

**F.H. MƏMMƏDOV
M.Y. ORUCOVA**

**“İNFORMASIYA
TƏHLÜKƏSİZLİYİ VƏ TƏMİNATI”**

**KOMPÜTER ŞƏBƏKƏLƏRİNDƏ
TƏHLÜKƏSİZLİYİN
TƏŞKİLİ PRİNSİPLƏRİ**

MƏMMƏDOV F. H., ORUCOVA M.Y.

**“İNFORMASIYA TƏHLÜKƏSİZLİYİ VƏ TƏMİNATI”
KOMPÜTER ŞƏBƏKƏLƏRİNDƏ TƏHLÜKƏSİZLİYİN
TƏŞKİLİ PRİNSİPLƏRİ**

Ali məktəblərdə təhsil alan magistrələr üçün dərs vəsaiti

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

“ZƏNGƏZURDA”

ç a p e v i

BAKİ – 2022

Rəyçilər:

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

Azərbaycan Texniki Universitetin
“Radiotexnika və telekommunikasiya”
kafedrasının, t.e.d., professor
B.Q. İbrahimov

Məmmədov F.H., Orucova M.Y. **“İnformasiya təhlükəsizliyi və təminatı”
(Kompüter şəbəkələrində təhlükəsizliyin təşkili prinsipləri).**
Bakı: “Zəngəzurda” çap evi, 2022. – 180 səh.

Dərs vəsaitində müasir elmi-texniki inqilabın texnoloji hadisəsi olan və cəmiyyətin informasiyalaşdırılması ilə sıx bağlı olan kompüter şəbəkələrində təhlükəsizliyin təmin edilməsi, onların modelləri, sintezi, strukturlarının paylanma prinsipləri və informasiyanın sızması yolları təhlili edilir. İnformasiya mühafizəsi sistemlərinin kriptografik vasitələri, mexanizmləri və modelləri işıqlandırılır. Bağlı və açıq açarlı kriptografiya 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 şifrələmə, maneədarlıq kodlama və informasiyanın sızılması 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 texnologiyaları və sistemləri mühəndisliyi” ixtisası üzrə təhsil alan magistrlər və kompüter şəbəkələrinin təhlükəsizliyi ilə məşğul olan mühəndis-texniki işçilər üçün də faydalı ola bilər.

DOI: <https://doi.org/10.36719/2022/175>

© Məmmədov F. H., 2022
© Orucova M.Y., 2022
© ZÇE, 2017

MÜNDƏRİCAT

GİRİŞ.....	6
I FƏSİL. İNFORMASIYA 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.....	18
1.5. İnformasiya mühafizəsinin kriptografik vasitələri.....	22
1.5.1. Kriptografik sistemlərin modelləri və şifrəlmə metodları.....	24
1.5.2. Sezar şifrəlmə metodu	27
II FƏSİL. SİMMETRİK ŞİFRLƏMƏ TEXNOLOGİYALARI.....	31
2.1. Simmetrik şifrələmənin struktur sxemi	31
2.2. Əvəzləmə metodu.....	33
2.2.1. Birəlifbəli əvəzləmə.....	32
2.2.2. Rəqəm şəkilli informasiyanın şifrələnməsi.....	37
2.2.3. Proporsional şifrəlmə üsulu	3
2.3. Çoxəlifbəli əvəzləmə üsulu	39
2.4. Qammalaşdırma üsulu	48
2.5. Yer dəyişdirmə metodu	53
2.6. Cədvəl üzrə yerdəyişmə	54
2.7. Proqram və aparat yolu ilə reallaşdırılan yerdəyişmə	56
2.8. Kompozisiya şifri anlayışı.....	57
2.9. Simmetrik şifrələmənin blok alqoritmlərində istifadə olunan əməliyyatlar	5
9	
2.10. Cədvəl əvəzlənməsi	61
2.11. Simmetrik şifrələmənin blok alqoritminin strukturu	62
2.12. Bağlı açarlı blok şifrənin qurulma prinsipi	63
2.13. DES və AES şifrəlmə alqoritmləri	64
2.13.1. Əsas məlumatlar	64
2.13.2. İkiqat DES və “ortada görüş” hücumu.....	69
2.13.3. Üçqat DES.....	70
2.13.4. Reyndal alqoritmı	71
2.14. DÜİST28147-89 –üzrə verilənlərin kriptografik çevrilməsi	

alqoritmi	75
2.14.1. Əsas məlumatlar	75
2.14.2. DÜİST28147-89-un raundunun strukturası.....	76
2.14.3 Şifrəlmə və şifrənin açılması əməliyyatları.....	77
2.14.4. Şifrələmənin əsas rejimləri.....	79
2.14.5. DÜİST 28147-89 və DES şifrəlmə alqoritmləri arasındakı fərq 80	
2.15. Kriptografik heş-funksiya.....	81
2.15.1. Heş- funksiya anlayışı	81
2.15.2. Heş-funksiyanı formalaşdırmaq üçün şifrələmənin blok alqoritmindən istifadə edilməsi 83	
2.16. Arakəsilməz şifrə və saxta təsadüfi ədədlər generatoru	85
2.16.1. Arakəsilməz şifrə	85
2.16.2. Arakəsilməz şifrələmə zamanı saxtatəsadüfi ədədlər generatorlarının istifadə olunması prinsipi 88	
2.16.3. Xətti konqruent saxtatəsadüfi ədədlər generatoru	89
2.17. Gecikmə ilə Fibonaççi metodu.....	90
2.17.1. BBS alqoritmi əsasında saxtatəsadüfi ədədlər generatoru	92
2.18. Əks əlaqəli sürüşmə registri əsasında saxta təsadüfi ədədlər generatoru	94
2.18.1. Saxta təsadüfi ədədlər almaq üçün OFB və CTR rejimlərindən istifadə olunması	9
6	
2.19. RC4-aqoritmi	98
2.20. Məxfi açarın idarə olunması.....	108

III FƏSİL. AÇIQ AÇARLI KRİPTOQRAFIYA

TEKNOLOGİ-YALARI.....	112
3.1. Açıq açarlı kriptografiyaya giriş	112
3.1.1. Birtərəfli funksiya.....	113
3.2. Açıq açarlı alqoritm əsasında rəqəmli imza.....	115
3.3. Asimmetrik alqoritmindən istifadə etməklə məxfi açarın formalaşdırılması 120	

3.3.1. Açıq açarlı şifrləmə alqoritminə tələblər	122
3.4. Kombinasıya olunmuş şifrləmə kriptosistemi	123
3.5. Elektron rəqəmli imza	126
3.5.1. Elektron rəqəmli imza və heşləmə funksiyası	126
3.5.2. Rəqəmli imzanın əsas prosedurları.....	127
3.5.3. Rəqəmli imzanın formalaşdırılması proseduru.....	128
3.5.4. Rəqəmli imzanın yoxlanılması proseduru	129
3.5.5. Heşləmə funksiyası	131

IV FƏSİL. TAM MƏXFİ SİSTEMLƏR 133

4.1. Məlumatın əldə edilməsi, emalı, ötürülməsi və qorunması	133
4.2. Entropiya və qeyrimüəyyənlik	135
4.3. Dil norması və məlumat artıqlığı.....	137
4.3.1 Dilin mütləq norması.....	137
4.3.2. Dilin artıqlığı	138
4.4. Tam məxfi sistemlər anlayışı	138
4.4.1. Təklif (yaxud nadirlik) məsafəsi	140
4.5. Şifrləmə, maneə davamlı kodlama və informasiyanın sıxılması	142
4.5.1. Maneə davamlı kodlama	142
4.5.2. Kod sözü.....	145
4.6. Verilənlərin sıxılma prinsipləri.....	149

V FƏSİL. VPN TEXNOLOGİYASI BAZASINDA LOKAL KOMPÜTER ŞƏBƏKƏLƏRİNDƏ İNFORMASIYA MÜHAFİZƏSİNİN TƏŞKİLİ

154

5.1. VPN texnologiyası bazasında Lokal kompüter şəbəkələrinin qurulması 154	
5.2. Xüsusi tunel vasitəsilə ötürülən paketin bir nümunəsi.....	157
5.3. Lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması	159
5.4. VPN texnologiyası bazasında qurulmuş lokal kompüter şəbəkələrində verilənlərin mühafizə vasitələri	161
5.5. Lokal kompüter şəbəkələrinin müxtəlif VPN texnologiyaları bazasında qurulması	165
5.6. Lokal kompüter şəbəkələrinə uzaq daxilolmaların təmin	

olunması üçün istifadə olunan tunelləşmə protokolları	168
ƏDƏBİYYAT.....	174

GİRİŞ

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

Digər tərəfdən, kriptografiyanın yeni nailiyyətləri nəinki, klassik məsələləri həll edir, həm də digər növ mühafizə vasitələrinin 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. Kriptografiyanın inkişafı uzun illər ləng inkişaf etmişdir, lakin XX əsrdə riyaziyyatda əldə olunan nailiyyətlər sayəsində kriptografiya-ya sıçrayışla inkişaf etməyə başladı.

Nə vaxt deyilib, sirrli yazı mənasına ehtimal etmək olar ki, kriptografiya sözü yazısı ilə bir vaxtda həyata göz açmışdır. *Kriptografiya*-informasiyanın uzaq və ya qanuna tabə olmayan istifadəçilərdən mühafizə nail olmaq üçün çevrilməsi metodlarının hazırlanması haqqında bir elmdir.

Kriptografiya başqa ölkə dilində misal üçün yunan dilində *γραφω* (gizli,sirrli) və *kryptos* tərcüməsində «yazı» bu sözlərindən yaranmışdır. Kriptografiyada, həmişə olduğu kimi, kənar istifadəçilərin yəni belə desək əks kəşfiyyatın, rabitə kanallarına böyük və ciddi nəzarət etməsi fərziyyəsi son dövrlərdə alimlər tərəfindən diqqətə cəlb olunub. Kriptografiya məlumatların yəni informasiyanı yönləndirilməsi üçün qeydlərini "giz-lətmir", sadəcə əldə olunan informasiyanı həmin istifadəçilərin başa düşmək üçün mümkün olmayan (oxumaq, anlamaq) vəziyyətə çevirir. Kriptografiyanın haqqında genişlənməsi təxminən XIV əsrin bitmə vaxtlarına təsadüf edir. İctimai-siyasətdə, inqilabi işdə diplomatiyada və eləcədə hərbi siyasətdə eləcədə işlərdə ənənəvi tətbiqi ilə birgə kriptografiya intellektual mülkiyyətin mühafizəsində yəni qorunmasında və ya piratçılığın (oğurluğun) qarşısını almaqda və bəzi oxşar kimi işlərdə də istifadə olun-mağa başlanmışdır.

Kriptoqrafiyanın haqqında tarixindən informasiyalar.

Təxminən XIX-əsrin bitmə vaxtında hərbi-akademiyalarda öyrənilməsinə başlanması üçün kriptoqrafiyaya dəqiq bir elm əlamətləri verilib. Bir neçə akademiya birində “gouvion Saint-Cyr” Fransada yerləşən “SEN_SİR xə-t-keşi” ad verilən cəmiyyət tərəfindən məxsusi hərbi-səhra şifrəsi yəni gizli yazı hazırlanmışdır. “SEN_SİR xə-t-keşi”nin ideyasında eləcə də fikirlərin genişlənmək hərəkət edən hissədə hərflərin ixti-yari ardıcılıqda və ya müəyyən ardıcılıqla düzülən, düzülməsi ilə bağlıdır.

Bu cəmiyyətdə elmi alqoritmlər kriptoqrafiya haqqında birinci dəfə ərəb ölkələrində mey-dana gəlmişdir. Nəzərə alsaq ki, “şifrə” sözünün mənası (həmən bu dildə yəni ərəb dilində “sifra” (rəqəm deməkdir)) ərəb mənşəlidir. Ən birinci sırf bu ərəb milləti açıq mətni (informasiyanı) mühafizə,etmək, qorumaq məq-sədilə əlifba hərfləri rəqəmlərlə dəyişdirə bildilər. Təxmini olaraq bir neçə şifrə-yə həsr olunan-“İnsanların qədim yazıların sirlərini açmasına böyük cəhdlər”i mövzusunda bir kitab adlandırılmışdır. İlk dəfə bu kitab yəni birinci kitab nəşr olunmuş 855-ci ildə işıq üzü görülmüşdür. İtaliyada yaşayan bir riyaziyyatçı, həkimi və həmdə o böyük filosof Cerolamo Kardano seçmə fəsiləri kriptoqrafiya mövzusu haqqında həsr edilmiş-“İncəliklər haqqında” kitab nəşr etmişdir. Kardano Cerolamo gizli açarların sayını nəzərə almaqla şifrələrin davamlığının-isbatını təklif etmiş, açıq mətni bir açar kimi istifadə edərək ye-ni şifr-Kardano qəfəsi kimi bir qəfəs olaraq təkliflərin vermişdir.

Bu Kardano qəfəsi adlanan bir qəfəs bərk maddələrdən hazırlanmış lövhə tərəfindən müxtəlif fərqliliklərə malik olan intervallarda bir hərflə hündürlüyündə və cürbəcür uzunluğa malik olan düz- bucaqlı kəsiklər açmaqla təəşkil olunur. Kağız üzərində istifadəçi kimi, Kardano qəfəsi qoy- maqla kəsiklərə məxfiləşdirilməli lazımı informasiyanı qeyd edərildilər. Növbəti addımda, Kardano qəfəsini gö- türüldükdən sonra kağız üzərinə boş olan sahələrə təxmini məzmunlu bir mətn elə yazılırdı ki, məxfiləşdirilmiş informasiya fərqliliklərə malik olan uzunluqlu kəsik yerlərinə yerləşdirərək gizli bir (kriptomətin) mətn kimi tərkib

hissəsinə görünürdü (yuxarı baxan, aşağı baxan, şaquli və fırlanmış) vəziyyətdə tutularaq yerləşdirilərək qəfəsin yerləşdirilməsinin mümkün sayı dörd dəfə artır. Ümumiyyətlə bu dövrlərdə kriptografiyaya haqqında bir neçə yeni fikirlər gətirilmişdir. Tomas Cefferson-Amerikanın Birləşmiş Ştatlarının 3-cü prezidenti, birinci dövlət katibi, kriptografiya dövründə xüsusi bir yer tutmuşdur qurğu. Kəsiklərin üz tərəfinə ingilis əlifbasının hərfləri ixtiyari ardıcılıqda qeyd olunur. Silindirin səthi üzrə oxa paralel çubuq bərkidilir. Şifrələmə zamanı açıq mətn 36 hərf üzrə qruplaşdırılır. Mətni təşkil edən hərflər öz qrupunda durduğu sıra nömrəsinə uyğun nömrəli dairədə çubuq üzrə düzülür. Şifrələnmiş mətn həmin çubuğa paralel istənilən sıradan seçilə bilər.

Alınmış kriptomətn analoji şifrələyicidə dairələri fırlamaqla yığılır, açıq mətn isə ona paralel sıralar içindən seçilir.

Decius Wadsworth 1817-ci ildə prinsipial olaraq yeni şifrələmə qurğusunu işləyib hazırladı. Bu inkişafda yeni olan odur ki, açıq məlumat və şifrələnmiş məlumat müxtəlif uzunluqlara malikdir. Alim August Kerkhoffs 19-cu əsrin 80-ci illərində "Hərbi Kriptografiya" adlı bir kitab nəşr etmək qərarına gəldi. Bu kitab cəmi 64 səhifədən ibarət olsa da, kriptografiya tarixində bu səhifələr onun ölməzliyini təmin edib. Bu kitab bu gün də aktual olan parollar üçün altı əsas tələb irəli sürür:

1. Sistem nə fiziki, nə də riyazi mülahizələrin təsirinə məruz qalmamalıdır

2. Sistemin gizli saxlanması ehtiyac olmasa da, icazəsiz şəxslərin ona daxil olması problem yaratmamalıdır.

3. Açar sadə olmalı, kağız üzərində yazmadan (məlumat daşıyıcılarında) saxlanmalı və müəllif tərəfindən asanlıqla dəyişdirilməlidir.

4. Sistem teleqrafla (rabitə sistemi) ötürülə bilən informasiyaya uyğun olmalıdır.

5. Sistem asanlıqla tanınır (tərcümə olunur) və inkişafı birdir, bir neçə istifadəçinin (fərdlərin) iştirakı tələb olunmamalıdır.

6. Nəhayət, sistem müxtəlif şəraitlərdə istifadə olunacağı üçün dərin zəka və çoxlu sayda qaydalar tələb etmədən istifadəsi asan

olmalıdır.

Bu tələblərdən ikincisi *Kerkqoffs prinsipi* kimi məşhurlaşmışdır. 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 ardıcılığından ibarət alqoritmin açar adlanan 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.

I FƏSİL. İNFORMASIYA 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;
- kriptografik vasitələrə.

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

İnformasiya sistemlərinin perimetrlərinin mühafizəsi üçün aşağıdakı 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 kabledən istifadə olunması;

- rabitə xəttinə yüksək tezlikli 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 yayılmışlar aşağıdakılardır [1,2]:

- mühafizə rekvizitlərinin saxlanması 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 şifrənməsi qurğusu (kriptoqrafik üsullar).
- kompüterin etibarlı yüklənməsi modulu.

Proqram vasitələri istifadəçilərin eyniləşdirilməsi, daxilol-maya nəzarət, informasiyanın şifrənməsi, müvəqqəti növlü qalıq fayllarının kənar edilməsi, mühafizə sistemlərinə testlə nəzarət edilməsi və s. üçün proqram vasitələrindən ibarətdir. Proqram vasitələrinin üstün cəhətlərinə, onların universallığı, çevikliyi, etibarlılığı, qurulmasının sadəliyi, modifikasiyaya və inkişaf qabiliyyətləri 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 ziyan-verici 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 korporativ 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 firewal-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 vasitə-si ilə həyata keçirilir. Aşkardır ki, bu zaman qlobal şəbəkədən lokal şəbəkəyə prinsipə müraciət mümkün olmur. Bu metod daha yüksək səviyyələrdə, məsələn, tətbiq səviyyəsində (virus-lar, Java kodu və Java Script) hücumdan mühafizəni kifayət dərəcədə təmin edə bilmir.
- VPN (xüsusi virtual şəbəkə) şəbəkə üzərindən məxfi informa-siyanın 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, daxil-olmanın 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

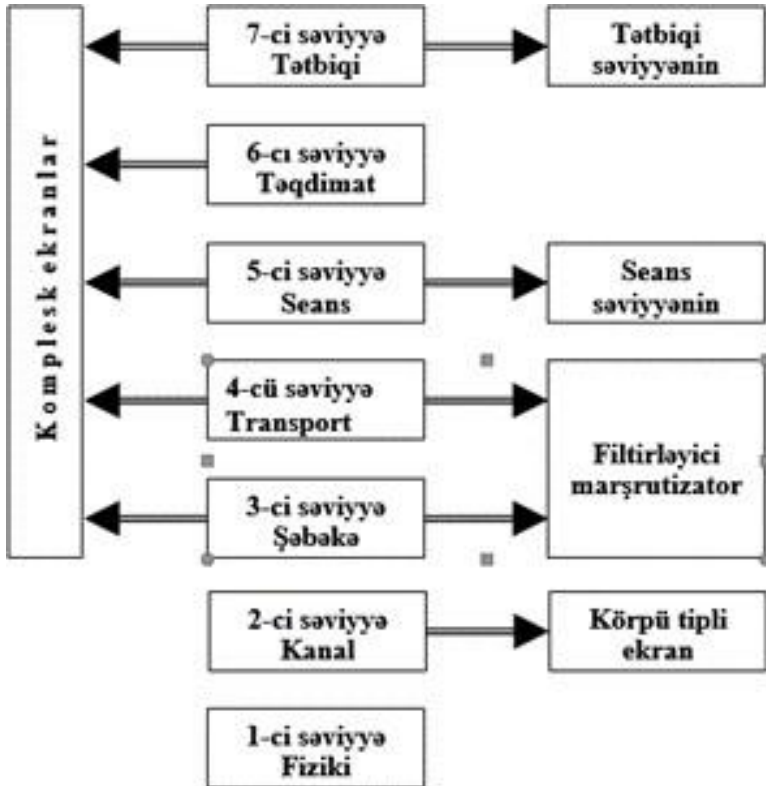
Şəbəkələrarası ekran.

İnformasiya təhlükəsizliyinin proqram- aparat vasitələri haqda danışarkən qəbul etmək lazımdır ki, lokal şəbəkələrin obyektlərinin açıq şəbəkələrin (məsələn, İnternet şəbəkəsinin) təsirlərindən mühafizə etmək üçün ən effektiv üsul, onla-rın arasında hər-hansı bir elementin yerləşdirilməsi üsuludur. Bu elementdən keçən şəbəkə paketlərinin verilən qaydaya uyğun olaraq nəzarətdir və süzgəcləyir. Bu element şəbəkələrarası ek-ran yaxud fayrvol, brandmuer (“firewall”) adını almışdır. Mühafizə olunan korporativ şəbəkələrin resurslarından istifadə etmək üçün çıxışı və girişiməhdudlaşdırmaq eləcədə həmin şəbəkə vasitəsi ilə xarici şəbəkələr arasında, və şəbəkə seqmentləri arasında məlumat axınına ciddi nəzarət etmək üçün təhlükəsizlik cihazlarından və firewalllardan

istifadə etmək lazımdır.

Firewallard yəni şəbəkələr-arası ekran (bunan sonra ŞAE kimi qeyd olunacağ)-korporativ kompüter şəbəkələrində avtomatlaşdırılmış məlumatların sistemlərinə da-xil edilən və yaxud onlardan qeriye dönen məlumat axınına ciddi nəzarət edən və bunu həyata keçirən lokal eləcədə funksional tərəfdən verilən proqram (pro-qram-apparat) vasitələridir (şək.1.1). Korporativ kompüter şəbəkə-lərində şəbəkə ekranının qoşulma sxeminin göstərilən təsnifatını ver-mək mümkündür [1,2] (şək. 1.2):

№	Təsnifatı	Osi modelin səviyyəsi
1	Körpü tipli ekranlar	Osi modelin 2-ci səviyyəsi
2	Filtirləyici marşutizatorlar	Osi modelin 3-cü və 4-cü səviyyəsi
3	Seans səviyyəsinin şlüzləri	Osi modelin 5 ci səviyyəsi
4	Tətbiqi səviyyənin şlüzləri	Osi modelin 7 ci səviyyəsi
5	Kompleks ekranlar	Osi modelin 3 və 7-ci səviyyələri



Şəkl.1.2. Şəbəkərarası ekranın Open Systems Interconnection modelinin fərqli səviyyələrində həyata keçirilməsi

Şəbəkərarası ekran Open Systems Interconnection 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 portunda.

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 axınının 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 tətbiqlərin 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 qabiliyyətinin olması

Çatışmayan cəhətləri [1,2]:

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

Şəbəkələrarası ekran ŞAE-nin nəzərə salınan təsnifatından əlavə göstərilən növləri müəyyənolunub:

Ekspert səviyyəli şəbəkələr arası ekranın-Open Systems Interconnection modelinin ən əsas üç səviyyəsində qəbul olunan paketlərin məzmununu yoxlayır. Bu səviyyənin: ilk öncə Osi modelinin şəbəkə səviyyəsi, seanas səviyyəsi Osi modelinin və tətbiqi səviyyə.

Müxtəlif şəbəkələrarası ekranların hansı növ sistem funksiyaların yaxud hansısa bir proseslərin şəbəkənin məlumatlarına giriş imkanını nəzərə alaraq eləcədə hüquqlarına malik olmasına görə idarəetmə prinsiplərini qeyd edərək, gələcəkdə qorunmanı, geniş- ləndirməyə imkana malik olur. Belə növlər ŞAE trafikinin icarəyə verilməsi yaxud qəbul etməməsi üçün müxtəlif, fərqli siqnatura və şərtləri istifadə edə bilirlər. Dinamik şəbəkələr arası ekran əvvəllərdə qeyd olunan standart ŞAE-ları və şəbəkəyə girişlərin aşkarlanması üsullarını cəmləşdirir, onların köməyi ilə müəyyən imzalara (siqnaturalara) uyğun gələn şəbəkə əlaqələrinin dərhal bloklanmasını təmin edir və digər mənbələrdən bu porta qoşulmağa imkan verir. Məsələn, şəbəkə qurdlarını real normal əməliyyatları pozmadan dayandırmaq mümkün olar.

1.3. Hücumların aşkarlanması sistemləri

Korporativ İS(informasiya sistemlərinin) təbii fəaliyyətinin təşkil edilməsi üçün lazımı olan standart qoruma vasitələri (misal üçün, ŞAE, ehtiyat sürətin saxlanması sistemləri, qoruyucu proqramları) ilə yanbayan hücumların qeyd olunması, tapılması sistemlərinin istifadəsinə möhtaclıq yaranır. Hücumların aşkarlanması sistemlərinin, şəbəkə attaklardan qorunması üçün əsas vasitədir.

Hal-hazırda hücumların aşkarlanması sistemlərinin, kompüter şəbəkələrinin, təhlükəsizliyinin qorunması üçün vəziyyətin ciddiyyətini anlayanda bu sistemlərdən daha çox istifadə olunur. İnformasiya toplama vasitələri yəni sensor; toplanmış informasiyanın təhlili vasitələri yəni analizator; reaksiya verən

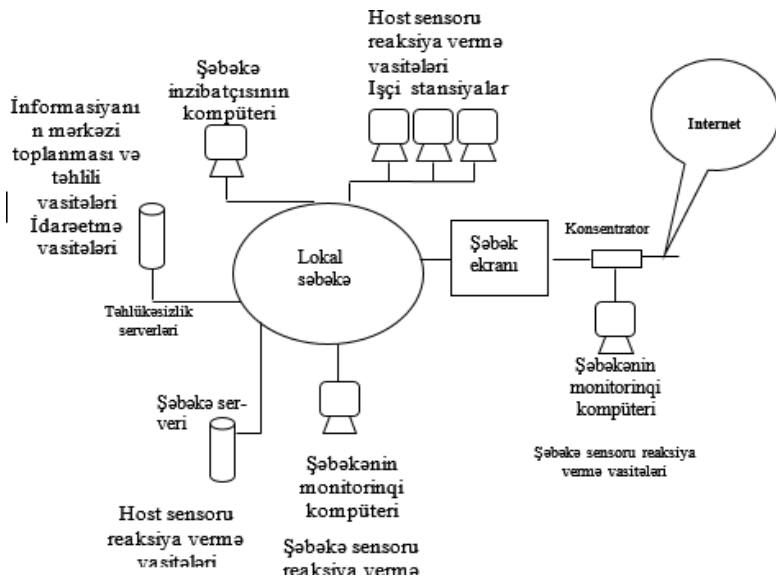
vasitələr;

idarəetmə

vasitələri. Bu vasitələr hücumların aşkarlanması sistemlərinin arxitekturasına, qəbul edilir [1,2]:

Açıqcası, hücumların aşkarlanması sistemlərinin nəzərə alınan bütün komponentləri kompüterdə yaxud bir proqram əlavəsi üzrə fəaliyyət göstərə bilər. Bununla belə, onları ərazi və funksional olaraq korporativ şəbəkənin hissələri üzrə yaymaq daha məqsəduyğundur. Xarici şəbəkəyə müdaxilənin aşkarlanması sisteminin analizatoru və idarəetmə elementlərinin firewall arxasında yerləşdirilməsi çox təhlükəlidir.

Beləliklə, əgər bu alətlər ələ keçirilərsə, təcavüzkar (cinayətkarlar) müdaxilənin aşkarlanması sistemlərində istifadə olunan əsas qaydaları təhlil edərək qorunan daxili şəbəkənin strukturu haqqında məlumat əldə edə biləcək. Hücumların aşkarlanması sistemlərinin 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

Müasir korporativ kompüter şəbəkələrinin heterojenliyi və sürətli inkişafı zəif yerlərin çoxalmasına təkcə xarici deyil, həm də daxili şəbəkə xidmətlərində yayılmasına səbəb olur.

Şəbəkə nə qədər böyükdürsə, idarəçinin təhlükəsizliyini etibarlı şəkildə təmin etməsi bir o qədər çətinidir. Qeyd etmək lazımdır ki, təkcə iş stansiyaları, serverlər və ya kommunikasiya xətləri deyil, həm də məlumat axınlarının daxili şəbəkə marşrutlaşdırılması funksiyalarını yerinə yetirən ixtisaslaşdırılmış qurğular şəbəkəyə icazəsiz daxil ola bilər.

Son dövrdə korporativ kompüter şəbəkələri müxtəlif növ heterojen proqram təminatı və texniki dəstəkdən istifadə edilir. Bu baxımdan belə şəbəkənin çətinliyi əhəmiyyətli dərəcədə yüksəlir. Beləliklə, görülən şəraitdə korporativ şəbəkənin ortaq resurslarına onun daxili istifadəçiləri tərəfindən icazəsiz daxil olmaq təhlükəsi də artır. Bu vəziyyətdən çıxış yolu olaraq, daxili şəbəkəyə giriş məhdudiyyətlərinin səviyyəsinə nəzarət etməklə korporativ şəbəkənin paylaşılan resurslarının qorunmasını gücləndirə bilərsiniz. Bu firewall yaxud Brandmauer şəbəkə yoxlama alətlərindən istifadə etməklə edilə bilər. Şəbəkə daxilində informasiya axınının sərhədlərində icazəsiz girişlə mübarizə aparmaq üçün firewallar yerləşdirilməlidir.

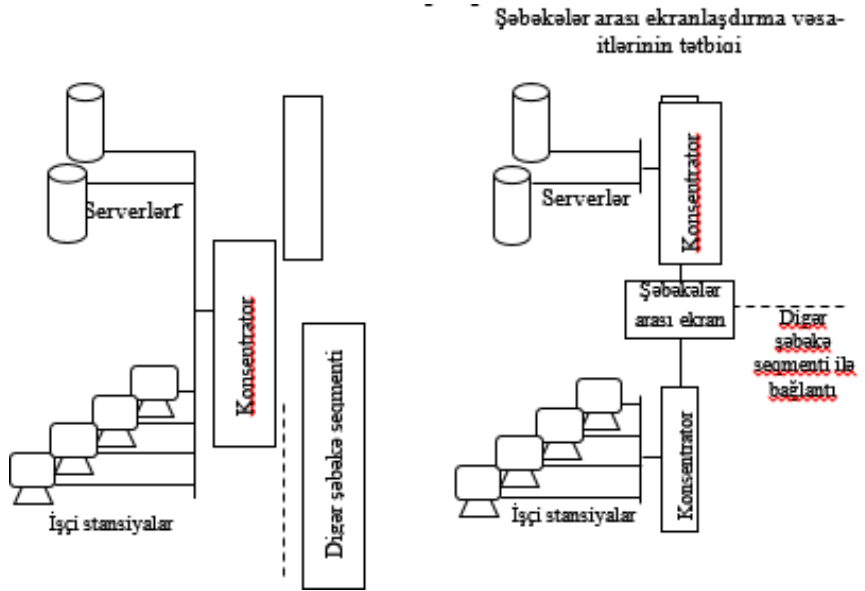
Lakin, korporativ şəbəkənin ayrı-ayrı seqmentləri arasında, eləcə də onun istifadəçiləri yəni müştəriləri və daha vacib şəbəkə xidmətləri arasında qarşılıqlı əlaqə yalnız firewall vasitəsilə həyata keçirilməlidir. (şək.1.4).

Şəbəkələr arası ekran, əlbəttə ki, asimmetrikdir. Bunun üçün bir şəbəkə seqmentindən digərinə keçidi məhdudlaşdıran və əlbəttə ki, əksinə olan xüsusi qaydalar müəyyən edilir. Ümumiyyətlə, firewallun bütün fəaliyyəti iki qrup funksiyanın dinamik icrasına əsaslanır. [1,2]:

- ❖ ondan keçən məlumat axınının süzgəcdən keçirilməsi;
- ❖ internet işinin qarşılıqlı əlaqəsinin həyata keçirilməsində

vasitəçilik.

Aşağıdakı parametrlər məlumat axınının təhlili üçün meyar kimi istifadə edilə bilər: [1,2]:



Şək. 1.4. Şəbəkələr arası ekranı birləşdirmədən əvvəl və sonra korporativ kompüter şəbəkəsinin fraqmentləri

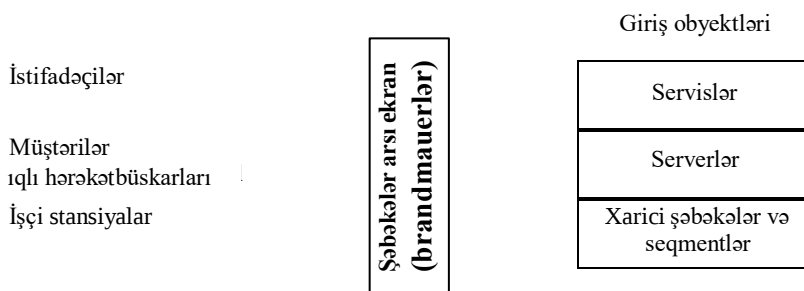
- ❖ interfeys ünvanlarını, şəbəkə ünvanını, port nömrələrini və digər vacib məlumatları ehtiva edən məlumat paketlərinin xidmət sahələrini ehtiva edən identifikatorlar;
- ❖ yoxlanılan məlumat paketlərinin məzmunu, məsələn, kompüter virusunun olması;
- ❖ informasiya axınının xarici xüsusiyyətləri, məsələn, vaxt, tezlik xüsusiyyətləri, verilənlərin həcmi və s.

Skrining agentləri internet şəbəkəsi ilə qarşılıqlı əlaqənin həyata keçirilməsi zamanı vasitəçilik prosesində məlumat axınının şəffaf

ötürülməsini bloklamaqla aşağıdakı sadalanan funksiyaları yerinə yetirə bilər. [1,2]:

- ❖ istifadəçilərin autentifikasiyası və identifikasiyası;
- ❖ ötürülən məlumatların autentifikasiyası;
- ❖ qorunan şəbəkə seqmentinin resurslarına çıxış əldə etmək məhdudiyyəti;
- ❖ informasiya axınının filtrasiyası və transformasiyası, məsələn, dinamik virus axtarışı və məlumatın şəffaf şifrələnməsi;
- ❖ gedən məlumat paketləri üçün daxili qovşaqların ünvanlarının tərcüməsi;
- ❖ hadisələrin qeydiyyatı, bu hadisələrə reaksiya verilməsi, qeydə alınmış məlumatların təhlili və hesabatların hazırlanması;
- ❖ tələb olunan məlumatın keşləşdirilməsi.

Şəbəkəni effektiv şəkildə qorumaq üçün mürəkkəb firewall ondan keçən bütün trafikə nəzarət etməli və onun statusunu izləməlidir. (şək.1.5).



Şək.1.5. Məlumat paketlərinin nəzarət edilməsi sxemi

Şəbəkə kommunikasiyalarını effektiv şəkildə qorumaq üçün firewall düzgün formada quraşdırılmalıdır həm də konfigurasiya edilməlidir. Qeyd olunan məsələ aşağıdakı addımları ardıcıl olaraq yerinə yetirməklə həyata keçirilməlidir. [1,2]:

- ❖ qarşılıqlı əlaqə siyasətinin inkişafı;

❖ birbaşa firewalllar üçün əlaqə diaqramlarının, eləcə də qoşulma

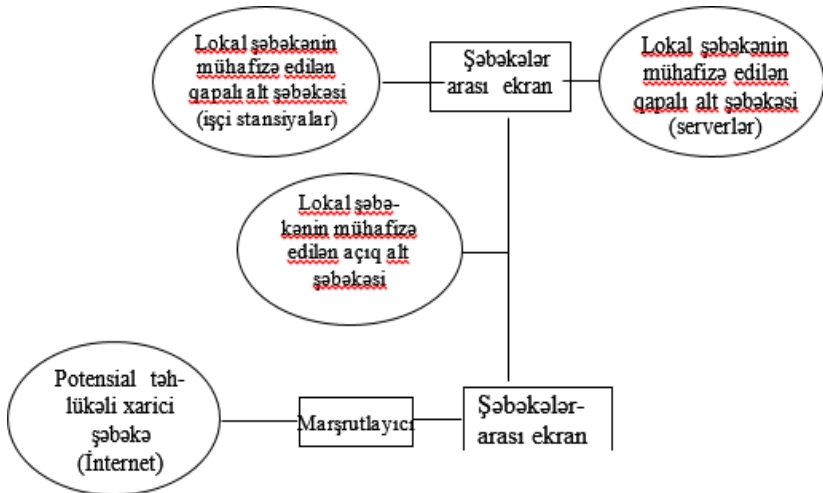
- ❖ diaqramlarının müəyyən edilməsi;
- ❖ firewall əməliyyat parametrlərinin köklənməsi.

Şəbəkə ilə qarşılıqlı əlaqə siyasəti təşkilatın xarici mühitlə məlumat mübadiləsi üçün təhlükəsizlik tələblərini müəyyən edən və aşağıdakı iki aspekti müəyyən edən təhlükəsizlik siyasətinin bir hissəsidir: [1,2]: giriş siyasəti şəbəkə xidmətlərinə və ŞAE-nin iş siyasəti.

Firewall siyasəti firewallun fəaliyyətinin əsasını təşkil edən şəbəkə rabitəsini idarə etmək üçün əsas prinsipləri müəyyən edir. Burada iki əsas yanaşmanı nəzərə almaq lazımdır. [1,2]:

- ❖ Açıqca icazə verilməyən hər şey qadağandır.
- ❖ açıq şəkildə qadağan olunmayan hər şeyə icazə verilir.

Şəbəkələr arasında qalxanları birləşdirmək üçün müxtəlif sxemlərdən istifadə edilə bilər. Belə sxemlər iş şəraitindən və firewallın şəbəkə interfeyslərinin sayından asılıdır. Kiçik olan korporativ şəbəkələr üçün iki firewalldan yəni ŞAE-dan istifadə etmək kifayətdir. (şəkl.1.6).



Şəkl. 1.6. Şəbəkələrarası ekranların(ŞAE) qoşulmasının misalı təklif olunub

Həmçinin burada qorunan açıq alt şəbəkə qoruyucu alt şəbəkədə göstərilir.

Hər vaxt olduğu kimi, qoruyucu alt şəbəkə elə açılır ki, alt şəbəkədəki kompüterlərə potensial olaraq həm düşmənin xarici şəbəkəsindən, həm də yerli şəbəkənin qoşulmuş alt şəbəkələrindən daxil olmağa icazə verilir.

Həmçinin, xarici şəbəkəsi ilə əlaqəli, alt şəbəkələr arasında birbaşa məlumatların mübadiləsi də mümkün olmayandır. Qoruyucu alt şəbəkəsi olan sistemə attakları etmək üçün ən azı iki heçnədən asıllığı olmayan yəni müstəqil təhlükəsizlik maneəsini aşmaq lazımdır ki, bu da təbii ki, çox çətin və ciddi bir məsələdir. Belə olduğu halda, firewall monitoring alətləri bu cür cəhdləri aşkar edəcək və sistem administratoru icazəsiz girişin qarşısını almaq üçün lazımi tədbirlər görəcək.

1.5. İnformasiya mühafizəsinin kriptografik vasitələri

Həmçinin, kriptografik şifrələmə alqoritmləri telekommunikasiya şəbəkələrində və sistemlərində informasiyanın birbaşa mühafizəsi üçün xüsusi olaraq istifadə olunur. [3,4]. Şifrələmə vasitələri informasiyanın mühafizəsinin mühüm məqsədi ilə yanaşı, informasiyanın bütövlüyünü, onun imzalanmasını, məlumat sahibinin həqiqiliyinin təsdiqini, təhlükəsiz istiqamətləndirilmiş kanalların təşkilini və digər mühüm həlledici məsələlərin həllini təmin etməyə kömək edir.

Kriptografiya informasiyanın istənilən formada, o cümlədən saxlama qurğularında saxlanılan və ya kompüterdə emal edilən, habelə rabitə kanalları ilə ötürülən informasiyanın mənasının gizlədilməsi deməkdir. Kriptografiya proqram təminatının qorunması üçün də istifadə edilə bilər. Daha əvvəl qeyd edildiyi kimi, informasiya təhlükəsizliyinin əsas istiqamətləri məhz məxfiliyin, bütövlüyün və əlçatanlığın təmin edilməsidir. Hər üç sahədə təhlükəsizliyi təmin etmək üçün kriptografik üsullardan istifadə olunur. Hətta bir aspektin pozulması hər şeyi xaosə aparacaq.

Belə ki, bu üsulların köməyi ilə məlumatın məxfiliyini şifrələmək və icazəsiz şəxslərin ondan istifadəsinin qarşısını almaqla təmin etmək olar. Şəbəkə üzərindən ötürülən məlumatın heç bir təhrif olmadan alıcıya çatmasını təmin etməklə yanaşı, böyük əhəmiyyət kəsb edir. Ən vacib və lazımı, onun bu xüsusi müəllif tərəfindən göndərildiyini müəyyən etmək olacaq. Belə ki, çox müddət insanlar özünü başqasının adı ilə təqdim edir, və öz adından məlumatları göndərir, informasiyaları alır eləcədə ötürür və s. Bu məqsədlə habelə istifadəçi, sistem və şəbəkə məlumatlarının həqiqiliyini yoxlamaq və autentifikasiya etmək lazımdır və məqsəddə yönümlü kriptografik üsullardan, metodlardan əsasən istifadə olunmalıdır.

Kriptologiya informasiyanın qorunması üsullarını inkişaf etdirən bir elmdir. (şək.1.7). Kriptoanaliz yəni şifrələmənin açılması və kriptografiya yəni şifrələmə hər iki sahə üzrə kriptologiya əhatə edir.



Şək.1.7. Kriptologiya

Kriptografiya informasiyanın məxfiliyinin təmin edilməsi yollarını, üsullarını öyrənən elmdir [3,4]. Kriptografiya məlumatı elə çevirməyə, şifrələməyə imkan verir ki, onu oxumaq, yəni müəyyən bir açar, bu halda paroldur məlumdursa, məlumatı bərpa etmək mümkün olsun. Şifrənin açılması üsulları kriptoanalizdə öyrənilir [3,4]. Buna görə də kriptologiyada verilənlərin şifrələnməsi və deşifrələnməsi üsulları öyrənilir. Şifrələncək və deşifrələnen məlumatlar konkret əlifba əsasında tərtib edilmiş mətn kimi başa düşülür.

Adətən şifrələmə proseduru xüsusi kriptografik metodun həm də açarın (açar, K-key) istifadə etmək üçün nəzərdə tutulur. Açar istənilən mətni sərbəst şifrələmək və deşifrələmə etmək üçün lazım olan bir məlumatdır. Yalnız bu açar haqqında bilik şifrəni açmaq imkanına zəmanət verir. Şifrələmə və şifrənin açılması (deşifrələnmə) proseslərində istifadə olunan üsulla (qaydaya)

kriptoqrafik alqoritm deyilir. Kriptoqrafik alqoritm, şifrə və ya kriptoalqoritm adlanan şifrələmə və deşifrə üçün məlumatların çevrilməsi üsuludur. Kriptoqrafik terminologiyada düz sənədlər açıq mətn-Plaintext, P və ya açıq mətn-hesab olunur.

Məzmunu qoruyarkən orijinal mətnin dəyişdirilməsi şifrələmə (E hərfi ilə qeyd olunur, *encryption*), şifrələnmiş məlumat isə şifrəli mətn (C hərfi ilə qeyd olunur, *cipher-text*) və ya kriptoqramma adlanır. Şifrə mətnindən açıq mətnin bərpası əks prosesdir və şifrənin açılması (D hərfi ilə qeyd olunur, *decryption*) adlanır. Parol dedikdə, verilmiş açardan eləcədə kriptoqrafik çevirmə alqoritmindən istifadə edərək açıq məlumat dəstini şifrələnmiş verilənlər dəstinə çevirən geri çevrilə bilən məsələn, ikili təyinatlı, yəni bərpa oluna bilən və ya orijinal vəziyyətinə qayıda bilən, çeviricilər dəsti başa düşülür [3,4] .

Şifrənin açılması üçün istifadə olunan açar (Şəkil 1.8) məxfi məlumatı göndərən şəxs açıq mətni bərpa etmək üçün məlum olduğu kimi, alıcıya da məlum olmalıdır. Müasir kriptoqrafiyada bu açardan istifadə etməklə şifrənin məxfiliyi təmin edilir.



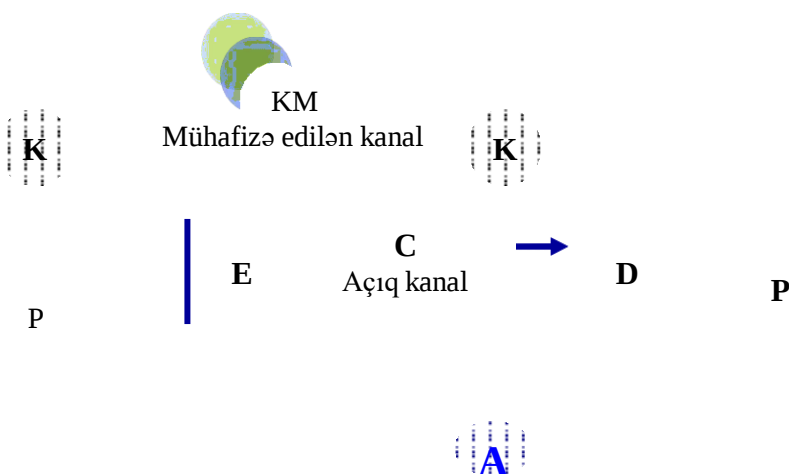
Şək.1.8. Deşifrəlmə açarları

Ən əsası odur ki, belə bir sistemin təhlükəsiz işləməsi üçün bu açar məxfi saxlanılmalıdır, ona görə də belə sistemlər gizli açar kriptosistemləri adlanır.

1.5.1. Kriptoqrafik sistemlərin modelləri və şifrələmə metodları

İnformasiyanın müəllifi adınan yönləndirilən açıq mətn Plaintext informasiya mənbəyində KM yaradılan açar (K-key) vasitəsilə şifrələnir (E), şifrəli mətnə *cipher-text* çevrilir və açıq kanal vasitəsilə ötürülür (şək. 1.9). [3,4]. Müəllif tərəfində şifrələnmiş bu mətn şifrənin açılması üçün təyin edilmiş açardan istifadə etməklə *decryption* orijinal vəziyyətinə qaytarılır.

Gizli açar kriptografik sisteminin alqoritminin mühüm hissəsi gizli açarın ötürüldüyü təhlükəsiz kanaldır. Bu kanal yüksək səviyyədə təhlükəsizlik və məxfiliyə malik olmalıdır ki, məxfi açar ötürülə bilsin. Bir sözlə, şəxsi açarın istifadə olunduğu sistemin bütün elementləri qorunmalıdır. Şifrələnmiş məlumatı göndərən üçün onun deşifrə edilə bilən qalması vacibdir. Şifrənin gücü o deməkdir ki, yad şəxslər tərəfindən ələ keçirilən şifrəli mətnin açıq mətnini deşifrə etmək cəhdlərinə müqavimət göstərir. Bu cəhddə kriptoolitliklər (A) əvvəlcə şifrənin kriptogramının qurulması prinsipini, sonra isə şifrəni açmaq üçün açarı müəyyən etməyə çalışırlar. Şifrənin bu xüsusiyyəti kriptografik güc yaxud kriptodavamlıq adlanır.

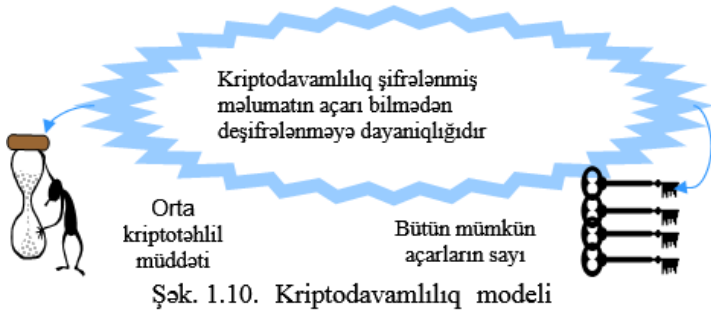


Şək.1.9. Şifrələnmə/deşifrələnmə sxemi

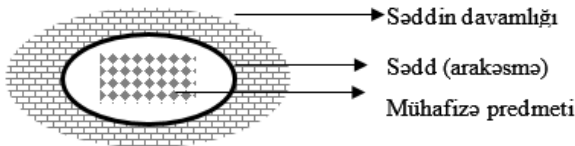
Şifrələrin müqayisəli gücü müasir hesablama vasitələri ilə təchiz edilmiş maraqlı şəxsin istənilən vasitə ilə məlumatın şifrəsini açmaq

cəhdi üçün tələb olunan vaxt nəzərə alınmaqla qiymətləndirilir. Açarın(K-key) variantları nə qədər çox olarsa, sərf olunan vaxta görə mətnin şifrəsini açmaq bir o qədər çətin olacaq (şək. 1.10) [3,4]. Modelin təhlükəsizliyinə görə, maneənin müddəti, təcavüzkarlar tərəfindən onu aradan qaldırmaq üçün sərf etdiyi vaxt məlumatın mühafizəsi predmetinin aktualıq müddətindən artıq olduqda kifayət hesab olunur. Beləliklə, verilən müddət zaman mühafizə predmeti qeydə alınmaqla informasiya təhlükəsizliyinin elementar modeli əsasında müəyyən edilməlidir (şək. 1.11) [3,4].

K.Şennon açıq məlumatın şifrələnməsini riyazi olaraq $C = F_i P$ modeli ilə göstərilmişdir. Qeyd etdiyimiz düstürdə (i)-indeksi dəqiq açara istinad, modelin F_i isə çevirmə funksiyasını təyin edir.



Şək. 1.10. Kriptodavamlılıq modeli

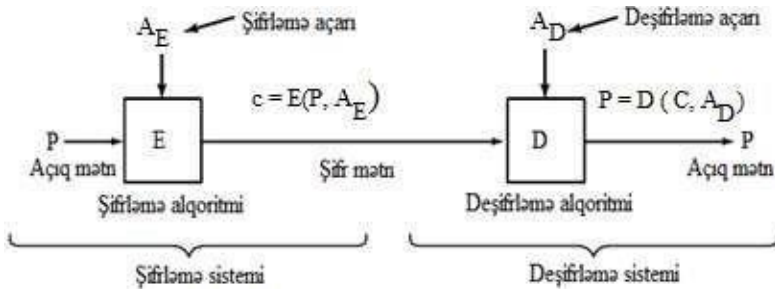


Şək.1.11.Informasiyanın elementar mühafizə modeli

Deşifrələnmənin birqiymətliliyinin lazımı olduğu müddətdə onun tərs funksiyası (F_i^{-1}) qeyd olunmalıdır: $P = F_i^{-1} C$

Şennonun şifrələmə/deşifrələmə modeli. Aşağıdakı göstərilən strukturda gizli açarlı kriptosistemlərin K.Şennon modeli göstəril-mişdir (şəkil.1.12)

[3,4].



Şək.1.12. Şifrlənmə/deşifrlənmə modeli

1.5.2. Sezar şifrləmə metodu

Birinci kriptosistemlər bizim artıq yeni eranın əvvəlində həyatımızda çıx-mışdır. Məsələn, Romadan ən məşhur Yuli Sezar sərkərdəsi eradan əvvəl yüzüncü illər öz yazdıqlarında hal-hazırdakı dövüdə Yuli Sezar adını olan şifrləmə geniş istifadə olunur.

Məsələn bizim əlifbanı nəzərə alsaq misal üçün azərbaycan əlifbası Bütün əlifba yazılırdı, onan sonra həmən əlifbanın altında yazırdıq, ancaq sola üç (yaxud, başqa bir sayla əvəz olun bilər, misal üçün altı hərf sürüşmə) hərf dövrü sürüşməsi ilə qeyd olunurdu [4]:

A	B	C	Ç	D	E	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	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						

İnformasiyanı şifrləmə müddətdi azərbaycan əlifbasında olan A hərfi Ç hərfi ilə əvəz olunur. C hərfi E ilə, X hərfi J hərfi ilə əvəz olunurlar və s. Açarla (bizim qeyd etdiyimiz açar üç hərf sürüşmə ilə qeyd olunub)şifrlənmiş informasiyanı qəbul edən şəxs hərfləri azərbaycan əlifbasının ikinci göstərilən sətirdə tapırdı və həmin

üstündəki hərflərə görə açıq informasiyanı bərpa edə bilirdi.

Gaius Julius Caesar şifrəsində əsas əlifbanın ikinci sətirindəki yerdəyişmə dəyəridir. Gaius Julius Sezarın modelinin bir neçə modifikasiyası olunub. Sezar şifrəsi tərəfindən həyata keçirilən şifrələmə addımı tez-tez Vigenere şifrəsi kimi daha mürəkkəb sxemlərin bir hissəsi kimi qəbul edilir. (şək.1.13).

Misal üçün, kvadratda qeyd olunan açıq mətn -LİMONAD açar ilə şifrələnmişdir. Məlumatın müəllifi açarın mətnini dövrü olaraq təkrarlamaqla məlumatın uzunluğu ilə aşağıdakı kimi eyniləşdirir [4]:

Açıq mətn:	A	R	M	U	D	S	A	R	I	D	İ	R
Açar sözü:	L	İ	M	O	N	A	D	L	İ	M	O	N
Şifrmətn:	L	Z	Y	İ	Q	S	D	C	Q	P	Ü	E

Orijinal mətnin ilk simvolu ("A") açarın birinci simvolu olan L ardıcılığı ilə şifrələnir. Şifrə mətninin ilk simvolu ("L") Vigenere cədvəlində L sətri ilə A sütununun kəsişməsində yerləşir. Eynilə, mənbə mətninin ikinci simvolu üçün açarın ikinci simvolu istifadə olunur; yəni şifrəli mətnin ikinci simvolu ("R") İ sətri ilə Zsütununun kəsişməsində alınır. Açıq mətnin qalan hissəsi də analoji şəkildə şifrələnir. [4]:

Şifrmətn: LZYİQSDCQPÜE

Şifrənin açılması isə aşağıdakı kimi həyata keçirilir: biz Vigenere cədvəlində açar sözün birinci simvoluna uyğun olan xətti tapırıq; bu sətirdə biz şifrəli mətnin birinci simvolunu tapırıq. Bu simvolun yerləşdiyi sütun mənbə mətnin birinci simvoluna uyğun gəlir. Şifrə mətnindəki aşağıdakı simvollar oxşar şəkildə deşifrə edilir.

Şifrmətn:	L	Z	Y	İ	Q	S	D	C	Q	P	Ü	E
Açar sözü:	L	İ	M	O	N	A	D	L	İ	M	O	N
Açıq mətn:	A	R	M	U	D	S	A	R	I	D	İ	R

Məsələn, axırıncı yazılışda açarın birinci hərfi L-dir, Vigenere cədvəlində onun yerləşdiyi sətirdə 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

Şək. 1.13. Vijnin kvadrati

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

Açıq mətn: ARMUDSARIDIR.

Digər bir misala baxaq. Tutaq ki, şifrəlmə üçün “OXUMAQMARAQLIDIR” sözünü “RAZIYAM” açarı ilə şifrəlmək tələb olunur. Bu sözü şifrəlmək üçün, onu birinci sətirdə yazırıq, onun alt sətirində isə açarın mətnini dövrü olaraq təkrarlamaqla məlumatın uzunluğu ilə aşağıdakı kimi eyniləşdiririk, yəni:

Açıq mətn:	O	X	U	M	A	Q	M	A	R	A	Q	L	I	D	I	R
Açar sözü:	R	A	Z	I	Y	A	M	R	A	Z	I	Y	A	M	R	A
Şifrmətn:	F	X	T	U	Y	Q	Y	R	R	Z	Y	J	A	P	Z	R

Yuxarıda göstərilən qaydanı tətbiq edərək aşağıdakı şifrmətni alırıq:
Şifrmətn: FXTUYQYRRZYJAPZR.

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

Şifrmətn:	F	X	T	U	Y	Q	Y	R	R	Z	Y	J	A	P	Z	R
Açar sözü:	R	A	Z	I	Y	A	M	R	A	Z	I	Y	A	M	R	A
Açıq mətn:	O	X	U	M	A	Q	M	A	R	A	Q	L	I	D	I	R

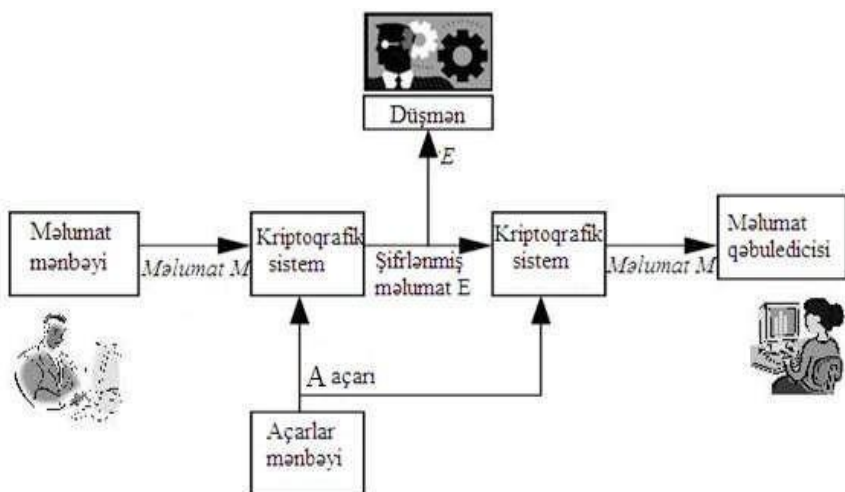
Beləliklə, yuxarıdakı qaydadan istifadə edərək biz aşağıdakı açıq mətni tapırıq:

Açıq mətn: OXUMAQMARAQLIDIR.

II FƏSİL. SİMMETRİK ŞİFRLƏMƏ TEXNOLOGİYALARI

2.1. Simmetrik şifrələmənin struktur sxemi

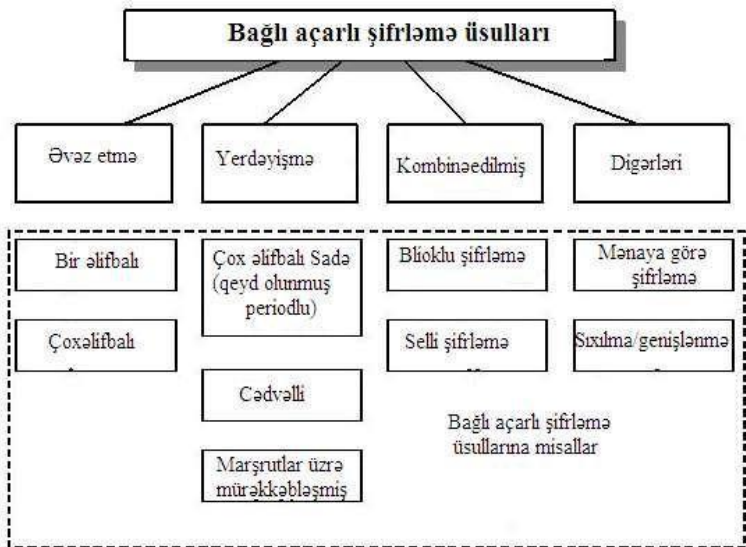
Klassik yaxud biraçarlı kriptografiya simmetrik şifrələmə alqoritmlərinə əsaslanır. Belə texnologiyada şifrələmə və deşifrələmə yalnız yerinə yetirilmə qaydalarına və bəzi addım istiqamətlərinə görə fərqlənilir. Bu texnologiyada eyni bir məxfi element (açar) istifadə edilir və deşifrələmə əməliyyatı şifrələmənin sadə çevirməsidir. Ona görə də mübadilə iştirakçılarından hər biri məlumatı həm şifrələyə, həm də deşifrələyə bilər. Simmetrik şifrələmənin struktur sxemi şəkl.2.1-də verilib [3,4].



Şəkl.2.1. Simmetrik şifrələmənin struktur sxemi

Şifr dedikdə ilkin məlumatın mühafizəsi üçün əvvəlcədən şərtləşdirilmiş çevirmə üsullarının məcmuu başa düşülür. Açar-məlumatların şifrələnməsi və deşifrələnməsi 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 tərəfə verilir, hərçənd güman edilir ki, onu ələ keçirmək olmaz, məsələn, bu açar xüsusi

kuryer vasitəsilə verilir (ona görə simmetrik şifrələmə bağlı açarlı şifrələmə adlanır). Məlumat mənbəyi hər hansı bir M məlumatı hasil edir, sonra bu məlumat seçilmiş açarı istifadə etməklə şifrlənir. Şifrələmə prosedurunun nəticəsində kriptogramma adlanan şifrlənmiş E məlumatı alınır. Sonra E kriptogramı rabitə kanalı üzrə verilir. Rabitə kanalı (radiokanal, yaxud kompüter şəbəkəsi) açıq və mühafizə olunmamış olduğundan verilən informasiya düşmən tərəfindən tutulub saxlanıla bilər. Qəbul tərəfdə E kriptogramını açar vasitəsilə deşifrəleyib 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 məlumatından və A açarından asılı olan hər hansı bir funksiyadır. Kriptografik sistemdə istifadə olunan şifrələmə üsulları və alqoritmləri yuxarıda göstərilən ifadədə f funksiyasını təyin edir [3,4]. Bağlı açarlı şifrələmənin müxtəlif üsulları mövcuddur (şəkl.2.2).



Şəkl.2.2. Bağlı açarlı şifrələmə 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 qayda 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 məlumatın şifrələnməsi üçün məhdud sayda simvollar toplusudur. Kodlaşdırılan mətn isə verilmiş əlifbanın elementlərinin ardıcılığıdır.

2.2.1. Birəlifbəli əvəzetmə.

Əsas əvəzetmə metodlarından biri birəlifbəli əvəzetmə metoduudur. Bu metodda A məlumatının ilkin əlifbasının hər bir a_i işarəsi ilə şifrələnmiş E mətninin uyğun e_i işarəsi arasında birmənalı uyğunluq yaranır. Birəlifbəli əvəzetmə ən sadə əvəzetmə şifri oldu-ğundan bəzən sadə əvəzetmə adlanır. Birəlifbəli əvəzetməyə misal olaraq ən sadə şifrləmə sistemlərindən biri olan və “Gaius Julius Caesar şifri” adını daşıyan şifrləmə sistemini göstərmək olar. Belə fərziyə var ki, bizim erayadək 1-ci əsrdə yaşayan məşhur 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 hərfi 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 Zhərfi 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 “UNİVERSİTET” açıq mətnini şifrləsək aşağıdakı şifrmətni alırıq.

Həlli: “UNİVERSİTET”-şifrləmə -“ZPQAĞTUQVĞV”-şifrmətn.

Sezar şifrləmə metoduna əsasən burada U hərfi Z hərfinə, N hərfi P-ya, İ hərfi Q-yə, V hərfi A-yə, E hərfi Ğ-ya, R hərfi T-yə, S-hərfi U-

la, I hərf Q -yə, T hərfi V hərfə, E hərfi Ğ hərfə, T hərfi V hərfi ilə əvəz edilir.

Beləliklə, “UNİVERSİTET” sözü “Gaius Julius Caesar şifri” şifrələmə metoduna əsa-sən “ZPQAĞTUQVĞV” sözünə çevrilir.

Şifrmənin deşifrəlməsi zamanı şifrələnmiş mətnin hər bir hərfi sola doğru olan üçüncü hərfə əvəz edilir. Məsələn yuxarıda gös-tərilən şifrməni deşifrələsək aşağıdakı açıq mətni alırıq

“ZPQAĞTUQVĞV” – deşifrələmə “UNİVERSİTET”- deşifrələnmiş mətn.

Bu metod çox çətin metod deyil, xüsusən ona görə ki, bir neçə sözdən ibarət məlumatın şifrəlməsi zamanı ilkin mətnin neçə söz-dən ibarət olması dərhal aydın olur. Bundan başqa, şifrələnmiş məlu-matda hərflərin təkrarlanması üzrə hər hansı məlumatı almaq olar. Məsələn, şifrələnmiş “ZPQAĞTUQVĞV” sözündə hərfərdən birinin “Ğ” hərfi və “V” eləcədə “Q” hərfəri iki dəfə təkrar olunması aydın olur.

Buna baxmayaraq, Sezar kriptografiya tarixinə düşdü, “Gaius Julius Caesar şifri” isə ilk şifrələmə sistemlərindən biri kimi qiymətləndirilir.

“ZPQAĞTUQVĞV” sözünün şifrini açmaq üçün yalnız şifrələmə al-qoritminin özünü bilmək vacibdir. Şifrələmə üsulunu bilən istənilən adam, məxfi məlumatın şifrəsini asanlıqla aç-a bilər. Beləliklə, bu metodda açar alqoritmin özüdür.

Üç, beş, yeddi açarı bu primitiv alqoritmin kriptografik gücünü, davamlığını qismən artırmaq üçün də istifadə etmək mümkündür. Simvolların yerdəyişməsi əvvəlcə hər üç, sonra hər beş və yeddi hərfdən bir baş verəcək və bu proses mətnin sonuna qədər təkrarlanacaq. Bu zaman açarı təşkil edən simvolların ardıcılığı açar söz, bir neçə sözdən ibarət olduqda isə açar söz birləşməsi adlandırılır. Müxtəlif verilənlərin şifrələmək, kodlaşdırılmağ üçün hər dəfə istifadə edilən eyni açar statik açar deyilir. Hər bir verilənlərin kodlaşdırmaq üçün istifadə edilən yeni açarlara isə dinamik açar deyilir. Burada birinci sətir ilkin əlifba, ikinci (dövrü olaraq qədər sürüşmə ilə sola) isə əvəz etmə vektoru adlanır.

Birəlifbəli şifrələmə metodunda əvəzləmə cədvəlindən də istifadə etmək olar. Bunu aşağıdakı cədvəlin təmsalında 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 cədvəl əsasən əvəzləmə aşağıdakı kimi aparılır.

Cədvəl 2.1

Açıq mətn	Şifr 1	Şifr 2	Açıq mətn	Şifr 1	Şifr 2	Açıq mətn	Şifr 1	Şifr 2
A	G	^	X	B	№	P	D	Σ
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	ω
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 “Plain text(açıq mətn)” sütununda onun mövqeyi təyin edilir. Şifrlənmiş məlumatı əvəzləmə cədvəlinin bu sətrindən şifrlənmiş işarə qoyulur.

Misal:Azərbaycan əlifbası ilə verilmiş cədvəldə açıq mətni 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
Şifr 1-i istifadə etməklə şifrlənmiş məlumat															
Z	I	O	T	K	F	S	Ğ	Y	U	K		Z	Ş	F	S
Şifr 2-ni istifadə etməklə şifrlənmiş məlumat															
*	ω	)	%	√	!	<	-	▽	⊗	√		*	®	!	<

Bunun üçün ilkin məlumatın birinci hərfi açıq mətnin “G”-nı götürürük. Cədvəl 2.1-də Simvolar verilən “Şifr1” sütununda “G”-hərfi üçün əvəzləmə işarəsini tapırıq. Bu “Z”-hərfdir. 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”-sütunundan-“Plaintext”-in-“Ü”-hərfinin qarşısında duran hərfi tapırıq. Bu-“T”-hərfdir. Beləliklə, şifrələnmiş məlumatın ikinci hərfi olan-“T”-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 şifrələnmiş 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. Kriptografiyada qəbul olunub ki, düşmən şifrələmə 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. Düşməne 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 sətirdə 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										

“FÜZCİKA”

- | | | |
|----------------|-----------------|-----------------|
| 1. G V A Ç Q B | 7. J Ç Ə Ğ P F | 13. O Ğ İ 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 İ Ş H | 16. R İ 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”-sözüdür. Bu söz 17-ci mövqedə yerləşir. Beləliklə, şifrələnmiş 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 şifrələnmiş 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 şifrənməsi

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 şifr-ləyir və 45678 ədədini alıb, onu öz abonentinə göndərir. Düşmənin bu kriptogramı 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 işarəsürüşməsindən alınan bütün variantları yazaq (cədvəl 2.3).

Görünür ki, alınan bütün variantlar eyni qiymətlidir və cına-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.

Cədvəl 2.3. Qıfılın şifrlənmiş kodunu açmaq üçün variantların seçilməsi

Tutulub saxlanılan kriptogram 45678

1	56789
2	67890
3	78901
4	89012
5	90123
6	01234
7	12345
8	23456
9	34567

Proporsional şifrın 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 variant 1	İşarə	Əvəz- ləmə variant 1	İşarə	Əvəz- ləmə variant 1	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. Çoxəlifbəli əvəzləmə üsulu

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

Çoxəlifbəli əvəzləməyə misal olaraq Vijiner cədvəlinə əsaslanan sxemi göstərmək olar. Bu metod artıq XVI əsrdə, 1585-ci ildə fransız Blez Vijiner tərəfindən yazılmış “scientific work on cipher”-dən məlumdur. Bu metodda şifrləmə üçün özündə elementlərinin sayı $N \times N$ olan kvadratik matrisanı əks etdirən cədvəl istifadə olunur, burada N əlifbadakı işarələrin sayıdır. Matrisanın birinci sətrində ilkin əlifbanın növbəlik qaydasında hərfləri yazılır, ikinci sətrində hərflərin həmin ardıcılığı saxlanılır, lakin dövrü olaraq bir işarə, üçüncüdə isə iki 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	
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	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	U	Ü	V	Y											

Mətnin şifrəlməsi 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 reallaşdırılır (cədvəl 2.6-ya bax). Məsəl 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-ya bax). Bu cədvəl ilkin mətnin şifrəlməsinə imkan verir. Cədvələ əsasən ilkin mətnin şifrəlməsi aşağıdakı qaydada həyata keçirilir.

Cədvəl 2.6

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

Bu məqsədlə aşağıda göstəriləyi 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: BƏYAZBƏYAZBƏYAZB

Bundan sonra cədvəl 3.6-ın A hərfi ilə başlayan birinci sətrinin sırasında ilkin mətnin birinci hərfi olan Y hərfini tapırıq, sonra həmin cədvəlin açarın birinci hərfi B ilə başlayan ikinci sətrinin sırası üzrə sağ tərəfə ilkin mətnin Y hərfi ilə kəsişmə nöqtəsinədək irəliləyib bu nöqtədə yerləşən hərfi tapırıq, bu hərflər cədvəl 2.6-ın ikinci sətrində qalın qara rənglə qeyd edilmiş Z hərfidir. Elə bu hərflər də şifrəmənin 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 açarın 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 hərflər cədvəl 2.6-ın üçüncü sətrində qalın qara rənglə qeyd edilmiş X hərfidir. Bu hərflər şifrəmətin 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 həmin 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 hərflər cədvəl 2.6-ın dördüncü sətrində qalın qara rənglə qeyd edilmiş Ö hərfidir. Bu hərflər şifrəmətin üçüncü hərfi olacaq.

Sonra cədvəl 2.6-ın A hərfi ilə başlayan birinci sətrinin sırasında 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 hərflər cədvəl 2.6-ın birinci sətrində qalın qara rənglə qeyd edilmiş D hərfidir. Bu hərflər şifrəmətin 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 hərflər cədvəl 2.6-ın beşinci sətrində qalın qara rənglə qeyd edilmiş E hərfidir. Bu hərflər şifrəmətin beşinci 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 hərflər cədvəl 2.6-ın ikinci sətrində qalın qara rənglə qeyd edilmiş Z hərfidir. Bu hərflər şifrəmətin 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 şifrəmətin 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 şifrəmət-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 cədvəlin 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 şifrəmətin 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 şifrəmətin 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 şifrəmətin 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 cədvəl-in açarın onüçüncü Y hərfi ilə başlayan dördüncü sətrinin sırası üzrə sağ tərəfə ilkin mətnin E hərfi ilə kəsişmə nöqtəsindək 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 nöqtəsindək 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 nöqtəsindək 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-“ZXÖDEZNRMENXSOÇÜ”-şəklində şifrlənmiş mətni alırıq.

Məlumatın şifrinin açılması (deşifrlənməsi) prosesini Vijiner metodu timsalında nəzərdən keçirək. Fərz edək ki,-“BƏYAZ”-aça-rının köməyi ilə şifrlənmiş-“ZXÖDEZNRMENXSOÇÜ”-şifrmətni mövcuddur (şifrlənmə zamanı boşluq buraxılıb). Mətnin deşifrə olunması aşağıdakı ardıcılıqla həyata keçirilir.

Şifrmətni deşifrlemək üçün əvvəlcə açarın hərfləri tələb olunan sayda təkrarlanaraq ardıcıl olaraq birinci sətrdə yazılır, onun altında isə aşağıda göstəriləndiyi 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 doğru 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 açıq 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 Vijnere 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 ,2.8 a-ya baxaq:

cædvæl 2.8

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	
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	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	U	Ü	V	Y											

Cædvæl 2.8a

abcçdeəfgğhxiijkqlmnoöprsstuüvyz
 1bcçdeəfgğhxiijkqlmnoöprsstuüvyza
 2cçdeəfgğhxiijkqlmnoöprsstuüvyza b
 3çdeəfgğhxiijkqlmnoöprsstuüvyz a bc
 4deəfgğhxiijkqlmnoöprsstuüvyza bcç
 5eəfgğhxiijkqlmnoöprsstuüvyza bcçd
 6əfgğhxiijkqlmnoöprsstuüvyza bcçde
 7fgğhxiijkqlmnoöprsstuüvyza bcçdeə
 8gğhxiijkqlmnoöprsstuüvyza bcçdeəf
 9ğhxiijkqlmnoöprsstuüvyza bcçdeəfg

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 şifrə etmək lazımdır. Açar kodu halında 345 ədədini götürürük.

Bu kodu ilkin mətnin altında lazımı 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 üçə uyğun olan sətrinin kəsişməsində olan hərfi tapırıq. Bu hərf-ç-hərfdir, elə bu hərf də şifrəmənin birinci hərfi olacaq.

Əsas əlifbanın ikinci-z-hərfi ilə dördə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərfi-ç-hərfdir, bu hərf şifrəmənin ikinci hərfi olacaq. Əsas əlifbanın üçüncü-a-hərfi ilə beşə uyğun olan sətrin kəsişməsində olan hərfi tapırıq, Bu hərfi - e-hərfdir, bu hərf şifrə mətnin üçüncü hərfi olacaq. Əsas əlifbanın dördüncü-d-hərfi ilə üçə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərf-f-hərfdir, bu hərf şifrəmənin dördüncü hərfi olacaq. Əsas əlifbanın beşin-ci-l-hərfi ilə dördə uyğun sətrinin kəsişməsində olan hərfi tapırıq. Bu hərf-ö-hərfdir, bu hərf şifrəmənin beşinci hərfi olacaq. Əsas əlifbanın altıncı hərfi-ı-iləbeşə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərfi-l-hərfdir, buhərfşifrəmənin altıncı hərfi olacaq.

Həhayət, əsas əlifbanın yeddinci-q-hərfi ilə üçə uyğun sətrin kəsişməsində olan hərfi tapırıq. Bu hərfi-n-hərfdir, bu hərf də şifrəmənin yeddinci hərfi olacaq.

Beləliklə, biz nəticəvi şifrəməni alırıq:-ç-ç-e-f-ö-l-n-.

Deşifrəlmə prosesində aşağıda göstəriləni kimi birinci sətrdə açar kodu, onun altında isə əsas əlifba yazılır, yəni

Açar kodu 3 4 5 3 4 5 3

Şifrəmə ç ç e f ö l n

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

Beləliklə, şifrəməni deşifrəleyərək aşağıdakı ilkin mətni alırıq:

-azadlıq-.

2.4. Qammalaşdırma üsulu

Çoxəlifbəli əvəzləmənin xüsusi üsullarından biri də qammalaşdırma üsuludur. Bu üsulda şifrləmə 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 kriptografiyada qammaların üst-üstə qoyulması adlanır.

Fərz edək ki, ilkin əlifbanın işarələri 0 (A)-dan 32 (Z)-ə qədər olan aralıqda dəyişir. Əgər ilkin mətnin işarələrinə 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 yaxudondan böyük nəticə verirsə, onda toplanmanın 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 olunur, onda yazmaq olar:

$$z = x + a \pmod{2} = x \oplus a$$

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

Misal. Fərz edək ki, bizdən 14 onluq ədədini 12 açarını istifadə etməklə qammalaşdırma metodu ilə şifrləmək tələb olunur. Bunun üçün əvvəlcə ilkin ədədi və açarı (qammanı) ikili formaya çevirmək 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:

$$\begin{array}{l} 0 \oplus 0 = 0 \\ 0 \oplus 1 = 1 \\ 1 \oplus 0 = 1 \\ 1 \oplus 1 = 0 \end{array}$$

İki 1110 və 1100 ikili ədədləri modul iki üzrə toplayaq:

$$\begin{array}{rcl} \text{İlkin ədəd} & 1 & 1 & 1 & 0 \\ \text{Qamma} & 1 & 1 & 0 & 0 \\ \text{Şifrəmətn} & 0 & 0 & 1 & 0 \end{array}$$

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

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

$$\begin{array}{rcl} \text{Şifrələnmiş məlumat} & 0 & 0 & 1 & 0 \\ \text{Qamma:} & 1 & 1 & 0 & 0 \end{array}$$

$$\text{İlkin məlumat: } 1 \ 1 \ 1 \ 0$$

Alınan ikili ədədi, yəni 1110-ı onluq ədədinə çevirsək ilkin ədədi-14-ü alırıq. Beləliklə, iki modulu üzrə qammalaşdırma zamanı həm şifrəlmə və həm də şifrın açılması üçün eyni əməliyyat aparmaq lazımdır. Bu həm şifrəlmə və həm də şifrın açılması üçün proqram reallaşdırılması zamanı eyni bir alqoritm və uyğun olaraq eyni bir proqramı istifadə etməyə imkan verir. İki modulu üzrə toplama əməliyyatı digər hesablama əməliyyatlarına nisbətən kompüterdə 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 qammalaşdırmanın 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 şifrəlmək tələb olunur. Bu misalda ilkin məlumatın uzunluğu 12 bayt, açarın uzunluğu isə 5 bayta bərabərdir.

Buna görə də, şifrələmə zamanı qamma iki dəfə tam və hələ bir dəfə də natamam təkrar olunmalıdır. Şifrələmə 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 şifrələmək 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 axırcı 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-cü blok. İlk bitlər: 1010 1101 1010 1000 1010 0101

Qamma (açar): 1000 0010 1010 0101 1110 0001

Nəticə: 0010 1111 0000 1101 0100 0100

Şifrəni almaq üçün birinci blokun nəticəsini ayrı-ayrılıqda onaltılıq işarələrə çeviririk. Onda nəticədə olan birinci cütlik “0000 və 0001”- 01-ə; ikinci cütlik “0000 və 0101” cütlik-05-ə; üçüncü cütlik “0100 və 1101”-4D-yə çevrilir.

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

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

Nəhayət dördüncü blokun nəticəsindəki birinci cütlik “0010 və 1111” – 2F; ikinci cütlik “0000 və 1101”-0D; üçüncü cütlik “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:

Şifrə: 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 şifrəni, onun altında isə onaltılıq işarə ilə açar yazılır yəni:

Şifrlənmiş mətn: 01 05 4D 01 08 62 0B 43 0D 2F 0D 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, deşifrləmə zamanı qamma iki dəfə tam və hələ bir dəfə də natamam şəkildə təkrar olunmalıdır. Deşifrlənmiş mətnin və açarın onaltılıq işarələri yuxarıda göstəriləni kimi ayrı-ayrılıqda ikili kod şəklində yazılır və biri o birinin altında yazılır və 2 modulu üzrə toplanır.

I blok. Şifr mətn: 0000 0001 0000 0101 0100 1101

Qamma: 1000 0010 1010 0101 1110 0001

Nəticə: 1000 0011 1010 0000 1010 1100

II blok. Şifr mətn: 0000 0001 0000 1000 0110 0010

Qamma: 1010 1101 1010 0000 1000 0010

Nəticə: 1010 1100 1010 1000 1110 0000

III blok. Şifr mətn: 0000 1011 0100 0011 0000 1101

Qamma: 1010 0101 1110 0001 1010 1101

Nəticə: 1010 1110 1010 0010 1010 0000

IV blok. Şifr mətn: 0010 1111 0000 1101 0100 0100

Qamma: 1000 0010 1010 0101 1110 0001

Nəticə: 1010 1101 1010 1000 1010 0101

Deşifrəmə üçün birinci blokun nəticəsini ayrı-ayrılıqda onaltılıq işarələrə çeviririk. Onda nəticədə olan birinci cütlük “1 0 0 0 və 0 0 1 1” - 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 nəticəsinə 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 və 1 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 şifrələmənin də etibarlılığı 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 apararı 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” kriptografiyasınadək yerdəyişmə ilkin mətnin yazılması və şifrələnmiş mətnin həndəsi fiqurlar üzrə müxtəlif yol-larla oxunması nəticəsində alınır.

Yerdəyişməyə sadə misal olaraq qeyd edilmiş d periodlu yerdəyişməni göstərmək olar. Bu metodda məlumat d işalərindən ibarət bloklara bölünür 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 dəyişirlər, lakin digər qaydada verilir. Məsələn, $d = 6$ olduqda yerdəyişmə açarı kimi 436215-i götürmək olar. Bu onugöstərir 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 şifrənməsi tələb olunur:

BU_MƏTN_ŞİFRLƏMƏ_ÜÇÜNDÜR

İlkin mətnə işarələrin sayı 24-dür, buna görə məlumatı 4 bloka bölmək vacibdir. 436215 açarının köməyi ilə yerdəyişmənin nəticəsində şifrələnmiş məlumat aşağıdakı kimi olacaq:

M_TUBƏİŞR_NFƏMÜƏL_DNRÜÇÜ

Deşifrəlmə də açar vasitəsilə aparılır. Bu məqsədlə aşağıda göstəriləni kimi əvvəlcə birinci sətrdə açar təkrar olunmaqla yazılır, onun altında isə şifrəmətn 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

Deşifrəlmə 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. Axırncı misalda $d=6$ -dır, buna görə də yerdəyişmələrin sayı $6! = 1*2*3*4*5*6 = 720$ olacaq. Beləliklə, əgər düşmənin baxılan misaldakı şifrlənmiş məlumatı tutarsa, ona ilkin məlumatı açmaq üçün 720 cəhd lazım gələcək (əgər düşmənin 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 yerdəyişməni göstərmək olar. Bu metodda ilkin məlumatın bəzi cədvəllərin sətrlərinə yazılması və onu elə bu cədvəlin də sütunları üzrə oxunması həyata keçirilir. Sətrin doldurulması ardıcılığı və sütunların oxunması istənilən kimi açarlarla 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 olunur.

Aşağıda göstəriləni 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 yazmaq (cədvəl 3.8).

Sonra cədvəldən hər bloku ardıcıl olaraq sütunlar üzrə oxuyub yazmaqla aşağıdakı şifrlənmiş mətni aləcəyik:

BƏŞ UTİ_NFMM_RL_NƏÜD MÇU ƏÜD

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

bərabər olmayacağına, 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
–		Ç	Ü
N	Ü	Ü	D
	D		

hansı əlavə işarələrlə doldurmaq olar, məsələn, boşluqlarla. Lakin bunu etmək tövsiyyə edilmir, çünki, bu, düşməne informasiyanın kriptogramını tutduğu zaman istifadə olunan yerdəyişmə cədvəlinin ölçüsü (blokun uzunluğu) haqda informasiya əldə etməyə imkan verir. Blokun uzunluğunu tapdıqdan sonra düşmənin blokun uzunluğunun bölücüləri arasından açarın uzunluğunu tapa bilər.

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

zü şifrəyə: DƏYİŞMƏLİ

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

DŞİƏMYƏİL

Cədvəl 2.9

Cədvəl 2.9. Yerdəyişmə cədvəli üzrə natamam blokun şifrələnməsi

D	Ə	Y	İ
Ş	M	Ə	L
İ			

Şifri açmaq üçün əvvəlcə tam sütunların sayı təyin edilir, yəni

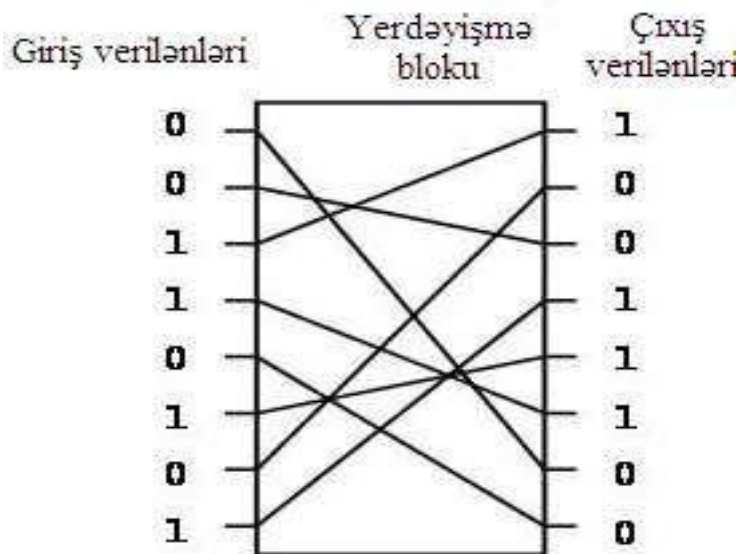
axırındakı işarələrin sayını (bizim misalda 1-dir). Bunun üçün məlumatın ölçüsünü (bizim misalda 9-dur) sütunların sayına bölürlər

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, şifrın açılması zamanı birinci üç işarəni (DŞİ) yerdəyişmə cədvəlinin birinci sütuna yazılır, növbəti iki işarə (ƏM) ikinci sütuna, növbəti iki işarə (YƏ)-üçüncü sütuna və axırcı 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. Şifrın 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, əvəzləmə) nəticədə kombinasiya edilmiş (kompozisiya) adlanır və çox çətin çevirmə verir. Bu şifr ayrı-ayrı əvəzləmələrə nisbətən daha güclü kriptografik 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 işarədən dördüncüsü- birinci yerdə, üçüncü işarə- ikinci yerdə, altıncı işarə - üçüncü yerdə və s. dururlar.

Seçilən $A = 436215$ açarla “SİQNAL” sözünü şifrləyək. Nəticə-də alırıq:

$$A = 436215$$

SİQNAL

NQLİSA

Fərz edək ki, düşməne şifrləmə metodu məlumdur, lakin açar məlum deyil. Əgər düşməni 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 düşməni 1 saniyə itirir. Onda 720 cəhdə 12 dəqiqə vaxt tələb olunur. Beləliklə, 12 dəqiqədən çox olmayan bir vaxtda düşməni bizim açarımızı öyrənir və həmin bağlı açarla da bütün məlumatın şifrini açar bilər. Əgər düşməni tərəfindən axtarış kompüterlə aparılırsa, NQLİSA məlumatının şifrəsinin açılmasına daha az vaxt sərf olunur.

Bu zaman belə bir sual yaranır, bizim şifrini kriptolanizini 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 ($1 \leq a_1 \leq 31$)-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	U	Ü	V	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 $31 \times 720 = 22320$ -yə bərabərdir. Beləliklə, həqiqətən alınan kompozisiya şifr ayrı-ayrı yerinə yetirilmiş əvəzləmə və yerdəyişmədən kifayət dərəcədə güclüdür.

Statistik üsulla kriptanalizi mürəkkəbləşdirmək üçün eyni bir açarla kompozisiya şifri 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

Dalbada iki yerinə yetirilən şifrləmə dövrünün nəticəsində SİQNAL sözü RUHTVC sözünə çevrildi. Bu zaman şifrin açarlar məkanı dəyişmədi, lakin iqiqat şifrəmətin hesabına ilkin mətnin statistik qanuna uyğunluğu güclü olaraq maskalanmışdır.

Deşifrləmə aşağıdakı qaydada aparılır:

Birinci mərhələ

$a_2=436215$

I Mərhələ: RUHTVC $\rightarrow$ VTURCH

$a_1=5$

II Mərhələ: VTURCH $\rightarrow$ SÖPMVE

İkinci mərhələ

$a_2= 436215$

I Mərhələ: SÖPMVE $\rightarrow$ VMÖSEP

$a_1=5$

II Mərhələ: VMÖSEP $\rightarrow$ SİQNAL

Simmetrik alqoritmlər ilkin mətni bloklarla və sellərlə emal edə bilirlər. Buna görə də simmetrik şifrələmə 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 üzərində bir neçə sadə əməliyyatlar istifadə olunur. Kriptodayanıqlığı artırmaq üçün bu əməliyyatlar raundlar yaxud addımlar yaratmaqla dövrü olaraq bir neçə dəfə yerinə yetirilir. Şifrənin dayanıqlığına blokun ölçüsü, açarın ölçüsü, şifrələmə raundlarının sayı kimi faktorlar təsir göstərir. Bağlı açarlı müasir şifrlər yalnız ikili verilənləri 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 şifrələmənin blok alqoritmlərində istifadə olunan əməliyyatlar

Bu alqoritmlərdə əməliyyatlar ikili verilənlərə tətbiq edirlər. İstənilən informasiya, məsələn, təsvir yaxud mətn ikili şəkildə ifadə edilə bilər. Bunun sayəsində şifrələmə zamanı verilən informasiya-nın mənası haqda düşünmək lazım gəlmir. Tez-tez istifadə olunan əməliyyatlardan biri-2modulu üzrə bitlərin toplanması əməliyyatıdır. 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 modulu üzrə 16-ışarəli

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: 1101100110011001

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

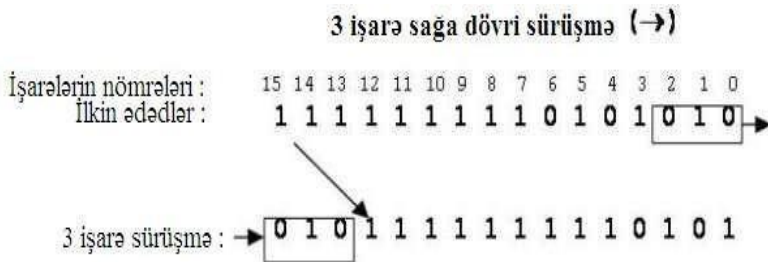
Dövrü sürüşmə bit zəncirlərini bir neçə işarə sola yaxud sağa sürüşdürür. Sola dövrü sürüşmə zamanı, soldan işarələr torundan çıxan bitlər, sağdan azad olan yerlərə yazılır (şək.2.4). Sağa dövrü sürüşmə zamanı bütün bitlər zəncirvari olaraq sağa hərəkət edirlər, hansılarının yer çatmır, onlar zəncirin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

Analoji olaraq sağa dövrü sürüşmə yerinə yetirilir (şək. 2.5). Göstəriləndiyi kimi sağa 3 işarə sürüşmə zamanı, ilkin ədədlərin sıfırıncı, 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 cədvəl üzrə digər 3 işarədən ibarət olan blokla əvəz etmək olar.

Əgər “Introduction” və “Exit” sütunlarında yazılmış hər bir qiyməti ikili şəkildə deyil, onluq şəkildə yazarsaqsa, onda həmin cədvəli aşağıdakı 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 yazmamaq, 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 nömrəsilə, əvəzlənən blokun qiymətinə bərabər element götürülür.

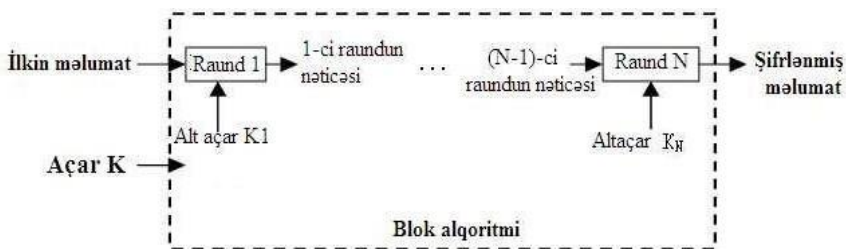
Əgər 4 ikili ədəddən ibarət qrupu əvəzləmək vacibdirsə, onda əvəzləmə cədvəli 16 ədəddən ibarət olacaq. Ümumi halda n bitli blok üçün əvəzləmə cədvəli 2^n elementdən ibarət olmalıdır.

Cədvəl əvəzlənməsini ədəbiyyatlarda bəzən S-blokun istifadə olunması ilə əvəzləmə adlandırırlar (S hərfi ingilis sözündən götürülüb 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, dövrü sürüşmə, əvəzləmə və yerdəyişmə əməliyyatları işlənir. Bu əməliyyatlar alqoritmə 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 strukturu

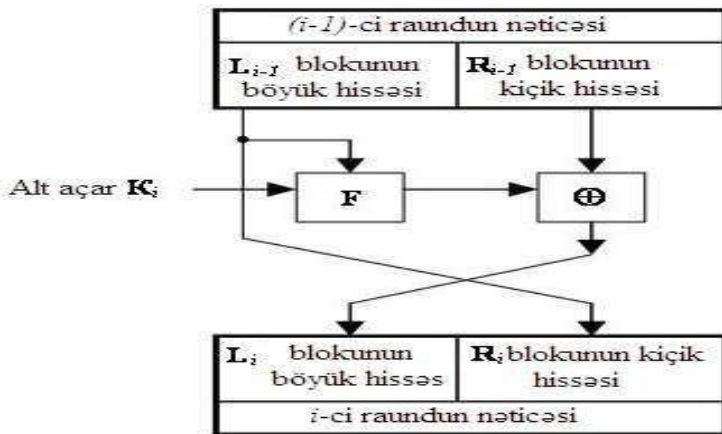
Şifrləmənin blok alqritmi ikili verilənlərə tətbiq olunur. Ümumi halda blok şifrləmə əməliyyatı açıq mətnin n -bitli blokunu şifrlənmiş mətnin k -bitli blokuna çevirir. n uzunluqlu blokun uzunluğu 2^n -ə

bərabərdir. Çevirmənin ilk vəziyyətinə qayıtmaq qabiliy-yətinə malik olması üçün, bu bloklardan hər biri şifrələnmiş mətnin öz nadir blokuna çevrilməlidir. Blokun uzunluğu həmişə 2-in dərəcəsinə n -ə bərabər seçilir, məsələn 64, 128, 256.

2.12. Bağlı açarlı blok şifrinin qurulma prinsipi

Feystel şəbəkəsi. Şifrələmənin blok alqoritminin ümumi strukturu şək.2.7-də 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 şifrələnmiş 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 şifrələmənin 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-dağ 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 dövrü 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 hesablanmasıdan və F funksiyasının nəticələrini digər budaqla iki modulu üzrə toplama-əmaliyyatının 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 şifrələmə alqoritmləri

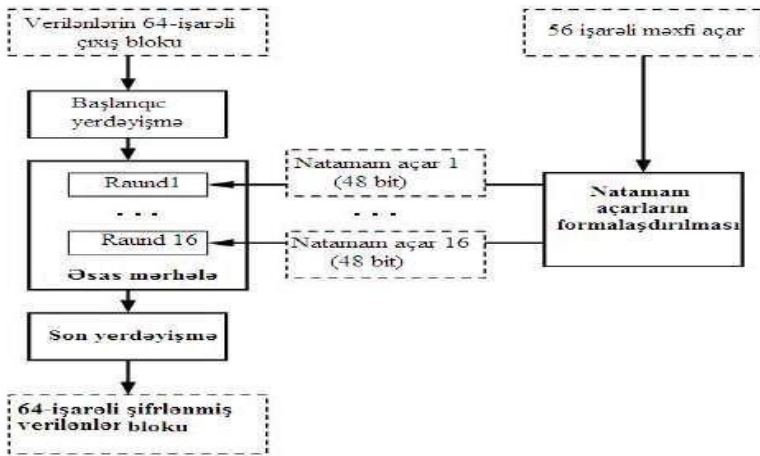
2.13.1. Əsas məlumatlar

Bağlı açarlı kriptografik sistemlərdən ən məşhur olanlardan biri DES (*Data Encryption Standard*) alqoritmidir [3,5]. Bu sistem verilən-lərin şifrələnməsi sahəsində ilk dövlət standartı adını almışdır. DES alqoritmı IBM 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 şifrələmə 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 lazımı olan kombinasiyasını qeyd etmək ilə qırmaq mümkündür. Uzunluğu açarın əlli altı bit olan zaman 2^{56} fərqli açarlar mümkündür. Lakin, kompüter saniyyədə 1 000 000 açar (təxminən 2^{20} –yə bərabər) key qeyd edə bilir-sə, demək bütün 2^{56} açarların seçilməsinə 2^{36} vaxt yəni saniyyə yaxud iki ildən bir qədər çox vaxt tələb olunur, bu əlbətdəki düşməyə qəbul olunan deyil. Lakin personal kompüterlərdən başqa daha bahalı və cəld işləyən hesablama sistemlərimümkündür. 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 biro qədər çox deyil və kriptanalitik bu bahalı texnikaya malik olarsa, onda DES-lə şifrlənmiş məlumatın şifrini açə 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 öyrənilməsinə bir qədər sonra başlayacağıq. 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 göstərib. İlk mətnin hər bir altıмыш dörd bitli bloklarının şifrlənmə prosesini üç etaplara bölmək mümkündür [3,5]:

1. Məlumat blokunun ilkin hazırlanması;
2. “Main Cycle”nin on altı raundları;
3. Məlumat blokunun son emalı.



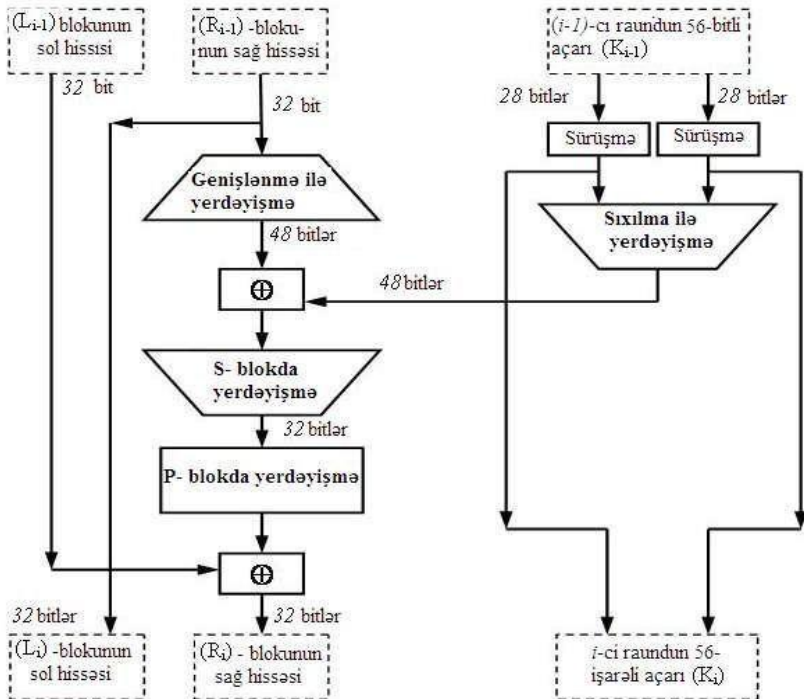
Şək. 2.8. DES-in ümumi sxemi

Birinci mərhələdə mətnin 64-bitli çıxış blokunun ilk yerdəyişməsi 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 kriptografik çevirmələrin bütün mərhələlərinə təfəssilatı ilə baxaq. Birinci mərhələdə ilkin verilənlərin 64-ışarəli bloku başlanqı yerdəyişməyə məruz qalır. Başlanqı yerdəyişmə zamanı verilənlər blokunun bitləri müəyyən şəkildə yenidən nizama salınır. Bu əməliyyat ilkin məlumatlara bir qədər xaotiklik verir və bununla da statistik metodla kriptozanalizin istifadə olunma imkanını azaldır. Eyni zamanda verilənlər bloku-nun başlanqı yerdəyişməsilə 56 bitli açarın başlanqı yerdəyişməsi yerinə yetirilir. Şəkil 2.8-dən görünür ki, raundların hər birində 48- bitli uyğun natamam

K_i açarı istifadə olunur. K_i açarı başlanqıç açarın hər bir bitindən bir neçə dəfə istifadə etməsi müəyyən al-qoritm ilə alınır. Raundların hər birində 56-bitli açar 28-bitdən ibarət iki hissəyə bölünür. Növbətti atdımında həmin hissələr raundun sırasından asılı olaraq bir və yaxud iki bit sola sürüşmək mümkündür. Nəhayət,sürüşməni bitirdikdən sonra lazımı qaydada əlli altı bitdən qırx səkkizi qeyd olunur. Habelə nəin ki, bitlər çoxluğu se-çilir, həm də onların nizamları dəyişdirilir. Bu əməliyyat “sıxılma ilə yerdəyişmə” adlanır. Onun nəticəsi 48 bit komplektidir. Ümumi he-sabla ilkin əlli altı bitli açarın-key hər bir biti on altı alt key-lərdən on dördündə istifadə olunur, bəzən də bitlərin hamısı eyni sayda istifadə olunurlar. Da-ha sonra Feystel şəbəkəsi üzrə təşkil olunmuş və eyni cür olan 16 raundlardan ibarət çevirmənin əsas dövrü 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 budaqları 32-bitli qiymət kimi ayrıca emal edilir. Əvvəlcə blokun sağ hissəsi R_i yerdəyişmə plyus 16 işarə genişlənmə cədvəlindən istifadə edərək 48 bitlərə dək genişləndirilir. Bu əməliyyat sağ yarının ölçüsünü XOR (2 modulu üzərə toplama) əməliyyatının yerinə yetirilməsi üçün açarın ölçüsü ilə uyğunlaşdırır. Bu əməliyyatın yerinə yetirilməsi hesabına nəticənin bütün bitlərinin ilkin verilənlərin və açarın bitlərindən asılılığı tez artır (bu “flood effect” adlanır). Bu və ya digər alqoritmin istifadə olunması zamanı “flood effect” özünü nə qədər möhkəm göstərsə, o qədər də yaxşıdır. Qırx səkkiz bitli say üçün artımı ilə yerdəyişmə yerinə yetirildikdən sonra qırx səkkizbitli K_i açaraltı ilə XOR operation həll olunur. Nəhayət, 48-bitli qiymət, nəticəsi 32-bit olan S yerdəyişmə blokunun girişinə verilir. Yerdəyişmə səkkiz yerdəyişmə blokunda yaxud səkkiz S -blokunda yerinə yetirilir. Bu əməliyyatın yerinə yetirilməsi zamanı 48 bit verilənlər 6-bitli 8 altbloka bölünür. Bu altblokların hər biri öz əvəzləmə cədvəli üzrə dörd bitlə əvəzlənir. S -bloku ilə yerdəyişmə 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 sonradan vahid ottuz iki-bitli qiymətə cəmləşirlər.

Daha növbəti addımda alınan ottuz iki-bitli qiymət istifadə olunan key-lərdən mümkün olmayan P yerdəyişməsinin köməyi ilə həll olunur. Yerdəyişmənin iş prinsipi bitlərin yenidən nizamlanmasını maksimum qiymətə çatdırılmalıdır, şifrləmənin onan sonra ki hər raundunda bir bit böyük digər S -blokunda həll olunsun. Bununla, yerdəyişmənin nəticəsi EOR əməliyyatının köməyi ilə 64-bitli ilkin verilənlər blokunun sol yarısı ilə birləşir. Sonra sol və sağ yarımlar yerlərini əvəz edilir və bunun sonra ki raund başlayır. Şifrləmənin 16 raundundan sonra nəticənin son yerdəyişməsi yerinə yetirilir.

Bu yerdəyişmə başlanğıc yerdəyişməyə əksinədir. Lazımı olan addımlar həll olunan sonra məlumatlar bloku hamısı şifrlənmiş sayılır və növbəti ilkin məlumatın şifrlənməsinə keçmək olar. DES

alqoritmi hal hazırda həm aparat və həm də proqram variantında həyata keçirilir.

Şifrin açılması. Məlumdur ki, kriptografik 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 komponentlərini elə seçiblər ki, məlumatın şifrlənməsi və onun şifrinin açılması üçün eyni bir alqoritmədən istifadə edilsin. Şifrin açılması zamanı alqoritmənin girişinə şifrlənmiş mətn verilir. Bircə fərq natamam K_i açarların 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 “meet in the middle” hücumu

Hazırkı zamanda DES-in çatışmayan cəhəti açarın kiçik uzunluğa malik olmasıdır. Kriptoanaliz prosesinin mürəkkəbləşdirilməsi-nin ən sadə üsulu müxtəlif açarlı eyni bir alqoritmənin 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 şifrəmətn 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 $56 \cdot 2 = 112$ 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 “meet in the middle” hücumu adlanır. Bu hücum alqoritmənin aşağıdakı xüsusiyyətinə əsaslanır. Yuxarıda göstəriləndiyi 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 yazı bilərik [3,5]:

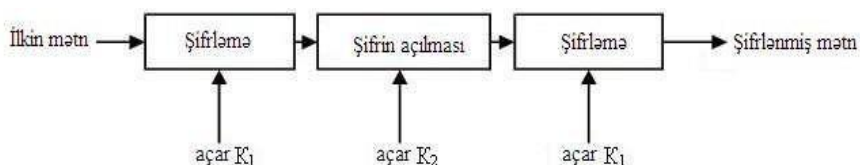
$$X=f(M,K_1)=f^{-1}(E,K_2).$$

Hücum aşağıdakından ibarətdir. Tələb olunur ki, hücumçu bir neçə cüt “plaintext, ciphertext” (M, E) bilsin. Bu halda əvvəlcə K_1 -in bütün mümkün olan 256 qiyməti üçün M şifrlənir. Bu nəticə EHM-in yaddaşında yadda saxlanılır. Yadda saxlanılan verilənlər X qiymətinə görə nizama salınır. Növbəti addım K_2 -in bütün mümkün olan 2^{56} qiymətlərini istifadə etməklə E-in deşifrəlməsindən ibarətdir. Yerinə yetirilən hər bir deşifrəlmə üçün birinci cədvəldə ona bərabər qiymət axtarılır. Əgər belə qiymət tapılırsa, onda hesab olunur ki, bu açarlar həqiqidir və onlar növbəti məlum “plaintext, ciphertext” cütə yoxlanırlar.

Şifrləməyə mümkün olan maksimum cəhdi $2 \cdot 2^n$ yaxud 2^{n+1} -ə bərabər götürürük (burada n- şifrləmə mərhələlərinin hər birində olan açarların uzunluğu; DES üçün $n=56$). Hücum “meet in the middle” adı ona görə verilib ki, bir tərəfdən şifrləmə, digər tərəfdən şifrin açılması yerinə yetirilir və ortada alınan nəticə müqaisə edilir. “meet in the middle” 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 həcmi təsəvvür etmək çətindir, bundan başqa, belə böyük massivdə axtarış əməliyyatının aparılması üçün uyğun vaxt tələb olunur. Buna baxmayaraq, iqtisadi DES şifrləməsi praktiki olaraq heç vaxt istifadə olunmayıb.

2.13.3. Üçqat DES

“Meet in the middle” hücumunun əksinə olaraq iki açarlı iqtisadi şifrləmənin istifadə olunması təklif olunmuşdur [3] (şəkl. 2.10).



Şək.2.10. İki açarlı üçqat DES şifrləməsi

Bu halda şifrləmə – şifrın açılması – şifrləmə ardıcılığı yerinə yetirilir (*Encrypt–Decrypt–Encrypt qısa formada EDE deyilir.*). Bu dönüş simvolik kimi aşağıdakı kimi yazmaq mümkündür. [3,5]:

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

Göndərici əvvəlcə birinci açarla məlumatı kodlayır, sonra növbəti açarla onun şifrini açır və sonda son olaraq birinci açarla şifrləyir. Alıcı əvvəlcə ilkin verilən açarla kodlayır açır, növbəti ikinci ilə kodlayır və sonda ilk açarları ilə şifrəni açır. Həmin vaxt keylərin uzunluğu iki dəfə yüksəlir və yüz on iki bit təşkil edir. İnandırıcı olaraq üç müxtəlif açar istifadədən (hər mərhələnin öz açarı) üçqat şifrləmə təklif olunur. Bu metodda açarın ümumi uzunluğu $(112+56=168)$ -ə dək artır, lakin bir neçə on bit yadda saxlamaq problem olmur. Üçqat DES kifayət dərəcədə *DES*-ə məşhur alternativdir və ANSI X9.17 və ISO 8732 standartlarında açarların idarə olunmasında istifadə olunur. Bir sıra kriptanalitiklər 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 şifrın 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 alqoritmının 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 alqoritmının əsasını Feystel şəbəkəsi deyil, xətti əvəzləmə adlanan əvəzləmə təşkil edir. Reyndal alqoritmının 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 ibarətdir. Bu qatlar aşağıdakılardan ibarətdir [3,5]:

1. Qeyri xətti qat. Bu qatda baytların əvəzlənməsi yerinə yetirilir. Bu qat optimal qeyrixətliyə malik olan S-blokların vasitəsilə reallaşdırılır və differensial, xətti və digər müasir kriptanaliz metodlarının istifadə olunması imkanlarının qarşısını alır.
2. Xətti qarışdırma təbəqəsi. Bu qat statistik əlaqələrin maskalanması 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 şifrləmə bilavasitə yerinə yetirilir.

Şifr açarlarla toplama ilə başlayır və qurtarır. Bu, məlum mətnə hücum zamanı birinci raundun girişini bağlamağa və kriptografik cəhətdən əhəmiyyətli nəticə olan axrncı raundu əldə etməyə imkan verir. Alqoritmə 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 şifrləmədən fərqli olaraq, bu alqoritmə şifrləmə və deşifrəmə əməliyyatları başqa prinsipdə qurulurlar. Reyndal alqoritmı həm proqram və həm də aparat variantlarında yaxşı reallaşdırıla bilər.

Reyndal alqoritmində yaddaşa ciddi tələblər qoyulmur, bu da onu məhdud resurslu sistemlər üçün əlverişli edir. Reyndal alqoritminin etibarlılığı mütəxəssislər tərəfindən yüksək qiymətləndirilir.

Blok alqoritmlərinin iş rejimləri. Blok alqoritmləri müxtəlif məsələlərin yerinə yetirilməsi üçün istifadə edilə bilər. Ona görə də istənilən simmetrik blok alqoritmlərinin istifadəsi üçün bir neçə rejim müəyyən edilib. Rejimlərdən hər biri öz xüsusiyyətlərinə və istifadə olunma sahələrinə malikdirlər. Fərz edək ki, ilkin X verilənlər 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 istifadə etməklə digər yerdə qalan bloklardan asılı olmayaraq şifrlənir. Əgər məlumatın uzunluğu uyğun alqoritm blokunun uzunluğundan böyükdürsə, onda həmin məlumatın uzunluğu uyğun uzunluqlu $X_1, X_2, \dots, X_n$ bloklara bölünür, bu zaman son blok lazım olduğu təqdirdə sabit qiymətlərlə əlavə olunur. Hər bir blok, blok şifri ilə şifrlənir:

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

İlkin X_i verilənlərinin bütün bloklarının şifrləmə nəticəsində aşağıdakı şifrlənmiş məlumat alınır [3,5]:

$$Y = Y_1, Y_2, \dots, Y_n$$

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

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

ESB anlayışından belə çıxır ki, məlumatın deşifrəlməsini 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 şifrlənməsi şərtində şifrlənmiş verilənlər bazası ilə işləmək

olar.

Bu rejimin çatışmayan cəhəti ilkin mətnin eyni bloklarının eyni şifrəməyə çevrilməsidir. Əksər real şifrəli verilənlər dəstləri təkrar-lanan elementlərə malikdirlər. Məlumat yüksək artıqlığa, təkrarlan-başlıqlara yaxud uzun seriyalı sıfırlara yaxud boşluqlara malik ola bilər. Beləliklə, cinayətkar tezlik kriptanalizi 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, kriptografik açarın). Verilənlərin bir neçə blokunun ötürülməsi zamanı ESB rejiminin çatışmayan cəhətlərini aradan qaldırmaq üçün CBC (şifrəli bloklarının zəncirlənməsi) rejimini istifadə etmək olar.

CBC rejimində çevirmə aşağıdakı kimi yerinə yetirilir: açıq mətnin hər bir bloku əvvəlki blokun şifrələnməsinin nəticəsi ilə 2 moduldu ilə toplanır. Beləliklə, əvvəlki blokun şifrələnməsinin nəticəsi növbəti blokun şifrələnməsinə təsir göstərir. CBC rejimində şifrələmə əməliyyatı riyazi şəkildə aşağıdakı kimi yazılır [3,5]:

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

Yəni açıq mətn üzərində növbəti blokun şifrələnməsindən və növbəti blokun şifrələnməsinin nəticəsindən qabaq iki moduldu ilə toplama əməliyyatı yerinə yetirilir. Açıq mətnin bloku şifrələndikdə, o əks əlaqəli registr qurğusunda saxlanılır. Şifrələnmədən qabaq verilənlərin növbəti bloku, o əks əlaqəli registrlə birlikdə iki moduldu ilə toplama əməliyyatına məruz qalır və yalnız bundan sonra şifrələnir. Alınan şifrələnmiş blok yenidən əks əlaqəli registr qurğusunda saxlanılır və məlumatın sonuna qədər giriş verilənlərinin növbəti blokunun şifrələnməsi üçün istifadə olunur. Y_0 bloku giriş verilənlərinin birinci blokunun şifrələnməsindən qabaq forma-laşmalıdır. O başlanğıc vektoru adlanır və giriş verilənlərinin birin-ci bloku ilə 2 moduldu üzrə toplanmaq üçün istifadə olunur. Əks əlaqəli registr qurğusundan istifadə olunması nəticəsində hər bir blokun şifrələnməsi bütün əvvəlki bloklardan asılıdır. Şifrələnmiş məlumatı riyazi olaraq aşağıdakı kimi deşifrələmək

olarq

[3,5]:



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

Şifrələnmiş mətnin bloku əvvəlcə əks əlaqəli registr qurğusunda saxlanılır, sonra adi qaydada deşifrəlenir. Sonra növbəti blok deşifrəlenir və məlumatın sonuna qədər əks əlaqəli registrlə “2 modulu üzrə toplamaya” məruz qalır. Hətta bütün X_i ilkin verilənlərin bütün blokları eyni olsa belə, şifrələnmiş mətn Y -in müxtəlif blok-larından ibarət olacaq. Bu rejim ölçüsü blokun ölçüsündən artıq olan məlumatların şifrələnməsi zamanı daha geniş istifadə olunur. Bununla belə iki eyni məlumat eyni şifrələncək. Bunun qarşısını almaq üçün, hər şifrələmə zamanı müxtəlif başlatma vektorlarını istifadə etmək vacibdir. Başlatma vektorları həm də verilənlərin deşifrələnməsi üçün vacibdir, ona görə də onları şifrələnmiş məlumatla birlikdə ya ünvançıya göndərmək lazımdır, ya da hər hansı bir yalançı təsadüfi başlatma vektorlarının birgə formalaşması barədə razılığa gəlinməlidir. CBC rejimində şifrələnmiş məlumatın deşifrələnməsini yalnız ardıcıl olaraq ilk blokdan başlamaqla təmin etmək olar.

2.14. DÜİST28147-89 –üzrə verilənlərin kriptoqrafikçevrilməsi algoritmi

2.14.1. Əsas məlumatlar

Bağlı açarlı blok şifrələmə algoritmi 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 şifrə amerika DES-in prinsipində qurulmuşdur. Rusiya DES-in amerikanın 16 raundlu DES-ti ilə müqayisədə proqram reallaşdırılması üçün çox əlverişlidir, uzunluğu 256 bitə bərabər olan daha uzun açara və 32 şifrələmə raunduna malikdir. Beləliklə, rusiya standartının əsas parametrləri aşağıdakılardır: blokun ölçüsü 64 bit, açarın uzunluğu 256 bit və raundların sayı 32-dir. Alqoritm özündə Feystel şəbəkəsini əks etdirir. Şifrələnen verilənlər bloku iki eyni cürhissəyə 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 alqoritmın istifadə olunmasına imkan verir.

DES şifrələmə alqoritmində aşağıdakı əməliyyatlar istifadə olunur [3,5]:

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

Bu standartın alqoritmlərinin fərqli etaplarında verilənlər fərqli şəkildə təsvir və eləcə də istifadə olunur. Bir necə situasiyalarda 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 şəkl.2.11-də verilib.



Şəkl.2.11 DÜİST28147-89 bir raundunun strukturası

Şifrələnən 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 dəyişmə həyata keçirilir. Bunun öncə kimi etaplarda alınan otuz iki bitli qiymət (onu S-lə işarə edək) kodun səkkiz dörd-bitli bloklar masiv kimi təsvir mümkündür. [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, yer-dəyişmə cədvəlindən göstərildiyi kimi qeyd olunur. Həmin S_i blokunun qiyməti əvəzləmə cədvəlinin S_i -ci sətirinə (nömrələmə sırası-0-dan başlamaqla) əvəzlənir. Başqa sözlə, blokun qiyməti üçün əvəz kimi yer-dəyişmə blokunun sayına tam uyğun sətirin nömrəsilə və əvəzlənən blokun qiymətinə dördbitli mənfi olmayan bütün ədəd olan sütunun nömrəsilə element seçilir.

Əvəzləmə cədvəlinin hər sətirində 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 sətiri 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-ışarəli S ədədinin 4 kiçik biti) nömrəsi əvəzlənən blokun qiymətinə bərabər olan mövqedə duran ədədə əvəzlənir.

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 dövrü olaraq 11 bit sola sürüşür. Nəhayət, bitlər üzrə iki modulu ilə toplama əməliyyatının köməyi ilə nəticə sol yarım ilə 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 şifrələmə alqoritminin bir raundunun yerinə yetirilməsinin nəticəsi kimi baxılır.

2.14.3 Şifrələmə və şifrin açılması əməliyyatları

DÜİST 28147-89 blok şifridir, ona görə də verilənlərin çevrilməsi *baza dövrü* adlanan bloklarla həyata keçirilir [3,5]. Baza dövrü verilənlər bloku üçün əsas raundun çoxdəfəli yerinə yetirilməsidir. Hər bir raund da səkkiz mümkün olan 32-ışarəli 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 ardıcılıqla dörd raundda istifadə olunur. Şifrın açılması eyni ilə şifrləmə alqoritmı ilə yerinə yetirilir. Yəgənə fərq K_i altaçarının istifadə qaydasındadır. Şifrın açılması zamanı altaçarlar cədvəl 2.10-də göstərildiyi kimi əks qaydada istifadə olunmalıdır.

Cədvəl 2.10. Şifrləmə zamanı altaçarların istifadə olunması ardıcılıqlığı

Cədvəl 2.10.

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-laşdırma və “imitasiya” adlanan bir əlavə rejim.

Cədvəl 2.11. Şifrın açılması zamanı altaçarların istifadə olunması qaydası.

Cədvəl 2.11.

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 məs-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 asılı olmayaraq şifrlənir. Bu rejiminin xüsusiyyəti ondan ibarətdir ki, ilkin mətnin eyni blokları eyni şifrəməyə çevrilir. Ona görə də DÜİST 28147-89 sadə şifrələmə rejimini yalnız açarların şifrlənməsi üçün istifadə etməyi tövsiyə 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 üçün istifadə oluna bilərlər.

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

DÜİST 28147-89–un şifrlənmiş məssivində təhriflərin aşkar olunması üçün kriptografik çevirmənin əlavə rejimi olan imitasiyanın hasil olunması nəzərdə tutulub. İmitasiya–bu açıq mətndən və

informasiyanın məxfi açarından asılı olan nəzarət kombinasiyasıdır. İmitasiyanın istifadə olunmasında məqsəd informasiya massivində bütün təsadüfi və qəsdən törədilən dəyişiklikləri aşkar etməkdir. İmitasiyanın hasil olunması rejimində giriş mətn aşağıdakı şəkildə bloklarla emal olunur [3,5]:

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

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

İmitasiya-kimi çıxışda alınan, onun adı 32 kiçik biti Y_n blokun-bir hissəsi götürülür. Beləliklə, cinayətkar, şifrləmə açarına malik olmadan informasiyanın verilən açıq massivi üçün İmitasiyanı tapa bilməz, eləcə də verilən İmitasiyaya 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 dərəcədə çox böyük ehtiyat var [3,5]. Bu hər şeydən əvvəl şifrləmə açarının böyük uzunluğu ilə bağlıdır. Məlum olduğu kimi, müasir kriptosistem işləyənlər şifrlənmiş məlumatın məxfiliyi açarın məxfiliyi ilə təyin olunmalıdır prinsipinə tərəfdardırlar. Bu o deməkdir ki, əgər şifrləmə alqoritmının özü kriptanalitikə 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, Data Encryption Standard və Advanced Encryption Standard alqoritmlərində olduğu kimi, güman edilir ki, şifrın 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 fərqlə 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 dövrü sürüşmə istifadə olunur. Axıncı əməliyyat 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. Kriptografik heş-funksiya

2.15.1. Heş- funksiya anlayışı

İxtiyari uzunluqlu sətir üçün bəzi tam ədədi yaxud qeyd olunmuş uzunluqlu digər sətiri hesablayan funksiya riyazi heş-fun-

ksiya deyilir. Riyazi olaraq bunu aşağıdakı kimi yazıla bilər [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 əlamətlərinin heş-funksiyasının qiymətinin təyin olunmasıdır. Bu funksiya adətən sabit ölçüyə malik olur, məsələn, 64 yaxud 128 bit. Heş-funksiyası daha sonralar hər-hansı bir məsələ üçün istifadə edilə bilər. Məsələn, heşləmə verilənlərinin müqaisə edilməsi üçün istifadə oluna bilər. Əgər iki verilənlərin heş-kodu müxtəlifdirsə, onda məsələlər müxtəlifdir, yox əgər onların heş-kodu eynidirsə çox ehtimal ki, məsələlər də eynidirlər.

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

Adi heş-funksiyası iki modul ilə toplanan əməliyyatının istifadə olunması ilə aşağıdakı kimi yaradıla bilər: giriş sətirini alır, bütün baytları 2 modulu üzrə toplayırıq və nəticəni heş-funksiya-sının qiyməti kimi qaytarırıq.

Heş-funksiyasının uzunluğunun qiyməti bu halda giriş məlumatının

ölçüsündən asılı olmayaraq 8 bit olur.

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

Bu məlumatı ikili şəkllə 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 kriptografik məqsədlər üçün istifadə etmək olmaz, məsələn, elektron imzanı formalaşdırmaq üçün, nəzarət cəminin qiymətini dəyişmədən imzalanan məlumatın məzmununu dəyişmək kifayətdir. Ona görə də baxılan heş-funksiyanın kriptografiyada tətbiq olunması yaramır. Əgər bərabər qiymətli heş-funksiyalı iki başlanğıc verilənləri çətin yaratmaq olarsa, eləcə də əgər funksiyanın çıxışında girişdən açıqdan-açığa asılılıq yoxdursa, onda kriptografiyada heş-funksiyası yaxşı hesab olunur. Kriptografik 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 məlumatda 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 üçün heş-funksiyasının hesablanması zamanı alınan nəticədir.

Nəticədə heş-funksiyasının çıxışı h_n giriş məlumatının bütün

nblokunun 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 alqoritmı dayanıqlıdırsa, onda onun əsasında heş-funksiya da etibarlı olacaq. Heş-kodunun alınması üçün blok alqoritmının istifadə olunmasının sadə üsulu məlumatın CBC rejimində şifrlənməsidir. Bu halda məlumat, uzunluğu şifrləmə alqoritmının blokunun uzunluğuna bərabər olan bloklar ardıcılığı şəklində təsvir olunur. Vacib olduğu zaman axırıncı blok lazımı uzunluqlu blokun alınması üçün sağdan sıfırlarla doldurulur. Heş-qiyməti mətnin axırıncı şifrlənmiş bloku olacaq. Şifrləmənin etibarlı blok alqoritmının 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 masivində

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 imitasiyanın göndəri-cinin bağlı açarı ilə şifrlənməsi, yəni imzanın yaradılması ola bilər. Əgər göndərici və alıcı simmetrik şifrləmənin ümumi açarına malikdirlərsə, 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 olunur. Axırncı blok vacib olduqda sıfırlarla doldurulur, bəzən axırncı bloka ikili ədədlər şəklində məlumatın uzunluğunu əlavə edirlər. Hər bir mərhələdə açar halında məlumatın cari blokunu götürərək əvvəlki mərhələdə alınan heş- qiymətini şifrləyirik. Axırncı alınan şifrlənmiş qiymət son heş-nəticə olacaq. Beləliklə, əgər məlumatın M adi şifrləmə sxemini K açarında blok şifrinin köməyi ilə $E=f(M,K)$ kimi yazdıq, onda heş-kodunun alınması sxemi yuxarıda yazılan alqo-ritm ilə aşağıdakı kimi yazmaq olar [3,5]:

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

Başlanğıc 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 məlumatının 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]:

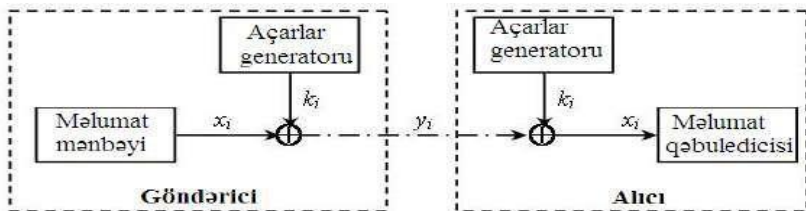
$$\begin{aligned} h_i &= f(M_i h_{i-1}) \oplus M_i, & h_i &= f(M_i, h_{i-1}) \oplus h_{i-1} \oplus M_i h_i, \\ h_i &= f(h_{i-1}, M_i) \oplus h_i, & h_i &= f(h_{i-1} \oplus M_i, M_i) \oplus h_i \end{aligned}$$

Bu sxemlərin hamısında formalaşdırılan heş-qiymətinin uzun-luğu şifrələmə zamanı blokun uzunluğuna bərabərdir. Blok alqoritminin 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 alqritmi müəyyən uzunluqlu blokun şifrənməsi üçündür. Lakin verilənlərin şifrənməsi bloklarla deyil, işarələr üzrə də şifr-lənə bilər. Arakəsilməz şifr giriş məlumatının bir bit (yaxud bayt) üzrə çevrilməsi əməliyyatını həyata keçirir. Arakəsilməz şifrələmə alqritmi məlumatın kifayət dərəcəli böyük uzunluqlu tam ədədlə-rə bölünməsinə aradan qaldırır, buna görə də, o real zamanda işləyə bilər. Beləliklə, əgər işarələr seli verilirə, onda hər bir işarə dərhal şifrələnər 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 şifrələnmiş məlumat y_i alınır [3,5]:

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

$y_1, y_2, \dots, y_n$ şifrəməndən $x_1, x_2, \dots, x_n$ məlumatlarını bərpa etmək üçün şifrələmədə olduğu kimi eyni ilə $k_1, y_k, \dots, k_n$ açar ardıcılığını generasiya

etmək vacibdir və şifrın açılması üçün olan ifadəni aşağıdakı kimi yazmaq olar [3,5]:

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

Adi çıxış məlumatı və açar ardıcılığı 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 ardıcılıq 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 zamanı onun statistik metodla şifrının açılması təhlükəsi mövcud olur. Bunu qammalaşdırma metodu ilə qısa rəqəmli kodlu açarla bağlı sadə rəqəmli mətnin təmsalında izah edək.

Misal. Fərz edək ki, çıxış məlumatı özündə ikili-onluq ədədi əks etdirir, yəni 0...9 onluq ədədlərinin ikili şəkli çevrilməsindən alınan hər tetradanı (dörd bit). Şifrlənmiş Y məlumatının 24 biti tutulub, yəni altı

$Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$

tetrada, məhz

110011011110111100000001

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 $0 \leq K \leq 9$ 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 mümkün olan qiymətləri X_1 və K -nı, hansıların ki, modul 2 üzrə cəmi 1100-a gətirir:

$$\begin{array}{r} K = 0000 \ 0001 \ 0010 \ 0011 \ 0100 \ 0101 \ 0110 \ 0111 \ 1000 \ 1001 \\ Y_1 = 1100 \ 1100 \ 1100 \ 1100 \ 1100 \ 1100 \ 1100 \ 1100 \ 1100 \ 1100 \\ \hline X' = 1100 \ 1101 \ 1110 \ 1111 \ 1000 \ 1001 \ 1010 \ 1011 \ 0100 \ 0101 \end{array}$$

Çıxış qiymətləri 0-dan 9-a dək olduğundan, baxılan qiymətlərdən açarın 0000000010010001101100111bu qiymətlərini çıxarmaq olar, çünki, onlarla toplama zamanı qiymət 9 ekvivalentindən çox qiymət alır. Belə qiymət açıq mətdə 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 etmək və açarın qalan variantlarını tapan, hansıların ki, modul iki üzrə cəmi $Y_2 = 1101$ nəticəsinə gətirir:

$$\begin{array}{r} K = 0100 \ 0101 \ 1000 \ 1001 \\ Y_2 = 1101 \ 1101 \ 1101 \ 1101 \\ \hline X_2' = 1001 \ 1000 \ 0101 \ 0100 \end{array}$$

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

$$\begin{array}{r} K = 0100 \ 0101 \ 1000 \ 1001 \\ Y_3 = 1110 \ 1110 \ 1110 \ 1110 \\ \hline X_2' = 1010 \ 1011 \ 0110 \ 0111 \end{array}$$

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

$$1000_{(2)} = 8_{(10)}$$

və

$$1001_{(2)} = 9_{(10)}.$$

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 açıardan hər birini məlumatın deşifrəlməsi 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 bərpaetməyə imkan verir.

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

Müasir informatika müxtəlif tətbiqlərdə saxta təsadüfi ədədləri riyazi statistika metodlarından və imitasiya modelləşdirilməsindən tutmuş kriptografıyadək 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 ardıcılığı yaradır [3,5]. Belə ardıcılıqlar müəyyən qayda ilə hesablanır və təsadüfi olurlar, ona görə də onlar həm verici, həm də qəbuledici tərəflərdə tam dəqiq-liklə yenidən hasil edilir. Şifrləmədə istifadə olunan açar işarələr ardıcılığı, yalnız lazımınca uzun olmalıdırlar. Əgər açarlar genera-toru hər qoşulmada eyni bitlər ardıcılığı 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 kriptografik məqsədlərlə istifadə olunmaq üçün aşağıdakı xüsusiyyətlərə malik olmalıdır [3,5]:

1. Ardıcılıq periodu çox böyük olmalıdır;
2. Yaradılan ardıcılıq təsadüfdən-təxminən-fərqlənməməlidir;

3. Müxtəlif qiymətlərin yaranma ehtimallıqları dəqiq bərabər olmalıdır;
4. Qanuni alıcının məlumatın şifrəsini açma 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 ardıcılığı ilə hesablanması açarı bilmədən müərkəb məsələ olmalıdır.

Bu göstərilən xüsusiyyət zamanı saxta təsadüfi ədədlər ardıcılığı arası kəsilməz şirləmədə istifadə oluna bilər.

2.16.3. Xətti konqruent saxta təsadüfi ədədlər generatoru

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

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

burada, simvollar hər hansı sabit kəmiyyətdirlər, k_{i-1} –əvvəlki saxtatəsadüfi ədəddir. k_1 –in alınması üçün k_0 başlanğıc qiymət verilir. **Misal:** $a=7$, $b=5$, $c=11$ götürək və qoy $k_0 = 1$ olsun.

Bu halda biz yuxarıda göstərilən ifadə ilə 0-dan 10-a dək qiymətləri ala bilərik ($c=11$ olduğu üçün). Ardıcılığın bir neçə elementlərini hesablayaq: 0-dan 10-a dək ($c=11$ olduqda).

$$\begin{aligned} k_1 &= (7 \times 1 + 5) \bmod 11 = 1; \\ k_2 &= (7 \times 1 + 5) \bmod 11 = 6; \\ k_3 &= (7 \times 6 + 5) \bmod 11 = 9; \\ k_4 &= (7 \times 9 + 5) \bmod 11 = 10; \\ k_5 &= (7 \times 10 + 5) \bmod 11 = 0. \end{aligned}$$

Alınan qiymətlərin (1, 6, 9, 10, 0) təsadüfi qiymətlərə oxşaması görünür. Lakin növbəti k_6 işarəsi yenidən 1 olacaq [3,5]:

$$k_6 = (7 * 1 + 5) \bmod 11 = 1,$$

k_7 və k_8 içəriləri uyğun olaraq 6 və 9 –a bərabər olacaq [3,5]:

$$\begin{aligned} k_7 &= (7 * 8 + 5) \bmod 11 = 6; \\ k_8 &= (7 * 10 + 5) \bmod 11 = 9. \end{aligned}$$

Belə çıxır ki, bizim saxtatəsadüfi ədədlər generatoru 1, 6, 9, 10, 0 periodik ədədləri yaradaraq təkrarlanır. Təəssüflər olsun ki, bu xüsusiyyət bütün xətti konqruent 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 konqruent saxtatəsadüfi ədədlər generatorunun üstün cə-həti onların sadəliyi və saxtatəsadüfi ədədlərin yüksək sürətə malik olmasıdır. Xətti konqruent saxtatəsadüfi ədədlər generatorlar modeləşmə və riyazi statistikada tətbiq olunurlar, lakin kriptografik məqsədlərdə onları istifadə olunmağa tövsiyə etmək olmaz, çünki, kriptozanaliz mütəxəssisləri saxtatəsadüfi ədədlər ardıcılığını bir neçə qiymətlər üzrə bərpa etməyə öyrəniblər. Məsələn, fərz edək biz, düşmənlər d_0, d_1, d_2, d_3 qiymətlərini təyin edə bilər: $d_1 = (a \cdot d_0 + b) \bmod c$

$$d_2 = (a \cdot d_1 + b) \bmod c$$

$$d_3 = (a \cdot d_2 + b) \bmod c$$

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]:

$$d_i = (a_1 \cdot 2 \cdot d_{i-1} + a_2 \cdot d_{i-1} + b) \bmod c$$

$$d_i = (a_3 \cdot d_{i-1} + a_2 \cdot d_{i-1} + a_3 \cdot d_{i-1} + b) \bmod c$$

Lakin belə generatorlar da yuxarıda göstərilən səbəbə görə kriptografik 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

əmaliyyatların aparılması sürəti ilə müqaisə olunan andan məşğurlaşmağa başladı, Fibonaççiyev vericiləri təbii olaraq real hesabda reallaşır. Gecikmə ilə Fibonaççi metodunun istifadə olunmasının müxtəlif sxemləri mövcuddur. Ən geniş yayılmış Fibonaççi vericilərləri 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 $k_i \in [0,1]$ 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 saxlanması üçün a və b parametrlərindən asılı olan bəzi yaddaş həcmi tələb olunur.

Misal. Birinci on ədədlərdən gecikmə ilə Fibonaççi metodu ilə generasiya olunan ardıcılığı k_5 -dən başlayaraq aşağıdakı başlanğıc verilənləri istifadə etməklə hesablayaq:

$$a = 4, b = 1,$$

$$k_0=0.1; k_1=0.7; k_2=0.3; k_3=0.9; k_4=0.5;$$

$$k_5 = k_1 - k_4 = 0.7 - 0.5 = 0.2; \quad k_6 = k_2 - k_5 = 0.3 - 0.2 = 0.1;$$

$$k_7 = k_3 - k_6 = 0.9 - 0.1 = 0.8; \quad k_8 = k_4 - k_7 + 1 = 0.5 - 0.8 + 1 = 0.7;$$

$$k_9 = k_5 - k_8 + 1 = 0.2 - 0.7 + 1 = 0.5; \quad k_{10} = k_6 - k_9 + 1 = 0.1 - 0.5 + 1 = 0.6;$$

$$k_{11} = k_7 - k_{10} = 0.8 - 0.6 = 0.2; \quad k_{12} = k_8 - k_{11} = 0.7 - 0.2 = 0.5;$$

$$k_{13} = k_9 - k_{12} + 1 = 0.5 - 0.5 + 1 = 1;$$

$$k_{14} = k_{10} - k_{13} + 1 = 0.6 - 1 + 1 = 0.6.$$

Görürük ki, hasil olunan ədəd ardıcılığı təsadüf ardıcılığına oxşardır. 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 zamanda 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 kriptografik alqoritmlər 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 kriptografik 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 Matlabsistemində 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 qalıklı adla-nan alqoritm geniş yayılmışdır. Kriptografik 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. $x_0 = x_2 \bmod M$ -i hesa-blayaq. x_0 generatorun start ədədi adlanır. Generatorun hər bir n -addımında $x_{n+1} = x_n^2 \bmod M$ 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 götürülür. Əgər yazılışda vahidlərin sayı cütdürsə -bit cütlüyü "0"-a bərabər götürülür, əgər cüt deyilsə, onda bit cütlüyü 1 götürülür.

Misal. Verilir

$$p = 11,$$

$$q = 19 \text{ (inanırıq ki, } 11 \bmod 4 = 3, 19 \bmod 4 = 3).$$

$$\text{Onda } M = p * q = 11 * 19 = 209.$$

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 algoritmi üzrə birinci on ədədi x_i hesablayaq (cədvəl 2.12-yə bax). Təsadüfi bit halında ədədlərin ikili yazılışında x_i kiçik biti götürəcəyik [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

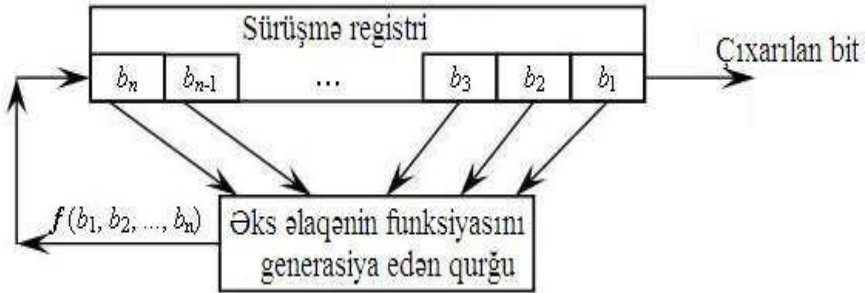
$x_8 = 157^2 \bmod 209 = 24649 \bmod 209 = 196$	Kiçik bit :	0
$x_9 = 196^2 \bmod 209 = 38416 \bmod 209 = 169$	Kiçik bit :	1
$x_{10} = 169^2 \bmod 209 = 28561 \bmod 209 = 137$	Kiçik bit :	1

Praktiki olaraq bu metodun maraqlı xüsusiyyəti ardıcılığın 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]:

$$x_n = x^{2^n \bmod ((p-1)(q-1))} \bmod M$$

2.18. Əks əlaqəli sürüşmə registri əsasında saxta təsadüfi ədədlər generatoru

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

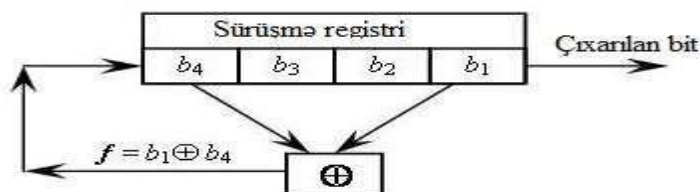


Şək. 2.13. Əks əlaqəli sürüşmə registri

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 ədədlərin (ST Ə) alınması sxemini müəyyənləşdirir. Aşkardır ki, registrin bir neçə takt işindən sonra bitlər ardıcılığı təkrar olunmağa başlayacaq. Alınan ardıcılığın 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 bağlı idi ki, onlar rəqəmli aparatların köməyi ilə çox yaxşı reallaşdırılırdılar.

Əks əlaqəli sürüşmə registrinin sadə növü əks əlaqəli xətti sürüşmə 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 ardıcılığı yara-dırlar. Əks əlaqəli xətti sürüşmə registrləri yaxud onların modifi-kasiyaları kriptografiyada 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

Şəkində təsvir olunmuş registrə başlanqıç qiyməti 1011-i yazaq. Registrin daxili vəziyyətinin ardıcılığını 2.13-də təsvir olunmuş cədvəllə hesablayaq.

Cədvəl 2.13. Xətti sürüşmə registrinin iş ardıcılığı

Vəziyyərin nömrəsi	Registrin daxili vəziyyəti $b_4b_3b_2b_1$	Əks əlaqə funksiyasının hesablanması 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

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 ardıcılığı cədvəlin axıncı sütununu yaradır (çıxarılan bitlər).

Ölçüsü n bit olan xətti sürüşmə registri 2^n-1 vəziyyətlərdən birində ola bilər. Ona görə də belə registr nəzəri olaraq maksimum 2^n-1 periodlu saxta təsadüfi ardıcılıq hasil edə bilər. Əks əlaqəli xətti sürüşmə registri bitlərin maksimum periodlu dövrü ardıcılığını, yalnız budaq ardıcılığı halında müəyyən bitlərin seçilməsi zamanı hasil edə bilər. Əks əlaqəli xətti sürüşmə registri əksər vaxtlar arasıkəsilməz verilənlərin şifrələnməsində istifadə olunmuşdur və indi də olunmaqdadır.

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

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

İnformasiyanın arasıkəsilməz şifrələnməsi üçün istənilən blok alqoritmindən, 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 $z_1, z_2, \dots, z_k$ -dan ibarət j - bitli saxta təsadüfi ədədlər formalaşdırır, hansılar ki, sonralar mə-lumatın şifrələnməsi üçün qamma kimi istifadə oluna bilər. Şifr-ləmənin nəticəsi ilkin məlumatın növbəti blokunun şifrələmə əmə-liyyatının girişi sayılır. Şifrələmənin hər mərhələsində şifrələnmiş blok Y_i -dən j -kiçik bitlər seçilir. Beləliklə, saxta təsadüfi ədədlər almaq üçün aşağıdakı sxem istifadə olunur [3]:

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

Əgər şifr-in blokunun ölçüsü N -ə bərabədirsə, onda j parametri 1-dən

N-ə dək qiymət ala bilər. Y_0 qiymətini *təşəbbüsləndirici vek-tor* adlandırırlar. z_i ədədlər ardıcılığını z_i işarələrdən ibarət ilkin verilənlərin şifrənməsi üçün qamma kimi istifadə etmək olar [3]:

Bunun nəticəsində y_i işarələrinin şifrələnmiş 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 ardıcılığını alırıq. Ona görə də hər bir yeni məlumatın verilməsi üçün açarın K qiymətinin dəyişdirilməsi tövsiyə olunur. Bu rejim üçün məlumatın şifrənin açılması yalnız ardıcılığın başlanğıcından ola bilər, çünki, əvvəlkiləri hesablamadan z_i ardıcılıqlı ixtiyari ele-ment almaq mümkün deyil. OFB rejiminin əsas üstün cəhəti məlumat sellərinin alınması anında, onları tez şifrələmək yaxud şifrələrini açmaq üçün z ardıcılığının 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 verilənlərin ötürülməsi zamanı səhv baş verirsə o növbəti şifrələnmiş bloka keçmir, bununla da sonrakı blokların şifrənin açılması imkanı saxlanılır. Məsələn, küylü rabitə kanalı üzrə veriliş zamanı y_i blo-kunda səhv bit yaranırsa, onda o yalnız bu blokun şifrənin 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 şifrənin əvvəlki çıxışı deyil, hər addımda 1 vahid artan sayğac şifrələnir. Sayğacın ən birinci qiyməti hər hansı bir Y_0 təşəbbüscü qiymətlə təyin olunur. Ümumi ifadə

aşağıdakı kimidir [3]:

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

CTR rejiminin üstün cəhəti z - ardıcılığının istənilən elementi-nin bilavasitə hesablanma bilməsidir. bu fakt Y_i –in hər addımda 1 vahid artması ilə bağlıdır. Ona görə də, 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 şifrələməyə və deşifrələməyə imkan verir.

2.19. RC4-aqoritmı

Bu alqoritm saxta təsadüfi ədədlərin generasiya olunması alqoritmidir. Bu alqoritm R.Rivest tərəfindən dəyişən uzunluqlu açarlı informasiya seli üçün xüsusilə işlənmişdir. Bu alqoritmın köməyi ilə qurulan saxta təsadüfi ədədlər generatoru, bir qayda olaraq, blok şifrinə əsaslanan generatorlardan xeyli sürətlidir. RC4 alqoritmı 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 alqoritmələr sinfinə mənsubdur. Adətən $n = 8$, lakin digər ölçülərdə də istifadə etmək olar. Alqoritmın 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 j ilə işarə edək. Bütün hesablamalar 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 mümkün olan n -bitdən (bizim halda 4-bitli) ibarətdir. Qiy-mətlərin konkret yer dəyişməsi açarla təyin olunur. Cədvəlin hər bir elementinin sıfırdan on beşədək aralığında qiymət aldığı üçün, onda onu iki cür yazmaq olar: ya ədəd kimi, yaxudda cədvəldə digər elementin nömrəsi kimi.

RC4 alqoritmı iki mərhələdən ibarətdir [3,5]. Birinci, hazırlıq mərhələsində S əvəzləmə cədvəlinin təşəbbüslənməsi yerinə yetirilir. İkinci, əsas mərhələdə saxta təsadüfi ədədlər hesablanır.

S cədvəlinin necə təşəbbüslənməsinə baxaq. Əvvəlcə o sıfırdan on beşədək ədədlərlə ardıcıl olaraq doldurulur. Açar 4-bitli söz ardıcılığı 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. $j = (j + S_i + K_i) \bmod 16$; 3. S_i və S_j . –in yerlərini dəyişmək; 4. $i = i + 1$; 5. əgər $i < 16$, onda 2-ci bəndə keçək.

Bu alqoritmın yerinə yetirilməsi nəticəsində S əvəzləmə cədvəlinin 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 başlanqıç “0” işarəsi verilir. Sonra hər yeni z_i qiymətini aldıqdan sonra sonrakı fəaliyyət başlayır (alqortitm 2) [3,5]:

$$i = (i + 1) \bmod 16; j = (j + S_i) \bmod 16; S_i S_j \text{-in yerlərini dəyişmək;} \\ a = (S_i + S_j) \bmod 16; z_i = S_a.$$

Alınan 4- işarəli z_i qiyməti, növbəti giriş verilənlər selinin 4-bitli blokunu şifrələmək 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 alqortimi üzrə ədəd ardıcılığını generasiya edək. S cədvəlini “0”-dan 15-ə dək ədəd ardıcılığı ilə dolduraq.

S cədvəli

Elemen	0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1
tin nömrəsi											0	1	2	3	4	5
Qiymətlər	0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1
											0	1	2	3	4	5

Sonra K cədvəlini, ona lazımı sayda açar yazmaqla hazırlayaq:

K-cədvəli [3]

Elemen	0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1
tin nömrəsi											0	1	2	3	4	5
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 alqortim 1-i istifadə edəcəyik. Yerinə yetirilən prosesi isti-qamət göstərən cədvələ yazaq (cədvəl 2.14). Hasablanma 16 modu-lu üzrə aparılır.

Cədvəl 2.14.

RC4 alqoritmin hazırlıq mərhələsi (əvəzləməcədvəlinin təşəbbüslənməsi)			
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) keçmək		
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	$i < 16$, ona görə b.2-yə keçmək		

2	$j = (j + S_i + K_i) \bmod 16 = (3 + 2 + 3) \bmod 16 = 8$	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	$j = (j + S_i + K_i) \bmod 16 = (8 + 0 + 4) \bmod 16 = 12$	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	$j = (j + S_i + K_i) \bmod 16 = (12 + 4 + 5) \bmod 16 = 5$	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	$j = (j + S_i + K_i) \bmod 16 = (5 + 4 + 6) \bmod 16 = 15$	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	$j = (j + S_i + K_i) \bmod 16 = (15 + 6 + 1) \bmod 16 = 6$	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	$j = (j + S_i + K_i) \bmod 16 = (6 + 7 + 2) \bmod 16 = 15$	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	$j = (j + S_i + K_i) \bmod 16 = (15 + 2 + 3) \bmod 16 = 4$		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	$j = (j + S_i + K_i) \bmod 16 = (4 + 9 + 4) \bmod 16 = 1$		1
3	Yerlərini 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	$j = (j + S_i + K_i) \bmod 16 = (1 + 10 + 5) \bmod 16 = 0$		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	$j = (j + S_i + K_i) \bmod 16 = (0 + 11 + 6) \bmod 16 = 1$	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	$j = (j + S_i + K_i) \bmod 16 = (1 + 0 + 1) \bmod 16 = 2$	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	$j = (j + S_i + K_i) \bmod 16 = (2 + 13 + 2) \bmod 16 = 1$	1
3	Yerlərini dəyişmək S_i və S_j , yəni S_{13} və S_1	
4	$i = i + 1$	14
5	$i < 16$, ona görə b.2-yə keçmək	
2	$j = (j + S_i + K_i) \bmod 16 = (1 + 14 + 3) \bmod 16 = 2$	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	$j = (j + S_i + K_i) \bmod 16$ $= (2 + 7 + 4) \bmod 16$ $= 13$	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

Elem entin nömr əsi	0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1
											0	1	2	3	4	5
Qiym ətlər	1	1	1	1	2	1	6	4	5	3	1	9	8	7	0	1
	0	3	4	2		5										1

S cədvəli hazırlandıqdan sonra, 4-bitli təsadüfi sözün generasiyasına başlamaq olar. Alqoritm 2-ni istifadə etməklə birinci 5 saxta təsadüfi ədədlər ardıcılığını hesablayaq. Ədədlər ardıcılığının hesablamasının 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 ardıcılığın elementlərinin hesablanması)

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

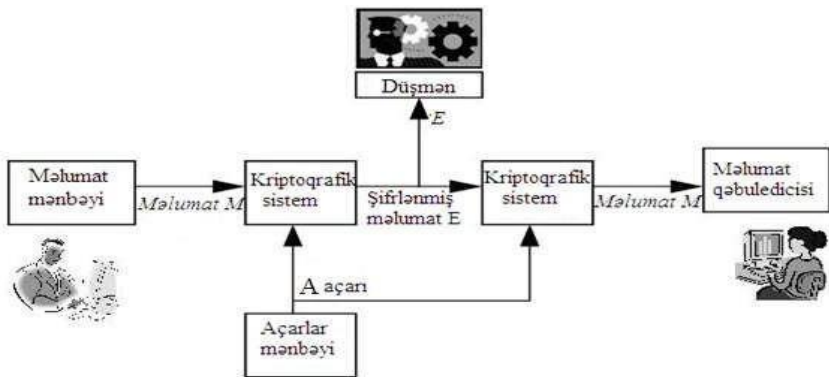
	3. yerlərini dəyişmək S_3 və S_7		
	4. $a = (S_i + S_j) \bmod 16 = (4 + 12) \bmod 16 = 0$		0
	5. $z_3 = S_0 = 10$		
z_4 -ün hesablanması	1. $i = (i + 1) = 3 + 1 = 4$	4	
	2. $j = (j + S_i) \bmod 16 = (7 + 2) \bmod 16 = 9$		9
	3. yerlərini dəyişmək S_4 və S_9		
	4. $a = (S_i + S_j) \bmod 16 = (3 + 2) \bmod 16 = 5$		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 hesablamaları 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 qiymətin 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 şəkl.2.15-də göstərilib. Özündə məlumat mənbəyini əks etdirən göndərici və alıcı (şifrlənmiş məlumatın



Şəkl.2.15. Simmetrik şifrəlməni istifadə edən məxfi sistemin ümumi strukturası

qəbuledicisi) qəbul oluna bilən şifrın və açarın seçilməsi haq-qında razılığa gəlirlər [3,4]. Sonra göndərici öz seçilmiş məlumatını şifr-ləmə alqoritmını 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 kriptoaanalitiki şifromətni açmağa cəhd edə bilər. Güman edəcəyik ki, göndərici və alıcı

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

Bu halda şifrələmənin təhlükəsizliyi açarın təhlükəsizliyindən asılıdır. Açarın açılması ötürülən verilənlərin şifrinin açılmasına gətirib çıxarır. Beləliklə, açar verilənlərin bağlanmasıadək məxfilikdə saxlanılmalıdır. Ona görə də açarların ilkin paylanması üçün etibarlı rabitə kanalı vacibdir. Beləliklə, məxfi danışanlara açarın verilməsi kanalının etibarlılığı 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 çoxməlumatı açma bilər [3,4]. Hətta açar açılmayacaqsa, kriptanaliz düşməne, eyni bir açarla şifrələnmiş öz ixtiyarında olan lazımi sayda məlumatları ötürür. Şifrələnmiş məlumatın hər bir mübadilə seansı üçün *seans açarı* adlanan nadir açardan istifadə olunması optimal sayılır [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 saxlanması və vacib olduqda dəyişdirilmə tələb olunur.

Fərz edək ki, lokal şəbəkədə 100 istifadəçi var. Bu istifadəçilər biribirləri ilə biri-hər-biri-prinsipində məxfi verilənləri mübadilə etmək istəyirlər. Bu halda hər bir cüt abonent üçün məlumatın şifrələnməsi üçün özünün məxfi açarı olmalıdır. Yüz abonent üçün $100 \times 99 / 2 = 4950$ 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 paylanmalıdır. Bundan başqa, yüz istifadəçilərin hər biri 99 müxtəlif açarı yadda saxlamalıdır. Əgər mübadilədə 100 deyil, 1000 adam iştirak edərsə, onda açarların paylanması məsələsi daha da mürəkkəbləşir.

Göstərilən çətinliklərlə əlaqədar praktikada açarların paylanmasının xüsusi avtomatlaşdırılmış idarə sistemləri istifadə olunur [3,4]. Belə sistemlər açarların generasiya olunmasına, onların saxlanılmasına və arxivləşdirilməsinə, itirilmiş açarların bərpa olunmasına, dəyişdirilməsinə 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 funksiyası 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 şifrələmə 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 abonentini arasında seansın aparılması üçün məxfi açarların paylanması proseduru necə görünür [3,4]:

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

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

Bu protokol olduqca sadədir 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 paylanması mərkəzi hər hansı bir şəkildə şəbəkənin bütün abonentlərinin məxfi açarlarını saxlamalıdır. Əgər cinayətkar sistemin istifa-dəçilərinin məxfi açarına daxilolma imkanına malik olarsa (sistemi giriş edib administratoru bəxşiş və s. ilə ələ ala bilər), onda o verilən bütün məlumatı oxuyar və dəyişdirə bilər. Nəhayət, istifa-dəçinin şəbəkəyə daxil olması zamanı məxfi açarın ilk başlanğıc paylanması problemi qalır. İlk başlanğıc məxfi açar mütləq etibarlı rabitə kanalı üzrə çatdırılmalıdır, başqa cür bütün protokol özünün hər cür mənasını itirir. Yaxşı olar ki, ilk başlanğıc açar yeni abonentin şəxsən özünə verilsin, lakin bəzi hallarda bu mümkün olmur, məsələn, verilənlər şəbəkəsinin territorial paylanması zamanı. Simmetrik şifrəlmə alqoritmlərinin bu və ya digər çatışmayan cəhətləri asimmetrik şifrəlmə alqoritmlərinin vasitəsilə aradan qaldırıla bilər.

III FƏSİL. AÇIQ AÇARLI KRİPTOQRAFIYA TEKNOLOGİYALARI

3.1. Açıq açarlı kriptografiyaya giriş

Bağlı açarlı şifrləmədə iki ciddi problem yaranır. Birinci problem 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 partnyorların əsilliyinin təmin edilməsidir [3,4].

İşgüzar yazışmalar və elektron kommersiya hər-hansı partnyorun 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 adı imzanın analoqu olmalıdır.

Əksər kriptograflar bu problemlərin həll olunması üzərində işlədilər, bunun nəticəsində XX əsrin 70-ci illərinin ikinci yarısında prinsipial olaraq bu problemlərin həll olunmasına imkan verən yeni yanaşmalar işlənib hazırlandı.

Bu yanaşmaların əsası *asimmetrik kriptoaqloritmlər yaxud metodlar* oldu [3]. Bu alqoritmlər və yaxud metodlarda düz və əks kriptovirgələr 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 əsaslanır. Şifrləmənin asimmetrik alqoritmləri həm də açıq açarlı alqoritmlər adlanır. Şifrləmə və şifrın açılması üçün eyni bir açardan istifadə olunan simmetrik şifrləmə alqoritmlərdən (bağlı açarlı şifrləmə alqoritmlərdən) fərqli olaraq asimmetrik alqoritmlərdə bir açar şifrləmə üçün, birincidən fərqli olan digər açar isə şifrın açılması üçün istifadə olunur. Alqoritm asimmetrik adlanır, çünki, şifrləmə və şifrın açılması açarları müxtəlifdir, əsas kriptografik proseslərin simmetriyası olmur. İki açarlardan biri *açıq* olur və hamıya bildirilə bilər, ikinci açar isə *bağlı* olur və məxfi saxlanılmalıdır. Açarlardan hansının, açıq

yaxud

bağlı,

şifrləmə

üçün

istifadə

olunması, hansının isə şifrın açılması üçün istifadə edilməsi kriptografik sistemin təyinatından asılıdır. Hazırkı dövrdə asimmetrik 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; müxtəlifbank və ödəmə sistemlərində.

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

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

3.1.1. Birtərəfli funksiya

Açıq açarlı şifrəmə alqoritmlərinin hamısı bir tərəfli funksiya-yanın istifadə olunmasına əsaslanırlar. Nisbətən asan hesablanan, lakin arqumentin qiymətinə uyğun olan funksiyanın qiyməti üzrə tapılması çətin olan riyazi funksiya bir tərəfli funksiya deyir.Yəni, x - bilərək $f(x)$ funksiası asan həll olunur, lakin məlum $f(x)$ üzrə x -in uyğun gələn qiymətini tapmaq çətin olur. Mürəkkəb hesablamalar dedikdə bunun üçün EHM-i istifadə etməklə bir ildən çox vaxt tələb olunur. Birtərəfli funksiya kriptografiyada heş funksiyası kimi istifadə olunur. Mühafizə məqsədilə məlumatın şifrənməsi üçün birtərəfli funksiyanın istifadə olunması mənasızdır, çünki, əks olaraq şifrələnmiş məlumatın şifrəsini açmaq artıq mümkün olma-yacaq. Şifrəmə üçün xüsusi birtərəfli funksia istifadə olunur- məxfi birtərəfli funksiya. Bu funksiya birtərəfli funksiya-ların xüsusi növüdür ki, funksiyanın əks qiymətinin tezhesablanmasına imkan verir.

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 çətin-dir;

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

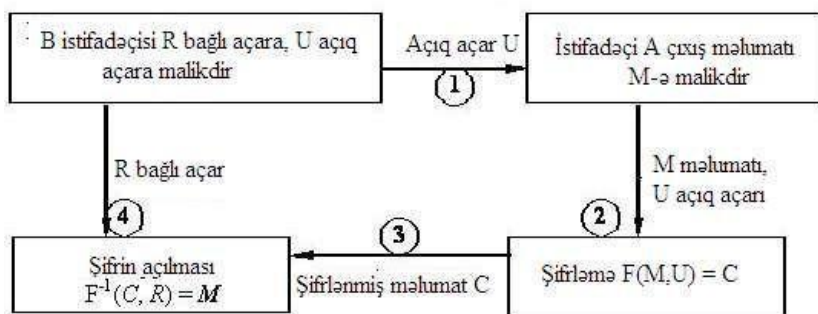
Şifrələmə üçün asimmetrik alqoritmlərin istifadə olunması. XX əsrin 70-ci illərində amerika alimləri Diffi və Helman iki müxtəlif açarın istifadə olunmasına əsaslanan şifrələmə prinsipini təklif etdilər. Bu açarlar öz aralarında əlaqəli olmalarına baxmayaraq elə quruluşlar ki, biri ilə (açıq) digərini (bağlı) açmaq praktiki olaraq mümkün deyil. Bu prinsip istifadəçiləri şifrələmə/şifrənin 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 şifrələmə 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 istifadə olunmasının bu prinsipi açıq şifrələmə yaxud açıq açarlı şifrələmə adını almışdır. Bu prinsipə əsasən, istənilən arzu edən şəxslər məlu-matı açıq açarla şifrəyə bilərlər. Məlumatın şifrəsinin açılmasını yalnız bağlı açarın mülkiyyətçisi edə bilər.

Fərz edək ki, elektron məlumatla mübadilə aparan A və B istifadəçiləri, açıq şifrələmə sxemini istifadə edirlər. Tutaq ki, A istifadəçisi B istifadəçisinə məxfi məlumatı elə verməlidir ki, onu heç kim oxuya bilməsin. Bunun üçün aşağıdakı hərəkətləri yerinə yetirmək 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 şifrələyir və şifrələnmiş C məlumatını alır.
3. Şifrələnmiş C məlumatı istifadəçi B-yə göndərilir.
4. İstifadəçi B özünün bağlı R açarı ilə alınan C məlumatının şifrəsini açır.

Əgər şifrələmə əməliyyatını F-lə, şifrənin açılması əməliyyatını isə

F^{-1} işarə etsək, onda istifadəçilər arasında informasiya mübadiləsi protokolunun sxemini aşağıdakı kimi təsvir edə bilərik (şəkl.4.1).



Şək.3.1. Açıq şifrləmə sxemi

Açıq şifrləmənin istifadə olunması açarların paylanması problemini 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 kriptografiya 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 şifrələnməsi üçün istifadə edə bilər.

3.2. Açıq açarlı alqoritm əsasında rəqəmli imza

Bütün insanlar kimi verilənlərin ötürülməsi şəbəkəsinin istifadəçiləridə biri-birlərinə etibar etməyə bilərlər yaxud özlərini şərəfsiz adam kimi apara bilərlər. Onlar özgə məlumatlarını saxtalaşdırı bilərlər, özlərinin müəllifliyindən imtina edərlər yaxud özlərini digər 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 aşağıdakı xüsusiyyətə malik olmalıdır [3,4]:

1. İmza yalnız bir şəxslə yaradılır, onun əsilliyinin 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 şifrələmə 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 ardıcılığını 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 hesablanması nəticəsi şifrələnir. Axırncı 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 təfəsilatı ilə baxaq.

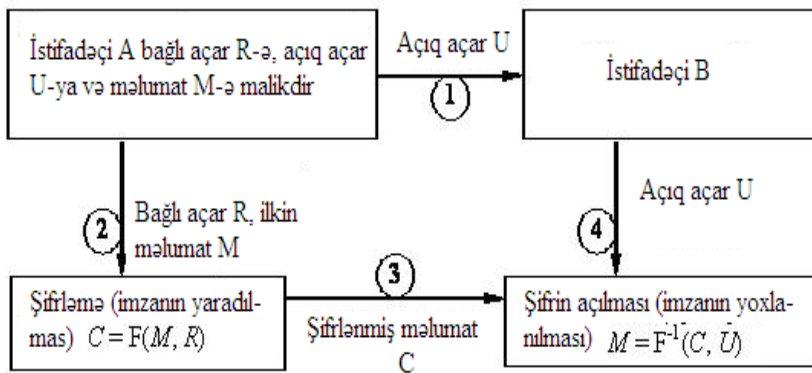
Ən sadə üsul açıq şifrələmədə olduğu kimi öz aralarında əlaqəli olan açarların istifadə olunmasına əsaslanır (açıq və bağlı açarlara). Lakin bağlı və açıq açarların rolu dəyişirlər- imzalanma açarı məxfi açar, yoxlama açarı isə açıq açar sayılır.

Əgər bu zaman xüsusiyyət saxlanılırsa, açıq açarla bağlı açarı tapmaq praktiki olaraq mümkün deyil, onda imza halında məxfi açarla şifrələnən 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, istifadəçi 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 şifrələnmiş məlumat C alır.
3. Şifrələnmiş 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 autentikliyi və bütövlüyü təmin olunur. Açar cütü-lüyünün 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, məsələn, istifadəçi haqda

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

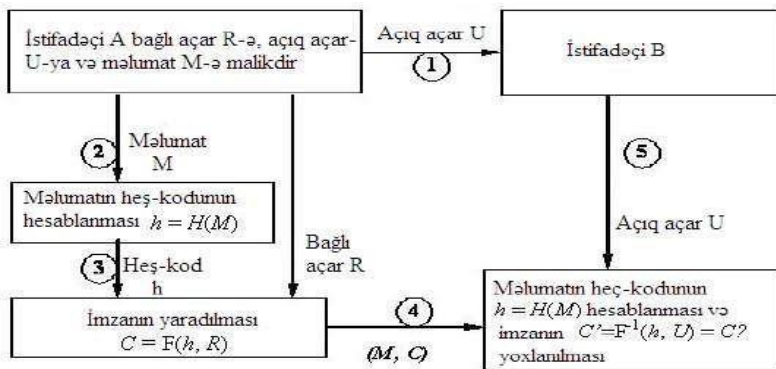
Açarın mülkiyyətçisi haqda məlumatlar ERİ-in digər vacib funksiyasını reallaşdırmağa, məsələn, müəllifliyin müəyyən edil-məsinə imkan verir, çünki, imzanın yoxlanılması zamanı bu və ya digər məlumatın kim tərəfindən imzalanması dərhal məlum olur. Adətən ERİ-in yoxlanılmasını həyata keçirən, proqram məhsulu,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

Sənədin bərpası ilə rəqəmli imza özündə imzalanan sənədi saxlayır [3,4]: imzanın yoxlanılması prosesində həm də sənədin məzmunu yekunlaşdırılır. Əgər şifrın açılması zamanı məlumat düzgün bərpa olunursa, deməli, imza doğru olub. Sənədin bərpası ilə rəqəmli imza formalaşdırıcı ERİ-in ən məşhur 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 alqoritmı kifayət dərəcə də ləngdir, bundan başqa, məlumatın bütövlüyünü təsdiq etmək üçün çox yaddaş tələb olunur. Praktiki olaraq ERİ-in hesablanması 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 şifrələyir 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 (şəkl.3.3).



Şəkl.3.3. Rəqəmli imzanın yaradılması və yoxlanılmasının ikinci variantı

Heş-funksiya ERI-n algoritminin bir hissəsi deyil, ona görə də sxemdə istənilən etibətli 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 şifrələməklə də məxfilik təmin olunmur, belə ki, istənilən şəxs göndəricinin açıq açarını istifadə etməklə məlumatın şifrəsini açmaqla 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 göstərilməsinə görə qoyulmuş qəbz olub. İstifadəçi B inandırır 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 bilməz (ona görə ki, sənəd elektrondur) və periodik olaraq kiçik intervallarla pulu götürmək üçün qəbz bankı təqdim edir. 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. Çəkin ödənilməsi zamanı vaxt nişanı bankla qeyd oluna bilər və verilənlər bazasına yerləşdirilir. Təkrar təqdim olunma cəhdi zamanı bank bunu aşkar edir və uyğun ölçü götürür.

Rəqəmli imzanın növlərindən biri *inkar edilməyən rəqəmli imza*dır [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 icazəsi olmadan yoxlanıla bilməz. Beləliklə, korrespondensiya alıcısı məlumatı imzalayan şəxsin icazəsi olmadan imzanı göstərə bilməz (yaxud imzanın doğruluğunu sübut edə bilməz).

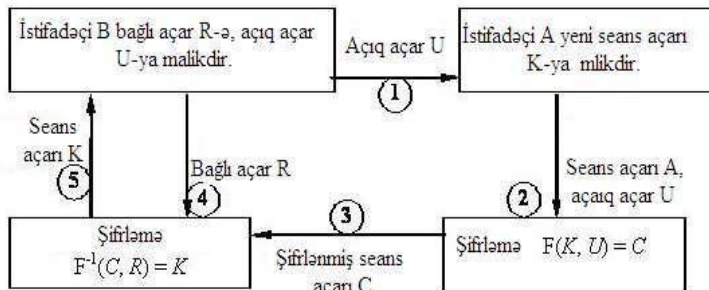
3.3. Asimmetrik alqoritmədən istifadə etməklə məxfi açarın formalaşdırılması

Açıq açarlı alqoritmlər praktikada məlumatın bilavasitə şifrələnməsi üçün nadir hallarda istifadə olunur [3/4]. Buna böyük həcmli verilənlərin şifrələmə və şifrin açılması zamanı asimmetrik alqoritmlərin 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 şifrələməyə nisbətən olduqca yavaş aparılmasına gətirib çıxarır [3,4]. Lakin qısa verilənlər blokunun emalı zamanı, məsələn, müəyyən uzunluqlu açarların açıq açarlı şifrələmə alqoritmləri əhəmiyyətli dərəcədə effektiv istifadə 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 şifrələnməsi 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 şifrələyir.
3. Şifrələnmiş seans açarını istifadəçi B –yə göndərir.
4. İstifadəçi B alınan paketin öz bağlı açarı ilə şifrəsini açır.
5. İstifadəçi A və B şifrələnmiş məlumat mübadiləsi üçün razılaşdırılmış seans açarını istifadə edirlər.

A və B istifadəçi cütünə şifrələmə -şifrın 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 alqoritm ilə şifrələmədə istifadə olunacaq. Ölçüsünə görə böyük olmayan verilənlər blokunun



Şək.3.4. Ümumi sekret açarının formalaşdırılması sxemi

şifrələnməsi kifayət dərəcədə tez yerinə yetirilir və telekommunikasiya proseslərini ləngitmir, hətta sistemdə 1000-lərlə istifadəçi olduqda belə. Açarların paylanmasının daha mürəkkəb protokolları mövcuddur. Belə protokollar rabitə seansının iştirakçılarının əsilliğini təsdiq edir, sorğu-cavab mexanizmi ilə seansın doğruluğunu 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 cütünü 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 alqoritmə 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.

Alqoritmə adları	İstifadə olunma imkanları		
	Şifrləmə /şifrin açılması	Rəqəmli imza	Açarın razılaşdırılması yaxud formalaşdırılması
RSA	Hə	Hə	Hə
Diffi- Helman alqoritmə	Yox	Yox	Hə
ƏL-Qamal alqoritmə	Hə	Hə	Hə

Elleptik
əyrlərin istifadə
olunması
alqoritmi

Hə

Hə

Hə

3.4. Kombinasıya olunmuş şifrləmə kriptosistemi

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

kin onların sürəti yüzlərlə (və daha çox) dəfə məxfi açarlı simmetrik 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 verilənlər zamanı məxfi açarın düşmən tərəfindən açılması təhlükəsi var. Bu kriptosistemlərin birgə istifadə olunması, informasiyanın məxfiliyinin təmin olunması üçün, ona kriptografik 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 şifrlənməsi üçün istifadə edirlər, açıq açarlı asimmetrik kriptosistemi isə yalnız simmetrik kriptosistemin sekret açarını şifrləmək üçün 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-digital converter-adlanır [6]. Fərz edək ki, istifadəçi A istifadəçi B-yə müha-fizə olunmuş məlumat M verilişi

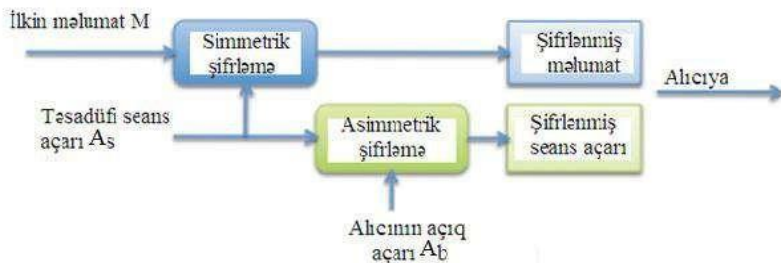
üçün kominasiya edilmiş şifrləmə metodunu istifadə etmək istəyir. Onda A və B istifadəçilərinin hərəkət ardıcılığı aşağıdakı kimi olacaq.

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 alqoritm ilə seans məxfi açarı A_s üzərində məlumatı M şifrləyir.
3. Asimmetrik alqoritm 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.

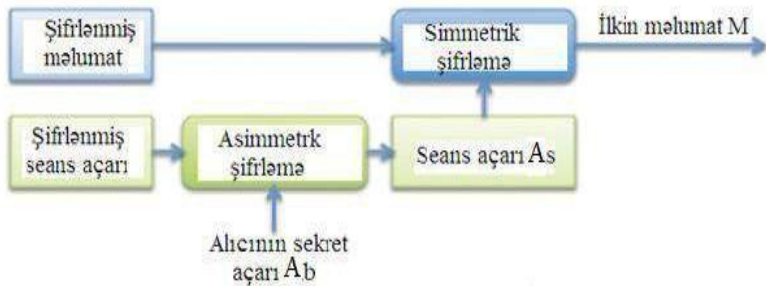
A istifadəçisinin hərəkəti aşağıdakı şəklin üzərində təsvir olunmuşdur (şək. 3.5).

İstifadəçi B-in hərəkəti (elektron digital converter-tin 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 alqoritmə şifrəsini açır. B istifadəçisinin hərəkəti aşağıdakı şəklin üzərində təsvir olunmuşdur (şək.3.6).



Şək.3.6. Kombinasiya olunmuş metodla məlumatın şifrəsinin açılması sxemi

Alınan elektron digital converter-ti yalnız qanuni alıcı–istifadə-çi B açar bilər. Yalnız şəxsi məxfi açarına k_b malik olan istifadəçi B, sekret seans açarının A_s şifrəsini düzgün açar bilər və sonra bu açarın köməyi ilə alınan məlumatın M şifrəsini açar və oxuya bilər.

Digital converter metodu zamanı simmetrik və asimmetrik kriptoaqloritmin çatışmayan cəhətləri aşağıdakı şəkildə kompensasiya olunur [6]:

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

Nəticədə sürətli şifrləmə ilə birlikdə açarların əlverişli paylanması alınlar.

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

şifrlənir. Bu halda simmetrik şifrləmənin açarının hamıya yayılmasının mənası yoxdur, çünki, növbəti məlumatın şifrlənməsi üçün digər təsadüfi məxfi açar istifadə olunacaq [6].

Kombinasiya edilmiş metod zamanı həm simmetrik, həm də asimmetrik kriptosistemlərin kriptografik 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 hesləmə funksiyası

Elektron rəqəmli imza telekommunikasiya kanalları üzrə verilən mətnin autentifikasiyası üçün istifadə olunur [7,8,9]. Belə mübadilə zamanı sənədlərin emalına və saxlanılmasına sərf olunan xərc azalır, və axtarma zamanı sürətlənir. Ancaq sənədin özündə həm də pdf sənədin müəllifinin autentifikasiyası problemi yaranır, daha doğrusu həmən istifadəçi əsilliyinin müəyyən edilməsi və qəbul edilmiş elektron formatda olan sənəddə dəyişikliyin olmaması.

Elektron sənədlərin autentifikasiyanın məqsədi onların mümkün olan pis niyyətlə edilən hərəkətlərdən mühafizəsidir. Belə pis niyyətlərə aiddirlər [7,8,9]:

- aktiv tutma-şəbəkəyə qoşulan pozucu, elektron formatda olan faylları tutubsaxlayır və onları əvəz edir;
- masquerade – istifadəçi E istifadəçidən C-in adından istifadəçiyə A-yə sənəd yönləndirir;
- treachery – istifadəçi A istifadəçiyə B-yə sənəd göndərmədiyini bildirir, amma iş ondadır ki, göndərüb;
- 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 informasiya texnologiyalarından istifadə edən xüsusi şəxslərə böyük ziyan verə bilər.

Məlumatın bütövlüyünün və onun müəllifinin əsilliyyənin yoxlanılması narazıcılığını elektron rəqəmli imza metodları ilə yüksək həll etməyə problemlərini imkan yaradır [7,8,9].

3.5.2. Rəqəmli signaturanın ən vacib 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 etməyə 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 qabiliyyətinə, eləcə də məlumatın içindəkilərin qarşılıqlı əlaqəsinə, imzanın özünə və açar cütliyinə əsaslanır. Bu elementlərdən heç olmasa birinin dəyişməsi rəqəmli imzanın əsilliyyənin tanınmasını mümkünəş 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 formalaşdırmaq üçün istifadə edir. Açıq açar isə bütün digər abonentlərə məlumdur və elektron sənəd alıcısının ERİ-ni yoxlaması üçün istifadə edilir.

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

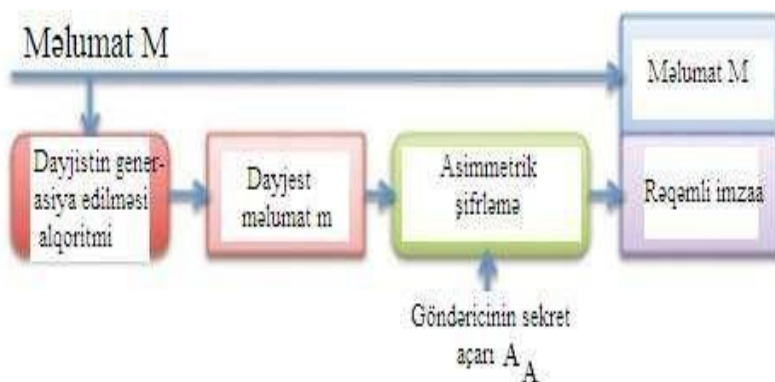
- rəqəmli imzanı formalaşdırmaq;
- rəqəmli imzanı yoxlamaq.

Rəqəmli imzanın formalaşdırılması prosedunda məlumatı göndərən məxfi açarı, rəqəmli imzanın yoxlanılması prosedunda – göndəricinin açıq açarı istifadə 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 daycestdə 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

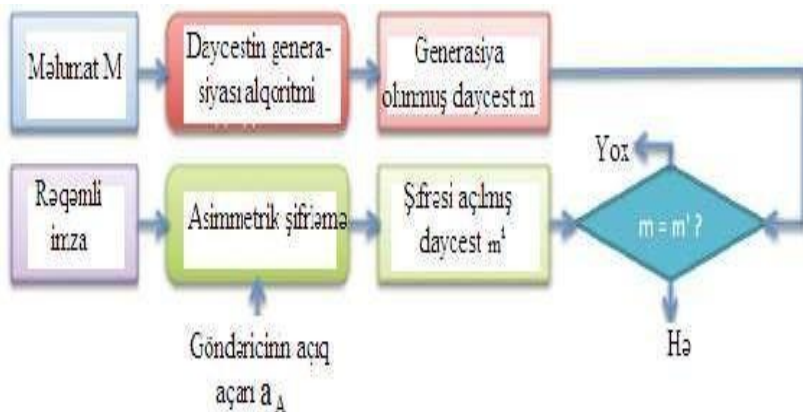
alıcının

adresinə

göndərilir.

3.5.4. Rəqəmli imzanın yoxlanılması proseduru

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 dəcestin şifrəsini açır. Bundan başqa, alıcı özü qəbul olunmuş məlumatın M heş –funksiyasının $h(M)$ köməyi ilə dəcesti m' hesablayır və onu şifrə olunmuşla yoxlayır. Lakin M eeləcədə M ilə oxşarlıq yəni bir-birinə düşürsə, demək rəqəmli imza düzgündür. Demək olar ki, imza ya kimlərsə tərəfindən saxtalaşdırılıb, ya da məlumatın məzmunu pozulub, yəni dəyişdirilib. ERİ sistemində prinsipial moment ondan ibarətdir ki, istifadəçinin ERİ- sinin saxtalaşdırılması, onun məxfi imza açarını bilmədən mümkün deyil. Ona görə də imza açarının gözlənil-məz təsadüfi hərəkətlərdən(GTH) mühafizə olunması vacibdir.

ERİ-in məxfi açarının simmetrik şifrələmə açarının mühafizə olunmuş şəkildə personal açar daşıyıcısında saxlanması 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 infor-masiyaya malikdir. Belə məlumatları sənədə hesablan-masınadək əlavə olunur ki, bu da onun bütövlüyünü təşkil edir. Bütün imzalar göstərilən məlumatlara malikdirlər[7,8,9]:

- tarix imza;
- müddət -son açar verilən imza;
- faylı imzalayan şəxs haqqında məlumat (A.A.S., vəzifəsi, firmanın 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 kriptografik örtülmə prosesindən aşağıdakı xüsusiyyətlərlə fərqlənir. Rəqəmli imzanın formalaşması zamanı göndəricinin bağlı açarı istifadə olunur, onda şifrələmə zamanı alıcının açıq açarı istifa-də edilir.

Rəqəmli imzanın yoxlanılması zamanı göndəricinin açıq açarı, şifrələmə zamanı isə alıcının bağlı açarı istifadə olunur [7,8,9]. Formalaşmış 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 şifrələməyə analogi olaraq, ERİ-in yoxlanması üçün istifadə olunan açıq açarın dəyişdirilməsinin qeyri mümkünliyünü 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 uzunluqlu əsas məlumatın sıxılmış ikili təsviridir. Heş-qiymət $h(M)$ heşləmə funksiyası ilə formalaşır. Heşləmə funksiyası (heş-funksiya) özündə, girişində dəyişən uzunluqlu məlumat M olan, çıxışında isə qeyd olunmuş uzunluqlu sətir $h(M)$ alınan çevirməni əks etdirir. Başqa sözlə desək, heş-funksiya $h(M)$ argument 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 yüz iyirmi səkkiz bitədək yaxud iki yüz əlli altı bit, onda məlumatın təxmini ölçüsü meqabayt yaxud yüksək nəticə ola bilərdi. Biliyimiz ki, HEŞ H funksiya $H-M$ hecdə asand olmayan şəkildə sənəddən $-M-$ asılıdır eləcədə sənədin özünü bərpa huququnu təmin etmir.

Heşləmə qeyd olunan göstəricilərin xüsusiyyətlərə ibarət olunmalıdır [7,8,9]:

- Hash function lazımı olan ölçüsü istifadə oluna bilər.
- Hash function sabit ölçüyə malikdir.
- Hash function $h(x)$ lazımcıca istənilən x üçün hesablamaqlar.

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

1. Heş-funksiyası mətndə əlavə etmə, sıçrayış, yerdəyişmə və s. kimi dəyişikliklərə həssas olmalıdır.

2. Heş –funksiya biristiqamətli olmalıdır.
3. İki müxtəlif sənədin heş-funksiyasının qiymətinin üst-üstə düşmə ehtimalı (onların uzunluğundan asılı olmayaraq) çox cüzii olmalıdır.

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

Beləliklə, heşləmə funksiyası məlumatın dəyişməsinin aşkar olunmasında istifadə oluna bilər, yəni kriptografik 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 autentifikasiya olunmaları üçün istifadə olunur.

Heşləmənin aşağıdakı məşhur 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 alqoritmı istifadəçilərin parolunu 16-baytlıq ədədə çevirmək məqsədilə Micro-soft Windowsun axıncı versiyasında istifadə olunur;
- SHA-1 (Secure Hash Algorithm)-bu, məlumatın daycestini hesablamaq alqoritmidir və dünyada geniş yayılmışdır.
- Heş-funksiya həm də istifadəçilərin autentifikasiyası üçün geniş istifadə olunur.

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 statistiki 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 olunan məlumatların müxtəlif variantları ilə bağlıdır, yəni başqa sözlə desək məlumat mənbəyinin müxtəlif vəziyyətləri ilə əlaqəlidir. Bununla əlaqədar olaraq, ayrı-ayrı məlumatlarla göndərilən informasiyaların miqdarını N müxtəlif məlumatların ümumi sayına (ya da informasiya mənbəyinin vəziyyətinə) mütənəib olmasını hesab etmək olar. Amma praktikada informasiya miqdarı halında N -in özü deyil, onun 2 əsasinə görə loqarifması götürülür [10]:

$$I = \log_2 N$$

Bu ifadə bizə nəticəni bitlə təmin etməyə imkan verir. İnformasiya miqdarının belə təyin olunması informasiyanın formal məntiqi 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]:

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

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

$$I_1 = \log_2 32 = 5 \text{ bit}$$

Belə yanaşma zamanı hər hansı bir məlumatda informasiya həcmi-nin 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 daşıdığını tapaq [10]:

$$I_4 = 4 \log_2 32 = 20 \text{ bit}$$

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

Xartli ölçüsü həmişə məlumatın düzgün xarakteristikası sayılır, çünki, istənilən mümkün məlumat bərabər ehtimalı nəzərdə tutur. Məlumatın mövcudluğu mövcud qeyrimüəyyənliyi aradan qaldırmaq olduğundan, yüksək ehtimalı olan məlumatlar daha az dəyərlidir. Çünki, informasiyanın dəyəri mövcud olan qeyrimüəyyənliyi aradan qaldırmaqdan ibarətdir, yüksək ehtimala malik olan informasiya 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 kəmiyyətə 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]:

$$I = H_{\text{başl}} - H_{\text{son}}$$

burada $H_{\text{başl}}$ -məlumatın alınmasına dək məlumat mənbəyi ilə xarakterizə olunan qeyrimüəyyənlikdir.

İnformasiya mənbəyinin qeyrimüəyyənliyi aşağıdakı ifadə ilə qiymətləndirilir [10]:

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

burada p_i -mənbənin i -ci vəziyyətinin ehtimalıdır.

Cəmin qarşısındakı çıxacaq işarəsi ona görə qoyulub ki, ehtimalın qiyməti düzgün kəsrdir və mənfi loqarifməyə malikdir, qeyrimüəyyənliyin qiymətləndirilməsini isə cəmləmə işarəsilə almaq lazımdır.

Misal. Qutuda olan bir qara və bir ağ şarı çıxaranarkən, qeyrimüəyyənlik aşağıdakı kimi təyin olunur:

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

Qeyrimüəyyənlik bir bitə bərabər oldu.

$$H = (7/8)\log_2(7/8) - (1/8)\log_2(1/8) = (7/8)(\log_2 8 - \log_2 7) + (1/8)(\log_2 8) = (7(3 - \log_2 7) + 3)/8 \approx (7(3 - 2,8) + 3)/8 \approx 0,55 \text{ bit}$$

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 $p_i = p_j$, $\forall i, j = \overline{1, M}$ 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 informasiyaya 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, eləcə də kilo, həm də meqa və s. əlavə etməklə daha böyükölçü vahidi almaq olar.

4.2. Entropiya və qeyrimüəyyənlik

Beləliklə, biz aydınlaşdırdıq ki, bir məlumatda informasiya miqdarının ölçülməsini qeyrimüəyyənlik dəyişikliyi nəzərə almaqla həyata keçirə bilərik. K. Şennon entropiya anlayışını qeyrimüəyyənlik ölçüsü olaraq təqdim edib. Entropiya $H(m)$ məlumatda informasiya miqdarını $(m-i)$ təyin edir və onun qeyrimüəyyənliyi yəni. Fərz edək ki, məlumat mənbəyi $p_1, p_2, \dots, p_n$ ehtimalla müxtəlif məlumatları $m_1, m_2, \dots, m_n$ hasil edir. Bu halda entropiya aşağıdakı ifadə ilə təyin edilir [10]:

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

Beləliklə, bu ifadədə ikili loqarifma istifadə olunur, onda entropiya bitlə ölçülür, bu ümumiyyətlə kriptografiya və informasiya nəzəriyyəsində qəbul edilib.

Entropiyanın başqa mənası entropiyanın qeyrimüəyyənlik kəmiyyəti ölçüsüdür. Məsələn 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 ehtimalı $p(m_1)=0$, 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 qeyrimüəyyənlik sıfıra bərabərdir. Həqiqətən, əgər əvvəlcədən məlumdur ki, iki məlumatdan yalnız biri hasil olunursa, onda heç bir qeyrimüəyyənlik yoxdur. İkinci məlumat mənbəyinin entropiyasını təyin edək [10]:

$$H_2 = -(1/2)\log_2(1/2) - (1/2)\log_2(1/2) = -\log_2(1/2) = -(-1)$$

Bu, bərabərdir $=1$ 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 mənbəyinin 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 saxlanması 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 məhdudlaşdırma entropiyası h ilə kifayət qədər böyük uzunluqlu n mətni hasil edərsə, 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, "Yes" və ya "Not" cavablarını), o zaman məlumatın mənasını düzgün müəyyən etmək üçün bir biti doğru təyini bilmək kifayətdir [7]. "Yes" və "Not" sözlərini şifrələmək üçün biz nəqədər 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 normasını 1,0-dan 1,5 bit-ə qədər diapazonda qiymətləndirirlər. Hesab edəcəyik, 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 ardıcılığının bərabər ehtimallı olması şərtində bir işarəsilə verilə bilən informasiyanın bitlərinin sayıdır. Əlifbası L işarələrdən ibarət olan dilin mütləq norması aşağıdakı kimi hesablanı bilər [10]:

$$R = \log_2 L$$

Əlifbası 33 hərfdən ibarət olan rus dili üçün dilin norması bərabərdir [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 hərflərinə digərlərinə nisbətən məlumatda daha tez-tez rast gəlinir. İkinci səbəbi sözlərdə hər-hansı söz birləşmələrinin qəbul edilməzliyidir.

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

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 dillərdə malikdir, məsələn, ingilis dili.

Bütün işarələri bərabər ehtimallı olan məlumatların minimum artıqlığı sıfır 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 şifrələnmiş mətnin analizi onun mümkün olan uzunluğundan başqa heç bir informasiya vermirsə, belə kriptografik sistem tam məxfi sistem adlanır [10].

Əgər kriptografik sistem tam məxfi deyilsə, onda məlumatın şifrəməni ilə tanışlıq uyğun açıq mətn haqqında bəzi məlumatlar verir. Əksər sadə şifrəmələr məsələn, bir əlifbalı əvəzləmə yaxud yerdəyişmə metodları üçün, cinayətkar tərəfindən tutulub saxlanılmış şifrələnmiş məlumatın uzunluğu artıqca şifrəmə açarları yaxud açıq mətn haqqında bəzi nəticələri əldə etmək olar. Bu təbii dillərin artıqlığının böyük olması ilə bağlıdır. Məsələn, əgər cinayətkar tərəfindən tutulub saxlanılmış məlumat yerdəyişmə metodu ilə şifrələ-nib-sə, 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 şifrələnmiş məlumat DKDK məlumdursa, onda əlavə informasiya olmadan ilkin mətnə nəyin olmasını birmənalı olaraq təyin edə

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

1. İlk mətnə 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 kriptografik 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 şifrənin 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]:

$$m = 1100101110\dots$$

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

$$k = 1001100111\dots$$

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

$$\text{İlkin mətn} \quad m = 1100101110\dots$$

$$\text{Açar ardıcılığı bitləri} \quad k = 1001100111\dots$$

$$\text{Şifrlənmiş mətn} \quad c = 0101001001\dots$$

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 hərflə olacağını deyə bilmərik. Bu onu göstərir ki, qammanın bütün işarələr ardıcılığı bərabər ehtimallıdır. Bu o deməkdir ki, Vernam şifrəsinin köməyi ilə şifrlənmiş məlumat uyğun uzunluqlu istənilən açıq mətnə kodlaşdırıla bilər, çünki, qammanın nəzərdə tutulan işarələr ardıcılığı, onu istənilən digər ardıcılıqdan fərqləndirmə xüsusiyyətinə malik deyil [10]. Vernam şifrində, daşıyıcı açar verilənləri halında, məhz lentdən istifadə 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 çatdırılmalı və onda saxlanılmalıdır. Tam məxfi sistemlər praktikada reallaşdırılmalıdır. Nə üçün onlar bütün hallarda istifadə olunmur? Bu bir neçə səbəblərlə izah olunur. Birinci, istənilən bağlı açarlı şifrləmə sistemləri kimi, onlarda açarların paylanma problemi mövcuddur. İkinci, tam məxfi sistemlərdə şifrləmə açarının uzunluğu açıq mətnin uzunluğu kimi olmalıdır. Bundan başqa, hər bir məlumatı şifrləmək üçün özünün yeni açarı olmalıdır. Bütün bu faktörlər 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. Təklif (yaxud nadirlik) məsafəsi

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

genişləndirəcək, nəticədə məlumatın şifrəsi-ni açə biləcəək. Şennon şifrin təklük məsafəsi U anlayışını verib. Bu anlayışda o, cinayətkar tərəfindən açarın birmənalı bərpa edilməsi üçün şifrlənmiş məlumatda neçə hərfin olmasını göstərir. Təklük məsafəsini hesablamaq üçün açarın entropiyasını $H(K)$ bilmək vacibdir. Simmetrik şifrlər üçün açarın entropiyası təqribən açarla-rın sayının N_K -in 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 $N_k = 33! \approx 8,68 \cdot 10^{36}$ kimi təyin edilir, ona görə də açarın entropiyası bərabər olacaq [10]:

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

Əgər bizə bəzi şifrlər üçün açarın entropiyası (K) məlumdursa, onda onun üçün təklük 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 təklük məsafəsini təyin edək [10]:

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

Yəni cinayətkar tərəfindən tutulub saxlanılan şifrlənmiş məlumatın uzunluğu 35 işarədən çox olur, onda onu hər şeydən əvvəl birmənalı deşifrə etmək mümkün olacaq. Əgər şifrlənmiş məlumatın uzunluğu 35 işarədən az olarsa, onda onun birmənalı deşifrə olunması mümkün olmayacaq.

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

Cinayətkara açarın təyin edilməsini və bizim məxfi məlumatımızın deşifrə edilməsini çətinləşdirmək üçün, istifadə olunan şifrdə təklük məsafəsini istənilən qədər (bəlkə də sonsuzluqadək) artırmaq vacibdir. Təklük məsafəsinin hesablanması ifadəsini analiz edərək, bu məsələnin iki üsulla həllinin mümkün olmasını təyin etmiş olarıq.

Əgər açarın entropiyası sonsuzluğa bərabədirsə, 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 işə-rələri bərabər ehtimallıdır, ona görə də belə şifrin entropiyası sonsuz qədər böyük olacaq. Buna görə də, Vernam şifrinin təklik məsafəsi sonsuzluğa bərabərdir [10].

Yuxarıda göstəriləni 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 sıfıra bərabədirsə, açar heç vaxt təyin olunmayacaq və şifrləli məlumat açılır, çünki təklik məsafəsi sonsuza bərabər olacaq [10]. Təəssüf ki, praktikada 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 formasını entropiya saxlanılır, uzunluğu isə azalır. Buna görə, sıxılmış mətnə bir hərfə düşən entropiya ilkin mətnə olan entropiyaya nisbətən böyükdür, artıqlıq isə azdır. Belə ki, sıxıcı kodlaşdırmadan sonra şifrin vahidlikməsafəsi artır.

4.5. Şifrləmə, maneədavamlı kodlama və informasiyanın sıxılması

Vericidən qəbulediciyə informasiyanın ötürülməsi prosesində informasiyaya mənfi faktorlar təsir edir [10].

Kriptografik 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 ötürül-məsinin və multimediya texnologiyalarının meydana gəlməsi ilə böyük həcmli informasiyanın şifrələnməsi problemi yaranır [10].

Əvvəllər şifrələnmiş və ötürülən məlumatların əsas növü mətn məlumatları idisə, XXI əsrdə kriptografik 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 şifrələnməsi prob-lemi yaranır. Telekonferans, audio və ya video rabitə kimi inte-raktiv sistemlər üçün bu cür şifrələmə real vaxtda həyata keçiril-məlidir və mümkünse 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]: kriptografik şif-rələmə, maneədavamlı kodlama və sıxılma.

İyirminci əsrin bəzi elmi işlərində məlumatların çevirmə üsul-larınınüçü də kodlaşdırma adlandırılırdı [10]: kriptografik 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, kriptografik çevirmənin məqsədi, məlum olduğu kimi, icazəsiz daxilolmadan mühafizə, autentifikasiya və qəsdən edilən dəyişikliklərdən mühafizədir.

Maneədavamlı kodlamanın məqsədi veriliş zamanı informasi-yanı və onun saxlanması təsadüfi maneələrdən mühafizə etmək-dir [10]. Effektiv kodlama ötürülən və saxlanılan verilənlərin həcmi-ni 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, kriptografik şifrələmə, maneədavamlı kodlama və sıxılma qismən bir-birini tamamlayır və onların kompleks istifadə olunması ötürülən informasiyanın etibarlı mühafizəsi üçün rabitə kanallarının effektiv istifadə olunmasına kömək edir. Praktikada kriptografik 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

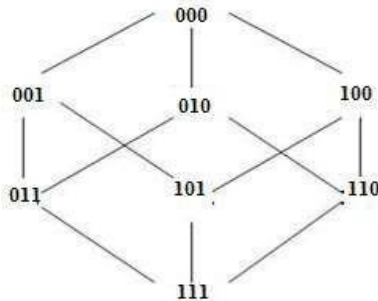
Qeyd olunduğu kimi, informasiyanın kriptografik çevirmə məsələləri məlumatın maneədavamlı kodlama məsələləri ilə sıx bağlıdır [10]. Bu onunla bağlıdır ki, bir tərəfdən (nəzəri olaraq), kriptografik şifrələmə və maneədavamlı kodlama zamanı informasiya nəzəriyyəsinin eyni qanunları istifadə olunur. Digər tərəfdən (praktiki olaraq) informasiyanın yığılması, saxlanması və ötürülməsi prosesləri saxlanılan və emal olunan verilənləri təhrifə uğratmaq qabiliyyətinə 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. Kriptografiyada şifrələmə anlayışına analogi 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. Ümumiyyətlə, iki kod sözü arasındakı amerika riyaziyyatçısı R.U.Xem-minqin adı ilə adlanan Xemminq məsafəsi müxtəlif işarələrin sayıdır. 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 fərqlənən kod sözlərinə qonşu olanlar adlandırılır. Məsələn, 101 və 111 kod sözləri yalnız orta işarə ilə fərqlənirlər, 101 və 110 sözləri qonşu deyillər, çünki, onlarda yalnız iki son işarələr fərqlənirlər.

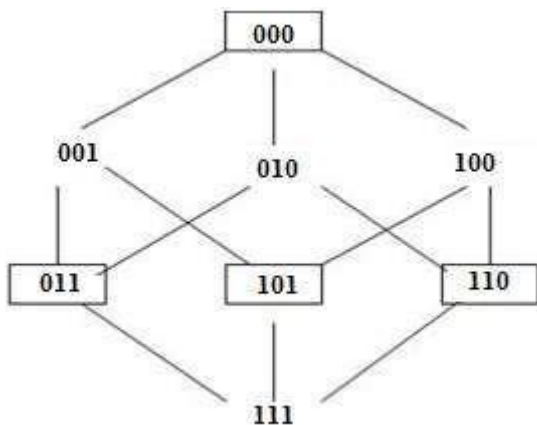
Bütün üç işarəli ikili kombinasiyanı və qonşu kod sözlərini xətlə birləşdirək. Onda biz şəkil.5.1-də göstərilən sxemi alırıq [10]. Sözlər arasındakı minimal kod məsafəsi adi qeyri maneədavamlı məlumat üçün kod məsafəsi vahidə bərabərdir.



Şəkil. 4.1. Üçişarəli ikili kod sözü

Məlumatların verilməsi üçün bütün üçşərəli ikili sözlərinin istifadə olunması zamanı onların hamısı icazəli sayılır. Cütlüyə yoxlama şərti üzrə nəzarəti istifadə edək. Onda yalnız çərçivə ilə ayrılan cüt vahidlisözlər 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 üçşərəli kod sözü

məsafəni artırmaq üçündür. Nəzarət edici işarə informasiyalı işarələrdən 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 qabiliyyətini əldə etmək üçün kodun artıqsızlığından imtina etmək vacibdir. Bu-nun üçün ikili işarələrin bütün mümkün olan kombinasiyalarını iki altçoxlığa bölürlər: icazəli kod sözlərinə və icazəsiz kod sözlərinə. Bölmə icazəli

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

aşkar etməyə imkan verir.

Təbii ki, artıq nəzarət işarələrinin əlavə edilməsi kodlaşdırılmış informasiyanın saxlanılmasına yaxud verilişinə xərcləri artırır. Bu zaman faydalı informasiyanın faktiki həcmi dəyişməz qalır. Bu halda maneə davamlı kodun artıqlığı haqda danışmaq olar və onu formal olaraq nəzarət işarələrinin sayının kod sözünün ümumi işarələrinin sayına nisbəti ilə təyin etmək olar. Yuxarıda deyil-diyi kimi nəzarət işarələri informasiya vermir və bu mənada faydasızdır. Nəzarət işarələrinin nisbi sayına maneə davamlı kodun artıq -

lığı deyilir və aşağıdakı ifadə ilə təyin edilir [10]:

$$Q = (k/n) * 100\%,$$

burada n – blokda ki ikili işarələrin ümumi sayı, k – isə nəzarət işarələrinin sayıdır.

Məsələn, cütüyə yoxlanılan üç işarəli kodun artıqlığı bərabərdir [10]:

$$Q = (k/n) * 100\% = (1/3) * 100\% \approx 33\%$$

Artıqlıq kodun əhəmiyyətli bir xarakterikasıdır və artıqlıq həddindən artıq artım arzuolunmazdır. İnformasiya nəzəriyyəsinin vacib məsələsi tələb olunan aşkarlama və korrektə edici qabiliyyətini 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 $0 \dots 010 \dots 0$, vektorla 2 modulu üzrə toplanmasından ibarətdir. n - işarəli kod sözü üçün bir qat 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 $n \leq 2^m - 1$ bərabərsizlik 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, hansını ki 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, alırıq [10]:

$$s_0 = a_0 \oplus a_3 \oplus a_5 \oplus a_6 s_1 = a_1 \oplus a_3 \oplus a_4 \oplus a_6 s_2 = a_2 \oplus a_3 \oplus a_4 \oplus a_5$$

İşarələrin birində səhv yaranan zaman s_1 funksiyası vahidə, səh-vin olmaması zamanı isə sıfır çevrilir. Bu tələbin təmin olunması cədvəl4.1-də vrilib [10].

Cədvəl.4.1. Səhv vektorları və ona uyğun sindromları

a6	a5	a4	a3	a2	a1	a0	s2	s1	s0
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_2 sıralarına uyğun tənliklərdə iştirak edən yerdə qalan işarələrin 2 modulu üzrə çevirməsi kimi baxmaq olar [10]:

$$a_0 = a_3 \oplus a_5 \oplus a_6 a_1 = a_3 \oplus a_4 \oplus a_6 a_2 = a_3 \oplus a_4 \oplus a_5$$

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) maneədavamlı Xemminq ko-dunun icazəli kod sözünə çevirmək üçün yuxarıda tapılan asılılıq üzrə nəzarət işarələrini hesablayırıq [10]:

$$a_1 = 1 \oplus 0 \oplus 1 = 1 a_1 = 1 \oplus 0 \oplus 1 = 0 a_2 = 1 \oplus 0 \oplus 1 = 0$$

Nəzarət işarələrini nəzərə almaqla kod sözü 110100 -ə bərabər olacaq. Əgər veriliş yaxud saxlanma prosesində təhrifsiz söz qalıb-sa, onda onun $s_0 \dots s_2$ 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: $s_0 \dots s_{2-i}$ uyğun olaraq aşağıdakı 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 vektoru ilə toplamaq kifayətdir.

İndi də (7.4) Xemminq kodunun artıqlığını hesablayaq [10]:

$$Q = (k/n) \cdot 100\% = (7-4)/7 \cdot 100\% \approx 43\%$$

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 azaltmaq və tətbiq olunan dilin statistik qanunlarını uyğunlaşdırmaqdır [10]. Artıqlığın qismən aradan qaldırılması verilənlərin sıxılması yolu ilə əldə edilir. İnformasiyanın sıxılması özündə ilkin məlumatın bir kod sistemindən 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 sıxılmanı itgi ilə reallaşdıran (geri dönməz sıxılma) alqoritmlərə.

Tərs çevrilə bilən sıxılma, dekodlamadan sonra məlumatların tamamilə dəqiq bərpasını nəzərdə tutur və istənilən məlumatı sıxmaq üçün istifadə edilə bilər. O həmişə çıxış məlumatın informasiyivliyini dəyişdirmədən, yəni informasiya quruluşunu itirmədən ç1-x1ş informasiya axınlarının həcmnin azalmasına gətirib çıxarır.

Tərs çevrilə bilən sıxılma fayllar, yüksək keyfiyyətli səs və qrafik şəkilli mətnlər üçün istifadə olunur. Geri dönməz sıxılma adətən itgisiz kodlaşdırma ilə müqayisədə daha yüksək sıxılma dərəcəsinə malikdir, lakin dekodlaşdırılmış verilənlərin ilkin verilənlərə nisbətən bəzi dönmələrə yol verir. Praktikada çoxlu sayda praktiki məsələlər var ki, onlarda sıxılmadan sonra ilkin informasiyanın dəqiq bərpa olunmasına qoyulan tələblərə rəyat edilməsi məcburi deyil. Bu, xüsusilə multimediyaya informasiyalarının sıxılmasına aiddir. Məsələn, multimediyaya informasiyalarının JPEG və MPEG kimi formatları geniş istifadə olunur və bu sistemlərdə geri dönməz sıxılma tətbiq edilir. Geri dönməz sıxılma adətən kriptografik şifrələmə 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 kriptografik sistemə daxil edilməzdən əvvəl tez-tez geri dönməz sıxılmaya məruz qalır. Məlumat 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. Alqoritmın ideyası aşağıdakılardan ibarətdir: işarələrin məlumata 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 uzunluğuna baxmayaraq, onların birmənalı dekodlanmasına imkan verir. Klassik Xofman kodunun sintez proseduru, məlumat mənbəyinin statistik xarakteristikaları haqqında aprior informasiyanın olmasını təhmin edir. Sadə misal təmsalində 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 müxtəlif $S_1 \dots S_4$ 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]:

S_3	0,55	0,55	0,55	1
S_1	0,2	0,25	0,45	
S_2	0,15	0,2		
S_4	0,1			

a)

S_3	0,55	0,55	0,55	1
S_1	0,2	0,25	0,45	
S_2	0,15	0,2		
S_4	0,1			

b)

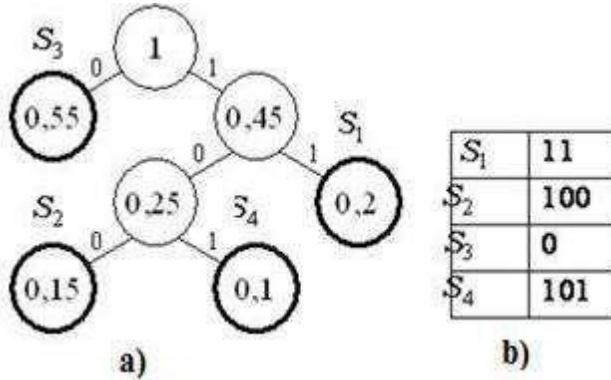
Şəkl.4.2. Xofman kodlamasının birinci mərhələsi

Birinci mərhələdə cədvəlin sətirinin əvəzlənməsi həyata keçirilir: ən kiçik ehtimalla yaranan işarələrə uyğun olan iki sətir bir ümumi ehtimalla əvəzlənir, bundan sonra cədvəl yenidən sıralanır. Əvəzləmə, cədvəldə yalnız bir ümumi ehtimallı sətir olana qədər davam edir (şəkl.4.2b).

İkinci mərhələdə əvəzləmə cədvəli üzrə kod ağacının qurulması həyata keçirilir (şəkl.4.3a) [10]. Ağac cədvəlin axıncı sütunundan başlayaraq qurulur.

Ağacın kökü sonuncu sütunda yerləşən bir vahid təşkil edir (şəkl.4.3a). Baxılan misalda bu vahid ağacın kökü ilə əlaqəli iki qovşaqlı şəkildə təsvir edilmiş 0,55 və 0,45 ehtimallarından yaranır. Onlardan birincisi S_3 işarəsinə uyğundur və beləliklə, bu qovşaqların 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 ehtimalı isə öz növbəsində,

0,15 ehtimalı ilə S_2 işarəsinin gəlişini, 0,1 ehtimalı ilə S_4 işarəsinin gəlişini təmin edir. Kod ağacının ayrı-



Şəkl.4.3. Xofman kodlamasının ikinci mərhələsi
ayrı qovşaqlarını birləşdirən qabırqalar 0 və 1 rəqəmləri ilə
nömrələnilər (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 tutuşdurulur. Bu kod sözləri ağacın kökündən uyğun işarələrə yol təşkil edən qabırqaların qeyd olunduğu rəqəmləri oxumaqla yaradılır. Baxılan misal üçün Xofman kodu şəkl.4.3b-də verilən cədvəldə göstərilən şəkil alır. Lakin klassik Xofman alqoritmı 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 qabağında göndərilən tezlik cədvəlinin uzunluğu ilə artır, bu da məlumatı sıxmaq üçün bütün söyləri sıfıra yendirə bilər.

Xofmanın statistik kodlamasının digər variantı giriş axınına baxmaq və yığılmış statistika əsasında kodlamanın qurulmasından ibarətdir. Buzaman fayl üzrə iki yanaşma tələb olunur [10]: biri baxmaq üçün və statistik informasiyanın toplanması, ikinci kodlama üçün. Xofmanın statistik kodlamasında giriş işarələri (müxtəlif uzunluqlu bitlərin zəncirləri) kimi bitlərin zəncirlərinə uyğun, onların dəyişən uzunluqlu kodları qoyulur. Hər bir işarənin kodunun uzunluğu ikili loqarifmaya

proporsional onun əks işarəli tezliyi götürülür. Bütün rast gəlinən işarələrin ümumi yığımı axının əlifba-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 bilər. Xofman kodlaşdırma-sını istifadə edərkən, alqoritmin komplikasiyası giriş axınındakı dəyişən statistika 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 kodlaşdırılması minimum 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 paylanmasıyla məlum olması şərtində itgisiz olaraq qablaşdırılması metodudur.

Baxılan üsullar, verilənlərin geri dönməz sıxılmasını təmin edir. Praktikada onların reallaşdırılmasının həm proqram və həm də aparat reallaşdırılması istifadə olunur. Belə reallaşdırmalar sıxılma əmsallarının 20-40% qiymətini əldə etməyə imkan verir.

Beləliklə, kriptografik şifrələmə, maneədarlıq kodlaşdırma və sıxılma bir-birini tamamlayır və onların kompleks istifadə olunması ötürülən verilənlərin etibarlı mühafizəsi üçün kommunikasiya kanallarından səmərəli istifadə etməyə imkan verir.

V FƏSİL. VPN TEXNOLOGİYASI BAZASINDA LOKAL KOMPÜTER ŞƏBƏKƏLƏRİNDƏ İNFORMASIYA MÜHAFİZƏSİNİN TƏŞKİLİ

5.1. VPN texnologiyası bazasında Lokal kompüter şəbəkələrinin qurulması

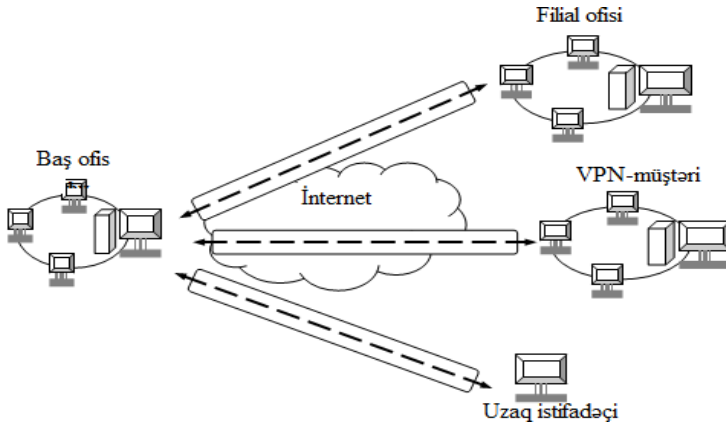
Lokal kompüter şəbəkələrində informasiya mühafizəsinin təşkili üçün VPN texnologiyasından istifadə edən zaman virtual tunelin qurulması və bu tunelə kənar istifadəçilərin daxil ola bilməməsi əsas şərtlərdəndir [11]. Virtual tunelin üstün cəhəti bəla başa gələn ayrılmış kanallar əvəzinə yüksək sürətli İnternet kanallarından istifadə edilməsidir ki, bu da maliyyə vəsaitlərindən qənaətlə istifadə olunmasına gətirib çıxarır. Maliyyə vəsaitlərinə edilən qənaət istehsalat 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 icazəsinin daxil olma.
- Qlobal açıq şəbəkələrin bütövlükdə və onların qarşılıqlı əlaqədə olduqları kompüterlərin informasiya təhlükəsizliyinin təmin etmək üçün iki yanaşmadan istifadə olunur [11]:
- lokal kompüter şəbəkələrə və onların qarşılıqlı əlaqədə olan kompüterlərinə xarici istifadəçilərin 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 istifadəçilərin icazəsinin daxil olmalarının qarşısının alınması üçün şəbəkə arası ekranlardan istifadə olunur. Bu ekran adətən lokal kompüter şəbəkələri və qlobal açıq şəbəkələrinin arasında fəaliyyət göstərir. Qlobal açıq şəbəkəyə qoşulmuş uzaq kompüter xarici

istifadəçilərin icazəsis daxilolmalarından qorumaq üçün bu kompüterdə personal ekran adlandırılan 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 kriptograf şifrələnməsinə, hə-qiqiliyinin və eləcə də bütövlüüyünün yoxlanılmasına əsaslanır [11]. Bu funksiyaların reallaşdırılması üçün effektivliyi simmetrik və asimmetrik kriptografik sistemlərin birgə istifadə olunması ilə təmin olunan kriptografik mühafizə üsullarından istifadə olunur. Lokal kompüter şəbəkələrinin xarici mühitlə birləşməsi əsasında yaradılan virtual şəxsişəbəkələrin 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 şifrələnməsi və autentifikasiyası 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 təhlükəsizlik şlüzü iki şəbəkə arasında fəaliyyət göstərən və çoxsaylı xostlar üçün şifrələməni və autentifikasiyanı təmin edən qurğudur. VPN şlüzü lokal kompüter şəbəkəsi və qlobal açıq şəbəkə arasında əl 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 şəbəkəarası 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 maliyyə cəhətdən səmərəliliyi açıq rabitə kanalının mühafizə olunma dərəcəsi ilə təyin edilir. Qlobal rabitə üzrərindən informasiyaların təhlükəsiz yönləndirilməsi, onların inkapsulyasiya edilməsi eləcə də tunelləşməsindən təmin 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 protokolu paketinin verilənlər sahəsinə yerləşdirir.

Şəbəkənin verici və alıcı cütlüyü arasında yerləşdirilən bu tunel məlumatları ancaq icazəsi olmayan girişlərdən və səhvlərdən müdafiyyə etmir, o həm də tunneling vasitəsilə veribnlər və prosedurun bir obyektə birləşməsini təmin olunmuş giriş paketlərinin tam kodlaşdırma qorunmasını həyata keçirir. Ötürüləcək informasiyanın məxfiliyini təşkil etmək üçün verici qəbul olunan paketlərini şifrələyir, İnternet Protocol başlıqları adı altında həmin yeni qəbul olunan paketə yükləyir və yeni rabitə kanalı üzrə alıcıya yönləndirir. Xüsusi tunel vasitəsilə ötürülən paketin bir nümunəsi şəkil 5.2-də verilib. Xüsusi tunelin əsas xüsusiyyəti yalnız verilənlər sahəsinə şifrələməkdən ibarət deyil, həm də başlıqla bir yerdə qəbul

olunan paketlərini tam hazır vəziyyətdə şifrələməkdən ibarətdir.
Yeni paket

Yeni IP ünvanı	AN başlıq	ESP başlıq	İlkin IP - başlıq	Verilənlər
-------------------	--------------	---------------	----------------------	------------

İlkin paket

5.2. Xüsusi tunel vasitəsilə ötürülən paketin bir nümunəsi

Xüsusi tunelin əsas xüsusiyyəti, cinayətkarın başlıq sahəsində olan vacib informasiyadan alt rabitə kanalların eləcədə qovşaqların sayı və həmcinin Internet Protocol ünvanları giriş paketinin şifrəsini açmaq üçün istifadə edə bilməməsidir, hansı ki, ən böyük və ən ciddi əhəmiyyət kəsb edirlər.

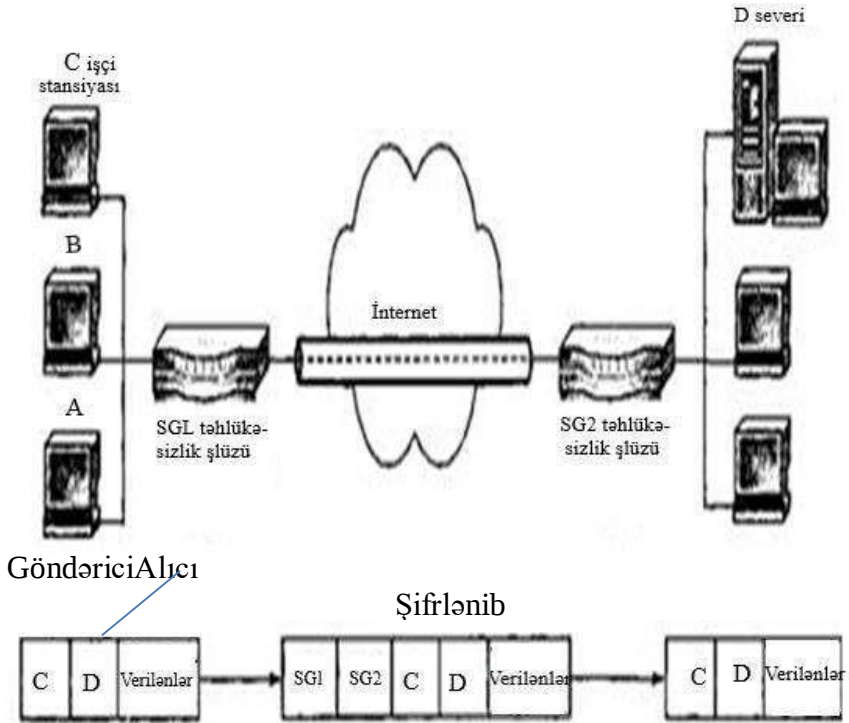
Nəzərə almaq lazımdır ki, başlığı şifrələnmiş paketin şəbəkə üzrə ötürülməsi bilavasitə həyata keçirilə bilməz. Ona görə də başlığı şifrələnmiş paketin şəbəkə üzrə ötürülməsi zamanı onun inkapsulya-sını və tunnəlləşməsindən istifadə olunur. Bu zaman paketi başlıqla birlikdə tam şəkildə şifrələyib, onu digər xarici paketə qablaşdırırlar və sonra onun açıq sahəsini mühafizə olunmuş kanal üzrə alıcıya ötürürlər. Alıcıda başlanğıc paketi xarici paketdən çıxarıb şifrələyib növbəti etaplarda veriliş üçün bərpa edilmiş, başlıq kimi mümkündür istifadə etmək. 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 bütövlüyü və autentifikasiyası üçün də istifadə olunur. Xüsusi tunneldən 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 alınması üçün paketlərin inkapsulyasından 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 tunnəlləşmədən geniş istifadə olunur. Tunnəlləşmə əksər hallarda informasiyanın məxfiliyinin və bütövlüliyünün pozulmasının baş verdiyi həm lokal kompüter şəbəkələrində və həm də qlobal açıq şəbəkələr mühitində yaradılır. Tunnel həm informasiyanın məxfiliyini və həm də şəbəkədə istifadə olunan müxtəlif protokollar arasındakı keçidi həyata keçirə bilər ki, bununla da müxtəlif protokollu şəbəkələrin qarşılıqlı əlaqəsi asanlıqla həyata keçirilir [11].

Qeyd etmək lazımdır ki, tunelləşmə sərnəşin protokolu, protokol daşıyıcısı və tunelləmə protokolunun əsasında yaradı-lır. Bu zaman sərnəşin protokolu halında IPX nəqliyyat protokolu, protokol daşıyıcısı protokolu halında IP protokolu, tunelləmə protokolu halında işə kanal səviyyəsinin PPTP və L2TP protokolları və şəbəkə səviyyəsinin IPSec protokolu isti-fadə olunurlar.

5.3. Lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması

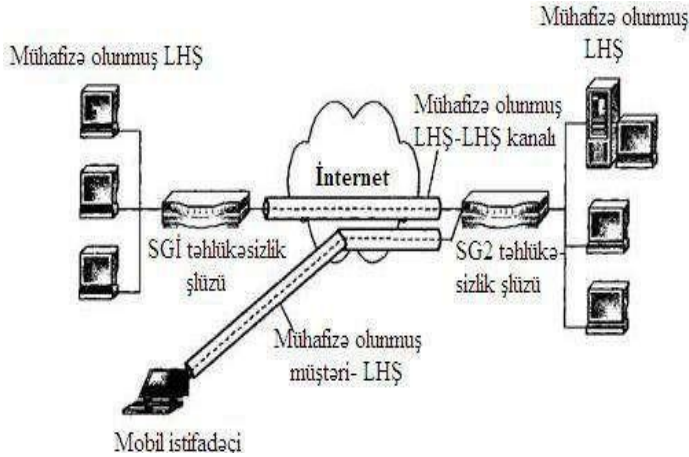
Həm lokal kompüter şəbəkələrinin qurulmasında və həm də bu şəbəkələrə uzaq (mobil) istifadəçilərin birləşdirilməsində verilənlə-rin təhlükəsizliyinin təmin edilməsi məsələsinin həll edilməsi və-cibliyi yaranır [11]. Bu məsələnin həll edilməsi üçün iki yanaş-madan istifadə olunur:

- lokal kompüter şəbəkələri arasında mühafizə olunmuş kanalın yaradılması;
- müştəri ilə lokal kompüter şəbəkələri arasında mühafizə olunmuş 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 müştərilərarasında 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, Internetin sərhəd provayderləri və lokal kompüter şəbəkələrinin şəbəkə ekranları arasında yaradıla bilər ki, bu da lokal kompüter şəbəkələrinin yaxşı miqyaslaşmasına və yük-sək idarəetmə qabiliyyətinin 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 təhlükəsizliyə malik olur. Mühafizə olunmuş tunelin yaradılmasını ISP provayderi öz üzərinə götürən zaman mühafizə olunmuş bütün xüsusi virtual şəbəkələr onların şəffaf olan şlüzləri üzərində qurula bilərlər. Bu variantın çatışmayan cəhəti xidmətlərin bəzi 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 məlumatla 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 provayderinin kommutatorlarını yaxud şlüzlərini əks etdirir, terminatorlar isə inkapsulyasiyanın əksinə olan prosesi reallaşdırır və yeni başlıqları kənarlaşdırıb hər bir ilk paketi şəbəkənin ünvançısına göndərir.

Lokal kompüter şəbəkələrində inkapsulyasiya olunmuş paketlərin məxfiliyi onların şifrələnməsilə, bütövlük və əsilliyi isə elektron rəqəmli imza ilə həyata keçirilir. Bu şəbəkələrdə verilənlərin müha-fizəsi üçün hal-hazırda çoxlu sayda kriptografik 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 informasiyanın məxfiliyinin, bütövlüüyünün və əlverişliliyinin təyin olunması vacibliyi yaranır [12].

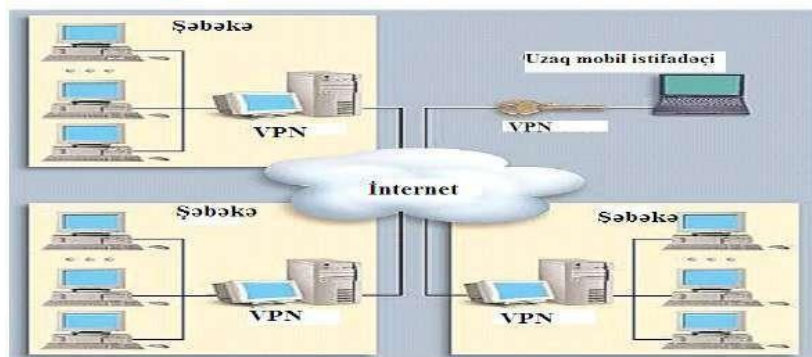
Məxfilik dedikdə şəbəkə üzrə verilənlərin ötürülməsi zamanı onların legal vericiyə və alıcıya məlum olmasına, bütövlük dedikdə şəbəkə üzrə ötürülən verilənlərin yaxşı vəziyyətdə saxlanılmasına, əlverişlilik dedikdə isə lokal şəbəkə vasitələrinin legal istifadəçi-lərə daim məlum olmasına zəmanətin verilməsi 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 dərəcəsi ilə əldə olunur.

VPN texnologiyası əsasında qurulan lokal kompüter şəbəkə-lərində verilənlər audentifikasiya olunmaqla, birləşmələr isə legal abunəçilər

arasında həyata keçirilir, ki bunun da sayəsində xarici istifadəçilərin şəbəkəyə arzu olunmaz daxilolmalarının qarşısı alınır. Avtorizasiya zamanı legal abunəçilərə çoxsaylı xidmətlər, informasiyaların bir-birindən fərqlənən şifrələmə üsulları təqdim olunur. VPN texnologiyası əsasında qurulan lokal kompüter şəbəkələrində autentifikasiya və şəbəkəyə daxilolmaların idarə olunması eyni xarakteristikalara malik olan texniki vasitələrlə həyata keçirilir. Bu şəbəkələrdə verilən informasiyaların mühafizəsinin təmin edilməsi üçün abunəçilərin qarşılıqlı autentifikasiyası, məxfiliyi, avtorizasiya, zorla soxulması, şəbəkə təhlükəsizliyinin idarə olunması və s. məsələlər həll olunmalıdır.

VPN texnologiyası bazasında qurulmuş lokal kompüter şəbəkələrinin 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 protokollarının paketlərinə malik olan vasitələr qoyulur, hansılar ki, bütün ilkin məlumatları şifrələyir, elektron rəqəmli imza vasitəsilə verilənlərin bütövlüyünə nəzarət edirlər.

Bu növ şəbəkələrdə verilənlərin ötürülməsindən əvvəl alıcıda şifrələmə alqoritmləri və elektron rəqəmli imzanın köməyi ilə IP paketinin mühafizəsi üçün vacib olan mühafizə alqoritmı və açar seçilir [15]. Əgər bunlara uyğun alıcı olmasa, onda verilənlərin göndərilməsi

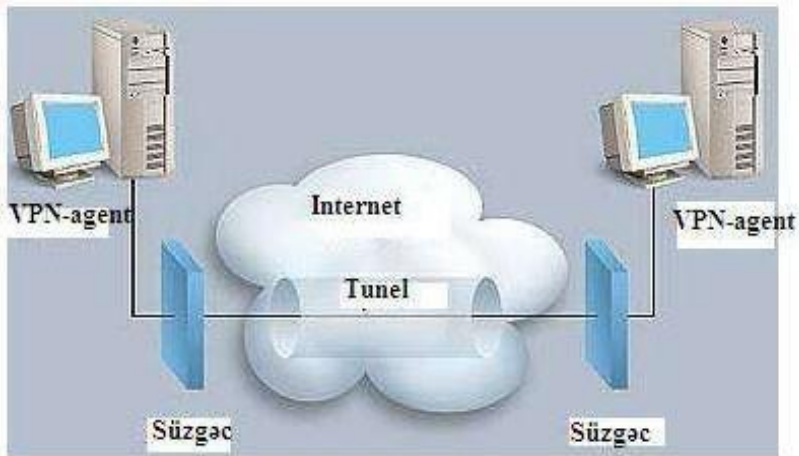
dayandırılır, sonra vericinin elektron rəqəmli imzası-nın paketi təyin edilir və onlara əlavə edilir, paket başlıqla birlikdə şifrələnir və yeni paketə inkapsulya edilir.

Alıcı tərəfdə IP paketinin alınması zamanı əks əməliyyatlar aparılır, yəni vericinin VPN agentı haqqında məlumata malik odu-ğu başlıq yoxlanılır. Yoxlama zamanı başlıqda olan məlumat vericinin VPN agentı haqqda məlumata uyğun olursa, onda qəbul olunmuş vüerilənlər tullanılır. Sonra şifrələmə alqoritmi, elektron rəqəmli imza və kriptograf açar seçilir, paketin şifrəsi açılır, onun bütöliyü 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 agentı onların kompüterlərində yerləşdirilir ki, o da ötürülən informasiyaların mühafizəsini təmin edir.

VPN texnologiyası əsasında qurulan lokal kompüter şəbəkələ-rində agentlərin həm də marşrutlayıcılarla birləşdirilməsi müm-kündür. Bu zaman VPN agentı 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 tunnəlaşmə və süzgəc-lənməsi sxemi şəkil 5.6-da verilib [15]. Bu sxem vasitəsilə bir şəbəkə-dən 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 tunneldən digər tunnəle ötürülür və yoxlandıq dan sonra atılır [15].

Lakin bu üstünlüklərə baxmayaraq VPN texnologiyası bazasında qurulan şəbəkələrdə ciddi problemlərin 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. Tunnəlaşmə dedikdə müxtəlif növ paketlərin birinin digərinin içərisinə inkapsulyasiya edilməsi başa düşülür.



Şək. 5.6. Lokal kompüter şəbəkələri arasında IP paketlərinin tunelləşmə və süzəclənməsi sxemi

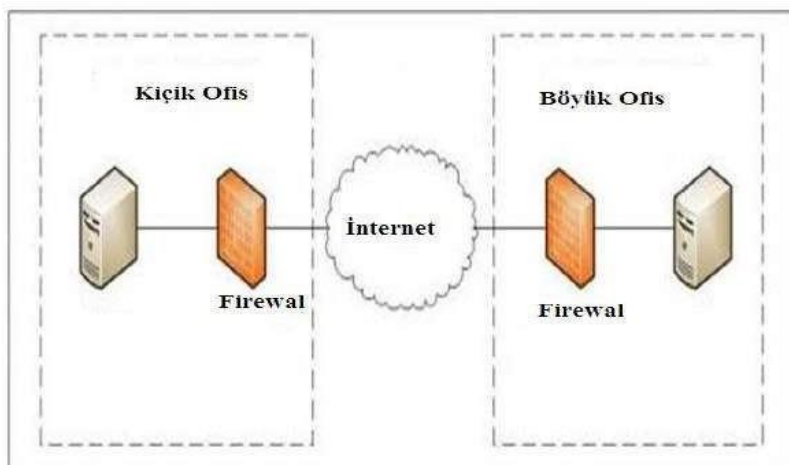
Şəkildən göründüyü kimi iki brandmaur arasında iki şəbəkə yerləşdirilib. Brandmaur IP paketlərini tələb olunan şəkildə çevirib şifrələyir, onlara yeni IP başlığını əlavə edir. Şifrələmə nəticəsində paketin IP başlığında olan faktiki informasiya gizlədilir. Bu paketi qəbul edən uzaq brandmaur onun şifrəsini açıb ilkin şəkildə çevirir. Hər iki şəbəkənin süzəcləri arasındakı segment tunel adlandırılır. IP paketlərinin şifrələnməsi və onların göndərilməsindən hər iki şəbəkənin qovşaqlarının xəbər edilmir. Demək olar ki, şəbəkənin qovşaqlarında xüsusi aparat-proqram təminatının edilməsinin və hər hansı bir düzəlişlərin düzəlməsi vacib olunur, lakin məsafədə olan alt-şəbəkənin qovşaqları tərəfindən qeyd olunmuş paketlər eləcədə şlüzvari qurğuların hər tərəfli nəzarət altında olunması həyata keçirilməlidir.

Qurulmasının ucuz başa gəlməsi, informasiyanın məxfiliyinin, bütövlüyünün və autentifikasiyasının təmin edilməsi VPN texnologiyası bazasında qurulan lokal kompüter şəbəkələrinin üstün cəhətləridir. Bu şəbəkələrin digər üstün cəhəti əlavə rabitə xətti

çəkilmədən mövcud şəbəkə infrastrukturunu üzərində qurulmasıdır.

5.5. Lokal kompüter şəbəkələrinin müxtəlif VPN texnologiyaları bazasında qurulması

Mühafizə olunmuş lokal kompüter şəbəkələri əsasən brandma-uer, marşrutlayıcı, əməliyyat sistemləri və aparat vasitələri üzərində qurulurlar. Brandmauer üzərində qurulan lokal kompüter şəbəkələrinin proqram təminatına şifrələmə modulu yerləşdirilir. Ona görə də belə şəbəkələrin brandmaurləri üzərindən ötürülən informasiyalar trafikinin şifrələnməsinə əsaslanır [16]. Qeyd etmək lazımdır ki, brandmauer texnologiyası yalnız kiçik həcmli verilənlərin ötürülməsini həyata keçirən lokal kompüter şəbəkələrinin qurulmasında istifadə olunurlar. Lokal kompüter şəbəkələrinin brandmauer üzərində qurulması sxemşəkil 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-
lənmesi funksiyasını da yerinə yetirirlər. Bu məqsədlə marşrut-
layıcıların proqram təminatına şifrlemə modulu yerləşdirilir. Lokal
kompüter şəbəkələrinin marşrutlayıcılar üzərində qurulması sxemi şəkil
5.8-də verilib [16]. Lokal kompüter şəbəkələrinin marşrutlayıcılar

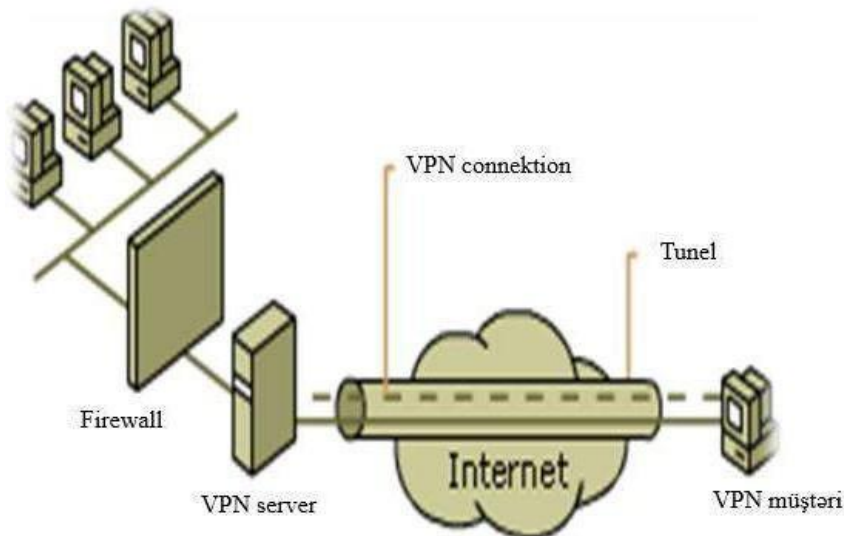


Şəkil 5.8. Lokal kompüter şəbəkələrinin marşrutlayıcılar
üzərində qurulması sxemi

üzərində qurulması zamanı istifadə edilmiş cihazları məsələn
göstərmək olar Cisco Systems şirkətinin cihazlarını göstərmək olar.
Hal-hazırda şirkətin marşrut-layıcılarında əsasən Layer 2 Tunnelling
Protocol və IP Security protokollarından istifadə olu-nur. Tunel
birləşməsinin yaradılması zamanı Cisco Syst Ems şirkətinin
avadanlıqları eyni zamanda həm eyniləşdirmə, həm də açarların
mübadilə funksiyalarını yerinə yetirirlər.

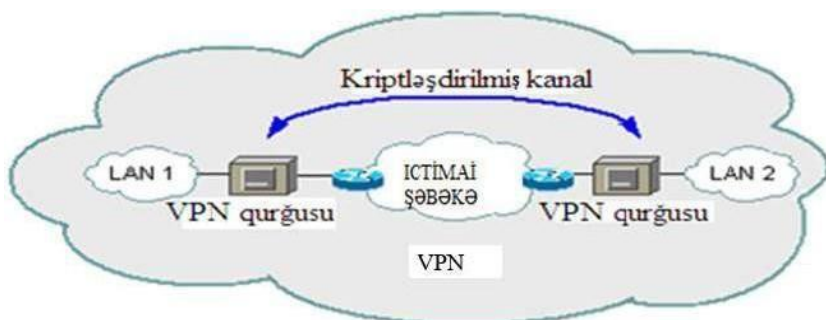
Lokal kompüter şəbəkələrinin əməliyyat sistemləri üzərində
qurulması üçün çoxlu yanaşmalar mövcuddur. Bu yanaşmaların analizi
göstərir, konfiqurasiyaləşdirmə eləcədə köklənməyə görə, onlardan
çox əlverişlisi həmdə ucuz başa gələn sistem Windows 2003 Server
əməliyyat sistemidir, hansı ki, marşrutlaşma 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 istifadə olunur. Bu məhsul qəbul edilən məlumatlarının aparat-proqram kodlaşdırılmasını təmin edir və yüz Mbit/saniyyə sürətində məlumat selini göndərməyə qabiliyyətinə malikdir. [16]. Bundan əlavə, qeyd olunan bu cihaz şəbəkə ünvanlarının tərcümə sistemindən istifadə edir və o, firewall funksiyasını yerinə yetirən xüsusi cihazla təchiz olunub. 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 şifrələnməsini təmin edir və onların istifadəçilərə bilavasitə çatdırılmasını həyata keçirirlər [17]. Bu şəbəkələrin qurulması zamanı OSI modelinin kanal səviyyə-sinin, şəbəkə səviyyəsinin və eləcə də nəqliyyat səviyyəsinin protokollarından istifadə olunur.

Lokal kompüter şəbəkələrinə daxilolmaların təmin olunması üçün OSI modelinin kanal səviyyəsində mühafizə olunmuş kanal-ların yaradılması üçün PPTP tunelləşmə protokolu istifadə olunur. 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 standartlaşdırılmışdır, hansı ki, özündə həm PPTP və L2F protokollarının üstün cəhətlərini ehtiva edir. OSI modelinin kanal səviyyəsində mühafizə olunmuş kanalların yaradılması üçün istifadə olunan PPTP tunelləşmə potokolu üzrə ötürülən IP paketinin strukturu şəkil 5.11-də verilib.



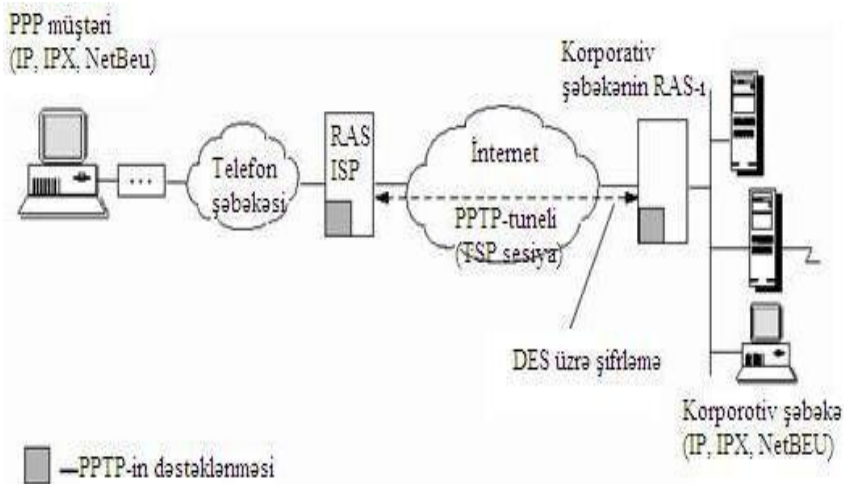
Şəkil 5.11. OSI modelinin kanal səviyyəsində mühafizə olunmuş kanalların yaradılması üçün istifadə olunan PPTP tunelləşmə protokolu üzrə ötürülən IP paketinin strukturu

PPTP tunelləşmə protokolu üzrə ötürülən IP paketinin strukturuna İnternet səviyyəsində istifadə olunan rabitə kanalları səviyyəsinin başlıqları, o cümlədən ethernet şəbəkəsinin kadrının başlıqları, internet protocol başlıqları, generic routing encapsulation başlıqları və internet protocol, internetwork packet exchange yaxud Net-BIOS extended user interface paketlərini cəmləşdirilən ilk paketlər daxildir. Point-to-Point Tunneling Protocol tunelləşmə protokolu point-to-point Protocol protokolu-nun kadrını, rabitə səviyyəsinin protokollarına inkapsulyasiya edən GRE paketinə inkapsulyasiya edir, hansı ki, sessiya yaratmaq və cinayətkardan mühafizə etmək qabiliyyətinə malik deyil. Sessiya yaratmaq və cinayətkarın icazəsiz daxilolmalarının qarşısını almaq üçün PPTP protokolunun tunelinin idarə etmək qabiliyyətindən istifadə olunur.

Qeyd etmək lazımdır ki, GRE paketinin inkapsulyasiya etmək qabiliyyəti 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 kadrı inkapsulyasiya olunur. Bundan sonra PPTP protokolu PPP protokolunun başlığına son işarəsini verir və göndərici mühafizə tuneli vasitəsilə verilənləri alıcıya göndərir, hansı ki, olan xidmətləri başlıqlardan azad olunur, yalnız point-to-point protokolunun verilənlərini qoruyur [17]. Bu proses bir necə variantda həyata keçirilir.

Birinci variantda daxilolma serveri ilə korporativ şəbəkənin sərhəd marşrutlayıcıları arasında mühafizə olunmuş kanal istifadə olunur.

Giriş serveri ilə korporativ şəbəkənin sərhəd marşrutlaşdırıcıları arasında təhlükəsiz kanaldan istifadə sxemi şəkil 5.12-də təqdim edilmişdir.

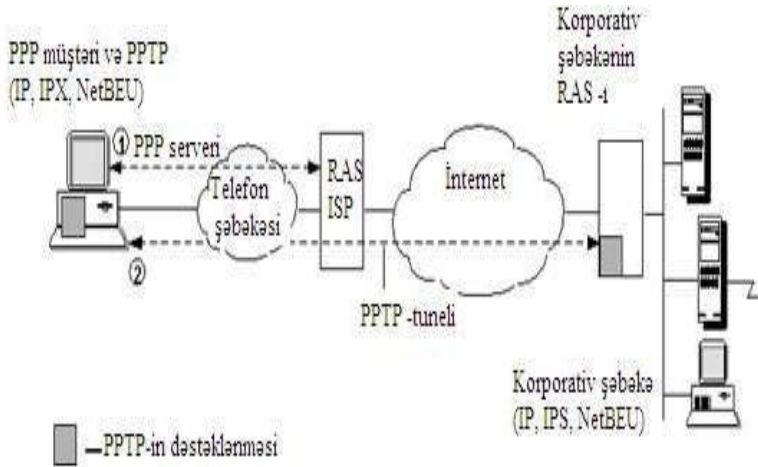


Şək.5.12. Daxilolma serveri ilə korporativ şəbəkənin sərhəd marşrutlayıcıları arasında mühafizə olunmuş kanalın istifadə olunması sxemi

Bu cəmdə PPTP protokolunu dəstəkləməyən uzaq istifadəçinin kompüteri İSP-də yerləşən PPP protokolu vasitəsilə PPTP protokolunu dəstəkləyən uzaq daxilolma serveri RAS vasitəsilə pro-vayderdə birinci autentifikasiyanı keçir. İstifadəçilərin verilənlər siyahısında İSP, korporativ 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 kadrılarının çıxarması və onları IP, IPX kimi vacib olan for-matda şəbəkə üzrə göndərməsi ilə izah olunur.

İkinci variantda korporativ şəbəkələrin sərhəd marşrutlayıcıları arasında mühafizə olunmuş kanal yaradılır. Uzaq istifadəçilərin

korporativ şəbəkələrin marşrutlayıcıları arasında mühafizə olunmuş kanalın yaradılması sxemi şəkil 5.13-də verilib.

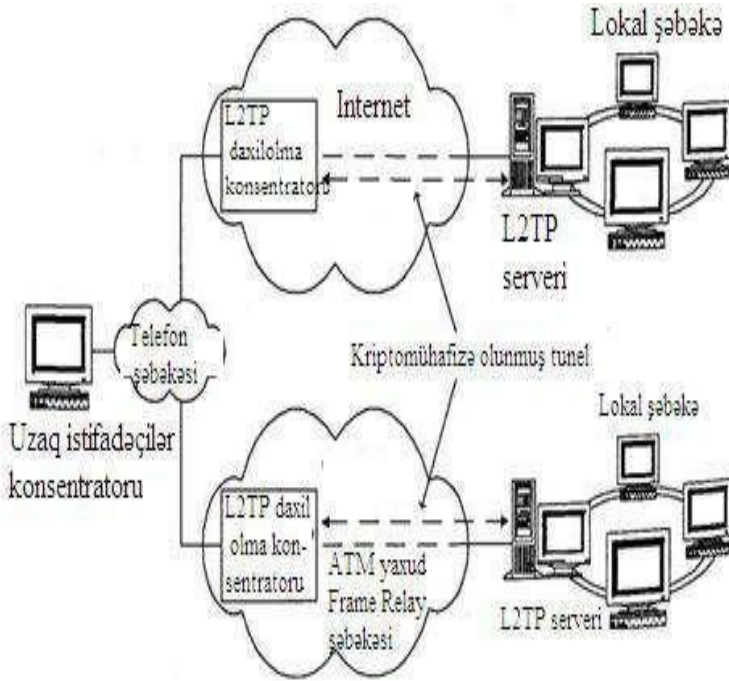


Şəkil 5.13. Uzaq istifadəçilərin korporativ şəbəkələrin marşrutlayıcıları arasında mühafizə olunmuş kanalın yaradılması sxemi

Bu sxem üzrə informasiyanın ötürülməsi prosesi aşağıdakı qaydada həyata keçirilir. RAS əvvəlcə ISP serverinə zəng etməklə PPP protoklu vasitəsilə onunla əlaqə yaradır. Bundan sonra o, provayderlə autentifikasiyadan keçdikdən sonra korporativ şəbəkənin uzaqdan giriş serverinə ikinci zəng edir.[17]. Bu zaman korporativ şəbəkə tərəfindən qoşulmuş RAS adı telefon nömrəsinin əvəzinə Windows NT-in IP-ünvanını göstərir. Bu ünvanla müştəri kompüterləri ilə RAS kompüterləri arasında PPTP protokolu vasitəsilə sessiya yaranır. Bundan sonra istifadəçi remote access service serverində yenidən autentifikasiyadan keçir və bununla da informasiya verilişi həyata keçirilir.

PPTP protokolundan fərqli olaraq L2TP protokolu mühafizə olunmuş kanalı local kompüter şəbəkəsinin məsafədən giriş zamanı serveri ilə əlaqəsini yaradılması, istifadəçilərin autentifikasiyası və kriptomühafizə olunmuş tunelin konfiqurasiyalasdırılması kimi üç mərhələdə formalaşdırır [17]. Layer 2 Tunnelling Protocol ilə

mühafizə olunmuş kanalın formalaşdırılması sxemi şəkil 5.14-də göstərilib.



Şəkil 5.14. Layer 2 Tunnelling Protocol ilə mühafizə olunmuş kanalın formalaşdırılması sxemi

Bu sxemdə məsafədə olan müştəri point-to-point protokolu vasitəsilə Layer 2 Tunnelling Protocolun daxili konsentratoru ilə birləşərək lokal kompüter şəbəkəsini uzaq daxilolma serveri ilə birləşdirir. Bu əlaqə zamanı Layer 2 tunnelling protocoluna giriş konsentratoru provayder adından istifadəçinin autentifikasiyasını həyata keçirir. Bundan sonra, provayderin giriş konsentratoru tələb olunan yerli kompüter şəbəkəsinin IP ünvanını abunəçinin adı ilə layer 2 tunnelling protocolun serverinə təyin edir. Bu ünvan əsasında L2TP protokolu vasitəsilə provayderin daxilolma konsentratoru ilə lokal kompüter şəbəkəsi arasında sessiya yaradılır. Bu sessiya yadaldıqdan sonra

lokal

kompyuter şəbəkəsinin servisində istənilən alqoritmdən istifadə etməklə istifadəçinin audentifikasiyası aparılır. Belə alqoritmə misal olaraq CHAP alqoritmini göstərmək olar. PPTP və L2F protokollarında audentifikasiya metodlarından istifadə olunmadığı kimi L2TP protokolunda da audentifikasiya metodlarından 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 şifrələmənin müxtəlif standartlarından istifadə edir, lakin kriptomühafizənin konkret metodunu spesifikləşdirmir. Tunnel IP-şəbəkəsində formalaşan zaman informasiyanın mühafizəsi IPSec protokoluna uyğun aparılır və L2TP protokolunun paketləri UDP protokolunun paketlərinə inkapsulyasiya olunaraq 1701 UDP-portu vasitəsilə provayderin daxilolma konsentratorundan L2TP serverinə ötürülür.

ƏDƏBİYYAT

1. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Bakı. MTN-in nəşriyyatı. 2009. -342 s.
2. Məmmədov Səbuhi 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 Havar Ə.,Məmmədov Famil H., Cəfərov Zəfər Ə. "İnformasiya mühafizəsi üsulları və vasitələri". Dərslik.,Bakı, 2010.-305 s.
4. Лекций по предмету «Защита информации»/Государственный Университет имени А. Г.Столетов и Н.Г. Столетов; А. Ю. Шагурина.—: ИздательствоВлГУ, 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. Баранова Е.К., Бабаш А.В «Информационная безопасность и защита информации»: учебное пособие/3-е издание перераб. и доп.-Москва:2017. - 322 с. - (Высшее образование).- www.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 безопасност. 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 СФЕРА .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. 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. «Основы информационной безопасности в Интернете» В.А. Галатенко— ИНТУ ИТ.ру, 2008г.

MƏMMƏDOV F. H., ORUCOVA M.Y.

**“İNFORMASIYA TƏHLÜKƏSİZLİYİ VƏ TƏMİNATI”
KOMPÜTER ŞƏBƏKƏLƏRİNDƏ
TƏHLÜKƏSİZLİYİNTƏŞKİLİ PRİNSİPLƏRİ**

Bakı: “Zəngəzurda” çap evi, 2022 – 180 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: 11.25 ç.v.
Sifariş: 557
Sayı: 100

ZƏNGƏZURDA” çap evində çap olunub
Ünvan: Bakı şəh., Mətbuat prospekti, 529-cu məh.
Tel.: +994 50 209 59 68
+994 55 209 59 68
+994 12 510 63 99
e-mail: zengezurda1868@mail.ru

