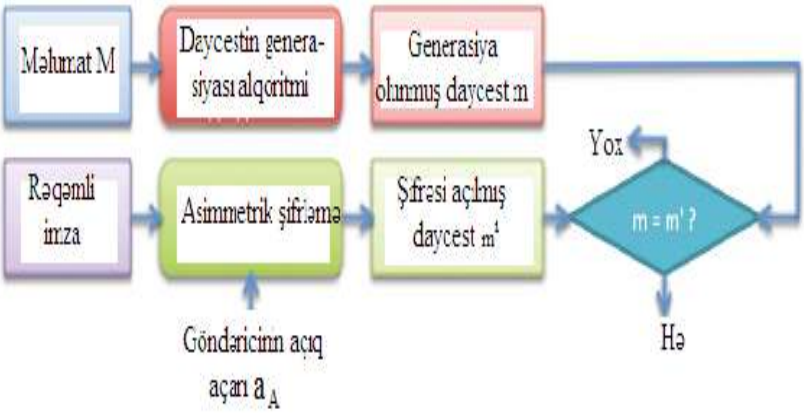
Heş-funksiya imzalanacaq ilkin mətnin M daycestə m (daycest dedikdə qeyd olunmuş kiçik bit ədədlərdən ibarət olan və bütün mətni M bütövlükdə xarakterizə edən nisbətən qısa ədədlər başa düşülür) sıxılmasını həyata keçirir.

Daha sonra göndərici A daycesti m özünün məxfi açarı $a_A$ ilə şifrələyir. Bu zaman alınan bir cüt ədəd özündə bu məlumat M üçün rəqəmli imzanı əks etdirir. Məlumat M rəqəmli imza ilə

birlikdə alıcının adresinə göndərilir.

### 3.5.4. Rəqəmli imzanın yoxlanılması prosedduru

Şəbəkənin abonentləri alınan məlumatı M bu məlumatın göndəricisinin açıq açarının $K_A$ köməyi ilə rəqəmli imzanı yoxlaya bilər-lər (şək.3.8) [7,8,9].




**Şək.3.8.** Elektron rəqəmli imzanın yoxlanılması sxemi

ERİ-in yoxlanılması zamanı abonent B (məlumatın M alıcısı) göndərici A-ın açıq açarı $A_A$ ilə qəbul olunan dacestin şifrəsini açır. Bundan başqa, alıcı özü qəbul olunmuş məlumatın M heş –funksiyasının h(M ) köməyi ilə daycesti m' hesablayır və onu şifrə olun-muşla yoxlayır. Əgər m və m üst-üstə düşürsə, onda rəqəmli imza əsldir. Əks halda imza ya saxtalaşdırılıb, ya da məlumatın məzmu-nu dəyişdirirlib. ERİ sistemində prinsipial moment ondan ibarətdir ki, istifadəçinin ERİ-sinin saxtalaşdırılması, onun məxfi imza açа-rını bilmədən mümkün deyil. Ona görə də imza açarının gözlənil-məz təsadüfi hərəkətlərdən (GTH) mühafizə olunması vacibdir.

ERİ-in məxfi açarının simmetrik şifrləmə açarının mühafizə olunmuş şəkildə personal açar daşıyıcısında saxlanılması tövsiyə olunur. Elektron rəqəmli imza özündə imzalanan sənəddən və abonentin məxfi açarından asılı olan nadir ədədləri əks etdirir. İmzalanan sənəd halında istənilən fayl ola bilər. İmzalanan fayl imzalanmamışa bir yaxud daha çox elektron imza əlavə etməklə yaradılır. İmzalanan fayla

yerləşdirilən ERİ srukturu adətən imzalanan sənədin müəllifini bir mənalı eyniləşdirən əlavə infor-masiyaya malikdir. Bu informasiya sənədə ERİ-in hesablan-masınadək əlavə olunur ki, bu da onun bütövlüyünü təmin edir. Hər bir imza aşağıdakı informasiyaya malikdir [7,8,9]:

- tarix imza;
- müddət -son açar verilən imza;
- faylı imzalayan şəxs haqqında məlumat (A.A.S., vəzifəsi, fir-manın qısa adı);
- imzalayan şəxsin eyniləşdiricisi (açıq açarın adı);
- rəqəmli imzanın özü.

Qeyd etmək lazımdır ki, son istifadəçi nöqteyi nəzərindən rə-qəmli imzanın formalaşması və yoxlanılma prosesi ötürülən veri-lənlərin kriptoqrafik örtülmə prosesindən aşağıdakı xüsusiyyətlərlə fərqlənir. Rəqəmli imzanın formalaşması zamanı göndəricinin bağlı açarı istifadə olunur, onda şifrləmə zamanı alıcının açıq açarı istifa-də edilir.

Rəqəmli imzanın yoxlanılması zamanı göndəricinin açıq açarı, şifrləmə zamanı isə alıcının bağlı açarı istifadə olunur [7,8,9]. Forma-laşmış imzanı istənilən şəxs yoxlaya bilər, çünki, imzanın yoxlanıl-ması açarı açıqdır.

İmzanın yoxlanmasının müsbət nəticəsi zamanı alınan məlu-matın əsilliyi və bütövlüyü haqqında qərar çıxarılır, yəni o haqdakı məlumat həqiqətən bu və ya digər göndəricidən göndərilib və şəbə-kə üzrə verilən zaman modifikasiya olunmayıb. Lakin, əgər istifa-dəçini alınan məlumatın əvvəlki məlumatın təkrarı olub olmaması yaxud onun rabitə kanalı üzrə hərəkəti zamanı yolda gecikib gecikməməsi maraqlan-dırırsa, onda o, onun göndərilmə tarixini və vaxtı-nı, mövcud olan zaman isə sıra nömrəsini yoxlamalıdır.

Asimmetrik şifrləməyə analoji olaraq, ERİ-in yoxlanması üçün

istifadə olunan açıq açarın dəyişdirilməsinin qeyri mümkünlüyünü təmin etmək vacibdir. ERİ-in açıq açarlarını dəyişdirilmədən qoru-maq üçün uyğun rəqəmli sertifikatdan istifadə olunur. Bu gün ERİ-in bir neçə standartı mövcuddur, məsələn, DÜİS T34.10-2001.

### 3.5.5. Heşləmə funksiyası

ERİ-in hesablanması üçün ilkin qiymət halında elektron sənədin özü deyil, onun heş-qiyməti yaxud daycesti götürülür [7,8,9]. Heş-qiymət h(M)-bu, məlumatın (M) daycestidir, yəni ixtiyari uzunluq-lu əsas məlumatın sıxılmış ikili təsviridir. Heş-qiymət h(M) heşlə-mə funksiyası ilə formalaşır. Heşləmə funksiyası (heş-funksiya) özündə, girişində dəyişən uzunluqlu məlumat M olan, çıxışın-da isə qeyd olunmuş uzunluqlu sətr h(M) alınan çevirməni əks et-dirir. Başqa sözlə desək, heş-funksiya h(M) arqument halında ixtiyari uzunluqlu məlumatı (sənədi) M qəbul edir və qeyd olunmuş uzunluqlu heş-qiymətə (heş)H=h(M) qaytarır (şək.3.9).


**Şək.3.9.** (heş)H=h(M)-in formalaşma sxemi

Heşləmə funksiyası imzalanan sənədi M 128 daha çox bitə dək sıxmağa imkan verir (xüsusilə 128-bitədək yaxud 256 bit), onda M-in ölçüsü meqabayt yaxud daha çox ola bilər. Qeyd etmək lazımdır ki, heş-funksiya h(M) mürəkkəb şəkildə sənəddən M asılıdır və sənədin özünü bərpa etməyə imkan vermir.

Heşləmə funksiyası aşağıdakı xüsusiyyətlərə malik olmalıdır [7,8,9]:

1. Heş–funksiya istənilən ölçülü arqumentə istifadə oluna bilər.
2. Heş-funksiya sabit ölçüyə malikdir.
3. Heş-funksiyasını *h(x) lazımınca istənilən* x üçün hesablamaq olar.

Heş-funksiyasının hesablanma sürəti elə olmalıdır ki, heş –funksiyasının istifadə olunması zamanı ERİ-in hazırlanması və yoxlanılması sürəti, məlumatın özünün istifadə olunmasından çox olsun.

4. Heş-funksiyası mətndə əlavə etmə, sıçrayış,yerdəyişmə və s.kimi dəyişikliklərə həssas olmalıdır.
5. Heş –funksiya biristiqamətli olmalıdır.

6. İki müxtəlif sənədin heş-funksiyasının qiymətinin üst-üstə düşmə ehtimalı (onların uzunluğundan asılı olmayaraq) çox cüzii olma-lıdır.

Nəzəri olaraq iki müxtəlif məlumatı eyni bir yerə sıxmaq olar. Bu zaman toqquşma alınır. Heşləmə funksiyasının dayanıqlığını ar-tırmaq məqsədilə toqquşmadan qaçmaq lazımdır. Lakin toqquş-madan tam qaçmaq olmur, çünki, mümkün olan məlumatların sayı heşləmə funksiyasının çıxış qiymətindən daha çoxdur. Ona görə də toqquşma ehtimalı çox az olmalıdır.

Beləliklə, heşləmə funksiyası məlumatın dəyişməsinin aşkar olunmasında istifadə oluna bilər, yəni kriptoqrafik nəzarət cəminin (eyni zamanda dəyişikliyin aşkar olunması kodunun yaxud auden-tifikasiya kodunun) formalaşdırılması üçün istifadə oluna bilər. Bu xüsusiyyətlə heş-funksiya ERİ-in formalaşması və yoxlanılması zamanı məlumatın bütövlüyünün nəzarət olunması üçün istifadə oluna bilər. Heş-funksiya həm də istifadəçilərin audentifikasiya olunmaları üçün istifadə olunur.

Heşləmənin aşağıdakı məhşur alqoritmləri mövcuddur [7,8,9]:

- DÜİST.11-94. Bu 32 bayt ölçülü heşi hesablayır;
- MD (Message Digest) – heşləmənin bir sıra alqoritmləri dünyada geniş yayılmışdır. Məsələn, MD5 alqoritmi istifadə-çilərin parolunu 16-baytlıq ədədə çevirmək məqsədilə Micro-soft Windowsun axırıncı versiyasında istifadə olunur;
- SHA-1 (Secure Hash Algorithm)-bu, məlumatın daycestini he-sablamaq alqoritmidir və dünyada geniş yayılmışdır.
- Heş-funksiya həm də istifadəçilərin audentifikasiyası üçün geniş istifadə olunur.

# IV FƏSİL. TAM MƏXFİ SİSTEMLƏR

## 4.1. Məlumatın əldə edilməsi, emalı, ötürülməsi və qorunması

Məlumatın əldə edilməsi, emalı, ötürülməsi və qorunması məsələləri kəmiyyət ölçmə problemi ilə sıx bağlıdır [10]. Bu problemin həllinə bir neçə fərqli yanaşma var, bunlardan biri sözdə statistik (və ya əlifba) yanaşmadır. Onun mahiyyəti ötürülən məlumatların həcmi-nin kəmiyyət qiymətləndirilməsinin informasiya mənbəyinin statis-tik xüsusiyyətlərinin təhlili əsasında həyata keçirilir. Bu metodda informasiyanın hər-hası dilin köməyi ilə təsvir edilməsini nəzərə alır.Aşkardır ki, hər hansı məlumatın informasiya dəyəri hasil olu-nan məlumatların müxtəlif variantları ilə bağlıdır, yəni başqa sözlə desək məlumat mənbəyinin müxtəlif vəziyyətləri ilə əlaqəlidir. Bu-nunla əlaqədar olaraq, ayrı-ayrı məlumatlarla göndərilən informa-siyaların miqdarını N müxtəlif məlumatların ümumi sayına (ya da informasiya mənbəyinin vəziyyətinə) mütənasib olmasını hesab et-mək olar. Amma praktikada informasiya miqdarı halında N-in özü deyil, onun 2 əsasına görə loqarifması götürülür [10]:

$$\text{İ} = \log_2 N$$

Bu ifadə bizə nəticəni bitlə təmin etməyə imkan verir. İnforma-siya miqdarının belə təyin olunması informasiyanın formalməntiqi loqarifmik miqdarı, yaxud Xartli üzrə informasiya miqdarı adını almışdır. Bir hərfli məlumat üçün N informasiya qurğusunda olan əlifbanın hərflərinin sayına bərabərdir. Xüsusilə, hərflərin sayı iki-yə bərabər olan zaman informasiya miqdarı bərabərdir [10]:

$$\text{İ} = \log_2 2 = 1 \text{ bit}$$

Məsələn, 32 hərfdən ibarət olan azərbaycan əlifbasının tək hərf-lərindən ibarət olan məlumat hasil edən mənbəyə baxaq. Bir hərf-dən ibarət olan ayrı-ayrı məlumatların nə qədər informasiya daşı-dıqlarını təyin edək [10]:

$$\text{İ}_1 = \log_2 32 = 5 \text{ bit}$$

Belə yanaşma zamanı hər hansı bir məlumatda informasiya

həcminin təyin olunması üçün onda olan işarələrin sayını bir işarə-də olan informasiyanın sayına vurmaq lazımdır, yəni onun informa-

siyasının çəkisinə vurmaq vacibdir. Azərbaycan alifbasının dörd hərfindən ibarət olan məlumatın hansı sayda informasiya daşıdığı-nı tapaq [10]:

$$İ_4 = 4 \log_2 32 = 20 \text{ bit}$$

Beləliklə, əlifba yanaşması zamanı məlumatda informasiyanın həcmi məlumatın mənasına görə deyil, statistik xarakteristikalar (işarələrin sayı) üzrə təyin olunur.

Xartli *ölçüsü* həmişə məlumatın düzgün xarakteristikası sayıl-mır, çünki, istənilən mümkün məlumat bərabər ehtimalı nəzərdə tu-tur. Məlumatın mövcudluğu mövcud qeyrimüəyyənliyi aradan qal-dırmaq olduğundan, yüksək ehtimalı olan məlumatlar daha az də-yərlidir.Çünki,informasiyanın dəyəri mövcud olan qeyrimüəyənliyi aradan qaldırmaqdan ibarətdir, yüksək ehtimala malik olan infor-masiya az qiymətlidir. Onları hər-hansı bir dərəcədə əvvəlcədən görmək olar və əksinə az ehtimala malik olan məlumat böyük qiymətə malikdir. Ona görə də bəzən informasiyanın kəmiyyətcə qiymətləndirilməsi üçün Şennonun informasiya ölçüsündən istifadə olunur. Bu informasiya ölçü metodu mənalı yanaşma adlanır.

Bu metoda əsasən informasiya mənbəyinin vəziyyəti məlumatı alıcının almasına dək hər-hansı bir qeyrimüəyyənliklə xarakterizə olunur. Bu zaman informasiyanın alınması bu qeyrimüəyyənliyi (tam yaxud hissə-hissə) aradan qaldırır [10]:

$$İ = H_{başl} - H_{son}$$

burada $H_{başl.}$ məlumatın alınmasına dək məlumat mənbəyi ilə xa-rakterizə olunan qeyrimüəyyənlikdir.

İnformasiya mənbəyinin qeyrimüəyyənliyi aşağıdakı ifadə ilə qiymətləndirilir [10]:

$$H = - \sum_{i=0}^{N-1} p_i * \log_2 p_i,$$

burada $p_i$-mənbənin i-ci vəziyyətinin ehtimalıdır.

Cəmin qarşısındakı çıxaq işarəsi ona görə qoyulub ki, ehtimalın qiyməti düzgün kəsrdir və mənfi loqarifmaya malikdir, qeyrimüəy-yənliyin qiymətləndirilməsini isə "üstəgəl" işarəsilə almaq lazım-dır.

**Misal.** Qutuda olan bir qara və bir ağ şarı çıxararkan, qeyri-müəyyənlik aşağıdakı kimi təyin olunur:

H = - (1/2)$\log_2(1/2)$ – (1/2) $\log_2(1/2)$=- $\log_2(1/2)$=- (-1) =1bit.

Qeyrimüəyyənlik bir bitə bərabər oldu.

H = (7/8) $\log_2(7/8)$ - (1/8) $\log_2(1/8)$ = (7/8)($\log_2 8$ -$\log_2 7$) +
+ (1/8)($\log_2 8$) = (7(3 - $\log_2 7$)+3)/8 ≈ (7(3-2,8) +3))/8 ≈0,55 bit

Hər bir vəziyyətin ehtimalları bir-birinə bərabər olduqda və bu ehtimalların yayılması ilə azaldıqda qeyrimüəyyənlik maksimuma çatır. Həm də qeyd etmək lazımdır ki, ehtimallar öz aralarında biri-birinə bərabər olan zaman, yəni $p_i = p_i$, $\forall_i$, J = $\overline{0 \dots N-1}$, Şen-nona görə informasiya ölçüsü Xartliyə görə informasiya ölçüsü ilə üst-üstə düşür. Çox hallarda informasiya ölçüsünə əlifba yanaşması üstünlük təşkil edir. Məhz Xartli üzrə informasiya ölçüsü o zaman istifadə olunur ki, əgər biz deyir ki, bəzi fayllar 1,5 meqabayt infor-masiyaya malikdir, yaxud bəzi kitabların bir səhifəsində 17 kilo-bayt informasiya yerləşir. İnformasiya ölçüsünün vahidi bitdir. Lakin praktiki cəhətdən bu çox kiçik ölçü vahididir. Daha əlverişli ölçü vahidi səkkiz bitə bərabər olan baytdır. Sözə "bayt", "kilo", "meqa" və s. əlavə etməklə daha böyük ölçü vahidi almaq olar.

## 4.2. Entropiya və qeyrimüəyyənlik

Beləliklə, biz aydınlaşdırdıq ki, bir məlumatda informasiya miq-darının ölçülməsini qeyrimüəyyənlik dəyişikliyini nəzərə almaqla həyata keçirə bilərik. K. Şennon entropiya anlayışını qeyrimüəy-yənlik ölçüsü olaraq təqdim edib. Entropiya H(m) məlumatda informasiya miqdarını (m-i) təyin edir və onun qeyrimüəyyənli- yidir. Fərz edək ki, məlumat mənbəyi $p_1$, $p_2$,..., $p_n$ehtimalla müx təlif məlumatları $m_1$, $m_2$,..., $m_n$ hasil edir. Bu halda entropiya aşa-

ğıdakı ifadə ilə təyin edilir [10]:

$$H(m) = -\sum_{i=0}^{N-1} p_i * \log_2 p_i$$

Beləliklə, bu ifadədə ikili loqarifma istifadə olunur, onda entro-piya bitlə ölçüçür, bu ümumiyyətlə kriptoqrafiyada və informasiya nəzəriyyəsində qəbul edilib.

Entropiyanın "fiziki" mənası entropiyanın qeyrimüəyyənlik kə-miyyəti ölçüsüdür. Misal halında hər birinin yalnız iki fərqli $m_1$ və $m_2$ məlumat hasil edən üç məlumat mənbəyini nəzərdən keçirək. Aşkardır

ki, birinci mənbə üçün birinci məlumatın yaranma ehti-malı $p(m_1)=0$, ikinci məlumatın ehtimalı isə $p(m_1)=1$-dir.

İkinci mənbə üçün məlumatların yaranma ehtimalı bərabərdir, yəni $p(m_1)=0,5$ və $p(m_2)=0,5$. Üçüncü mənbə üçün məlumatların yaranma ehtimalı $p(m_1) = 0,9$ və $p(m_2) = 0,1$. Hər bir məlumat mənbəyinin entropiyasını təyin edək [10]:

$$H_1 = -0 * \log_2 0 - 1 * \log_2 1 = 0 - 0 = 0.$$

Birinci məlumat mənbəyi üçün entropiya yaxud qeyrimüəyyən-lik sıfra bərabərdir. Həqiqətən, əgər əvvəlcədən məlumdur ki, iki məlumatdan yalnız biri hasil olunursa, onda heç bir qeyrimüəy-yənlik yoxdur. İkinci məlumat mənbəyinin entropiyasını təyin edək [10]:

$$H_2 = -(1/2)\log_2(1/2) - (1/2)\log_2(1/2) = -\log_2(1/2) = -(-1) = 1 \text{bit}.$$

Göründüyü kimi ikinci məlumat mənbəyinin qeyrimüəyyənliyi bir bitə bərabər oldu.

İndi də üçüncü məlumat mənbəyinin entropiyasını təyin edək [10]:

$$H_3 = -0,9\log_2 0,9 - 0,1\log_2 0,1 \approx -0,9*(-0,152) - 0,1* *(-3,332) \approx 0,47$$

Üçüncü məlumat mənbəyyinin qeyrimüəyyənliyi ikinci məlumat mənbəyinin qeyrimüəyyənliyindən azdır, çünki, üçüncü məlumat mənbəyinin hasil etdiyi iki mümkün məlumatdan biri digərindən çox ehtimaldır.

Entropiya anlayışı informasiya nəzəriyyəsinin və informasiya saxlanmasının bir çox məsələlərində mühüm rol oynayır. Xüsusilə, entropiya verilənlərin maksimal sıxılma dərəcəsinin təyin edilmə-sində istifadə oluna bilər.

Daha doğrusu, əgər məlumat mənbəyi müəyyən bir məhdudlaş-dırma entropiyası h ilə kifayət qədər böyük uzunluqlu n mətni hasil edirsə, bu mətn nəzəri cəhətdən n*h bit qədər sıxılmış ola bilər. Məsələn, əgər h = 1/2, onda mətn iki qat sıxıla bilər və s. n*h qiyməti səddir və praktikada nadir hallarda əldə olunur.

Kriptoqrafiya baxımından entropiya bir məlumatın məzmununu bilmək üçün açıqlanmalı olan işarələrin sayını müəyyən edir [10].

Əgər bəzi 8 bit verilənlər bloku iki mümkün məlumatdan birini saxlayırsa (məsələn, "Bəli" və ya "Yox" cavablarını), o zaman mə-

lumatın mənasını düzgün müəyyən etmək üçün bir biti doğru ta-nıya bilmək kifayətdir [7]. "Bəli" və "Xeyr" sözlərini şifrələmək üçün biz nə qədər bit ayır-mış olsaq da, entropiya və ya qeyrimüəyyənlik hər zaman 1-dən az və ya 1-ə ona bərabər olacaqdır.

### 4.3. Dil norması və məlumat artıqlığı

Hər bir dil üçün, dilin norması r adlanan və aşağıdakı ifadə ilə təyin olunan bir qiyməti daxil etmək olar [10]:

$$r = H(m)/N,$$

burada H(m) -məlumatın entropiyasıdır, N – istifadə olunan dilin işarələri ilə məlumatın uzunluğudur.

Dilin normasına məlumatın bir işarəsinə düşən informasiyanın miqdarı kimi baxmaq olar. Müxtəlif dillər, eləcə də müxtəlif uzun-luqlu və məzmunlu məlumatlar üçün dilin norması müxtəlif olur. Məsələn, müxtəlif tədqiqatçılar ingilis dilinin bir işarəyə düşən nor-masını 1,0-dan 1,5 bit-ə qədər diapazonda qiymətləndirirlər. Hesab edəceyik, rus dili üçün bir işarəyə düşən norma isə təqribən 1,5 bitə bərabərdir.

#### 4.3.1. Dilin mütləq norması

Dilinin mütləq norması R, baxılan dilin işarələrinin bütün ardı-cıllığının bərabər ehtimallı olması şərtində bir işarəsilə verilə bilən informasiyanın bitlərinin sayıdır. Əlifbası L işarələrdən ibarət olan dilin mütləq norması aşağıdakı kimi hesablana bilər [10]:

$$R = \log_2 L$$

Əlifbası 33 hərfdən ibarət olan rus dili üçün dilin norması bəra-bərdir [10]:

$$R_{Rus} = \log_2 33 \approx 5 \text{ bit}$$

Beləliklə, görünür ki, rus dilinin mütləq norması real qiymətdən kifayət dərəcədə çoxdur. Bu, təəccüblü deyil, çünki bütün təbii dillərdə əhəmiyyətli artım vardır. Bu bir neçə faktorlarla bağlıdır.

Birinci, əlifbanın bəzi hərifl ərinə digərlərinə nisbətən məlu-matda daha tez-tez rast gəlinir. İkinci səbəbi sözlərdə hər-hansı söz birləşmələrinin qəbuledilməzliyidir.

Bundan əlavə, təbii dillər elə qurulub ki, bəzən bir sözün və ya sözün parçasını bilərək, onun çatışmayan hissəsini bərpa edə bilə-rik. Məsələn, salamlaşmada S.lam! sözündə biz asanlıqla "a" hərfini bərpa edə bilərik və tam "salam" sözünü alarıq.

### 4.3.2. Dilin artıqlığı

Dilin artıqlığı D aşağıdakı ifadə ilə təyin olunur [10]:

$$D = R - r.$$

Rus dilinin artıqlığı bir işarə üçün 3,5 bit-ə bərabərdir. Bu onu göstərir ki, rus dilinin hər bir hərfi 3,5 bit istifadə olunmayan informasiyaya malikdir. Belə bir artıqlığa təqribən digər təbii dil-lərdə malikdir, məsələn, ingilis dili.

Bütün işarələri bərabər ehtimallı olan məlumatların minimum artıqlığı sıfra bərabərdir,yəni D = 0 olur. Bərabər ehtimallı işarələrə hər hansı bir qaydada bir-birindən asılı olmayan məlumatlarda rastgəlinə bilər.

## 4.4. Tam məxfi sistemlər anlayışı

Əgər şifrlənmiş mətnin analizi onun mümkün olan uzunluğundan başqa heç bir informasiya vermirsə, belə kriptoqrafik sistem tam məxfi sistem adlanır [10].

Əgər kriptoqrafik sistem tam məxfi deyilsə, onda məlumatın şifrmətni ilə tanışlıq uyğun açıq mətn haqqında bəzi məlumatlar verir. Əksər sadə şifrmtinlər məsələn, bir əlifbalı əvəzləmə yaxud yerdəyişmə metodları üçün, cinayətkar tərəfindən tutulub saxlanıl-mış şifrlənmiş məlumatın uzunluğu artıqca şifrləmə açarları yaxud açıq mətn haqqında bəzi nəticələri əldə etmək olar. Bu təbii dillərin artıqlığının böyük olması ilə bağlıdır. Məsələn, əgər cinayətkar tə-rəfindən tutulub saxlanılmış məlumat yerdəyişmə metodu ilə şifrlə-nibsə, onda cinayətkar ilkin məlumatda hansı işarələrin və hansı sayda olmasını bilə bilər, bundan sonra o, yerdəyişmə qaydasını təyin etmək üçün daha mürəkkəb analiz aparmağa cəhd edə bilər. Əgər bizə monoəlifbalı yerdəyişmə metodla şifrlənmiş məlumat DKDK məlumdursa, onda əlavə informasiya olmadan ilkin mətndə nəyin olmasını birmənalı olaraq təyin edə

bilmərik. Lakin, mono-əlifbalı yerdəyişmə metodla şifrlənmiş DKDK məlumatı analiz edə-rək aşağıdakı nəticəyə gələ bilərik [10]:

1. İlkin mətndə əlifbanın cəmi iki hərfi istifadə olunub.
2. Açıq mətnin birinci və ikinci, eləcə də ikinci və dördüncü hərfləri eynidirlər.

Həm də güman etmək olar ki, ya D ya da K hərfləri sait hərfləri əvəz edirlər. Ola bilər ki, ilkin məlumat özündə ANA ,yaxud ATA sözünü, bəlkə də başqa bir şeyi əks etdirirlər. Onu bərmənalı de-şifrə etmək olmaz, amma şifrə ilə əlaqədar bəzi məlumatları müəy-yənləşdirə bildik. Beləliklə, belə nəticəyə gəlmək olar ki, yerdə-yişmə yaxud əvəzləmə metodu tam məxfi kriptoqrafik şifrləmə deyil.

Tam məxfi sistemin praktikada digər reallaşdırılması variantları mövcuddur. Bunlar birdəfəlik lent, birdəfəlik bloknot, yaxud XX əsrin ortalarında amerikalı mühəndis Vernamın adı ilə adlandırılan şifr adlanırlar. Şifrləmə prosesinə ikili verilənlər məruz qalırlar. Verici və alıcı tərəflərdə iki eyni lent hazırlanır, məsələn, maqnit lenti. Onlar şifrləmə açarlarına malikdirlər. Verici tərəfdə bu lent şifrləmə qurğusunda, qəbul tərəfdə isə şifrin açılması üçün istifadə olunan qurğuda yerləşdirilir. Göndərici məlumat göndərmək istə-yən zaman o, bir bit ilkin məlumatdan və bir bit maqnit lentindən götürüb iki modulu üzrə toplayır. Bundan sonra lent növbəti vəziy-yətə hərəkət edir və açarın ikinci bitini istifadə etməklə məlumatın ikinci bitini şifrləyir. Beləliklə, bütün məlumatlar şifrlənir. Qəbul edici tərəfdə də lent açarla birlikdə vericidəki lentə analoji olaraq istifadə olunur. Məsələn, ilkin məlumat m aşağıdakı ikili rəqəmlə-rə malikdir [10]:

$$m = 1100101110\ldots$$

Fərz edək ki, açar halında aşağıdakı ardıcıllıq istifadə olunur [10]:

$$k = 1001100111...$$

Hər bir sütundakı rəqəmləri 2 modulu üzrə toplamaqla birdəfəlik lent metodu ilə şifrləməni həyata keçirək [7]:

İlkin mətn m = 1100101110...

Açar ardıcıllığı bitləri k = 1001100111...

---

Şifrlənmiş mətn c = 0101001001...

Bu proses qammanın (açarın) giriş axınının üzərinə qoymağı xatırladır. Birdəfəli lentlə şifrləmə həqiqətən qammalaşdırmadır, lakin indiyədək baxılan kriptosistemlərdən fərqli olaraq onda sonsuz qamma nəzərdə tutulur. Birdəfəli lentdə bütün hərflər eyni tezliklə görünürlər. Ona görə, qammanın hansı sayda işarələri bizə məlum deyilsə, biz növbəti hərfin hansı hərf olacağını deyə bilmərik. Bu onu göstərir ki, qammanın bütün işarələr ardıcıllığı bərabər ehti-mallıdır. Bu o deməkdir ki, Vernam şifrinin köməyi ilə şifrlənmiş məlumat uyğun uzunluqlu istənilən açıq mətnə "deşifrlənə" bilər, çünki, qammanın nəzərdə tutulan işarələr ardıcıllığı, onu istənilən digər ardıcıllıqdan fərqləndirmə xüsusiyyətinə malik deyil [10]. Ver-nam şifrində, daşıyıcı açar verilənləri halında, məhz lentdən istifa-də etmək mütləq deyil. Əsas odur ki, göndəricidə və alıcıda ilkin məlumatın uzunluğundan az olmayan məxfi açar olsun. Problemlər böyük həcmli verilənlərin şifrlənməsi zamanı yarana bilər, çünki, açar rəqəmlərinin ehtiyatı əvvəlcədən informasiya alıcısına çatdırıl-malı və onda saxlanılmalıdır. Tam məxfi sistemlər praktikada real-laşdırılmalıdır. Nə üçün onlar bütün hallarda istifadə olunmur? Bu bir neçə səbəblərlə izah olunur. Birinci, istənilən bağlı açarlı şifr-ləmə sistemləri kimi, onlarda açarların paylanma problemi möv-cuddur. İkinci, tam məxfi sistemlərdə şifrləmə açarının uzunluğu açıq mətnin uzunluğu kimi olmalıdır. Bundan başqa, hər bir mə-lumatı şifrləmək üçün özünün yeni açarı olmalıdır. Bütün bu fak-torlar tam məxfi sistemlərin reallaşdırılmasını çox bahalı edir və bu da çox əlverişli deyil. Belə sistemləri yalnız ən mühüm vacib rabitə xətlərində, məsələn, hökumət rabitə sistemlərində istifadə etmək məqsədəuyğundur.

### 4.4.1.Təklik (yaxud nadirlik) məsafəsi

Əgər kriptoqrafik sistem tam məxfi deyilsə, onda şifrlənmiş məlumat kriptoanalitikə ilkin məlumat haqqında bəzi məlumatlar verə bilər [10]. Mütəxəssiz, ola bilər ki, şifrmətni dərhal deşifrə edə bil-məsin, lakin o, açar yaxud açıq mətn haqqında müəyyən mülahizələr edə bilər. Eyni açarla şifrələnmiş hər bir növbəti məlumatı aldıqdan sonra, kriptoqrafik şifrləmə açarı üzrə öz biliyini artıracaq və şifrlənmiş məlumatı

genişləndirəcək, nəticədə məlumatın şifrəsi-ni açа biləcək. Şennon şifrin təklik məsafəsi U anlayışını verib. Bu anlayışda o, cinayətkar tərəfindən açarın birmənalı bərpa edilməsi üçün şifrlənmiş məlumatda neçə hərfin olmasını göstərir.Təklik məsafəsini hesablamaq üçün açarın entropiyasını H(K) bilmək vacibdir. Simmetrik şifrlər üçün açarın entropiyası təqribən açarla-rın sayının $N_K$ –ın 2 əsası üzrə loqarifmasına bərabərdir, yəni [10]:

$$H(K) = \log_2 N_K$$

Məsələn, rus dilinə tətbiq edilən sadə əvəzləmə şifri üçün, mümkün olan açarların sayı mümkün olan bütün əvəzləmə cədvəllərinin sayı ilə müəyyən edilir və $N_k = 33^! \approx 8{,}68*10^{36}$ kimi təyin edilir, ona görədə açarın entropiyası bərabər olacaq [10]:

$$N(K) = \log_2 8{,}68 * 10^{36} \approx 122{,}7$$

Əgər bizə bəzi şifrlər üçün açarın entropiyası (K) məlumdursa, onda onun üçün təklik məsafəsi U aşağıdakı ifadə ilə təyin olunur [10]:

$$U = H(K) / D,$$

burada D – şifrlənmiş məlumatın artıqlığıdır.

İndi də rus dilinə tətbiq olunan sadə əvəzləmə şifri üçün təklik məsafəsini təyin edək [10]:

$$U = H(K)/D = 122{,}7/3{,}5 \approx 35{,}1,$$

Yəni cinayətkar tərəfindən tutulub saxlanılan şifrlənmiş məlu-matın uzunluğu 35 işarədən çox olur, onda onu hər şeydən əvvəl birmənalı deşifrləmək mümkün olacaq. Əgər şifrlənmiş məlumatın uzunluğu 35 işarədən az olarsa, onda onun birmənalı deşifrə olun-ması mümkün olmayacaq.

Təklik məsafəsi bizə tutulub saxlanılmış şifrmətnin asanlıqla birmənalı deşifrə etmək üçün, onun hansı ölçüdə olmasını göstər-mir, onu göstərir ki, o nə qədər böyük olmalıdır ki, onu birmənalı deşifrə etmək mümkün olsun.

Cinayətkara açarın təyin edilməsini və bizim məxfi məluma-tımızın deşifrə edilməsini çətinləşdirmək üçün, istifadə olunan şifr-də təklik məsafəsini istənilən qədər (bəlkə də sonsuzluğadək) artır-maq vacibdir. Təklik məsafəsinin hesablanması ifadəsini analiz edərək, bu məsələnin iki üsulla həllinin mümkün olmasını təyin etmiş olarıq.

Əgər açarın entropiyası sonsuzluğa bərabərdirsə, onda şifrin tək-lik məsafəsidə sonsuzluğa bərabər olacaq [10]. Açarın uzunluğu böyük olduqca onun entropiyası da böyük olur. Birdəfəli lentin istifadə olunması zamanı açar nəzəri olaraq sonsuz olur və onun bütün işa-rələri bərabər ehtimallıdır, ona görə də belə şifrin entropiyası son-suz qədər böyük olacaq. Buna görə də, Vernam şifrinin təklik məsafəsi sonsuzluğa bərabərdir [10].

Yuxarıda göstərildiyi kimi, sonsuz uzunluqlu açarlı şifri istifadə etmək məqsədəuyğun deyil [10]. Lakin praktikada bəzən şifrləmə açarını dəyişməklə cinayətkarın həyatını çətinləşdirmək olar. Mütəxəssislər elə sistemlərin istifadə olunmasını təklif edirlər ki, onlarda açarın dəyişməsi şifrin vahidlik məsafəsinə çatmadan baş versin. Buna seans şifrləmə açarını tətbiq etməklə, yəni hər bir məlumatın şifrlənməsi üçün yeni açarın istifadə olunması ilə nail olmaq olar.

Vahidlik məsafəsinin artırılmasının ikinci üsulu ilkin mətnin artıqlığının azadılmasından ibarətdir. Əgər məlumatın artıqlığı sıfra bərabərdirsə, açar heç vaxt təyin olunmayacaq və şifrəli məlumat açılır, çünki təklik məsafəsi sonsuza bərabər olacaq [10]. Təəssüf ki, pr-aktikada belə bir vəziyyət qeyrimümkündür, çünki hər hansı mənalı məlumat sıfırdan fərqli artıqlığa malik olacaq. Lakin məlumatda artıqlığın azaldılması verilənlərin sıxılması hesabına mümkündür. İş ondadır ki, verilənlərin sıxılması zamanı mətnin "sıxılmış" entro-piyası saxlanılır, uzunluğu isə azalır. Buna görə, sıxılmış mətndə bir hərfə düşən entropiya ilkin mətndə olan entropiyaya nisbətən böyükdür, artıqlıq isə azdır. Belə ki, sıxıcı kodlaşdırmadan sonra şifrin vahidlik məsafəsi artır.

### 4.5. Şifrləmə, maneədavamlı kodlama və informasiyanın sıxılması

Vericidən qəbulediciyə informasiyanın ötürülməsi prosesində informasiyaya mənfi faktorlar təsir edir [10]. Kriptoqrafik üsullar informasiyanı yalnız bir növ dağıdıcı təsirdən, yəni qəsdən məhv etməkdən və ya informasiyanın təhrif olunmasından qoruyur. Lakin praktikada informasiyanın bir abonentdən digərinə ötürülməsi zamanı

rabitə xəttində təsadüfi maneə, səhvlər, aparatların imtina etməsi və məlumat daşıyıcılarının qismən məhv edilməsi və s. mümkündür. Beləliklə, real rabitə sistemlərində informasiyanın təsadüfi təsirlər-dən mühafizəsi mövcuddur.

Yüksək buraxıcılıq qabliyyətinə malik olan verilənlərin ötürülməsinin və multimediya texnologiyalarının meydana gəlməsi ilə böyük həcmli informasiyanın şifrlənməsi problemi yaranır [10].

Əvvəllər şifrələnmiş və ötürülən məlumatların əsas növü mətn məlumatları idisə, XXI əsrdə kriptoqrafik mühafizə rəqəmli video və səsli məlumatların ötürülməsi, ərazi xəritələri və videokonferen-siyaların verilməsindən daha çox istifadə olunmuşdu. Məhz buna görə son vaxtlar böyük informasiya massivlərinin şifrlənməsi prob-lemi yaranır. Telekonferans, audio və ya video rabitə kimi inte-raktiv sistemlər üçün bu cür şifrləmə real vaxtda həyata keçiril-məlidir və mümkünsə istifadəçilər üçün görünməməlidir. Bu prob-lemlərin həlli, o cümlədən icazəsiz daxilolmadan mühafizə, infor-masiya nəzəriyyəsinin nailiyyətlərindən kompleks istifadə etməklə əldə edilə bilər. Prinsipcə, informasiya nəzəriyyəsində informa-siyanın çevrilməsi üçün üç növ çevirmə üsulu var [10]: kriptoqrafik şif-rələmə, maneədavamlı kodlama və sıxılma.

İyirminci əsrin bəzi elmi işlərində məlumatların çevirmə üsul-larının üçü də kodlaşdırma adlandırılırdı [10]: kriptoqrafik kodla-ma, maneədavamlı kodlama və səmərəli kodlama (verilənlərin sıxılma-sı). Ümumiyyətlə bütün üç növ çevirmə nəticəsində məlumatların bu və ya digər şəkildə təqdimat forması dəyişir, amma mənası dəyişmir. Müxtəlif növ kodlaşdırmaların biri-birindən fərqi aparılan çevirmələrin məqsədilə bağlıdır.

Beləliklə, kriptoqrafik çevirmənin məqsədi, məlum olduğu kimi, icazəsiz daxilolmadan mühafizə, audentifikasiya və qəsdən edilən dəyişikliklərdən mühafizədir.

Maneədavamlı kodlamanın məqsədi veriliş zamanı informasi-yanı və onun saxlanmasını təsadüfi maneələrdən mühafizə etmək-dir [10]. Effektiv kodlama ötürülən və saxlanılan verilənlərin həcmini minimallaşdırmaq məqsədilə aparılır. Praktikada bu üç növ çevirmə

birlikdə istifadə olunur. Belə ki, məsələn, şifrələmədən əvvəl proqram paketləri emal olunan verilənləri arxivləşdirir. Digər tərəf-dən, istər lokal istərsə də qlobal verilənlərin ötürülməsi şəbəkələrin, yaxud informasiyaların kompüter daşıyıcılarının (CD və ya DVD) tərkibində həmişə informasiyanın mühafizə sistemləri, nəzarət vasi-tələri və təsadüfi səhvlərin korreksiyası qurğuları olur.

Beləliklə, kriptoqrafik şifrələmə, maneədavamlı kodlama və sı-xılma qismən bir-birini tamamlayır və onların kompleks istifadə olunması ötürülən informasiyanın etibarlı mühafizəsi üçün rabitə ka-nallarının effektiv istifadə olunmasına kömək edir. Praktikada kriptoqrafik metodların daha səmərəli şəkildə istifadə edilməsi üçün informasiyanın mühafizə sistemlərində istifadə olunan maneə davamlı və effektiv kodlamanın əsas müddüalarına baxaq.

### 4.5.1.Maneədavamlı kodlama

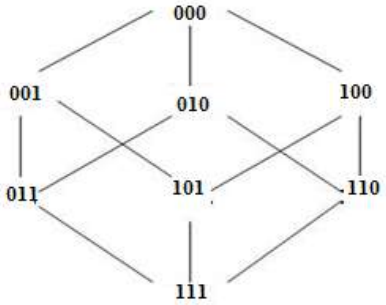
Qeyd olunduğu kimi, informasiyanın kriptoqrafik çevirmə məsə-lələri məlumatın maneədavamlı kodlama məsələləri ilə sıx bağlıdır [10]. Bu onunla bağlıdır ki, bir tərəfdən (nəzəri olaraq), kriptoqrafik şif-rələmə və maneədavamlı kodlama zamanı informasiya nəzəriyyəsinin eyni qanunları istifadə olunur. Digər tərəfdən (prak-tiki olaraq) informasiyanın yığılması, saxlanması və ötürülməsi prosesləri sax-lanılan və emal olunan verilənləri təhrifə uğratmaq qabliyyətinə malik olan maneənin təsiri altında həyata keçirilir. Bu, səhvləri aşkarlamağa və düzəldilməsinə imkan verən metodların işlənməsi və istifadə edilməsini daha da aktuallaşdırır. Riyazi baxımdan bu məsələ maneədavamlı kodlamanın sintezinə gətirib çıxarır. Kriptoqrafiyada şifrləmə anlayışına analoji olaraq maneə-davamlı kodlamanın və sıxılma məsələlərinin müzakirəsi zamanı kod anlayışını daxil edirlər. Ümumiyyətlə, işarələr yığımına, eləcə də məlumatın bu cür simvollar şəklində təqdim edilməsinə imkan verən qaydalar sisteminə kod deyilir [10].

### 4.5.2. Kod sözü

Buraxıla bilən (icazəli) işarələrin hər hansı bir sırasına kod deyilir. Məsələn, 1100 ikili ədədini ikili 4-bitli kod sözü hesab etmək olar. Maneədavamlı kodlamanın ümumi ideyası bütün müm-kün olan kod sözündən hamısı icazəli deyil, yalnız onlardan bəziləri icazəlidir. Məsələn, cütlüyə yoxlama kodunda tərkibində yalnız cüt vahid olan sözlər etibarlı sayılır. Səhv, etibarlı bir sözü yararsız hala çevirir və buna görə də aşkar edilir. Manedavamlı kodlar informasiyanı sabit uzunluqlu fraqmentlərə bölən və onların hər birini ayrı-ayrılıqda emal edən blok kodlarına bölünürlər. Maneədavamlı kodlar blok və burulmuş kodlara bölünürlər [10]. Blok kodları minimal kod məsafəsi ilə xarakterizə olunurlar. Ümu-miyyətlə, iki kod sözü arasındakı amerika riyaziyatçısı R.U.Xem-minqin adı ilə adlanan Xemminq məsafəsi müxtəlif işarələrin sayı-dır. Bu zaman minimal kod məsafəsi bütün Xemminq məsafələrindən ən azı seçilir [10].

Məsələn, biz yalnız üç rəqəmli ikili sözlərdən istifadə edirik. Belə kod sözlərinin sayı səkkiz ola bilər. Yalnız bir vahidlə fərq-lənən kod sözlərinə qonşu olanlar adlanırılır. Məsələn, 101 və 111 kod sözləri yalnız orta işarə ilə fərqlənirlər, 101 və 110 sözləri qonşu deyillər, çünki, onlarda yalnız iki son işarələr fərqlənirlər.

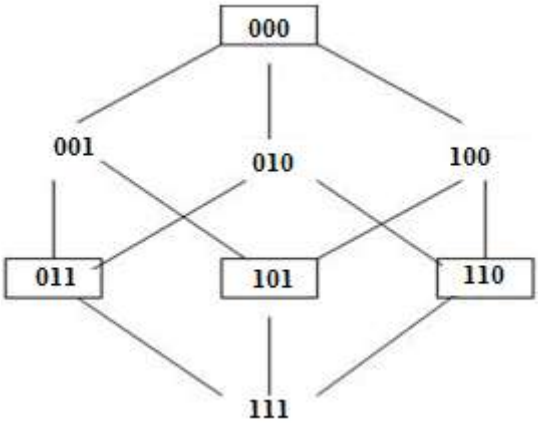
Bütün üç işarəli ikili kombinasiyanı və qonşu kod sözlərini xətlə birləşdirək. Onda biz şəkil.5.1-də göstərilən sxemi alarıq [10]. Sözlər arası minimal kod məsafəsi adi qeyri maneədavamlı məlu-mat üçün kod məsafəsi vahidə bərabərdir.




**Şək. 4.1.** Üçişarəli ikili kod sözü

Məlumatların verilməsi üçün bütün üçişarəli ikili sözlərinin isti-fadə olunması zamanı onların hamısı icazəli sayılır. Cütlüyə yoxla-ma şərti üzrə nəzarəti istifadə edək. Onda yalnız çərçivə ilə ayrılan cüt vahidli sözlər icazəli olacaq (şək.4.2) [10].

Cütlüyə yoxlanılan kodun icazəli sözləri arasındakı minimal məsafə ikiyə bərabərdir (şək.4.2-dən görünür ki, çərçivədə olan heç bir kod sözü xətlə birləşməyib, yəni qonşu deyillər). Məhz bu səbəbdən də kod sözündəki bir səhv bu sözü qəbul edilə bilməz hala gətirir. Ona görə də maneədavamlığı artırmaq üçün sözlərin uzunluğunu adi koda nisbətən artırmaq vacibdir. Bu misalda yalnız iki işarə informasiyalı işarələrdir. Onlar dörd müxtəlif sözlər əmələ gətirirlər. Üçüncü işarə nəzarət edicidir və icazəli sözlər arasındakı




**Şək.4.2.** Cütlüyə görə nəzarət edilən icazəli üçişarəli kod sözü

məsafəni artırmaq üçündür. Nəzarət edici işarə informasiyalı işarə-lərdən xətti asılı olduğu üçün informasiya verilişində iştirak etmir. Misal halında baxılan cütlüyə yoxlanılan kod verilənlərin ötürül-məsində verilənlər blokunda birqat səhvləri aşkar edir. Lakin, ikiqat səhvləri aşkar edə bilmir və kod sözünü digər icazəli sözə çevirir.

Beləliklə, səhvlərin aşkarlanması və düzəldilməsi qabliyyətini əldə etmək üçün kodun artıqsızlığından imtina etmək vacibdir. Bu-nun üçün ikili işarələrin bütün mümkün olan kombinasiyalarını iki altçoxluğa bölürlər: icazəli kod sözlərinə və icazəsiz kod sözlərinə. Bölmə icazəli

sözlər arasındakı minimum kod məsafəsini ar-tırmaq kimi bir şəkildə aparılır. Bu halda istənilən birqat səhvlər icazəli kod sözlərini icazəsiz kod sözünə çevirir ki, bu da birqat səhvləri

aşkar etməyə imkan verir.

Təbiidir ki, artıq nəzarət işarələrinin əlavə edilməsi kodlaşdı-rılmış informasiyanın saxlanılmasına yaxud verilişinə xərcləri artı-rır. Bu zaman faydalı informasiyanın faktiki həcmi dəyişməz qalır. Bu halda maneədavamlı kodun artıqlığı haqda danışmaq olar və onu formal olaraq nəzarət işarələrinin sayının kod sözünün ümu-mi işarələrinin sayına nisbəti ilə təyin etmək olar. Yuxarıda deyil-diyi kimi nəzarət işarələri informasiya vermir və bu mənada fayda-sızdır. Nəzarət işarələrinin nisbi sayına maneədavamlı kodun artıq -

lığı deyilir və aşağıdakı ifadə ilə təyin edilir [10]:

$$Q = (k/n)*100\%,$$

burada n – blokdakı ikili işarələrin ümumi sayı, k-isə nəzarət işarə-lərinin sayıdır.

Məsələn, cütlüyə yoxlanılan üçişarəli kodun artıqlığı bərabərdir [10]:

$$Q = (k/n)*100\% = (1/3)*100\% \approx 33\%$$

Artıqlıq kodun əhəmiyyətli bir xarakterikasıdır və artıqlıq həd-dindən artıq artım arzuolunmazdır. İnformasiya nəzəriyyəsinin vacib məsələsi tələb olunan aşkarlama və korrektə edici qabliyyətini təmin edən kodun sintezidir. Misal halında bir qat səhvləri aşkar edən və düzəldən sadə kodlardan biri olan Xemminq koduna baxaq. Fərz edək ki, uzunluğu n olan kod sözü k informasiyalı və m nəzarət edici işarələrə malikdir. Təhrif olunan i-ci işarənin korrek-siyası qəbul olunan kod sözünün i-ci işarəsində vahid olan $0\ldots 010\ldots 0$, vektorla 2 modulu üzrə toplanmasından ibarətdir. n- işarəli kod sözü üçün birqat səhvlərə uyğun olan n sayda vektor və səhfsiz sözün qəbulu halına uyğun olan bir sıfır vektoru mövcuddur. Beləliklə, m sayda nəzarət işarələri n+1 səhv vektorunu formalaşdırmalıdır, yəni $n \leq 2^m$- 1bərabərsizlik yerinə yetirilməlidir. Nəticədə Xemminq kodu adlanan ($2^m$-1, $2^m$-1-m) kod alınır. m =3-ə uyğun olan ən sadə qeyrişəffaf vəziyyət (7,4) kodunu yaradır, hansınıkı aşağıdakı kimi sintez etmək olar. Hər bir səhv vektoruna sıra nömrəsi-sindrom verək (cədvəl 4.1). Bu zaman sıfır

vektoruna sıfır sindromu uyğun gəlir. $s_i$ funksiyasına kod sözünün işarələrinin

2 modulu üzrə toplanması kimi baxsaq, alarıq [10]:

$$s_0 = a_0 \bigoplus a_3 \bigoplus a_5 \bigoplus a_6 s_1 = a_1 \bigoplus a_3 \bigoplus a_4 \bigoplus a_6 s_2 = a_2 \bigoplus a_3 \bigoplus a_4 \bigoplus a_5$$

İşarələrin birində səhv yaranan zaman $s_1$ funksiyası vahidə, səh-vin olmaması zamanı isə sıfra çevrilir. Bu tələbin təmin olunması cədvəl 4.1-də vrilib [10].

**Cədvəl.4.1. Səhv vektorları və ona uyğun sindromları**

| $a_6$ | $a_5$ | $a_4$ | $a_3$ | $a_2$ | $a_1$ | $a_0$ | $s_2$ | $s_1$ | $s_0$ |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

üçün işarələrin bir hissəsi xüsusi şəkildə formalaşdırılır.Xüsusilə $a_0$, $a_1$, $a_2$ sıralarına uyğun tənliklərdə iştirak edən yerdə qalan işarələrin 2 modulu üzrə çevirməsi kimi baxmaq olar [10]:

$$a_0 = a_3 \bigoplus a_5 \bigoplus a_6 a_1 = a_3 \bigoplus a_4 \bigoplus a_6 a_2 = a_3 \bigoplus a_4 \bigoplus a_5$$

Tapılan asılılıqlar bizə verilmiş məlumatlar üçün kod sözləri yaratmağa və alınan kod sözləri üçün sindromları hesablamağa im-kan verir. Fərz edək ki, çıxış informasiyalı söz 1101-ə bərabərdir, yəni $a_6$=1,$a_5$=1,$a_4$=1,$a_3$=1. Onu (7.4) maneəlavamlı Xemminq ko-dunun icazəli kod sözünə çevirmək üçün yuxarıda tapılan asılılıq üzrə nəzarət işarələrini hesablayırıq [10]:

$$a_1 = 1 \bigoplus 0 \bigoplus 1 = 1 a_1 = 1 \bigoplus 0 \bigoplus 1 = 0 a_2 = 1 \bigoplus 0 \bigoplus 1 = 0$$

Nəzarət işarələrini nəzərə almaqla kod sözü 110100 -ə bərabər olacaq. Əgər veriliş yaxud saxlanma prosesində təhrifsiz söz qalıb-sa, onda onun $s_0 \ldots s_2$ sindromu uyğun olaraq bərabər olacaq [10]:

$$s_0 = 1 \oplus 1 \oplus 1 \oplus 1 = 0, s_1 = 0 \oplus 1 \oplus 0 \oplus 1 = 0, s_2 = 0 \oplus 1 \oplus 0 \oplus 1 = 0$$

Sıfırlardan ibarət olan sidrom, səhvin olmamasını göstərir və səhvin sıfır vektoruna uyğun olur.

Fərz edək ki, veriliş və saxlanma proseslərində xarici faktorların təsiri nəticəsində kod sözünün təhrif olunmuş ayrıca işarəsi qalıb. Məsələn, 1101 001sözün yerinə 1001 001 sözü qəbul olunub. Bu halda sindrom sıfırdan fərqli olacaq: $s_0 \ldots s_{2\text{-}i}$ uyğun olaraq aşağı-dakı kimi təyin olunacaq [10]:

$$s_0 = 1 \oplus 1 \oplus 0 \oplus 1 = 1, s_1 = 0 \oplus 1 \oplus 0 \oplus 1 = 0, s_2 = 0 \oplus 1 \oplus 0 \oplus 0 = 1$$

101 sindromu 0100 səhv vektoruna uyğundur, bu zaman vahid səhvin baş verdiyi işarəni göstərir. Sonra onun korreksiyası üçün 2 modulu üzrə təhriflə qəbul olunmuş sözü 2 modulu üzrə səhv vek-toru ilə toplamaq kifayətdir.

İndi də (7.4) Xemminq kodunun artıqlığını hesablayaq [10]:

$$Q = (k/n)*100\% = (7-4)/7)* 100\% \approx 43\%$$

Bu çox böyük qiymətdir. Praktikada az artıqlığa və yaxşı maneədavamlıq xarakteristikalarına malik olan,eləcə də əhəmiyyətli dərəcədə daha mürəkkəb olan kodlar istifadə olunur.

### 4.6. Verilənlərin sıxılma prinsipləri

Yuxarıda qeyd edildiyi kimi, şifrələmə üçün məlumatların ilkin hazırlanmasının vacib vəzifələrindən biri onların artıqlığını azalt-maq və tətbiq olunan dilin statistik qanunlarını uyğunlaşdırmaqdır [10]. Artıqlığın qismən aradan qaldırılması verilənlərin sıxılması yolu ilə əldə edilir. İnformasiyanın sıxılması özündə ilkin məlu-matın bir kod sisteminsdən digərinə çevirməkdir ki, bunun da nəticəsində məlumatın ölçüsü azalır. İnformasiyanın sıxılması üçün istifadə olunan alqoritmlərini iki böyük qrupa bölmək olar [10]:

sıxılmanı itgisiz reallaşdıran (tərs çevrilə bilən sıxılma) və sıxıl-manı itgi ilə reallaşdıran (geri dönməz sıxılma) alqoritmlərə.

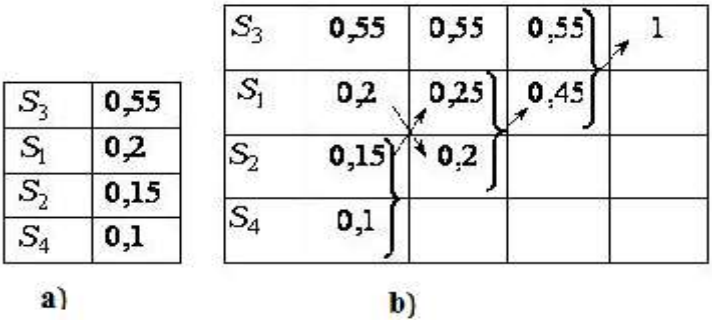
Tərs çevrilə bilən sıxılma, dekodlamadan sonra məlumatların tamamilə dəqiq bərpasını nəzərdə tutur və istənilən məlumatı sıx-maq üçün istifadə edilə bilər. O həmişə çıxış məlumatın informa-tivliyini dəyişdirmədən, yəni informasiya quruluşunu itirmədən çı-xış informasiya axınlarının həcminin azalmasına gətirib çıxarır.

Tərs çevrilə bilən sıxılma fayllar, yüksək keyfiyyətli səs və qra-fik şəkilli mətnlər üçün istifadə olunur. Geri dönməz sıxılma adətən itgisiz kodlaşdırma ilə müqayisədə daha yüksək sıxılma dərəcəsinə malikdir, lakin dekodlaşdırılmış verilənlərin ilkin verilənlərə nisbə-tən bəzi dönmələrə yol verir. Praktikada çoxlu sayda praktiki məsə-lələr var ki, onlarda sıxılmadan sonra ilkin informasiyanın dəqiq bərpa olunmasına qoyulan tələblərə rəyat edilməsi məcburi deyil. Bu, xüsusilə multimediya informasiyalarının sıxılmasına aiddir. Məsələn, multimediya informasiyalarının JPEG və MPEG kimi formatları geniş istifadə olunur və bu sistemlərdə geri dönməz sı-xılma tətbiq edilir. Geri dönməz sıxılma adətən kriproqrafik şifrləmə ilə birgə istifadə edilmir, çünki bu kriptosistem üçün əsas tələb deşifrələnmiş verilənlərin ilkin məlumatla eyni olmasıdır. Lakin, multimedia texnologiyasından istifadə edərkən rəqəmli formada təqdim edilən məlumatlar şifrələmə üçün kriptoqrafik sistemə daxil edilməzdən əvvəl tez-tez geri dönməz sıxılmaya məruz qalır. Məlu-mat istifadəçilərə verildikdən və deşifrələmədən sonra multimedia faylları bərpa edilmir.

Tərs çevrilə bilən sıxılmanın ən geniş yayılmış üsullarından bəzilərini nəzərdən keçirək. Onlardan ən geniş yayılmışı Xofman kodudur. Bu kodun koderi və dekoderi kifayət dərəcədə sadə aparat reallaşmasına malikdir. Alqoritmin ideyası aşağıdakılardan ibarətdir: işarələrin məlu-mata daxil olma ehtimallarını bilməklə, bitlərin tam sayından ibarət olan dəyişən uzunluqlu kodların qurulma prosedurnu təsvir etmək olar. Böyük ehtimallı işarələrə daha qısa, az-az görünən işarələrə isə daha böyük kodlar verilir.

Bunun sayəsində kod sözünün orta uzunluğu ixtisar olunur və sıxılmanın böyük effektivliyi əldə edilir. Xofman kodu nadir pre-fiksə

(kod sözünün başlığı) malikdir və onların dəyişkən uzunlu-ğuna baxmayaraq, onların birmənalı dekodlanmasına imkan verir. Klassik Xofman kodunun sintez proseduru, məlumat mənbəyinin statistik xarakteristikaları haqqında aprior informasiyanın olmasını təhmin edir. Sadə misal timsalında Xofman kodunun sintezinə baxaq. Fərz edək ki, informasiya mənbəyi yaranma ehtimalı $p(S_1) = =0,2$, $p(S_2) = 0,15$, $p(S_3) = 0,55$, $p(S_4) = 0,1$olan dörd müxtılif $S_1 \ldots S_4$ işarə hasil edir. Ehtimalın azalan sırası ilə işarələri seçək və onlardan cədvəl tərtib edək (cədvəl.4.2a). Kodun sintez proseduru üç əsas mərhələdən ibarətdir [10]:



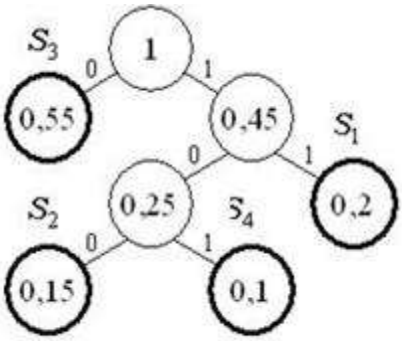

**Şək.4.2.** Xofman kodlamasının birinci mərhələsi

Birinci mərhələdə cədvəlin sətrinin əvəzlənməsi həyata keçirilir: ən kiçik ehtimalla yaranan işarələrə uyğun olan iki sətr bir ümumi ehtimalla əvəzlənir, bundan sonra cədvəl yenidən sıralanır. Əvəzlə-mə, cədvəldə yalnız bir ümumi ehtimallı sətr olana qədər davam edir (şək4.2b).

İkinci mərhələdə əvəzləmə cədvəli üzrə kod ağacının qurulması həyata keçirilir (şək.4.3a) [10]. Ağac cədvəlin axırıncı sütunundan baş-layaraq qurulur.

Ağacın kökü sonuncu sütunda yerləşən bir vahid təşkil edir (şək.4.3a). Baxılan misalda bu vahid ağacın kökü ilə əlaqəli iki qovşaq şəklində təsvir edilmiş 0,55 və 0,45 ehtimallarından yaradı-lır. Onlardan birincisi $S_3$ işarəsinə uyğundur və beləliklə, bu qovşa-ğın sonrakı budaqlanması baş vermir. 0,45 markerlənmiş ehtimalı ilə ikinci qovşaq, 0,25 və 0,2 ehtimalı ilə üçüncü səviyyənin iki qovşağı ilə birləşir. 0,2 ehtimalı $S_1$ işarəsinə uyğun gəlir, 0,25 ehti-malı isə öz növbəsində,

0,15 ehtimalı ilə $S_2$ işarəsinin gəlişini, 0,1ehtimalı ilə $S_4$ işarəsinin gəlişini təmin edir.Kod ağacının ayrı-




| | |
|---|---|
| $S_1$ | 11 |
| $S_2$ | 100 |
| $S_3$ | 0 |
| $S_4$ | 101 |

b)

**Şək.4.3.** Xofman kodlamasının ikinci mərhələsi ayrı qovşaqlarını birləşdirən qabırqalar 0 və 1 rəqəmləri ilə nömrə-lənirlər (məsələn,sol qabırqa-"0"-la, sağ qabırqa isə 1-lə).

Üçüncü son mərhələdə, cədvəl qurulur və bu cədvəldə mənbə işarələri və onlara uyğun Xofman kodunun kod sözləri tutuşdu-rulur. Bu kod sözləri ağacın kökündən uyğun işarələrə yol təşkil edən qabırqaların qeyd olunduğu rəqəmləri oxumaqla yaradılır. Baxılan misal üçün Xofman kodu şək.4.3b-də verilən cədvəldə göstərilən şəkil alır. Lakin klassik Xofman alqoritmi bir çatışmayan cəhətə malikdir. Sıxılmış bir məlumatın məzmununu bərpa etmək üçün dekoder kodlayıcı tərəfindən istifadə olunan tezlik cədvəlini bilməlidir. Buna görə, sıxılmış məlumatın uzunluğu məlumatların qaba-ğında göndərilən tezlik cədvəlinin uzunluğu ilə artır, bu da məlu-matı sıxmaq üçün bütün səyləri sıfra yendirə bilər.

Xofmanın statistik kodlamasının digər variantı giriş axınına bax-maq və yığılmış statistika əsasında kodlamanın qurulmasından iba-rətdir. Bu zaman fayl üzrə iki yanaşma tələb olunur [10]: biri bax-maq üçün və statistik informasiyanın toplanması, ikinci kodlama üçün. Xofmanın statistik kodlamasında giriş işarələri (müxtəlif uzunluqlu bitlərin zəncirləri) kimi bitlərin zəncirlərinə uyğun, onla-rın dəyişən uzunluqlu kodları qoyulur. Hər bir işarənin kodunun uzunluğu ikili loqarifmaya

proporsional onun əks işarəli tezliyi götürülür. Bütün rast gəlinən işarələrin ümumi yığımı axının alifba-sını təşkil edir.

Xofmanın adaptiv və dinamik kodlama kimi digər metodu da mövcuddur. Onun ümumi prinsipi giriş axınının xarakterinə uyğun olaraq kodlama sxemini dəyişdirməkdir [10].

Bu yanaşma bir keçidli alqoritmə malikdir və istifadə edilən kodlaşdırma barədə açıq şəkildə məlumat saxlamağı tələb etmir.

Giriş axınının tezliyinin dəyişməsi tam nəzərə alınması sayə-sində adaptiv kodlaşdırma statistik kodlaşdırmaya nisbətən daha yüksək dərəcədə sıxılma dərəcəsi verə bilir. Xofman kodlaşdırma-sını istifadə edərkən, alqoritmin komplikasiyası giriş axınındakı dəyişən statistikaya əsasən əlifbanın ağacını və xarakter kodlarını daim tənzimləməyə ehtiyac olur.

Xofmanın adaptiv kodlaşdırılmasından istifadə edilən zaman alqoritmin mürəkkəbləşdirilməsi ağacın və əsas əlifbanın işarələri-nin kodlarının giriş axınının dəyişən statistikasına uyğun olaraq daimi korreksiya edilməsi vacibliyindən ibarətdir [10].

Xofmanın üsulları kifayət qədər yüksək sürətli və orta səviyyədə yaxşı sıxılma keyfiyyətini təmin edir. Lakin Xofman kodlaşdırıl-ması minumum artıqlığa malikdir [10].

Əlifba kodlaşdırması ilə tamamilə fərqli bir həll təklif olunur. Bu metod, giriş axınının üzən nöqtəli bir ədədə çevrilməsi ideya-sına əsaslanır. Əlifba kodlaşdırılması, giriş əlifbasının işarələrini bu işarələrin tezliyinin paylanmasının məlum olması şərtində itgisiz olaraq qablaşdırlması metodudur.

Baxılan üsullar, verilənlərin geri dönməz sıxılmasını təmin edir. Praktikada onların reallaşdırılmasının həm proqram və həm də apa-rat reallaşdırılması istifadə olunur. Belə reallaşdırmalar sıxılma əmsallarının 20-40% qiymətini əldə etməyə imkan verir.

Beləliklə, kriptoqrafik şifrələmə, maneədavamlı kodlaşdırma və sıxılma bir-birini tamamlayır və onların kompleks istifadə olunması ötürülən verilənlərin etibarlı mühafizəsi üçün kommunikasiya ka-nallarından səmərəli istifadə etməyə imkan verir.

# V FƏSİL. VPN TEXNOLOGİYASI BAZASINDA LOKAL KOMPÜTER ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA MÜHAFİZƏSİNİN TƏŞKİLİ

## 5.1. VPN texnologiyası bazasında Lokal kompüter şəbəkələrinin qurulması

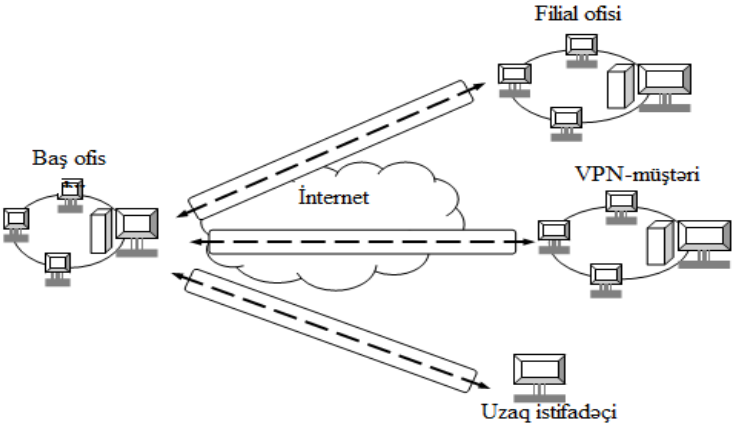
Lokal kompüter şəbəkələrində informasiya mühafizəsinin təşkili üçün VPN texnilogiyasından istifadə edən zaman virtual tunelin qurulması və bu tunelə kənar istifadəçilərin daxil ola bilməməsi əsas şərtlərdəndir [11]. Virtual tunelin üstün cəhəti baha başa gələn ayrılmış kanallar əvəzinə yüksək sürətli İnternet kanallarından isti-fadə edilməsidir ki, bu da maliyə vəsaitlərindən qənatlə istifadə olunmasına gətirib çıxarır. Maliyə vəsaitlərinə edilən qənaət isteh-salat müəsisələrinə informasiya mühafizəsinin təşkili üçün VPN texnologiyasından istifadə edilməsinə geniş imkanlar yaradır.

Lokal kompüter şəbəkələrinin qlobal açıq şəbəkələrə qoşulması zamanı aşağıdakı təhdidlər yaranır [11]:

- lokal kompüter şəbəkələrinin avadanlıqlarına icazəsiz daxil olmanın yaranması;
- qlobal açıq şəbəkə üzrə verilənlərin ötürülməsi prosesində, onların resurslarına icazəsis daxil olma.
- Qlobal açıq şəbəkələrin bütövlükdə və onların qarşılıqlı əlaqədə olduqları kompüterlərin informasiya təhlükəsizliyinin təmin etmək üçün iki yanaşmadan istifadə olunur [11]:
- lokal kompüter şəbəkəlrə və onların qarşılıqlı əlaqədə olan kompüterlərinə xarici istifadəçilərn icazəsiz daxil olmalarının qarşısının alınması;
- lokal kompüter şəbəkələri üzrə verilənlərin ötürülməsi zamanı rabitə kanallarının mühafizəsinin təşkil.

Lokal kompüter şəbəkələrə və onların qarşılıqlı əlaqədə olan kompüterlərinə xarici istifadəçiərin icazəsis daxil olmalarının qarşısının alınması üçün şəbəkə arası ekranlardan istifadə olunur. Bu ekran adətən lokal kompüter şəbəkələri və qlobal açıq şəbəkə-lərinin arasında fəaliyyət göstərir. Qlobal açıq şəbəkəyə qoşulmuş uzaq kompüteri xarici

istifadəçilərin icazəsis daxilolmalarından qorumaq üçün bu kompüterdə personal ekran adlandırılıan şəbəkə arası ekranının proqram təminatı yerləşdirilir. Verilənlərin rabitə kanalı üzrə ötürülməsi zamanı, onun mühafizəsi VPN texnolo-giyasının istifadə olunması ilə həyata keçirilir. Lokal kompüter şəbəkələrinin və onların çoxsaylı kompüterlərinin xarici mühitlə birləşməsi virtual şəxsi şəbəkəsini VPN yaradır. Bu şəbəkə, VPN tuneli adlanan açıq rabitə kanalı bazasında yaradılır və bu tunelin köməyi ilə mərkəzi ofisi, biznes partnyorlarının ofislərini, uzaq istifadəçilərin birləşməsini təmin edir, eləcə də İnternetin köməyi ilə verilənlərin təhlükəsiz ötürülməsinə imkan yaradır. VPN tuneli üzrə ötürülən verilənlərin mühafizəsi qarşılıqlı əlaqədə olan istifa-dəçilərin audentifikasiyasına, onların kriptoqraf şifrlənməsinə, hə-qiqiliyinin və eləcə də bütövlülüyünün yoxlanılmasına əsaslanır [11]. Bu funksiyaların reallaşdırılması üçün effektivliyi simmetrik və asimmetrik kriptoqrafik sistemlərin birgə istifdə olunması ilə təmin olunan kriptoqrafik mühafizə üsullarından istifadə olunur. Lokal kompüter şəbəkələrinin xarici mühitlə birləşməsi əsasında yaradılan virtual şəxsi şəbəkələrin struktur sxemi şəkil 5.1-də veri-lib.



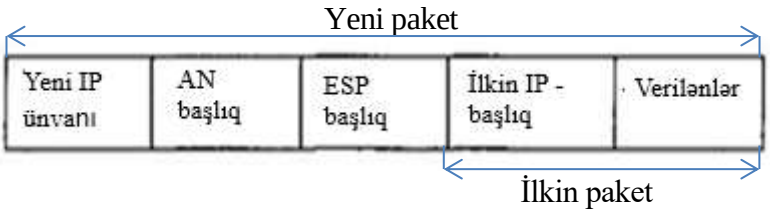

**Şək. 5.1.** Lokal kompüter şəbəkələrinin xarici mühitlə birləşməsi əsasında yaradılan virtual şəxsi şəbəkələrin struktur sxemi

Bu şəbəkənin tərkibində fəaliyyət göstərən VPN- müştəri trafi-kinin şifrlənməsi və audentifikasiyası üçün modifikasiya edilmiş proqram və proqram – aparat vasitələrindən istifadə edilir, hansılar ki, xarici mühitin mühafizəsini təmin edir, eləcə də mobil istifadə-çilərlə mühafizə olunmuş birləşməni həyata keçirir. VPN-in təhlü-kəsizlik şlüzü iki şəbəkə arasında fəaliyyət göstərən və çoxsaylı xostlar üçün şifrləməni və audentifikasiyanı təmin edən qurğudur. VPN şlüzü lokal kompüter şəbəkəsi və qlobal açıq şəbəkə arasında elə yerləşdirilir ki, ondan lokal kompüter şəbəkəsi üçün təyin olunmuş bütün trafiklər keçə bilsin və şəbəkələr arasında xətlərin ayrılmasını təmin etsin. Bu şlüz həm proqram, həm aparat qurğusu, həm marşrutlayıcı kimi və həm də şəbəkə arası ekran şəklində real-

laşdırılır. Bu zaman şəbəkələrin qarşılıqlı əlaqəsini təmin etmək üçün xarici veriliş mühiti həm sürətli İnternet şəbəkəsi və həm də sürətsiz telefon şəbəkəsinin kanalları kimi reallaşdırılır.

Virtual şəxsi şəbəkənin VPN maliyə cəhətdən səmərəliliyi açıq rabitə kanalının mühafizə olunma dərəcəsi ilə təyin edilir. Qlobal şəbəkə üzrərindən informasiyaların təhlükəsiz ötürülməsi, onların inkapsulyasiya edilməsi və tunelləşməsindən istifadə edilməklə həyata keçirilir. Bu zaman informasiyaların təhlükəsiz ötürülməsi məqsədilə şəbəkənin verici və alıcı cütlüyü arasında onları, xidməti sahəsi ilə birlikdə yeni "konvertə" qablaşdıran xüsusi tunel qurulur, hansı ki, aşağı səviyyəli protokolun paketini daha yüksək protoko-lun paketinin verilənlər sahəsinə yerləşdirir.

Şəbəkənin verici və alıcı cütlüyü arasında yerləşdirilən bu tunel verilənləri yalnız icazəsiz daxilolmalardan və təhriflərdən mühafizə etmir, o həm də tunelləşmə vasitəsilə inkapsulyasiya olunmuş giriş paketlərinin tam kriptoqrafik mühafizəsini həyata keçirir. Ötürüləcək verilənlərin məxfiliyini təmin etmək üçün verici giriş paketlərini şifrələyir, IP-başlıqları ilə onları yeni paketə qablaşdırır və tranzit şəbəkə üzrə alıcıya göndərir. Xüsusi tunel vasitəsilə ötürülən paketin bir nümunəsi şəkil 5.2-də verilib. Xüsusi tunelin əsas xüsusiyyəti yalnız verilənlər sahəsini şifrələməkdən ibarət deyil, həm də başlıqla birlikdə giriş paketlərini bütövlükdə şifrələməkdən ibarətdir.



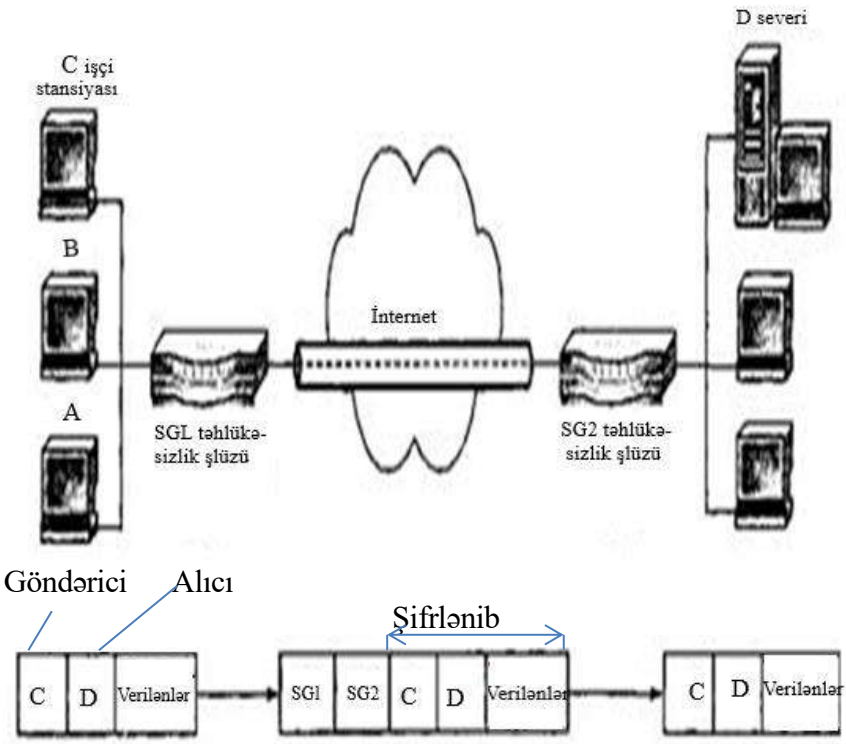

**5.2. Xüsusi tunel vasitəsilə ötürülən paketin bir nümunəsi**

Xüsusi tunelin əsas xüsusiyyəti, cinayətkarın başlıq sahəsində olan vacib informasiyadan (alt şəbəkələrin və qovşaqların sayı və onların IP ünvanları) giriş paketinin şifrəsini açmaq üçün istifadə edə bilməməsidir, hansı ki, çox böyük əhəmiyyət kəsb edir.

Qeyd etmək vacibdir ki, başlığı şifrələnmiş paketin şəbəkə üzrə ötürülməsi bilavasitə həyata keçirilə bilməz. Ona görə də başlığı şifrlənmiş paketin şəbəkə üzrə ötürülməsi zamanı onun inkapsulya-sını və tunelləşməsindən istifadə olunur. Bu zaman paketi başlıqla birlikdə tam şəkildə şifrələyib, onu digər xarici paketə qabıaşdı-rırlar və sonra onun açıq sahəsini mühafizə olunmuş kanal üzrə alıcıya ötürürlər. Alıcıda başlanqıc paketi xarici paketdən çıxarıb şifrələyib sonrakı veriliş üçün bərpa olunmuş başlıq kimi istifadə edirlər. Bərpa olunmuş başlıqlı paketin alınması və onun şəbəkə üzrə ötürülməsi sxemi şəkil 5.3-də verilib. Xüsusi tunel yalnız paketləri mühafizə etmək üçün deyil, o həmdə verilənlərin bütövlü-yü və audentifikasiyası üçün də istifadə olunur. Xüsusi tuneldən həm də elektron imzanın paketinin bütün sahələrində və həm də iki lokal kompüter şəbəkələri arasında verilənlərin toqquş-masının qarşısının alınmasında da istifadə oluna bilər.

Qeyd etmək lazımdır ki, İnternetlə əlaqəsi olmayan lokal kom-püter şəbəkələrinin qurulması zamanı istənilən IP ünvanı istifadə edilir, hansı ki, İnternet şəbəkəsində olduğu kimi bu ünvanlar biri- bir ilə toqquşa bilərlər, hansının ki, qarşısının alanması üçün paketlərin inkapslyasından istifadə olunur. Bu hal paketlərin inkap-sulyası zamanı onun əvvəlinci ünvanının gizlədilməsi və sonralar ayrılan şəbəkələr üzrə informasiya verilişi üçün istifadə olunan yeni ünvanın İnternetin IP-ünvanlar mühitinə əlavə olunması ilə izah olunur. Bu prosesdə IP-

ünvanının köklənməsi və şəbəkəyə birləş-miş mobil istifadəçilərin parametrləridə iştirak edirlər.




**Şək. 5.3.** Bərpa olunmuş başlıqlı paketin alınması və onun şəbəkə üzrə ötürülməsi sxemi

Şəbəkələrin mühafizə olunmuş kanallarının protokollarında tu-nelləşmədən geniş istifadə olunur. Tunelləşmə əksər hallarda infor-masiyanın məxfiliyinin və bütövlülüyünün pozulmasının baş verdi-yi həm lokal kompüter şəbəkələrində və həm də qlobal açıq şəbəkələr mühitində yaradılır. Tunel həm informasiyanın məxfili-yini və həm də şəbəkədə istifadə olunan müxtəlif protokollar arası keçidi həyata keçirə bilir ki, bununla da müxtəlif protokollu şəbəkələrin qarşılıqlı əlaqəsi uğurla həyata keçirilir [11].

Qeyd etmək lazımdır ki, tunelləşmə "sərnişin" protokolu, "protokol daşıyıcısı" və "tunelləmə" protokolunun əsasında yaradı-lır. Bu zaman "sərnişin" protokolu halında IPX nəqliyyat protokolu, "protokol daşıyıcısı" protokolu halında IP protokolu, "tunelləmə" protokolu halında isə kanal səviyyəsinin PPTP və L2TP protokolları və şəbəkə səviyyəsinin IPSec protokolu isti-fadə olunurlar.

### 5.3. Lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması

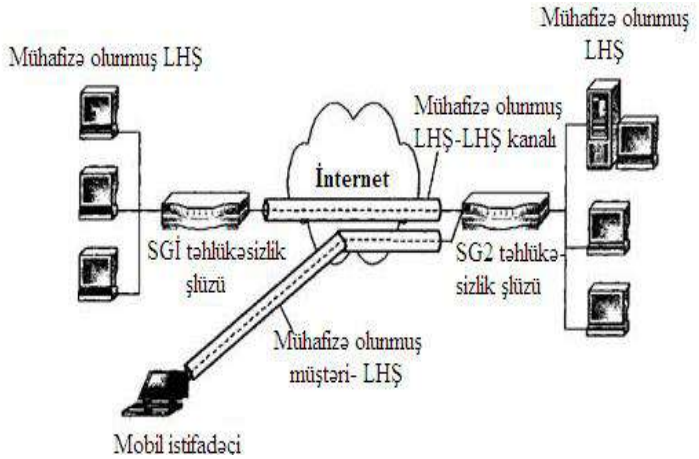
Həm lokal kompüter şəbəkələrinin qurulmasında və həm də bu şəbəkələrə uzaq (mobil) istifadəçilərin birləşdirilməsində verilənlə-rin təhlükəsizliyinin təmin edilməsi məsələsinin həll edilməsi va-cibliyi yaranır [11]. Bu məsələnin həll edilməsi üçün iki yanaş-madan istifadə olunur:

- lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması;
- müştəri ilə lokal kompüter şəbəkələri arasında mühafizə olun-muş kanalın yaradılması.

Lokal kompüter şəbəkələri arasında və bu şəbəkələrlə mobil istifadəçi arasında mühafizə olunmuş kanalın yaradılması sxemi şəkil 5.4-də verilib.

Lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması üçün təhlükəsizlik şlüzü tunel və interfeys kimi isti-fadə olunaraq ayrı-ayrı ofislər arasında daimi mühafizə olunmuş kanal yaradır və ofislərin qarşılıqlı əlaqəsi bu kanal vasitəsilə həyata keçirilir.

Uzaq və mobil istifadəçilərlə lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması xüsusi VPN vasitəsilə real-laşdırılır. Bu zaman uzaq (mobil) istifadəçi öz kompüterinə xüsusi müştəri proqram təminatı salaraq lokal kompüter şəbəkələrlə müştərilər arasında tunelin yaradılmasını həyata keçirir. Bu zaman yaradılmış tunel kommutasiyalı birləşməni aradan qaldırır və birləşməni uzaq daxilolma metodu ilə həyata keçirir.




**Şək. 5.4.** Lokal kompüter şəbəkələri arasında və bu şəbəkələrlə mobil istifadəçi arasında mühafizə olunmuş kanalın yaradılması sxemi

Lokal kompüter şəbəkələri arasında birləşmə yaradılan za-man mühafizə olunmuş tunel bu şəbəkələrin marşrutlayıcıları arasında yaradılır. Müştərilərlə lokal kompüter şəbəkələri arasında birləşmənin yaradılması zamanı mühafizə olunmuş tunel uzaq daxilolma serverləri, İnternetin sərhəd provayderləri və lokal kompüter şəbəkələrinin şəbəkə ekranları arasında yaradıla bilər ki, bu da lokal kompüter şəbəklərinin yaxşı miqyaşlaşmasına və yük-sək idarəetmə qabliyyətinin artmasına gətirib çıxarır. Bu yanaşma-da şəbəkə qovşaqlarının proqram təminatı dəyişməz qalır və yaradılan tunellər lokal kompüter şəbəkələrinin kompüterləri, eləcə də serverləri üçün tam şəffaf olur. Göstərilən üstünlüklərə baxma-yaraq bu variant aşağı təlükəsizliyə malik olur. Mqhafizə olunmuş tunelin yaradılmasını ISP povayderi öz üzərinə götürən zaman mühafizə olunmuş bütün xüsusi virtual şəbəkələr onuların şəffaf olan şlüzləri üzərində qurula bilərlər. Bu variantın çatışmayan cəhəti xidmətlərin baha başa gəlməsi və etibarlılığın aşağı düşməsi ilə xarakterizə olunur..

Mühafizə olunmuş tunelin yaradılması virtual şəbəkələrin tunelinin təşəbbüsçüsü və terminatoru adlanan komponentləri ilə həyata keçirilir. Bu komponentlər verici və alıcı haqqında məlumata malik olan ilkin

paketi yeni paketə inkapsulyasiya edir və ünvançıya göndərir. Mühafizə olunmuş tunelin qırılması virtual şəbəkələrin qurğuları, o cümlədən mobil istifadəçinin modemi və noutbuku bazasında reallaşdırıla bilər. Bu tunel özündə xidmətlər provayde-rinin kommutatorlarını yaxud şlüzlərini əks etdirir, terminatorlar isə inkapsulyasiyanın əksinə olan prosesi reaıllaşdırır və yeni başlıqları kənarlaşdırıb hər bir ilk paketi şəbəkənin ünvançısına göndərir.

Lokal kompüter şəbəkələrində inkapsulyaiya olunmuş paketlərin məxfiliyi onların şifrlənməsilə, bütövlük və əsilliyi isə elektron rəqəmli imza ilə həyata keçirilir. Bu şəbəkələrdə verilənlərin müha-fizəsi üçün hal-hazırda çoxlu sayda kriptoqrafik mühafizə üsulları və alqoritmləri mövcuddur. Lakin baxılan şəbəkələrdə informasiya-nın mühafizə edilməsi üçün onların ayrı-ayrılıqda istifadə edilməsi əlverişli deyil. Ona görə də yaradılan tunelin terminatoru və təşəb-büsçüsü arasında razılaşma yolu ilə ümumi universal bir mühafizə alqoritminin yaradılması və onun əsasında informasiya mühafizəsi-nin təmin edilməsi daha əlverişli olardı.

## 5.4. VPN texnologiyası bazasında qurulmuş lokal kompüter şəbəkələrində verilənlərin mühafizə vasitələri

Lokal kompüter şəbəkələrinin layihələndirilməsi zamanı infor-masiyanın məxfiliyinin, bütövlülüyünün və əlverişliliyinin təyin olunması vacibliyi yaranır [12].

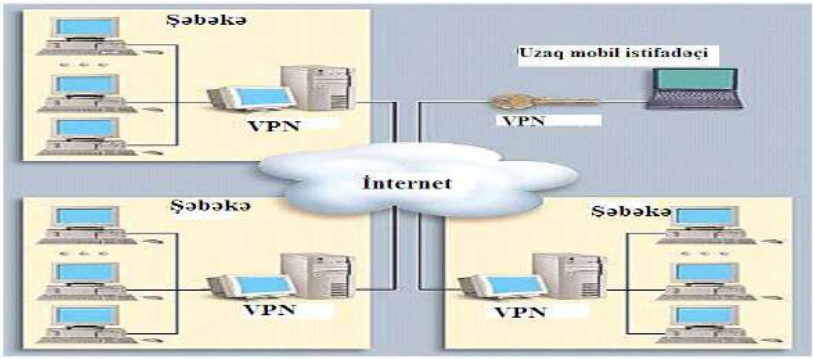
Məxfilik dedikdə şəbəkə üzrə verilənlərin ötürülməsi zamanı onların leqal vericiyə və alıcıya məlum olmasına, bütövlük dedikdə şəbəkə üzrə ötürülən veriliənlərin yaxşı vəziyyətdə saxlanılmasına, əlverişlilik dedikdə isə lokal şəbəkə vasitələrinin leqal istifadəçi-lərə daim məlum olmasına zəmanətin verilməsi başa düşülür. İnfor-masiyanın məxfiliyi müxtəlif metodlarla, yəni simmetrik və asim-

metrik alqoritmlərlə, bütövlüyü elektron imza texnologiyalarının müxtəlif variantları ilə, əlverişliliyi isə reallaşmanın etibarlığı, xid-mət keyfiyyəti və xarici təhdidin mühafizə dərəcəsiilə əldə olunur.

VPN texnologiyası əsasında qurulan lokal kompüter şəbəkələ-rində verilənlər audentifikasia olunmaqla, birləşmələr isə leqal abunəçilər

arasında həyata keçirilir, ki bunun da sayəsində xarici itifadəçilərin şəbəkəyə arzu olunmaz daxilolmalrının qarşısı alınır. Avtorizasiya zamanı leqal abunəçilərə çoxsaylı xidmətlər, informa-siyaların biri-birindən fərqlənən şifrləmə üsullrarı təqdim olunur. VPN texnologiyası əsasında qurulan lokal kompüter şəbəkələrində audentifikasia və şəbəkəyə daxilolmaların idarə olunması eyni xar-akteristikalara malik olan texniki vasitələrlə həyata keçirilir. Bu şəbəkələrdə verilən informasiyaların mühafizəsinin təmin edilməsi üçün abunəçilərin qarşılıqlı audentifikasiyası, məxfiliyi, avtoriza-siyası, zorla soxulması, şəbəkə təlükəsizliyinin idarə olunması və s. məsələlər həll olunmalıdır.

VPN texnologiyası bazasında qurulmuş lokal kompüter şəbəkə-lərinin struktur sxemi şəkil 5.5-də verilib [15]. Bu şəbəkələr əhatəsində




**Şək. 5.5.** VPN texnologiyası bazasında qurulmuş lokal kompüter şəbəkələrinin struktur sxemi

sində yerləşən bütün kompüterlərə VPN-i reallaşdıran, IP protokol-larının paketlərinə malik olan vasitələr qoyulur, hansılar ki, bütün ilkin məlumatları şifrələyir, elektron rəqəmli imza vasitəsilə veri-lənlərin bütövlüyünə nəzarət edirlər.

Bu növ şəbəkələrdə verilənlərin ötürülməsindən əvvəl alıcıda şifrləmə alqoritmləri və elektron rəqəmli imzanın köməyi ilə IP paketinin mühafizəsi üçün vacib olan mühafizə alqoritmi və açar seçilirr [15]. Əgər bunlara uyğun alıcı olmasa, onda verilənlərin göndərilməsi

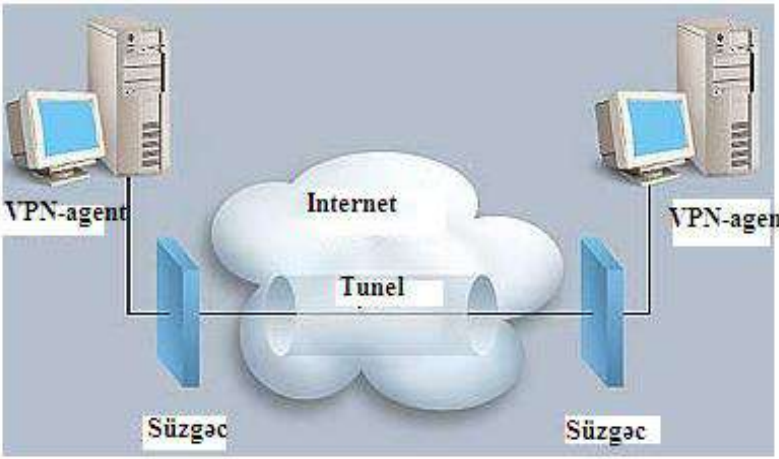
dayandırılır, sonra vericinin elektron rəqəmli imzası-nın paketi təyin edlir və onlara əlavə edilir, paket başlıqla birlikdə şifrələnir və yeni paketə inkapsulya edilir.

Alıcı tərəfdə IP paketinin alınması zamanı əks əməliyyatlar aparılır, yəni vericinin VPN agenti haqqında məlumata malik odu-ğu başlıq yoxlanılır. Yoxlama zamanı başlıqda olan məlumat veri-cinin VPN agenti haqda məlumata uyğun olmursa, onda qəbul olunmuş vüerilənlər tullanılır. Sonra şifrləmə alqoritmi, elektron rəqəmli imza və kriptoqraf açar seçilir, paketin şifrəsi açılır, onun bütölüyü yoxlanılır (elektron rəqəmli imza düz olmayan zaman o atılır) və bundan sonra paket ilkin şəkildə ünvançıya çatdırılır. Bu proseslər bütünlüklə avtomatik olaraq reallaşdırılır. Belə şəbəkələ-rdə VPN agenti onların kompüterlərində yerləşdirilir ki, o da ötürülən informasiyaların mühafizəsini təmin edir.

VPN texnologiyası əsasında qurulan lokal kompüter şəbəkələ-rində agentlərin həm də marşrutlayıcılıarla birləşdirilməsi müm-kündür. Bu zaman VPN agenti şəbəkələr arasında tunel adlanan mühafizə olunmuş rabitə kanalları reallaşdırır, hansılar ki, şəbəkə-lər arasında IP paketinin süzgəclənməsini həyata keçirir. Lokal kompüter şəbəkələri arasında IP paketlərinin tunelləşmə və süzgəc-lənməsi sxemi şəkil 5.6-da verilib [15]. Bu sxem vasitəsilə bir şəbə-kədən digər şəbəkəyə yol açılır və bütün IP paketlərinin süzgəc-lənməsi həyata keçirilir. Bu sxem vasitəsilə həm tunel yaradılır və həm də ötürülən IP paketlərinin süzgəclənməsi gerçəkləşdirilir, bu paketlər bir tuneldən digər tunelə ötürülür və yoxlandıq dan sonra atılır [15].

Lakin bu üstünlüklərə baxmayaraq VPN texnologiyası bazasında qurulan şəbəkələrdə ciddi problərin olması da müşahdə olunur.

Belə problemə misal olaraq xidmətdən imtinanı və daxili cinayət-karın törətdiyi təhdi göstərmək olar, hansı ki, maliyə vəsaitinin itirilməsinin 75%-zi bu təhdidin nəticəsində yaranır. Tunelləşmə dedikdə müxtəlif növ paketlərin birinin digərinin içərisinə inkap-sulyasiya edilməsi başa düşülür.



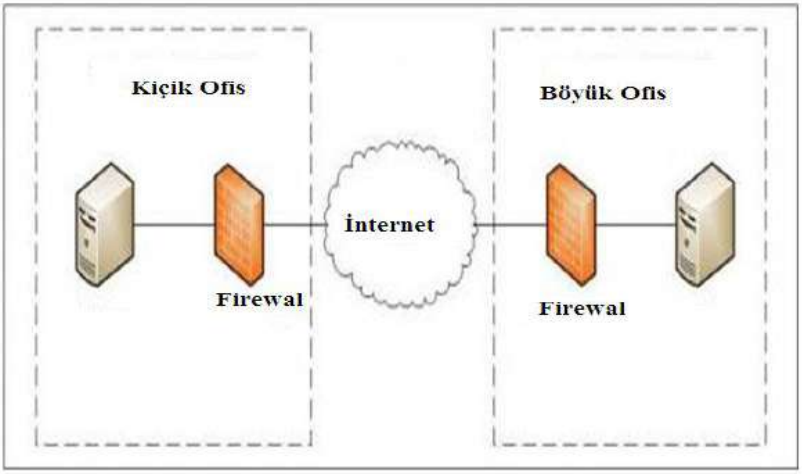

**Şək. 5.6.** Lokal kompüter şəbəkələri arasında IP paketlərinin tunelləşmə və süzgəclənməsi sxemi

Şəkildən göründüyü kimi iki brandmaur arasında iki şəbəkə yerləşdirilib. Brandmaur IP paketlərini tələb olunan şəkilə çevirib şifrələyir, onlara yeni IP başlığını əlavə edir. Şifrləmə nəticəsində paketin IP başlığında olan faktiki informasiya gizlədilir. Bu paketi qəbul edən uzaq brandmaur onun şifrəsini açıb ilkin şəkilə çevirir. Hər iki şəbəkənin süzgəcləri arasındakı seqment tunel adlandıdılır. IP paketlərinin şifrlənməsi və onların göndərilməsindən hər iki şəbəkənin qovşaqlarının xəbəri olmur. Bu zaman şəbəkənin qov-şaqlarında xüsusi proqram təminatının və hər hansı bir köklənmə-nin olması tələb olunmur, lakin uzaq altşəbəkənin qovşaqları üçün təyin olunmuş paket və şlüzvari qurğuların tam nəzarət olunması həyata keçirilməlidir.

Qurulmasının ucuz başa gəlməsi, informasiyanın məxfiliyinin, bütövlüyünün və audentifikasiyasının təmin edilməsi VPN tex-nologiyası bazasında qurulan lokal kompüter şəbəkələrinin üstün cəhətləridir. Bu şəbəkələrin digər üstün cəhəti əlavə rabitə xətti çəkilmədən mövcud şəbəkə infrastrukturu üzərində qurulmasıdır.

## 5.5. Lokal kompüter şəbəkələrinin müxtəlif VPN texnologiyaları bazasında qurulması

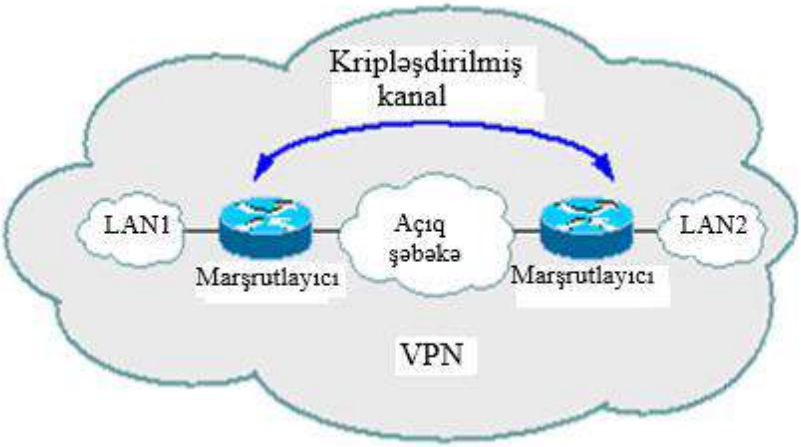
Mühafizə olunmuş lokal kompüter şəbəkələri əsasən brandma-uer, marşrutlayıcı, əməliyyyat sistemləri və aparat vasitələri üzə-rində qurulurlar. Brandmauer üzərində qurulan lokal kompüter şəbəkələrinin proqram təminatına şifrləmə modulu yerləşdirilir. Ona görə də belə şəbəkələrin brandmaurləri üzərindən ötürülən informasiyalar trafikin şifrlənməsinə əsaslanır [16]. Qeyd etmək lazımdır ki, brandmauer texnologiyası yalnız kiçik həcmli verilən-lərin ötürülməsini həyata keçirən lokal kompüter şəbəkələrinin qurulmasında istifadə olunurlar. Lokal kompüter şəbəkələrinin brandmauer üzərində qurulması sxemi şəkil 5.7-də göstərilib.




**Şəkil 5.7.** Lokal kompüter şəbəkələrinin brandmauer üzərində qurulması sxemi

Lokal kompüter şəbəkələrinin qurulmasının digər üsulu onun marşrutlayıcılar üzərində qurulması üsuludur. Belə şəbəkələrdə mühafizə olunmuş kanalların yaradılması üçün marşrutlayıcılardan istifadə olunur. Marşrutlayıcılar əsasında qurulan şəbəkələrdə mar-şrutlayıcılar öz funksiyalarından əlavə həm də informasiyanın şifr-lənməsi funksiyasını da yerinə yetirirlər. Bu məqsədlə marşrut-

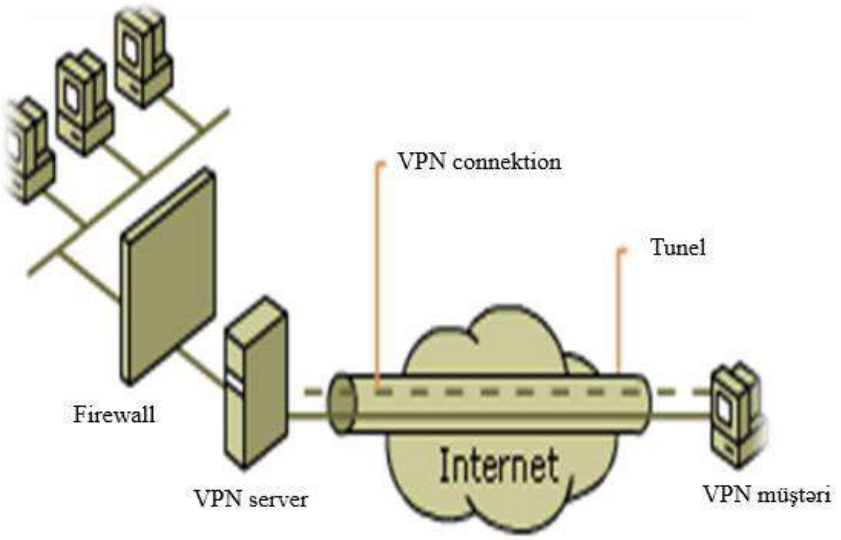
layıcıların proqram təminatına şifrləmə modulu yerləşdirilir. Lokal kompüter şəbəkələrinin marşrutlayıcılar üzərində qurulması sxemi şəkil 5.8-də verilib [16]. Lokal kompüter şəbəkələrinin marşrutlayıcılar




**Şəkil 5.8.** Lokal kompüter şəbəkələrinin marşrutlayıcılar üzərində qurulması sxemi

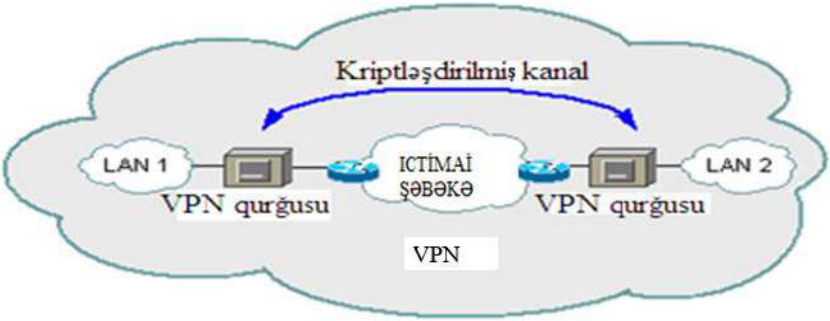
üzərində qurulması zamanı istifadə olunan avadanlıqlara misal olaraq Cisco Syst Ems şirkətinin avadanlıqlarını göstərmək olar. Bu şirkətin marşrut-layıcılarında əsasən L2TP və IPSec protokollarından istifadə olu-nur. Tunel birləşməsinin yaradılması zamanı Cisco Syst Ems şirkətinin avadanlıqları eyni zamanda həm eyniləşdirmə, həm də açarların mübadilə funksiyalarını yerinə yetirirlər.

Lokal kompüter şəbəkələrinin əməliyyat sistemləri üzərində qurulması üçün çoxlu yanaşmalar mövcuddur. Bu yanaşmaların analizi göstərir ki, konfiqurasiyalaşdırma və köklənməyə görə, onlardan ən əlverişlisi və ucuz başa gələn sistem Windows 2003 Server əməliyyat sistemidir, hansı ki, marşrutlaşma xidmətini və uzaq daxilolmanı reallaşdırmaga imkan verir. Lokal kompüter şəbəkələrinin əməliyyat sistemi üzərində qurulması zamanı istifadə olunan VPN-in topolgiyası şəkil 5.9-a verilib.




**Şək. 5.9.** Lokal kompüter şəbəkələrinin əməliyyat sistemi üzərində qurulması zamanı istifadə olunan VPN-in topolgiyası

Lokal kompüter şəbəkələrinin VPN-in xüsusi aparat vasitələri bazasında qurulması, onların yüksək məhsuldarlığını artırır [16]. VPN-in xüsusi aparat vasitələri üzərində qurulmuş şəbəkələrdə aparat qurğusu kimi Radguard şirkətinin IPro-VPN məhsulu isti-fadə olunur. Bu məhsul verilən informasiyanın aparat şifrlənməsini həyata keçirir və 100 Mbit/s sürətində informasiya selini buraxmaq qabliyyətinə malikdir [16]. Bunlardan başqa, bu qurğu şəbəkə ünvanlarının translyasiya sistemini istifadə edir və brandmauer funksiyasını reallaşdıran xüsusi qurğu ilə təhciz edilir. Lokal kompüter şəbəkələrinin VPN-in xüsusi aparat qurğusu bazasında qurulması sxemi şəkil 5.10-da verilib.




**Şək.5.10.** Lokal kompüter şəbəkələrinin VPN-in xüsusi aparat qurğusu bazasında qurulması sxemi

## 5.6. Lokal kompüter şəbəkələrinə uzaq daxilolmaların təmin olunması üçün istifadə olunan tunelləşmə protokolları

Lokal kompüter şəbəkələrinin qurulmasında istifadə olunan tunelləşmə protokolları informasiyanın şifrlənməsini təmin edir və onların istifadəçilərə bilavasitə çatdırılmasını həyata keçirirlər [17]. Bu şəbəkələrin qurulması zamanı OSİ modelinin kanal səviyyə-sinin, şəbəkə səviyyəsinin və eləcə də nəqliyyat səviyyəsinin protokollarından istifadə olunur.

Lokal kompüter şəbəkələrinə daxilolmaların təmin olunması üçün OSİ modelinin kanal səviyyəsində mühafizə olunmuş kanal-ların yaradılması üçün PPTP tunelləşmə protokolu istifadə plunur. Bu protokol uzaq istifadəçilərin lokal şəbəkələrə daxilolmalarını təmin etmək üçün PPP protokolunun genişləndirilməsi məqsədilə təklif olunmuşdur, hansı ki, həm kompüterlərin, həm də provayder-lərin bu şəbəkələrə telefon xətti ilə bilavasitə qoşulma-sını həyata keçirir.

Son zamanlar lokal kompüter şəbəkələrinə uzaq daxilolmaların təmin olunması üçün L2TP növ tunelləşmə protokolu standartlaş-dırılmışdır, hansı ki, özündə həm PPTP və L2F protokollarının üstün cahətlərini ehtiva edir. OSİ modelinin kanal səviyyəsində mühafizə olunmuş kanalların yaradılması üçün istifadə ounan PPTP tunelləşmə potokolu üzrə ötürülən IP paketinin strukturu şəkil 5.11-də verilib.

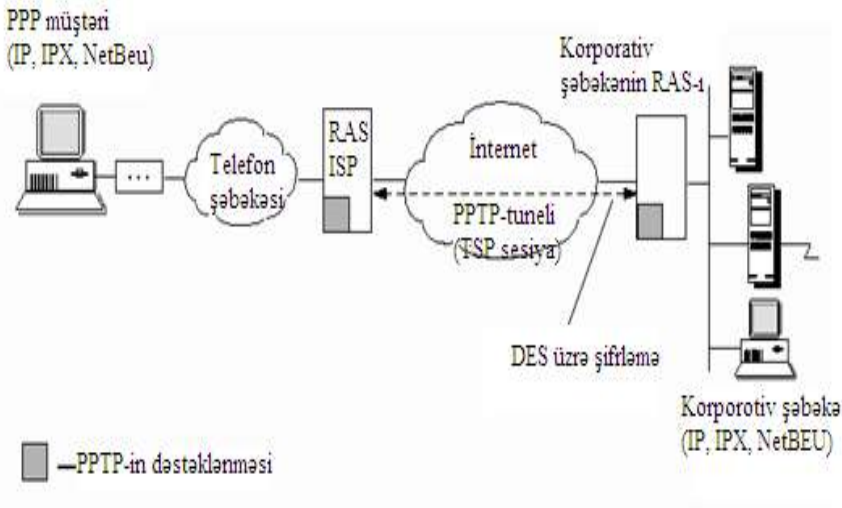

**Şəkil 5.11.** OSİ modelinin kanal səviyyəsində mühafizə olunmuş kanalların yaradılması üçün istifadə ounan PPTP tunelləşmə potokolu üzrə ötürülən IP paketinin strukturu

PPTP tunelləşmə protokolu üzrə ötürülən IP paketinin strukturuna İnternet daxilində istifadə olunan kanal səviyyəsinin başlıqları, o cümlədən ethernet şəbəkəsinin kadrının başlıqları, IP başlıqları, GRE başlıqları və IP, IPX yaxud NetBEUI paketlərini birləşdirən ilk paketlər daxildir. PPTP tunelləşmə protokolu PPP protokolu-nun kadrını, şəbəkə səviyyəsinin protokollarına inkapsulyasiya edən GRE paketinə inkapsulyasiya edir, hansı ki, sessiya yaratmaq və cinayətkardan mühafizə etmək qabliyyətinə malik deyil. Sessiya yaratmaq və cinayətkarın icazəsiz daxilolmalarının qarşısını almaq üçün PPTP protokolunun tunelinin idarə etmə qabliyyətindən istifadə olunur.

Qeyd etmək lazımdır ki, GRE paketinin inkapsulyasiya etmə qabliyyəti lokal kompüter şəbəkələrində PPTP protokolundan istifadə olunmasını məhdudlaşdırır. PPP protokolunun kadrının GRE paketinin kadrına inkapsulyasiya edilməsindən sonra paketin göndəricisinin və alıcısının ünvanlarına malik olan IP başlıqlı kadra inkapsulyasiya olunur. Bundan sonra PPTP protokolu PPP protokolunun başlığına son işarəsini verir və göndərici mühafizə tuneli vasitəsilə verilənləri alıcıya göndərir, hansı ki, bütün xidməti başlıqları tullayır, yalnız PPP protokolunun verilənlərini saxlayır [17]. Bu proses iki variantda həyata keçirilir.

Birinci variantda daxilolma serveri ilə korporativ şəbəkənin sərhəd marşrutlayıcıları arasında mühafizə olunmuş kanal istifadə olunur.

Daxilolma serveri ilə korporativ şəbəkənin sərhəd marşrut-layıcıları arasında mühafizə olunmuş kanalın istifadə olunması sxemi şəkil 5.12-də verilib.

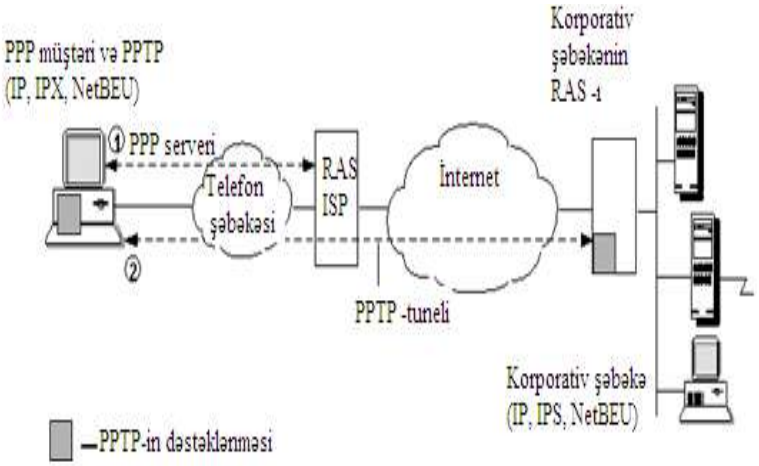



**Şək.5.12.** Daxilolma serveri ilə korporativ şəbəkənin sərhəd marşrutlayıcıları arasında mühafizə olunmuş kanalın istifadə olunması sxemi

Bu cxemdə PPTP protokolunu dəstəkləməyən uzaq istifadəçinin kompüteri İSP-də yerləşən PPP protokolu vasitəsilə PPTP proto-kolunu dəstəkləyən uzaq daxilolma serveri RAS vasitəsilə pro-vayderdə birinci audentifikasiyanı keçir. İstifadəçilərin verilənlər siyahısında İSP, korporotiv şəbəkənin sərhəd marşrutlayıcısında RAS istifadəçisinin IP ünvanının tapır, bundan sonra ISP, PPTP protokolu vasitəsilə sərhəd marşrutlayıcısı ilə sessiya yaradır [17]. Bu variantda həm də uzaq istifadəçilərin kompüterləri kimi korpo-rotiv şəbəkənin serveri də PPTP protokolunu dəstəkləməməlidir. Bu proses sərhəd marşrutlayıcısının IP paketindən PPP protokol-unun kadrlarının çıxarması və onları IP, IPX kimi vacib olan for-matda şəbəkə üzrə göndərməsi ilə izah olunur.

İkinci variantda korporotiv şəbəkələrin sərhəd marşrutlayıcıları arasında mühafizə olunmuş kanal yaradılır. Uzaq istifadəçilərin

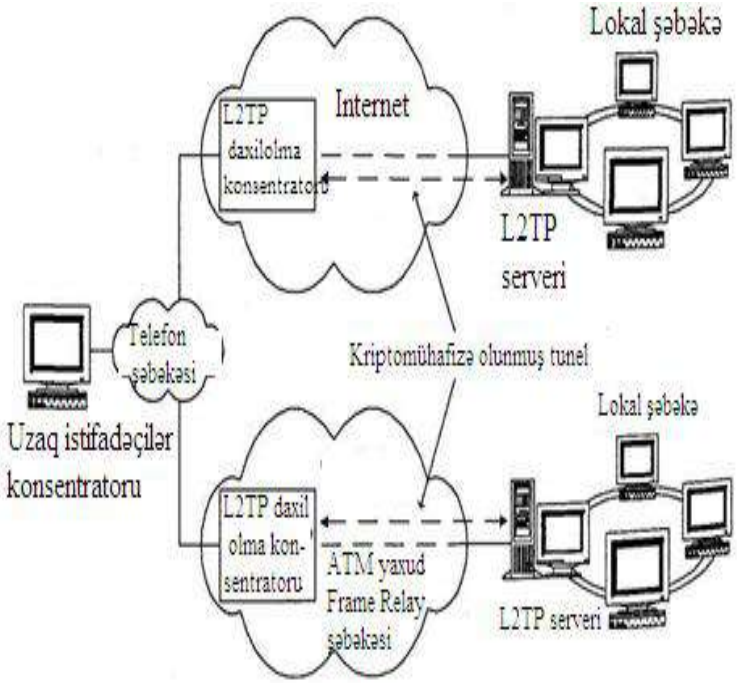
korporativ şəbəkələrin marşrutlayıcıları arasında mühafizə olunmuş kanalın yaradılması sxemi şəkil 5.13-də verilib.




**Şəkil 5.13.** Uzaq istifadəçilərin korporativ şəbəkələrin marşrutlayıcıları arasında mühafizə olunmuş kanalın yaradılması sxemi

Bu sxem üzrə informasiyanın ötürlməs prosesi aşağıdakı qaydada həyata keçirilir. RAS əvvəlcə ISP serverinə zəng etməklə PPP protoklu vasitəsilə onunla əlaqə yaradır. Bundan sonra provay-derdə audentifikasiyadan keçirərək ikinci dəfə korporativ şəbəkənin uzaq daxilolma serverinə zəng edir [17]. Bu zaman korporativ şəbəkə tərəfindən qoşulmuş RAS adi telefon nömrəsinin əvəzinə Windows NT-in IP-ünvanını göstərir. Bu ünvanla müştəri kompü-teri ilə RAS kompüteri arasında PPTP protokolu vasitəsilə sessiya yaranır. Bundan sonra müştəri RAS serverində yenə də audentifika-siyadan keçir və bununla da informasiya verilişi həyata keçirilir.

PPTP protokolundan fərqli olaraq L2TP protokolu mühafizə olunmuş kanalı lokal kompüter şəbəkəsinin uzaq daxilolma serveri ilə birləşmənin yaradılması, istifadəçilərin audentifikasiyası və kriptomühafizə olunmuş tunelin konfiquryasiyalaşdırılması kimi üç mərhələdə formalaşdırır [17]. L2TP protokolu ilə mühafizə olunmuş kanalın formalaşdırılması sxemi şəkil 5.14-də göstərilib.




**Şəkil 5.14.** L2TP protokolu ilə mühafizə olunmuş kanalın formalaşdırılması sxemi

Bu sxemdə uzaq istifadəçi PPP protokolu vasitəsilə L2TP protokolunun daxili konsentratoru ilə birləşərək lokal kompüter şəbəkəsini uzaq daxilolma serveri ilə birləşdirir. Bu birləşmənin həyata keçirilməsi zamanı L2TP protokolunun daxilolma konsen-tratoru provayder adından istifadəçinin audentifikasiyasını yerinə yetirir. Bundan sonra provayderin daxilolma konsentratoru istifa-dəçinin adı ilə L2TP protokolunun serveri tələb olunan lokal kompüter şəbəkəsinin IP ünvanının təyin edir. Bu ünvan əsasında L2TP protokolu vasitəsilə provayderin daxilolma konsentratoru ilə lokal kompüter şəbəksi arasında sessiya yaradılır. Bu sessiya yadaıldıqdan sonra lokal kompüter şəbəkəsinin servisində istənilən alqoritmdən istifadə etməklə istifadəçinin audentifikasiyası aparılır.

Belə alqoritmə misal olaraq CHAP alqoritmini göstərmək olar. PPTP və L2F protokollarında audentifikasiya metodlarından istifa-də olunmadığı kimi L2TP protokolunda da audentifikasiya metod- larından istifadə olunmur.

Qeyd etmək lazımdır ki, istifadəçi audentifikasiya olduqdan sonra provayderin daxilolma konsentratoru ilə L2TP protokolunun serveri arasında kriptomühafizə tuneli yaranır. Bu tunelin müxtəlif parametrlərinin köklənməsi idarəedici məlumat vasitəsilə aparılır. L2TP protokolunun bir neçə sessiyası bir tuneldə multiplekşdirilə bilər. Bu protokol şifrləmənin müxtəlif standarlarından istifadə edir, lakin kriptomühafizənin konkret metodunu spesifikləşdirmir. Tunel IP-şəbəkəsində formalaşan zaman informasiyanın mühafi-zəsi IPSec protokoluna uyğun aparılır və L2TP protokolunun paketləri UDP protokolunun paketlərinə inkapsylyasiya olunaraq 1701 UDP-portu vasitəsilə provayderin daxilolma konsentrato-rudan L2TP serverinə ötürülür.

## ƏDƏBİYYAYT


1. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Bakı. MTN-in nəşriyyatı. 2009. -342 s.
2. Məmmədov S.Z. Korporativ kompüter şəbəkələrində informasiya təhlükəsizliyi sisteminin modelləşdirilməsi. 05.12.13 – "Telekommunikasiya sistemləri, şəbəkələri və qurğuları" ixtisası üzrə texnika elmləri namizədi alimlik dərəcəsi almaq üçün dissertasiya. Bakı-2007. -s. 124.
3. Məmmədov H.Ə. , Məmmədov F.H., Cəfərov Z.Ə. İnformasiya mühafizəsi üsulları və vasitələri. Dərslik., Bakı, 2010. -305 s.
4. Курс лекций по дисциплине «Защита информации»/ Владим. гос. уни-т имени Александра Григорьевича и Николая Григорьевича Столетовых; А.О. Кучерик, А.Ю. Лексин, Д.Н. Бухаров, А.Ю. Шагурина. – Владимир: Изд-во ВлГУ, 2017. – 104 с.
5. Двинских А.Э., Панасенко С.П., Салманова Ш.А. Практические методы обеспечения безопасности информационных ресурсов с использованием средств защиты информации серии «КРИПТОН» Издательство: ТЕХНОСФЕРА.-ISBN: 978-5-948 36-494-02017. 2017г.-238с.
6. Информационная безопасность и защита информации : учеб. пособие / Баранова Е.К., Бабаш А.В. -3-е изд., перераб. и доп.-М.: РИОР: ИНФРА-М, 2017. - 322 с. - (Высшее образо-вание).- ww.dx.doi.org/10.12737/11380.
7. Родичев Ю. А.Нормативная база и стандарты в области информационной безопасности. Учебное пособие. Питер. 2017.- 2017г.-256 с. ISBN:978-5-496-02434-1
8. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.- 282 с.- Режим доступа:

http://www.iprbookshop.ru/16713.— ЭБС «IPRbooks», по паролю.
9. Бондарев В.В. Введение в информфционную безапасность.Учебное пособие. 252с. – ISBN 978-5-7038-4414-4.
10. Основы информационной безопасности. Учебное пособие. 2016 г.- 324 с. -ISBN978-5-8114-2290-6.
11. Панасенко С.П. Алгоритмы шифрования, специальный справочник.Издательство:ТЕХНОСФЕРА.ISBN: 978-5-94836-429-2. 2016г. 576с.
12. Романец Ю.В., Панасенко С.П., Заботин И.А., Петров С.В., Ракитин В.В., Дударев Д.А., Сырчин В.К., Салманова Ш.А. Фирма «АНКАД» -25 лет на службе обеспечения информационной безопасности России. Издательство:ТЕХНО СФЕ РА .ISBN: 978-5-94836-429-2. 2016г.- 256стр.
13. Криптографические методы защиты информации: Учебно-методическое пособие: Том 3 / Бабаш А.В., - 2-е изд. - М.:ИЦ РИОР, НИЦ ИНФРА-М, 2014. - 216 с.: 60x88 1/8. - (Высшее образование: Бакалавриат.-ISBN 978-5-369-01304-5.
14. Ишмухаметов Ш.Т. Технологии защиты информации в сети. Курс лекций. 2013. 89 с.
15. Бабаш А.В., Баранова Е.К., Ларин Д.А. Информационная безопасность. История защиты информации в России. М. : КДУ, 2013 . -736 с. -ISBN 978-5-98227-928-6
16. Бирюков А. А.. Информационная безопасность: защита и нападение. . Электронная книга. 2013г.- 476 с.- ISBN: 978-5-94074-647-8
17. Болелов Э.А. Криптографические методы защиты информации. Пособия к выполнению лабораторных работ. Москва. 2010.-33стр.
18. Басалова, Г. В. Основы криптографии [Текст]: Уч. Пособие / Г.В. Басалова – Тула: Тульский госуниверситет, 2009.-145 с.

19. Болелов Э.А. Криптографические методы защиты информации. Пособия к выполнению лабораторных работ. Москва. 2010.-33стр.
20. Галатенко В.А. Основы информационной безопасности Интернет-университет информационных технологий – ИНТУ ИТ.ру, 2008г.

**MƏMMƏDOV F. H., ORUCOVA M.Y.**

# “INFORMASİYA TƏHLÜKƏSİZLİYİ VƏ TƏMİNATI” KOMPÜTER ŞƏBƏKƏLƏRİNDƏ TƏHLÜKƏSİZLİYİN TƏŞKİLİ PRİNSİPLƏRİ

Bakı: “Zəngəzurda” çap evi, 2022 – 175 səh.

**Çap evinin rəhbəri:**
Mübariz Binnətoğlu

**Korrektor:**
Şəbnəm Allahverdiyeva

**Kompüter tərtibçisi:**
Tahirə İmamova

İmzalandı: 20.08.2022
Kağız formatı: 60x84 1/16
H/n həcmi: 11 ç.v.
Sifariş: 557
Sayı: 100

“ZƏNGƏZURDA” çap evində çap olunub.
**Ünvan:** Bakı şəh., Mətbuat prospekti, 529-cu məh.
“Azərbaycan” nəşriyyatı, 6-cı mərtəbə.
Tel.: +994 50 209 59 68
+994 55 209 59 68
+994 12 510 63 99
e-mail: zengezurda1868@mail.ru