**AZƏRBAYCAN RESPUBLIKASI TƏHSIL NAZIRLIYI**

**AZƏRBAYCAN TEXNIKI UNIVERSITETI**

**Əlizadə Murad Sərdar oğlu**

**KOMPYUTER ŞƏBƏKƏLƏRINDƏ TƏHLÜKƏSIZLIYIN TƏDQIQI**

**BAKI – 2012**

**Mündəricat**

|  |  |
| --- | --- |
| **GİRİŞ** | 4 |
| **I FƏSIL. KOMPYUTER ŞƏBƏKƏLƏRINDƏ INFORMASIYA**  **TƏHLÜKƏSIZLIYI VASITƏLƏRI** | 10 |
| **1.1. Kompyuter şəbəkələri və informasiya təhlükəsizliyi** | 10 |
| 1.2. Kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifati | 14 |
| **1.3. Kompyuter şəbəkələrində İnformasiya təhlükəsizliyinin əsas**  **istiqamətləri** | 15 |
| **1.4. İnformasiyanın məxfiliyinin təmini və tamlığına nə­za­rət vasitələri** | 16 |
| **1.5. Şəbəkə perimetrinin mühafizəsinin məqsədi və məhdudiyyətləri** | 18 |
| **1.6. İşçi stansiyalarının mühafizəsinin məqsədi və məhdudiyyətlər** | 18 |
| **1.7. Həmlələri aşkarlayan sistemlərin məqsədi və məhdudiyyətləri** | 18 |
| **1.8. Perimetrin mühafizəsi** | 19 |
| **1.9.Kompyuter şəbəkələrində şəbəkələrarası ekranlar** | 19 |
| **1.10. İsa Server 2004** | 25 |
| **1.11. İsa Server 2004-də yeniliklər** | 26 |
| **1.12. URLScan** | 27 |
| **1.13. Bütün səviyyələrdə mühafizə** | 28 |
| **1.14. Şəbəkəarası ekrandan keçən trafik** | 30 |
| **1.15. Bütün trafikin yoxlanması** | 30 |
| **1.16. SSL trafikinin yoxlanması** | 30 |
| **1.17. Naqilsiz şəbəkələrin mühafizəsi problemləri** | 30 |
| **1.18. Porblemlərin həlli yolları** | 31 |
| **1.19. İPSec – in icmalı** | 32 |
| * 1. **Təhlükəsizlik sinfinə görə şəbəkəarası ekranlara tətbiq edilən əlavə tələbatlar** | 34 |
| **1.21. Şəbəkələrarası qarşılıqlı təsir siyasətinin işlənib hazırlanması** | 38 |
| **1.22.Şəbəkələrrası ekranın qoşulma sxeminin müəyyənləşdirilməsi** | 39 |
| **1.23. Brandmauerin fəaliyyət parametrlərinin sazlanması** | 42 |
| **FƏSİL II. SİMMETRİK ŞİFRƏLƏMƏ ÜSULLARININ TƏT­BİQİ İLƏ**  **KOMPYUTER ŞƏBƏKƏLƏRINDƏ INFORMASIYA**  **MÜHAFIZƏSININ IŞLƏNMƏSI** | 46 |
| **2.1. AT-BAŞ şifrələməsi (sadə şifrələmə)** | 46 |
| **2.2. Yerdəyişmə üsulu ilə şifrələmə** | 47 |
| **2.2.1.** **Birqat yerdəyişmə şifrələməsi** | 47 |
| * + 1. **İki qat yerdəyişmə şifrələməsi** | 48 |
| **2.3. Sezar şifrələməsi** | 53 |
| **2.4. Sehirli kvadrat şifrələməsi** | 56 |
| **2.4.1. Mətn şifrələnməsi** | 60 |
| **2.5.** **Qronsfeld üsulu ilə şifrələmə** | 60 |
| **2.6. VİJNER şifrələməsi** | 63 |
| **2.7. Pleyferə görə şifrələmə və onun əsası. Biqramlar** | 67 |
| **III. ASİMMETRİK ŞİFRLƏMƏ ÜSULLARININ TƏTBİQİ İLƏ**  **KOMPYUTER ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA**  **MÜHAFİZƏSİNİN İŞLƏNMƏSİ** | 74 |
| **3.1. Asimmetrik şifrələmə** | 74 |
| * 1. **Əl Camal alqoritimi ilə şifrələmə** | 79 |
| * + 1. **Şifrələmək** | 81 |
| **3.2.2. Şifrədən azad etmək (deşifrə)** | 82 |
| Məlumatın imzalanmasının Əl Camal alqoritmi ilə realizəsiprinsipi | 83 |
| **NƏTICƏ** | 84 |
| **ƏDƏBİYYAT** | 86 |

**GİRİŞ**

Yeni informasiya texnologiyalarının saxlanması və emalı üç­­­ün gizli kom­pyuter sistemlərinin inkişafı informasiya müha­fi­­­zəsi səviyyəsinin qalxmasına səbəb oldu. Bu isə bilavasitə in­for­­­­masiya mühafizəsinin effektivliyinin verilənlərin saxlan­ma­sı ar­xitekturasının mürəkkəbliyi ilə birgə artmasına zəmin yar­at­­­­­dı. Belə ki, iqtisadi informasiyaların mühafizəsi önəmli ol­muş; informasiya mühafizəsi üçün bütün mümkün olan sə­nəd­­lər haz­ır­lanmalı; informasiya mühafizəsi üçün təkliflər for­ma­laş­­­­­mış və s.

Beləliklə informasiya mühafizəsi həmlələri informasiya təh­­­­lükəsizliyi vasitə­lərini informasiya sistemlərinin ən əsas xar­ak­­­­ter­istikalarından birinə çevrilmişdir. Kriptoqrafiya sözü “gizli məktub” məna­sını daşıyan yunan sözlərindən əmələ gəlmişdir. Kripto­qra­fi­ya­nın bir neçə minilliyi əhatə etdiyi uzun və yaxşı tarixi vardır. Kompyuterlər yaranana kimi kriptoqrafiyada ən əsas faktor­lar­dan biri şifrləyicinin lazımı çevirmələri aparmaq imkanına ma­l­ik olmaması idi. Kripto­qra­fiyanın əsas qanunu ondan iba­rət­dir ki, kriptoanalitikə (yəni kodu sındırana) istifadə olunan şi­fr­lə­mə üsulu məlum olur. Yerinə qoyma üsuluna əsaslanan rəq­­əm­lər­də hər bir simvol və ya simvollar qrupu başqa simvol və ya sim­­vollar qrupu ilə əvəz olunur. Ən qədim şifrlərdən biri Yuli Sezar tərəfindən yaradılan Yuli Sezar şifrləridir [1] . Bu üsul yerinə qoy­ma üsuluna əsaslanır, simvollar sırasını saxlayır, ancaq onları əvəz edir (əvəzləyir).Yerdəyişmə üsulunu istifadə ed­ən şifrlər, simvolların gəlmə cərgəsini dəyişir, ancaq sim­vol­ların öl­çülərini dəyişmirlər [1]. Sınması mümkün olmayan şifr yar­at­maq əslində çox sadədir. Bunun üçün lazım olan üsul artıq bir neçə ön illərdir ki, məlumdur. Belə ki, açar kimi istənilən bit sətri göt­ürülür [6]. Bu sətrin uzunluğu verilmiş mətnin uzun­lu­ğu ilə üst-üstə düşür. Maraqlı budur ki, şəbəkədə bir dəfəlik ard­ı­cıllıqla ötür­mə probleminin həlli çox qədim tarixi olan kvant mex­a­ni­ka­­sından gəlir.

Birinci kriptoqrafik prinsip belədir: bütün şifr­lən­miş materiallar müəyyən izafiliyə malik olmalıdır, başqa söz­lə məlumatı anlamaq üçün lazım olan infor­masiyaya malik olmalıdır [3]. Başqa sözlə, məlumatı əks şifrləmə zamanı qəb­ul­edi­ci onun doğruluğunu analiz vasitələri, hətta sadə hes­ab­la­ma­lar aparmaqla aydın etmək imkanına malik olma­lı­dır. İzafilik qə­b­ul­ediciləri yanlış məlumatlarla (tər­kibində zibil ol­an, ar­xiv­ləş­dirmə ehtiyyat nüsxəsinin hazırlanması, bazanın sıx­ıl­ması, kor­­lanmış bazanın bərpası) aldatmağa çalışan pis­niy­yət­lilərin həm­­lələrinə qarşı durmaq üçün lazımdır.

İkinci kriptoqrafik prinsip**:** Əvvəlcə göndərilmış məl­u­mat­ların təkrar gön­dərilməsi ilə mübarizənin zəruri olmasıdır. Uy­ğun üsullardan birisi hər bir məlu­mata, haradasa yalnız 10 san­iyə ərzində doğru olan ştampın əlavə olun­masıdır [12]/ .

Hal**-**hazırda geniş miqyasda informasiyanı saxlayan və em­al edən sistemlər möv­cuddur. Onların layihələndirilməsi za­ma­nı Azərbaycan Respublikasının infor­masiya təhlükəsizliyi, kon­­­­fidensial informasiyanın saxlanması əsas şərtlərdən biri ol­maq­­­­la mühim əhəmiyyət kəsb edir.

Ədəbiyyatlardan, mütəxəsislərdən bəzi hallarda infor­ma­si­ya mühafizəsi haq­qında müxtəlif, əksər hallarda isə tamamilə əks fikirlər, baxışlar söyləndiyinə rast gəlinir. İnformasiya təh­lü­kəsizliyinin birbaşa təyini məsələsində “veri­lənlərin müh­a­fizə­si”, “istifadənin nəzarəti”, “xakerlərlə müba­rizə” və s. ki­mi müx­təlif səviyyəli terminlərə rast gəlmək olur [5,6]. Buna bax­ma­ya­raq informasiya təhlükəsizliyinin və ona yaxın olan dairədə mü­­­əy­yən olunmuş təyini vardır. Bəzən onlar müxtəlif mü­tə­xəs­sis­lərdə (məktəblərdə) bir**-**birindən fərqlə­nir­lər [1,8,14]. Belə ki, bəzi hal­­larda təyin etmə zamanı, sadəcə olaraq sin­o­n­imlərdən isti­fa­də edilir, bəzi hallarda isə bir qrup anlayışların yer­­lərini dəyiş­dir­­­irlər. Hesab edirik ki, “infor­masiya təh­lü­kə­siz­li­yi” anlayışı da­­­ha genişdir [1,8]. Ona görə ki, o, informasiya ilə qar­şı­lıqlı təsirdə ol­­an hər şeyi və kompyuter təhlükəsizliyinin, şəb­əkə təh­lükə­siz­­liyinin, telekomnukasiya təhlükəsizliyinin, veri­lən­lərin təh­lü­­­­kəsizli­yinin və ya infor­ma­siya təhlükəsizliyinin ay­rı-ayrı isti­qa­­m­ət­lərini əhatə edir.

Müasir dünyada öz əhəmiyyətinə görə cəmiyyətin inki­şafı üçün xammal və enerji kimi əsas resurslarla yanaşı infor­masiya xüsusi əhəmiyyət kəsb edir. İnkişaf etmiş ölkələrdə iş­lə­­yənlərin əksəriyyəti istehsal sahəsində deyil bu və ya digər də­rəcədə informasiya emalı ilə məşğul olurlar. Bununla yanaşı ye­­­ni ənənəni qeyd etmək lazımdır. Belə ki, cəmiyyətin tam ola­raq və ayrıca hər bir insanın informasiya asılılığı hökm sür­mək­­­dədir. Ona görədə son zamanlar “infor­masiya siyasəti”, “in­­­­­for­masiya təhlükəsizliyi”, “informa­siya müharibəsi” və bir sı­­­­ra bir-biri ilə bu və ya digər formada əlaqəli olan yeni anla­yış­­­lar yaranmışdır.

Müasir işgüzar dünyada material aktivlərin informasiya aktivləri tərəfinə miq­rasi­yası baş verir. Təşkilatların genişlən­mə­si ilə onun informasiya sistemi də mürək­kəbləşir. Əsas mə­sə­lə isə bazarda olan daima dəyişən rəqabət şəraitində biznesin aparılmasının səmərəliliyini maksimal təmin etməkdir [1, 20].

Informasiyaya əmtəə kimi baxmaqla demək olar ki, in­for­masiya təhlükəsizliyi ümumiyyətlə vəsaitə kifayyət qədər qə­naət etməyə imkan verə bilər. İnformasiya təhlükəsizliyi mü­a­­­­­sir cəmiyyətin qarşılaşdığı əsas problemlərdən biridir. Bu pr­ob­­­le­min belə kəskinləşməsi bilavasitə informasiyanın top­lan­ma­sı, saxlanması, emalı və ötürülməsi avtomatlaşdırılmış sis­tem­­­lərinin geniş miqyasda istifadə edilməsi ilə əlaqədardır [3,9].

**Dissertasiya işinin aktuallığı:** Kompyuter şəbəkələrindən ilk vaxtlar, hətta demək olar ki ilk onillikdə unversitet tədqiqatçıları və korperasiyanın əm­ək­­daşları arasında elektron poçtla mübadiləni aparmaq, prin­ter­dən birgə istifadə üçün istifadə edilirdi. Sözsüz, belə hal­da təh­lü­­kə­sizlik məsələsi diqqəti cəlb etmirdi. Ilk yaxınlaşmada şəb­ə­k­ələrin təhlükəsizliyi şəbəkələrini bir-birilə kəsişən dörd sa­hə­yə: məxfilik, autentifikasiya öhdəliklərin ciddi olaraq yer­inə ye­tirilməsinin təmini və tamlığın təmininə ayırmaq olar. İki­nöq­­təli xətlə ötürülən paketlər verilənləri ötürmə səviy­yə­sin­də, xət­tə ötürülən zaman kodlaşdırıla və qəbul zamanı əks kod­­­­laş­dırmaya məruz qala bilərlər. Bu hadisənin bütün his­sə­ləri yal­nız verilənləri ötürmə səviyyəsinə məlum ola bilər. Bu zam­an hət­ta daha yüksək səviyyələr arada nə baş ver­di­yin­dən xəb­ərsiz ola bilər. Yuxarıda qeyd olunanlardan görünür ki, dissertasiya işinin mövzusu öz aktuallığı ilə fərqlənən, müasir informasiya cəmiyyətinin əsas informasiya mənbəindən biri olan kompyuter şəbəkələrində təhlükəsizliyinin tədqiqinə həsr olunmuşdur.

**Dissertasiya işinin məqsədi:** Müasir kompyuter şəbəkələrindətəhlükəsizlik problemlərinin tədqiqindən, şəbəkələrdə perspektiv informasiya mühafizə üsul və metodlarının araşdırılmasından, belə üsul və vasitələrdən kompyuter şəbəkələrində təhlükəsiz informasiya mübadiləsini təmin etmək üçün istifadə etməkdən ibarətdir.

**Elmi yenilik:** kompyuter şəbəkələrində informasiya təhlükəsizliyi vasitələ­rinin tədqiqindən:

- kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifatlaşdırılmasından;

* kompyuter şəbəkələrində İnformasiya təhlükəsizliyinin əsas istiqamətlərinin muəyyənləşdirilməsindən;
* ənənəvi yanaşmadan fərqli olaraq, kompyuter şəbəkələrində təhlükəsizliyin təmini mədsədilə istifadə olunan üsul və vasitələr haqqında, dissertasiya işinin həcminə qoyulan tələblərə riayət etmək məqsədilə, qıssa məlumatlar bloklarının hazırlanmasından;
* kompyuter şəbəkələrində informasiya mühafizəsinin təmini məqsədilə mövcud simmetrik şifrələmə üsullardan istifadə etməklə konkret mislların işlənməsi;
* asimmetrik şifrləmə üsullarinin tətbiqi ilə kompyuter şəbəkələrində şifrləmə,

deşifrləmə məsələlərinin həllindən ibarətdir.

**Elmi-praktiki əhəmiyyəti:** Kompyuter şəbəkələrində təhlükəsizliyin təmini mədsədilə istifadə olunan üsul və vasitələrin tədqiqindən, kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifatlaşdırılmasından, kompyuter şəbəkələrində İnformasiya təhlükəsizliyi­nin əsas istiqamətlərinin muəyyən­ləşdirilmə­sindən, kompyuter şəbəkələrində təhlükəsizliyin təmini mədsədilə istifadə olunan üsul və vasitələr haqqında işlənmiş qıssa məlumatlar bloklarından tədris prosesində əyani vəsait kimi istifadə etmək olar.

**Dissertasiya işinin strukturu:** Dissertasiya işi girişdən, üç fəsil, nəticə və istifadə olunmuş ədəbiyyat siyahasından ibarətdir.

Girişdə dissertasiya işinin mövzusunun aktuallıgı əsaslandırılır, işin məqsədi, onun elmi yeniliyi, eimi-praktiki əhəmiyyəti müəyyənləşdirilir, dissertasiya işinin strukturu verilir.

Birinci fəsil kompyuter şəbəkələrində informasiya təhlükəsizliyi vasitələ­rinin tədqiqinə həsr edilmişdir. Burada kompyuter şəbəkələri və informasiya təhlükə­sizliyi geniş tədqiq olunub, kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifati aparılmış, kompyuter şəbəkələrində İnformasiya təhlükəsizliyinin əsas istiqamətləri muəyyənləşdirilmişdir. Bununla yanaşı, İnformasiyanın məxfiliyinin təmini və tamlığına nə­za­rət vasitələri araşdırılmışdır. Bu fəsldə ənənəvi yanaşmadan fərqli olaraq, kompyuter şəbəkələrində təhlükəsizliyin təmini mədsədilə istifadə olunan üsul və vasitələrin tədqiqi aparılmış, dissertasiya işinin həcminə qoyulan tələblərə riayət etmək məqsədilə bu vasitələr haqqında qıssa məlumatlar blokları hazırlanmışdır. Bu bloklardan tədqiq olunan mövzu üzrə mühazirə və məşğələ dərslərində metodiki vəsast kimi istifadə etmək olar. Beləki, şəbəkə perimetrinin, işçi stansiyalarının, həmlələri aşkarlayan sistemlərin məqsədi və məhdudiyyətləri, perimetrin mühafizəsi, kompyuter şəbəkələrində şəbə­kə­lər­arası ekranlar geniş tədqiq olunmuşdur. İsa Server 2004, İsa Server 2004-də yeniliklər, URLScan haqqında nəzəri və praktiki məsələlərə aydınlıq gətirilmiş, bütün səviyyələrdə mühafizənin təşkili kimi məsələlər həll edilmişdir. Bu məqsədlə də şəbəkəarası ekrandan keçən trafik, bütün trafikin yoxlanması, SSL trafikinin yoxlanması, hətta naqilsiz şəbəkələrin mühafizəsi problemləri, porblemlərin həlli yolları, İPSec – in icmalı, təhlükəsizlik sinfinə görə şəbəkəarası ekranlara tətbiq edilən əlavə tələbatlar kimi məsələlər araşdırılmışdır.

Şəbəkələrarası qarşılıqlı təsir siyasətinin işlənib hazırlanması, şəbəkələrrası ekranın qoşulma sxeminin müəyyənləşdirilməsi, və eləcə də brandmauerin fəaliyyət parametrlərinin sazlanması kimi məsələlər tədqiq olunmuşdur.

İkinci fəsildə simmetrik şifrələmə üsullarinin tət­biqi ilə kompyuter şəbə­kələrində informasiya mühafizəsinin işlənməsi yerinə yetirilmişdir. Burada möcud simmetrik şifrləmə üsullarından: AT-BAŞ şifrələməsi (sadə şifrələmə), yerdəyişmə üsulu ilə şifrələmə, birqat və İki qat yerdəyişmə şifrələməsi, Sezar şifrələməsi, sehirli kvadrat şifrələməsi, mətn şifrələnməsi, Qronsfeld üsulu ilə şifrələmə, VİJNER şifrələməsi, Pleyferə görə şifrələmə və onun əsası verilməklə yanaşı, praktiki misallarla hər bir üsulun tətbiqi ilə konkrekt misallar həll edilmişdir.

Üçüncü fəsil asimmetrik şifrləmə üsullarinin tətbiqi ilə kompyuter şəbəkə­lərində informasiya mühafizəsinin işlənməsinə həsr olunmuşdur. Burada asim­metrik şifləmənin əsasları, dissertasiya işinin həcmini nəzərə alaraq, onlardan ən geniş istifadə olunan Əl Camal alqoritimi ilə şifrələmə, şifrədən azad etmək (deşifrə) kimi məsələlər həll edilmişdir.

Nəticədə yerinə yetirilən tədqiqatlar zamanı müəllifin fikr və mülahizələri verilmişdir.

**I FƏSIL. KOMPYUTER ŞƏBƏKƏLƏRINDƏ INFORMASIYA**

**TƏHLÜKƏSIZLIYI VASITƏLƏRI**

**1.1. Kompyuter şəbəkələri və informasiya təhlükəsizliyi**

İnformasiya təhlükəsizliyi dedikdə informasiyanın müha­fizəsi və onu dəs­tək­­ləyən infrastrukturun istənilən təsadüfi və ya qanunauyğun təsirlərdən qorun­ması üçün lazım olan kom­pleks tədbirlər başa düşülür.

İnformasiya mühafizəsi problemlərinin məzmunu müt­ə­xəs­sislər tərəfindən belə interpretasiya olunur. İnforma­si­ya em­alı prosseslərinin avtomatlaşdırılması forması və üsul­ları vas­i­tə­lərinin inkişafı və mürəkkəbləşməsi ilə əlaqədar ola­raq on­lar­ın zərifliyi də artır. Bu hadisənin törəməsinə səbəb olan əsas fak­­torlar aşa­ğıdakılardır [5]:

* EHM və başqa avtomatlaşdırılma vasitələrinin köməyi ilə top­­­­­­lanan, saxlanılan və emal olunan informasiya həcminin kəs­­­kin artması;
* müxtəlif təyinatlı və müxtəlif mənbəli informasiyaların vahid ver­ilənlər baza­sında toplanması;
* hesablama texnikası resurslarına və orada olan verilənlərə bila­vasitə dostupu olan istifadəçilər dairəsinin kəskin olaraq genişlənməsi;
* hesablama sistemlərinin texniki vasitələrinin fəaliyyəti rej­im­lər­inin mürəkkəb­ləşməsi: çoxproqramlı rejimlərin geniş tət­bi­qi, eyni zamanda zamanın bölünməsi və real zaman rejim­ləri­nin real tətbiqi;
* maşınlar arası informasiya mübadiləsinin və eyni zamanda böy­ük məsafələrdə avtomatlaşdırılması.

Bu şərtlər daxilində informasiya mühafizəsi problemləri iki növ olur: bir tərəfdən informasiyanın məhv edilməsi və ya kor­­­lanması (başqa sözlə onun fiziki tamlığının pozulması), baş­qa bir tərəfdən isə informasiyadan sanksiya olunmamış isti­fa­də olun­­­­ması imkanları. İkinci növ incəlik EHM isti­fadə­çi­ləri­nin xü­susi narahatlığına səbəb olur. Informasiya sız­ma­­sının pot­en­si­al ol­araq əsas mümkün olan kanalları bunlardır:

* daşıyıcıların və başqa sənədlərin bir başa oğurlanması;
* informasiyanın yadda saxlanması və ya nüsxələnməsi;
* aparatlara və əlaqə xətlərinə sanksiya olunmamış qoşulmalar və ya “qanuni” sistem aparatlarından qeyri qanuni istifadə.

Müasir informasiya mühiti cəmiyyətini iki toplanandan: in­­­­formasiya**-**texniki (insan tərəfindən eyni olaraq yaradılmış tex­­­­­­­­­ni­­ka, texnologiya və s. Dünyası) ­və informasiya**-**psixoloji (in­­­­­­san da daxil olmaqla canlı təbiətin təbii dünyası) ibarətdir. Uyğun olaraq, ümumi halda cəmiyyətin (dövlətin) informasiya təh­­­lü­kəsizliyini iki əsas hissə kimi: informasiya-texniki təhlü­kə­­­s­izlik və informasiya**-**psixoloji (psixo­fiziki) təhlükə­sizlik ki­­mi təsvir etmək olar.

Hal**-**hazırda təhlükəsizliyin standart modeli kimi, əksər hal­­larda aşağıdakı üç kateqoriyadan (faktordan) ibarət mod­el­dən istifadə edirlər [8].

* Konfidensiallıq**-**informasiyanın elə vəziyyətidir ki, ona dos­tup yalnız uyğun səlahiyyəti olan subyektlər tərəfindən ola bi­­lər.
* Tamlıq**-**informasiyanın sanksiya olunmamış modifikasi­ya­sından qaçmaq, yəni informasiyada dəyişiklikləri yalnız o subyektlər də bilər ki, onun bu işə səlahiyyəti olsun.
* Dostupluluq (əlyetərlik)**-**dostupa hüququ olan istifadə­çilə­r­dən informa­si­yanın müvəqqəti və ya daimi gizlədil­mə­sin­dən qaçmaqdır. Başqa sözlə, iş üçün sanksiya olunmuş iş vaxt­ına uyğun olaraq səlahiyyətli şəxslər tərəfindən infor­ma­siyaya avtorizasiya olunmuş dostupların alınma imkan­ları­dır. Bunlardan əlavə heç də həmişə əsas olmayan təhlü­kə­­­sizlik kateqoriyası modelləridə vardır:
* imtina olunmazlıq və ya apelyasiyalılıq;
* müəlliflikdən imtinanın mümkünsüzlüyü;
* hesabatlılıq**-**dostup subyektinin identifikasiyasının təmin ed­­­­­­­­­il­­­­­mə­si və on­un hərəkətlərinin qeydiyyatı;
* doğruluq**-**nəzərdə tutulmuş qaydaya və ya nəticəyə uyğun­luq xüs­usiyyəti;
* autentlik və ya əsaslılıq**-**subyektin və ya resursun elan ol­un­­muşa identik olmasına zəmanət.

Qeyd etmək lazımdır ki, adətən hesabat (üçüncü) elek­tron qey­­diyyat jurnalları vasitələri ilə aparılır. Onlar isə əsa­­sən yal­­nız səlahiyyətli xidmətlər tərəfindən isti­fadə olunur. Onun əs­­­as fər­qi isə bu jurnalların mütəmadi olaraq analizindən iba­rət­dir. Apelyasiyalılıq kriptoqrafiya vasitələri (elektron im­za) vas­itə­si­lə təmin edilir. Qeyd olunan obyektiv faktorlar və ya in­for­ma­si­ya təhlükəsizliyi aşağıdakı mexanizm və ya prin­siplərlə tə­min ol­un­urlar:

* Siyasət**-**informasiya təhlükəsizliyi mexanizminin işini tən­zim edən (reqlament­ləşdirən) formal qaydalar yığımı;
* İdentifikasiya**-**informasiya cəmiyyətinin hər birinin müəy­yən (təyin) olunması;
* Autentifikasiya**-**informasiya mübadiləsi iştirakçısının düz­gün identifikasiya olun­ma­sının təmin edilməsi, başqa sözlə onun təqdim etdiyi identifikatora uyğun olması;
* Dostupa nəzarət**-**informasiya mübadiləsi prosesi iştirakçı­sı­nın resurslara dostu­puna və bu dostupun səviyyəsinə ica­zə­nin yaradılması və dəstəklənməsi qaydaları;
* Avtorlaşma**-**dostupa nəzarət qaydları yığımından konkret in­­­­­­for­­­masiya em­­alı pro­­sesi iştirakçısı üçün hüquq profil­ləri­n­in­ for­­­­ma­laşdırılması;
* audit və monitorinq**-**diqqətçəkən və ya şübhə doğuran had­­­i­­­sə­­lərin qey­d­iyyatı və analizi ilə infor­masiya mübadiləsi pr­o­­­­­­­ses­ində baş ver­ən ha­disələrin müntəzəm izlənməsi;
* insidentlərə (münaqişələrə) reaksiya**-**informasiya təhlü­kə­siz­liyi tələblərinə uy­ğun olaraq informasiya mübadiləsi mü­h­­­­iti­nin yaradılması və işçi vəziyyətdə saxlanması;
* istifadəçilərin idarə olunması**-**informasiya təhlükəsizliyi tə­ləb­­lərinə uyğun olaraq informasiya emalı mühitində isti­fa­də­çi­­­lərin iş şəraitinin tə­min olunması. Burada istifadəçi ded­ik­də admistratorda daxil olmaqla bu informasiya müh­it­in­dən is­­­­­­ti­­fadə edən hər bir subyekt başa düşülür.
* risklərin idarə edilməsi**-**mühafizə vasitələrinin gücünün, in­for­­­masiya təhlükə­sizliyinin pozulmasından mümkün olan it­ki­­­­­lərinin uyğun­­luğunun təmini (başqa sözlə, onların qurul­ma­­­sına olan məsrəflərlə);
* dayanıqlılığın təmini**-**informasiya mübadiləsi mühitinin mi­­n­­­­i­­­mal dos­tupla işçi vəz­iyyətdə saxlanması və destruktiv da­xili və xarici təsirlər şəraitində infor­ma­siya təhlükəsizliyi tə­lə­b­­lərinə uyğunluğun saxlanması.

Beləliklə, yuxarıda qeyd edilən əsas anlayışlar vasitəsilə in­for­masiya təhlü­kəsizliyinə nail olunur. Müəssisə və təşkilata in­­for­masiya təhlükəsizliyinin vuraca­ğı itgiləri aşağıdakı kate­qo­­riyalara bölmək olar.

1. Avtorlaşmış istifadəçilərin hərəkətlərindən. Bu kate­qo­­­riya­ya aid­­dir: işçi stansiya və ya serverdən ver­ilənlərin məq­­səd­yön­­lü oğ­urlanması və ya məhv edilməsi; istifa­də­çi­nin ehti­yat­sız hər­ə­kət­indən verilən­lərin zəd­ələn­mə­si.
2. Xakerlərin “elektron” üsulla təsiri. Buraya kompyuter şəb­­ə­kəsinə sanksiya olunmamış müdaxilələr və DOS hü­cüm­lar aid­dir. DOS**-**hücum (xidmətdən imti­na) müəs­sisənin ef­fek­­­tiv və təh­lükəsiz işinə cavab verən şəbəkə qovşaqla­rı­na xar­­ici həm­­lə­dir. Pisniyyətlilər bu qovşağa çoxlu sayda ver­i­lən­lər pak­eti gön­­dərməklə, onun ifrat yük­lənməsinə nail olur­­lar, nət­i­cə­­də onu müəyyən müddətə sıradan çıxara bilirlər.
3. Kompyuter virusları. Kompyuter virusları və başqa bu yön­­ümlü proq­ramlar ayrıca kateqoriyalı elektron təsir üsul­larıdır. On­­lar kom­pyuter şəbəkələrindən geniş istifadə edən mü­­­a­­sir biz­nes strukturları üçün real təhlükə mənbəyidir. Kor­­­porativ şəb­­­əkə qovşaqlarına daxil olan virus pis­niy­yət­li­yə mü­əy­­yən dərəcədə və ya hətta tam olaraq mü­əs­sisənin işi­­­nə nə­za­rət etməyə imkan verə bilər.
4. Spam. Son zamanlar spam adi faktordan təhlükəsizlik həm­­lə­sinin əsas amillərindən birinə çevrilmişdir; elek­tron poçt­­lar son zaman­lar ziyanverici proqramların ya­yıl­ması üçün əsas kan­allardan birinə çevrilmişdir; spamlar on­lara bax­ma­ğa çox va­xt aparır; psixoloji diskomfort yaradır və s. Bu­na bax­ma­ya­raq, spam bir istifadəçi üçün normal info­r­ma­siya mən­bəyi, baş­qa birisi üçün lazım olmayan bir in­for­ma­si­ya ola bilər.
5. “Təbii” həmlələr. Kompaniyaların informasiya təhlükə­siz­liyinə müx­təlif faktorlar təsir edə bilərlər: düzgün saxla­ma­­maq, verilənlərin itirilməsinə, komp­yuter və daşıyıcıların oğ­ur­­lan­ma­sı­na, forsmajor vəziyyət və s.

Be­ləliklə, müasir şəraitdə, informasiya cəmiyyətinin hər bir üzvünün normal və tam informasiya ilə təmin olunması üç­ün in­­ki­şaf etmiş informasiya təhlükəsizliyi siste­minin olması is­­­­­­tən­­­ilən müəssisə və təşkilatın, dövlət və dövlət qurumlarının nor­­­­­mal işi üçün əsas amillərdən biridir.

## 1.2. Kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifati

## 

Təhlükə dedikdə sistemə dağılma, verilənlərin üstünün açılması və ya dəyiş­di­­rilməsi, xidmətdən imtina formasında ziyan vurulmasına səbəb ola bilən istənilən hal, şərait, proses və hadisələr nəzərdə tutulur.

Təhlükələri müxtəlif siniflərə ayırmaq olar. Meydana çıxma səbəblərinə görə təhlükələri təbii və süni xarakterli təhlükələrə ayırırlar. Süni xarakterli təhlükələr də öz növbəsində bilməyərəkdən və qəsdən törədilən təhlükələrə bölünür. Təsir məqsədlərinə görə təhlükələrin üç əsas növü ayırd edilir [6,10]:

* İnformasiyanın konfidensiallığının pozulmasına yönələn təhlükələr;
* İnformasiyanın bütövlüyünün pozulmasına yönələn təhlükələr;
* Əlyetənliyin pozulmasına yönələn təhlükələr (DoS hücumlar, Denial of Service - xidmətdən imtina).
* **Konfidensiallıq** informasiyanın subyektiv müəyyən olunan xassəsidir. Verilən informasiyaya müraciət icazəsi olan subyektlərin siyahısına məhdu­diy­yət qoyulmasının zəruriliyini göstərir. Konfidensiallığın pozulmasına yönələn təhlükələr məxfi və ya gizli informasiyanın üstünün açılmasına yönə­lib. Belə təhlükələrin reallaşması halında informasiya ona müraciət icazəsi olmayan şəxslərə məlum olur.
* **Bütövlük** - informasiyanın təhrifsiz şəkildə mövcudolma xassəsidir. İnfor­ma­siyanın bütövlüyünün pozulmasına yönələn təhlükələr onun dəyişdi­ril­mə­sinə və ya təhrifinə yönəlib ki, bunlar da onun keyfiyyətinin pozulmasına və tam məhvinə səbəb ola bilər. İnformasiyanın bütövlüyü bədniyyətli tərəfin­dən qəsdən və ya sistemi əhatə edən mühit tərəfindən obyektiv təsirlər nəti­cə­sində pozula bilər.
* **Əlyetənlik** – yolverilən vaxt ərzində tələb olunan informasiya xidmətini almaq imkanıdır. Həmçinin əlyetənlik – daxil olan sorğulara xidmət üçün onlara müraciət zəruri olduqda uyğun xidmətlərin həmişə hazır olmasıdır. Əlyetənliyin pozulmasına yönələn təhlükələr elə şəraitin yaradılmasına yönəlib ki, bu zaman müəyyən qəsdli hərəkətlər ya sistemin iş qabiliyyətini aşağı salır, ya da sistemin müəyyən resurslarına girişi bağlayır.

Təhlükələr digər əlamətlərinə görə də təsnif oluna bilər:

* Baş vermə ehtimalına görə (çox ehtimallı, ehtimallı, az ehtimallı);
* Meydana çıxma səbəblərinə görə (təbii fəlakətlər, qəsdli hərəkətlər);
* Vurulmuş ziyanın xarakterinə görə (maddi, mənəvi);
* Təsir xarakterinə görə (aktiv, passiv);
* Obyektə münasibətinə görə (daxili, xarici).

**1.3. Kompyuter şəbəkələrində İnformasiya təhlükəsizliyinin əsas**

**istiqamətləri**

İnformasiya təhlükəsizliyini iki yerə - fiziki və komp­yu­ter təh­lükəsizliyinə ayır­maq olar. Buna baxmayaraq, təyin ol­un­­­­­­­ma­da olan fərqləri nəzərə almaqla onları aşağıdakı kimi xar­ak­­­teri­zə etmək olar [9,11].

Fiziki təhlükəsizlik **-** informasiya mühitinin işlənməsi üç­ün lazım olan avadan­lıqların qorunmasının təmini, insanların bu qur­ğu və avadanlıqlara dostu­puna nəzarətdir. Buraya əlavə ol­­­­a­r­­aq, informasiya mühiti istifadəçilərinin pisniy­yət­lilərin fiz­iki təsirlərindən qorunmasını və eyni zamanda virtual xarakterli in­for­masiyanın mühafizəsini (çap olunmuş sənədlərin, xidməti tel­­e­fon sorğularının, əməkdaşların ev ünvanlarının, xarab ol­muş xarici informasiya daşıyıcılarının bərk nüsxələrinin) aid et­­­­mək olar.

Kompyuter təhlükəsizliyi (şəbəkə təhlükəsizliyi, verilən­lərin təhlükəsizliyi) **-** informasiyanın virtual görü­nüşdə müha­fi­zə­­­­sinin təminidir. Burada informasiyanın hansı mühitdə ol­ma­­­sın­dan asılı olaraq, misal üçün, kompyuter (informasiyanın ya­ran­ması və ya emal edilməsi yerinə) və şəbəkə (göndərilmə zam­­­anı) təhlükə­siz­liyinə bölmək olar.

**1.4. İnformasiyanın məxfiliyinin təmini və tamlığına nə­za­rət vasitələri**

İnformasiyanın məxfiliyinin təmini və tamlığına nə­za­rət üçün güclü vasitə­lərdən biri də kriptoqrafiyadır. Bir çox cə­hət­lər­­­­­dən o, proqram-texniki vasitələr arasında mər­­­­­kəzi yer tutur. Krip­toqrafiya onlardan bir çoxunun rea­­­lizə olun­ması üçün əsas rol oynayır, bəzən də ye­ga­nə mü­­ha­fizə va­si­tə­si olur. Məsələn, fi­­­­-zi­ki mühafizəsi ol­duqca çə­tin olan por­tativ kom­pyuterlər üçün yal­nız krip­­to­q­ra­fi­ya hətta oğur­lan­ma halında da məxfiliyə tə­mi­nat ve­rir. Krip­toqrafiyaya çox­lu kitablar və məqalələr həsr olu­­nub. Yalnız qısa xüla­sə ilə kifayət­lə­nək [2,14].

Şifrələnmənin simmetrik və qeyri-simmetrik (asim­met­­rik) ad­­­-­la­nan iki əsas üsulu fərqləndirilir.

**Simmetrik kriptosistemlər.** Simmetrik şif­­rə­lə­mə üsu­lun­da eyni açar(gizli saxlanılan) həm mə­lu­ma­­tı şif­rə­ləmə, həm də de­şifrələmə üçün istifadə olunur. Ol­­duq­­ca ef­fek­tiv (sürətli və eti­barlı) simmetrik şifrələmə me­­tod­ları möv­cuddur. Sim­met­rik şif­­rələmə alqoritm­lə­rin­­­dən DES, 3-DES, İDEA, FEAL, Ski­p­­­ja­ck, RC2, RC4, RC5, CAST, Blow­fish kimi blok şifrələri və bir sı­ra axın şif­rə­ləri (RC4, A5) daha geniş istifadə olunur.

Simmetrik şifrələmənin əsas nöqsanı ondan ibarətdir ki, giz­li açar həm göndərənə, həm də alana məlum olma­lı­­dır. Bu bir tə­rəf­­dən açarın göndərilməsi problemini qo­yur, di­gər tərəfdən alan şəxs şifrələnmiş və deşif­rə­lən­miş məlu­ma­tın varlığı əsa­sın­da bu məlumatı konkret gön­­dərəndən alma­sını sübut edə bil­məz. Çünki be­lə mə­lu­matı o özü də gene­ra­siya edə bilər.

**Asimmetrik kriptosistemlər.** Asimmetrik metodda iki açar istifadə olunur. On­lar­dan bi­ri, giz­li olmayan (sahibinin ünvanı ilə bir­lik­də nəşr olu­­­na bilər) şif­­rə­ləmə üçün istifadə olunur, digəri (gizli, yal­­nız alana mə­lum) deşifrələmə üçün isti­fadə olunur. Asim­­met­rik şifrə­lə­mə al­­qo­ri­tmlərinə mi­sal olaraq RSA, El Ga­mal, Şnorr və s. gös­tər­­­mək olar.

Asimmetrik metodların əsas çatışmayan cəhəti aşağı sü­rət­li olmalarıdır. Buna görə onlar simmetrik metodlarla bir­gə işlə­di­lir. Məsələn, açarların göndərilməsi məsə­lə­si­ni həll et­mək üçün əv­vəlcə məlumat təsadüfi açarla sim­met­rik şif­rə­lənir, sonra bu açarı alan tərəfin açıq sim­met­rik açarı ilə şif­rələyir, bundan son­ra məlumat və açar şə­bə­kə ilə ötürülür.

Diqqəti ona yönəldək ki, asimmetrik metodlardan isti­fa­də et­dikdə, adresatın (ad, açıq açar) cütünün həqiqi­liyi­nə zə­ma­nət tə­ləb olunur. Bu məsələnin həlli üçün sertifi­ka­­siya mər­kəzi an­la­­yışı daxil edilir. Sertifikasiya mərkəzi ad­lar/açıq açar­lar sorğu ki­tabını özünün rəqəm imzası vasi­təsi ilə təs­diq edir.

Kriptoqrafik metodlar informasiyanın tamlığına eti­barlı nə­za­rət etməyə imkan verir. Yalnız təsadüfi səhv­lərə da­vam gə­tir­mə­yə qadir olan ənənəvi nəzarət cəmlə­rin­­dən fər­qli ola­raq, giz­li açarın tətbiqi ilə hesablanmış krip­­to­qra­fik nəza­rət cəmi prak­tik olaraq verilənlərin bü­tün müm­kün hiss olun­mayan dəyi­şil­mə­lərini istisna edir.

Bi­rin­ci əsas əlamət, şifrələməni icra edərkən infor­ma­si­­ya­­nın məz­mununun (həcminin) üçüncü tərəfə mə­lum olma­ma­sı­dır. Bu halda, bədniyyətlinin xəbəri olma­dan al­­­­­qo­­­­­rit­min yeri­nə ye­tir­məsində məlumatın başqa şə­ki­lə sa­­lın­­­ma­sına **“gizli ya­zı”** de­yi­lir.

Bu gün gizli yazıdan fərqli olaraq alqoritmik şifrə­lə­mə **kriptoqrafiya açarı** ad­la­nır, hansı ki alqo­rit­min də­yiş­­di­ril­mə­­si mə­lumdur və daxil olub tətbiq edil­mə­si hər kəs üçün ar­zu olu­nan­dır, ancaq məhdud həcmdə in­­for­­ma­si­­yalarla şif­rə­­ləmə apa­rı­lır – **AÇAR**, açar ancaq gön­də­rən və qəbule­dən üçün mə­lum ol­ma­lıdır.

Daha çox açarı insanlar özləri yaradırlar, lakin göndərilən mə­­­­lu­mat proqram təminatının köməyilə ayrıca açar ya­ra­dır və ya hətta verilənlər bazası açarının uzaq­laşdı­rıl­ma­­sı­nı qa­da­ğan edir. Müasir kriptoqrafiya açarının riyazi öl­çü­sü 56-dan 4096 bi­tə qədər tərtib edilir. Böyük sadə rə­qəmlər ar­dı­cıl­lı­ğından iba­rət olan açarı yadda sax­la­maq­da insanlar çə­tinlik çə­kir bax­ma­yaraq ki, bunlar 2-lik və 10-luq rə­qəm­lər­dir. Ona görə də müasir sis­tem­­­­lər isti­fa­­də­­­­­çilərə açar­dan yox – şif­­rə yığımın­dan, pa­­rol isə açıq mətn­dən isti­fa­də etməyi tək­lif edir. Parol bir və ya bir ne­çə söz­dən ibarət ola bilər, əsas odur ki, istifadəçi onu asan yad­da sax­laya bilsin.

**1.5. Şəbəkə perimetrinin mühafizəsinin məqsədi və məhdudiyyətləri**

* Düzgün quraşdırılmış şəbəkələrin ekranı-şəbəkə perimetrini qoruyan daşdır.
* İnternetdən aktiv istifadə mobil istifadəçilər təhlükəsizlik risklərini artırır.
* VPN-nin inkişafı perimetri zəiflətdi və naqilsiz şəbəkələrlıə birlikdə ənənəvi şəbəkə perimetri konsepsiyanı pozdu.
* Paketlərin firtirləşməsini reallaşdıran ənənəvi şəbəkəarası ekranlar yalnız şəbəkə portlarını və kompüter ünvanlarını blokirovka edir.
* Müasir həmlələrin əksəriyyəti əlavələr səviyyəsində baş verir.

**1.6. İşçi stansiyalarının mühafizəsinin məqsədi və məhdudiyyətlər**

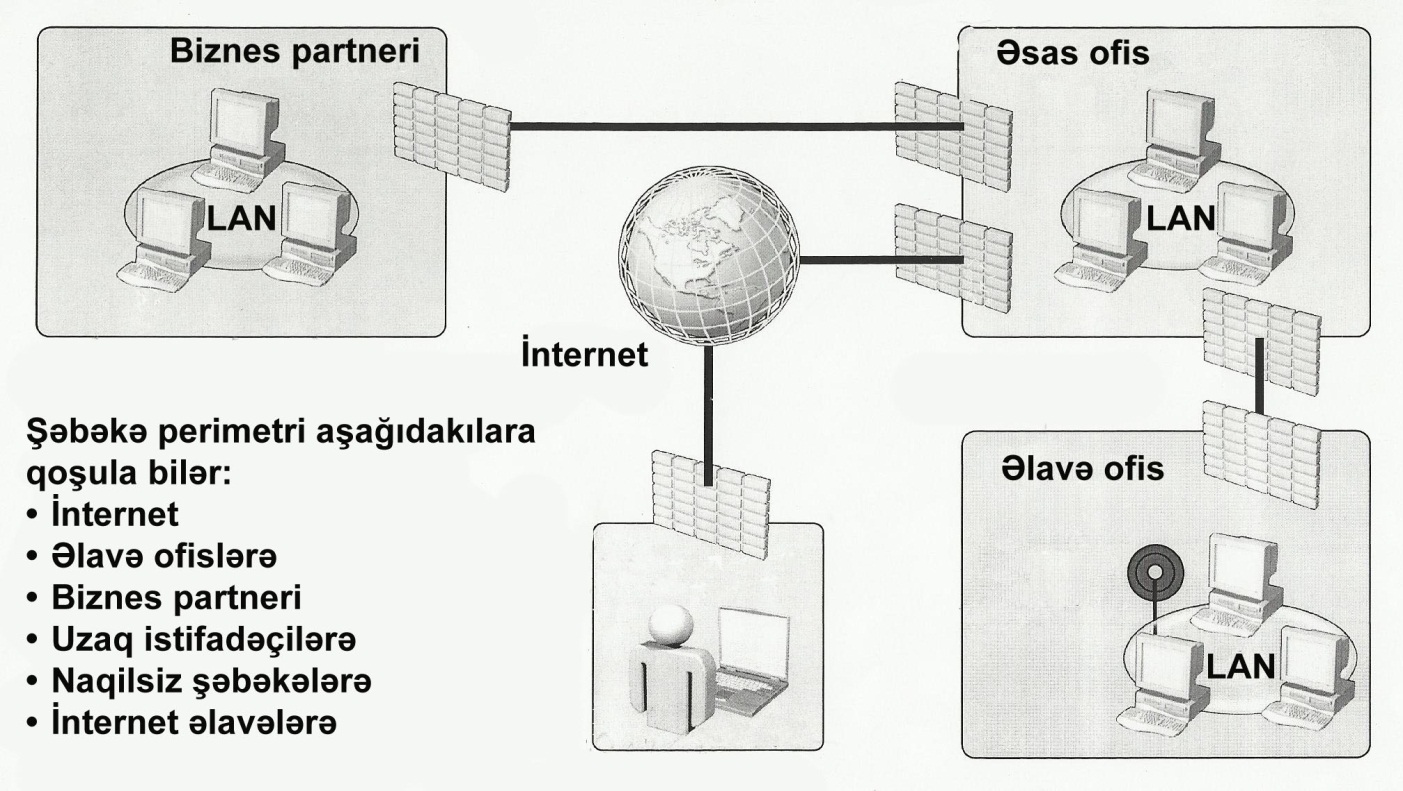
* Müştəri kompüterlərin mühafizəsindən keçən və ya perimetrin daxili şəbə­kədən çıxan həmlələri blokirovka edir.
* Bunlardan başqa işçi stansiyaların mühafizəsinə aşağıdakılar daxildir:
* OC-ni təhlükəsiz işə sazlamaq
* Antivirus proqramı təminatından istifadə
* Fərdi şəbəkəarası ekranlar
* İşçi stansiyalarının mühafizəsi çoxlusayda kompüterlərin mühafizəsi de­məkdir.
* Əgər şəbəkədə mərkəzləşmiş idarəetmə və müraciətə nəzarət tətbiq olun­mayırsa onda istifadəçilər stansiyaların mühafizəsini zəiflədə bilər.

**1.7. Həmlələri aşkarlayan sistemlərin məqsədi və məhdudiyyətləri**

* Nümunəvi həmlələrin əlamətlərini aşkarlayır,şübhəli trafikləri təhlükəsizlik jurnalına yazır və ya administratoraməlumat verir.
* Müntəzəm olaraq yeni həmlələr və uyğunluqlar görünür,bunlar isə sistem üçün belə hücunların əlamətləri toplama və həmlələri aşkarlayan sistem istehsalçılarına şamil olunana qədər təhlükə yaradacaqlar.

**1.8. Perimetrin mühafizəsi**

* İSA Server lazım olan bütün imkanları təmin edir.
* Paketli filtirləşmə
* Vəziyyəti saxlamaqla
* Əlavələr səviyyəsini yoxlamaqla
* İSA Server sizin icazə vermədiyiniz istənilən trafiki blokirovka edir.
* VPN-dən təhlükəsiz qoşulmanı təmin edir.
* İCSA sertifikatına malikdir və ümumi kriteriya ilə sertifikatlaşdırılıb.

****

Şəkil 1.1.Şəbəkə perimetrinin qoşulma sxemi

**1.9.Kompyuter şəbəkələrində şəbəkələrarası ekranlar**

Kompyuter şəbəkəsində informasiya təhlükəsizliyinin istənilən vasitəsinə qar­şı irəli sürülən tələbatları kateqoriyalara bölmək olar [19]:

-təhlükəsizlik məsələləri külliyatının tələb etdiyi funksional-həll;

-etibarlığa tələbatlar-əvvəlcədən nəzərdə tutulmuş bütün təhlükəsizllik funksi­yalarının vaxtında,düzgün və ehtiyyatla yerinəyetirilməsi ;

-adaptasiya olunmaya tələbatlar-kompyüter şəbəkəsinin sturuktur,texnoloji sxem və fealiyyət şəraitinin dəyişilməsi vaxtında məqsədyönlü adaptasiya qabilliyyəti;

-erqonomik-inzibatiliyinin,istismarın rahatlığına verilən tələbatkar və istifadəçinin əngəllərini minimallaşdırmaq;

Iqtisadi-maliyyə və vsaitlərinin minimallaşdırılması.

Şəbəkələrarası ekranlar növbəti qruplar üzrə daha dəqiq tələbatları təmin etməlidir. Məqsəd keyfiyyətləri üzrə -daxili şəbəkənin qorunmasının təhlükəsizliyini təmin etmək və xarici qoşulma və rabitə seansları üzərində tam nəzarəti həyata keçirmək. Şəbəkələrarası ekranın istifadəçilərin xarici qoşulmasını mümkün edən avtorizasiya vasitələri olmalıdır. Belə bir tipik vəziyyət mümkündür ki, personalın bir hissəsi məsələn,məzuniyyətə getməlidir.İş prosesində onlardan təşkilatın daxili kompyüter şəbəkəsinin bəzi vasitələrinə daxil olmaq tələb olunur. Brandmauer belə istifadəçiləri etibarlı şəkildə tanımalı və onlara lazımı imkanı yaratmalıdır.

İdar’ olunma v’ çeviklik üzrə-təşkilatın təlükəsizlik siyasətini həyata keçir­mək üçün güclü və çevik idarəetmə vasitələrinə malik olmalı. Brandmauer şəbə­kənin sturuktur dəyişikliyi zamanı sistemin sadə konfuqrasiyasını yenidən tə­min etməlidir. Əgər təşkilatda bir nçə xarici qoşulma ,o cümlədən,uzaq filiallarda qoşulmalar varsa, ekranlarla idarəetmə sostmeier onlar üçün vahid mərkəzləş­dirilmiş şəkildə təmin etməlidir.

Səmərəlilik və şəffaflıq üzrə-kifayət qədər effektiv işləmək və bütün daxil olan və xaric olan informasiyanı maksimum yükləmə ilə emal edə bilmək. Bu brandma­uerin böyük sayda çağrışlarla yükləyib,onun işini pozmaması üçün vacibdir. Şəbə­kə­lərarası ekran lokal şəbəkə istifadəçiləri üçün gizlin işləməli və onların leqal fealiyyətinə çətinlik yaratmamalıdır. Əks halda istifadəçilər qurulmuş müda­fiə səviyyəsini istənilən üsullarla pozmağa çalışacaqlar.

Özünümüdafiə üzrə-istənilən icazə verilməyən təsirdən özünü müdafiə xüsu­siyyətinə malik olmaq.Şəbəkələrarası ekran təşkilatda gizli informasiyanın həm açarı,həm də qapısı oldğu üçün o, onun parametrlərində istənilən icazə veril­məyən dəyişiklik cəhdlərini bloklaşdırılmalıdır.Həmçinin öz vəziyyətinə nəzarət və siqnalizasiya vasitələrini işə salmalıdır.Siqnalizasiya vasitələri istəni­lən icazəsi fəaliyyət üzə çıxarsa,təhlükəsizlik xidmətlərini vaxtında xəbərdar etməli,həmçinin, şəbəkələrarsı ekranın işinin pozulması zamanı da xəbərdarlıq etməlidir.

İndiki dövrdə informasiya-kompyüter təhlükəsizlik vasitələrinin qiymətlən­dirilməəsi kriterilərinin təhlükəsizlik altsistemlərin müəyyən keyfiyyətlərinə, onların effektivlyinə və effektiv həyata keçirilməsi olan tələbatlardan ibarətdir. Buna görə elə şəbəkələrarası ekranlar icazə verilməyən müdaxilələrdən müdafiə olunurlar.

Şəbəkələrarası qarşılıqlı əlaqə zamanı təhlükəsizlik səviyyəsini müəyyən et­mək üçün brandmauerlərə təhlükəsizlik göstəriciləri tətbiq olunur.Göstəricilərin konkret siyahısı kompyüter şəbəkələrin təhlükəsizliyinin təminatı üzrə şəbəkə­lər­arası ekranların siniflərini müəyyən edir [20]. Brandmauerlırin şəbəkələrarası informa­siya axınına nəzarət üzrə uyğun siniflərə bölünməsi informasiyanın şəbəkələrarası qarşılıqlı mübadiləsi zamanı lazımı təhlükəsizlik səviyyəsinin əldə olunması üçün əsaslandırılmış və iqtisadi cəhətdən təsdiqlənmiş tədbirlərinin işlənməsi məqsədi ilə vacibdir.

Təhlükəsizlik göstəricilərinə görə şəbəkələrarası ekran 5 sinifə bölünür. Təhlükəsizliyin ən aşağı sinifi-beşinci sinif və 1D daha avtomatlaşdırılmış sistem­lə­rin ətraf mühitlə qarşılıqlı əlaqəsi üçün,dördüncü-1Q üçün,üçüncüsü-1V üçün, ikinci-1B üçün,ən yüksək birinci isə -1A sinifindən olan avtomatlaşdırılmıış sistem­lərim ətraf mühitlə təhlükəsizlik qarşılıqlı əlaqəsi üçün istifadə olunur. Brandmauerin müəyyən təhlükəsizlikk sinfi olan avtomatlaşdırılmış sistemə (AS) qoşulması zamanı ilkin sistemə şəbəkələrarası ekranların qoşulması ilə alınan məcmu sistemin təhlükəsizlik sinfi aşağı düşməməlidir. 3 B, 2 B sinifindən olan AS üçün 5 ci sinifdən aşağı olmayan brandmauerlər istifadə olunmalıdır.3 A, 2 A sini­fndən olan AS üçün emal olunan informasiyanın vacibliyiindən asılı olaraq aşağıdakı sinifli brandmauerlər istifadə olunmalıdırlar:

-“məxfi “qrifli informasiyanın emalında-3-cü sinifdən aşağı olmayan;

-“tam məxfi”qrifli informasiyanın emalında 2 –ci-sinifdən aşağı olmayan;

-“xüsusi vacib” qrifli informasiyanın emalında 1-ci sinifdən aşağı olmayan;

Hər bir sinif təhlükəsizliyə tələbatlarınn müəyyən minimal külliyatını xarakterizə edir. Siniflər AS-də informasiya emalı xüsiyyətlərinə görə fərqlənən üç qrupq ayrılırlar. Hər bir qrupda dəyərindən(məxfiliyindən) asılı olaraq təhlükəsizlik tələbləri ierarxiyasina riayət olunur. Bu uyğun olaraq AS –in təhlükəsizlik sin­ifləri ierarxiyasıdır. Cari qrup üçün təhlükəsizliyin yüksək səviyyəsinə uyğun sinif NA indeksi ilə işarələnir. Burada N-1-dən 9-a qədər qrup nömrəsidir.Növbəti sinif NA ilə işarələnir və s.

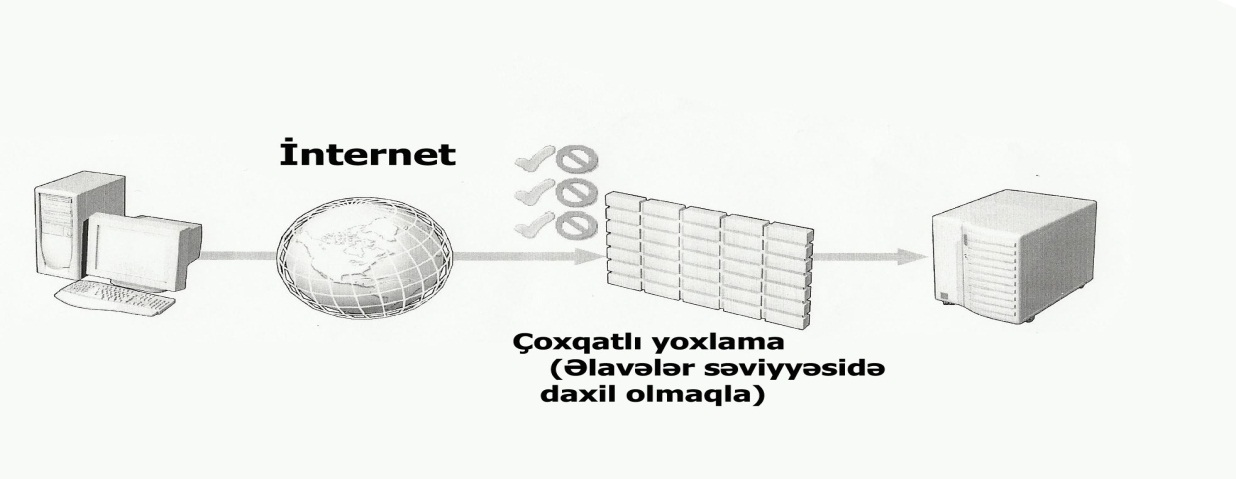
Üçüncü qrup eyni səviyyəli məxfilik daşıyıcılarında yerləşdirilmiş AS-in bütün informasiyasından istifadəyə icazəsi olan bir istifdəçinin işlədiyi AS-dir. Bu qrup iki sinifə ayrılır:3B və 3A. İkinci qrup müxtəlif məxfilik səviyyələri daşıyı­cılarda saxlanılan və ya emal olunan AS bütün informasiyasından eyni dərəcədə istifadə hüququ olan istifadəçilərin işlətdiyi AS-dir. Bu qrup iki sinfə ayrılır:2B və 2A. Birinci qrup müxtəlif məxfilik səviyyəli informasiyanı saxlayır və ya emal edir. Burada çox sayılı istifadəçilərin heç də hamısı AS-nin bütün informasi­yalarından istifadə hüququna malik deyillər.Cari qrup 5sinfə ayrılır :1D, 1Q, 1V, 1B və 1A.

* **Şəbəkəarası ekran aşağıdakılardan mühafizə edə bilmir:**
* İcazə verilmiş portdan gələn və ekranda əlavələr səviyyəsi filtirləri ilə analiz olunmayan bəlagətirən trafikdən
* Şifrələnmiş tünel və ya sessiyalardan keçən istənilən trafikdən
* Şəbəkəyə pisfikirlinin daxil oluş hücunlarından
* Legitim qrafikə oxşarlardan
* Virusları bilərəkdən və ya bilmədən yükləyən istifadəçilərdən və administratorlardan
* Pis parollu administratorlardan

**Ekran nə edir?**

* Paketli filtirasiya
* Vəziyyətini saxlamaqla

Əlavələr səviyyəsini yoxlamaq

****

Şəkil 1.2. Şəbəkəarası ekranın funksiyaları

**Bizə lazımdır...**

**İSA-nın funksiyaları**

**Tez-tez istifadə olunan veb-məzmunlara tez daxil olmaların təmini**

**İnternetə daxil olmalara nəzarət və istifadəçilərin internet hücumlarından mühafizəsi**

**Filialların əsas ofisə təhlükəsiz qoşulmalarının təmini**

**Korporativ şəbəkələrə yumşaq təhlükəsiz daxil olmalarının təmini**

**Şəbəkədə müəyyən daxili informasiyaya partnyorlara müraciətin açılması**

**İnternetdən daxili əlavələrə təhlükəsiz daxil olmaları təmin etməyi**

**Xarici şəbəkədən elektron poçta təhlükəsiz müraciəti təmin etmək**

**Poçt serverini nəşr etmək**

**Serverlərin nəşri**

**Serverlərin nəşri**

**VPN dəstəkləmək və mühafizə etmək**

**RRAS uzaqdan müraciət xidmətilə inteqrasiya**

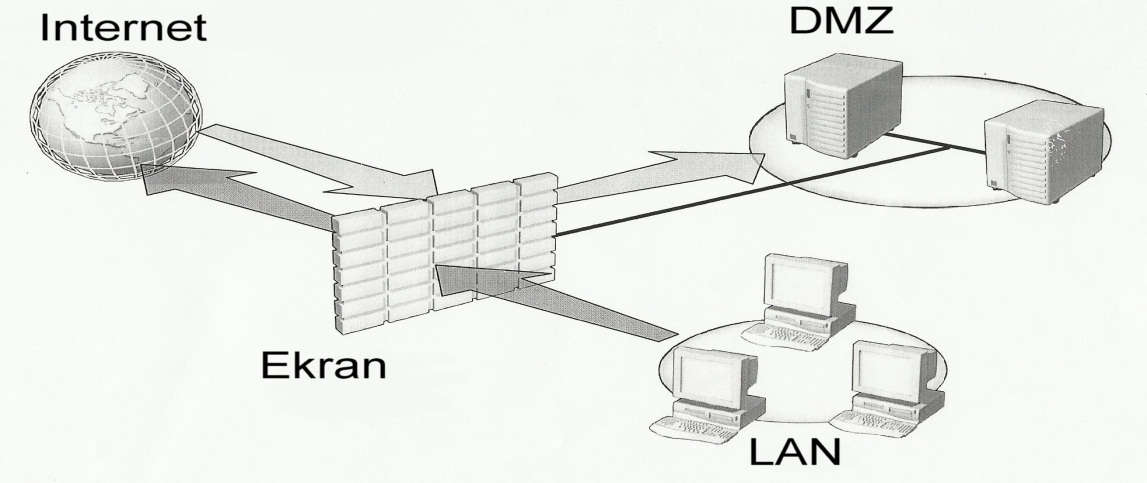
**Keşləmə xidməti**

**RRAS uzaqdan müraciət xidmətilə inteqrasiya** **Web proxy**

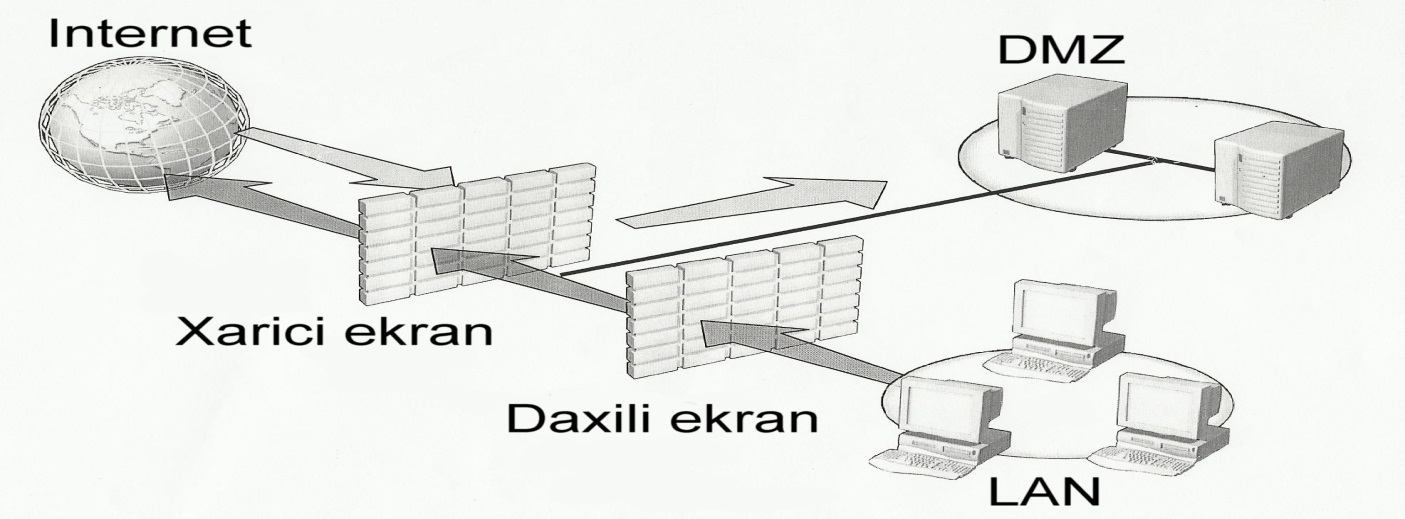
**Keşləmə xidməti** **Keşləmə**

**Web proxy**

**Keşləmə**



Şəkil 1.3. Üçnöqtəli ekran



Şəkil 1.4. İki ekran

**1.10. İsa Server 2004**

5 səhifə əlavə et A5-dən

**1.14. Şəbəkəarası ekrandan keçən trafik**

* SSL tunelləri şifrlənmiş şəkildə adi ekrandan keçirlər.Bu isə viruslara və qurdlara görünməz olmağa və daxili şəbəkəyə düşməyə imkan verir.
* VPN trafik şifrlənmiş və yoxlanıla bilməz
* Əksər hallarda ani məlumatlarla mübadilə xidməti İnstand Messenger(İM) trafiki yoxlanılır və faylların göndərilməsi üçün istifadə oluna bilər

**1.15. Bütün trafikin yoxlanması**

* VPN trafikini rassifrovka olunandan sonra yoxlama üçün həmlələrin aşkarlanması sistemindən istifadə etmək məqsədə uyğun olar.
* Yadda saxla:Çoxsəviyyəli mühafizə
* SSL trafikini yoxlaya biləcək şəbəkəarası ekrandan istifadə edin.
* Özünüzün şəbəkəarası ekranınızın imkanlarını genişləndirin
* Ani məlumatlarla mübadilə xidməti (İM) trafikini yoxlaya biləcək genişlənməni quraşdırın.

**1.16. SSL trafikinin yoxlanması**

* SSL trafiki şifrlənmiş olduğundan və yoxlanıla bilinmədiyindən şəbəkəarası ekran onu buraxır.Bu isə viruslara və daxili komputerləri yoluxdurmağa imkan verir.
* İSAServer SSL trafikini eksşifrləyə və yoxlaya bilər.Yoxlanmış trafik daxili serverə yenidən şifrlənmiş və ya adi görünüşdə verilə bilər.

**1.17. Naqilsiz şəbəkələrin mühafizəsi problemləri**

* **Wired Equivalent Privacy(WEP) məhdudiyyəti**
  + WEP-in sstatiki açarları dəyişdirilməyir və həmlələr üçün amil ola bilər
  + Müştəri komputerlərinə aid ola biləcək açarların yayılması üçün standart vasitələr yoxdur
  + Miqyaslaşdırılması : WEP-in açarının açılması bütün şəbəkəyə müraciətin açıq olmasını göstərir.
* **MAC adresslərə görə filtrləşməyə məhdudiyyətlər**
* Həmlə edən buraxıla bilən MAC adress təqdim edə bilər.

**1.18. Porblemlərin həlli yolları**

* **ΙΙ səviyyədə parola nəzərən autentifikasiyanın aparılması**
* ΙEEE8021.1xPEAP/MSCHAPv2
* **ΙΙ səviyyədə sertifikata əsasən autentifikasiyanin aparılması**
  + ΙEEE8021.1xEAP-TLS
* **Başqa üsullar**
* **VPN-ə qoşulma**
* L2TP/İpsec(təklif olunur) və ya PPTP
* Rouminq işləməyir
* İctimai müraciət nöqtələrini istifadə zamanı əlverişlidir.
* Komputerin autentifikasiyasi və qrup siyasətinin sazlanması istifadə olunmayır.
* **İPSec**
* Qarşılıqlı təsir və birgəlik sualları

**802.1x**

* **Portlarla müraciətlərə nəzarət mexanizmini təyin edir**
* Naqilli və naqilsiz birləşmələrdə işləyir
* Şifrləmə üçün açar lazım deyil
* **Extensible Autentication Protocol(EAP)-dan istifadəyə təsir etməyir**
* Autentifikasiya-zero seçilir.
* Müraciət nöqtələri EAP-dan istifadəyə təsir etməyir
* **Açarlarla avtomatik idarəetmə**
* Açarların şifrlənməsi üçün qabaqcadan proqramlaşdırmaya ehtiyac yoxdur.

**802.1x üçün sistemli tələbat**

* **Müştəri : Windows Xp**
* **Server : Windows Server 2003İAS**
* İnternet Authentication Service – RADİUS server
* İAS-ın sertifikatı
* **Windows 2000 - ə 802.1x**
* Müştəri və İAS SP3-ə malik olmalıdır
* Müştəriyə avtomatik konfiqurasiya dəstəklənməyirYalnız EAP-TLS və MS-CHAPv2

**1.19. İPSec – in icmalı**

* **İP Security (İPSec) nə deməkdi?**
* İP trafikini mühafizə üsulu
* İnternet Engineering Task Force (İETF) işlənmiş açıq standartlara əsaslanır.
* **İPSec – dən niyə istifadə etmək lazımdır?**
* İP üzərindən şifrlənmiş və autentifikasiya olunmuş birləşmələri təmin etmək üçün
* Əlavələr və ya əlavələr səviyyəsi protokollardakı asılı olmayan transportun təhlükəsizliyini təmin üçün

**İPSec-dən istifadə ssenarisi**

* Paketlərin filtirləşməsinə icazə/qadağa
* Şəbəkədaxili qarşılıqlı hərəkət təhlükəsizliyi
* Şəbəkəarası ekranlardan istifadə etməklə domenlərin replikası
* Açıq şəbəkələrdə tonnellərin quraşdırılması

**İPSec-də paketlərin filtirləşməsinin reallaşması**

* İcazəli və icazəsiz trafiklərin filtirləri
* Birneçə qayda olduqda daha sərt cütlüklər prioritetə malik olur
* Təhlükəsizlik üçün ″NoDefaultExempt=1″ parametrinin yüklənməsi əsasdır

**Paketlərin filtirləşməsi və serverlərin mühafizəsi**

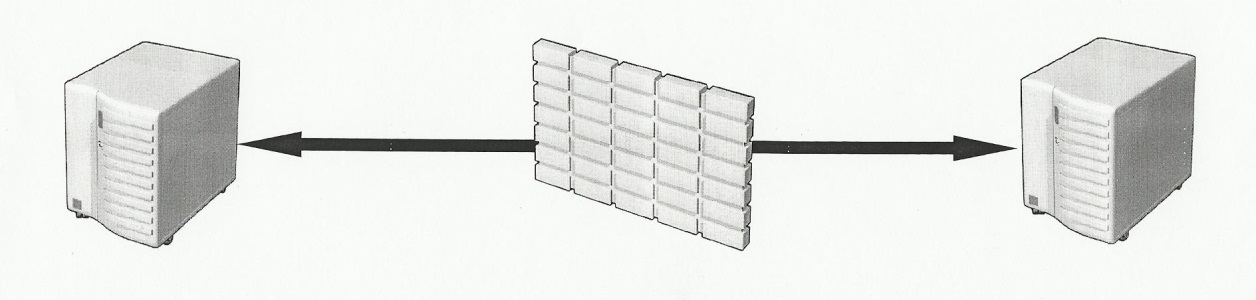
* Falsifikasiya olunmuş İP paketləri sorğu və ya sağlam olmayan koda malik ola bilər və şəbəkəarası ekrandan şəbəkəyə daxil ola bilər
* İPSec belə trafikin analizini təmin etməyir.
* Əksər sındırma alətləri daxili resurslara qoşulmaq üçün 80,88,135 və s. Kimi portlardan istifadə edirlər

**İPSec-in firtirləşmə aparılmayan trafik**

* **İP broadeast**
* **Mültificast ünvan**
* 224.000-dan 239.255.255-dək
* **Kerberas-ilkin və ya məqsədi UDP88 portları**
* Kerberos mühafizə olunan protokoldur.Bundan İnteruet Key Exchance (İKE) xidməti domendə başqa komputerlərin autifikasiya olunması üçün istifadə edə bilər
* **İKE-UDP500 məqsədi port**
* İPSec parametrləri ilə mübadilə imkanlarına malik olmaq üçün İKE xidməti tələb olunur.

**Domenlərin replikasiyası üçün İPSec**

* **İPSec-dən şəbəkəarası ekran vasitəsilə replifikasiya üçün istifadə edin**
* Domenin başqa kontrollerlərində İP ünvanına görə trafikin təhlükəsizliyini təmin etmək üçün domenin hərbir kontrollerin İPSec siyasətini yaradın
* **ESP3DES-dən şifrləmə üçün istifadə edin**
* **Şəbəkəarası ekranda trafiki aşağıdakı portlar vasitısilə həll edin**
* UDPPort500 (İKE)
* İP protocol50 (ESP)



* 1. **Təhlükəsizlik sinfinə görə şəbəkəarası ekranlara tətbiq edilən əlavə tələbatlar**

**- Birinci sinif təhlükəsizliyə malik şəbəkələrarası ekranlara təlabatlar.**

**İdentifikasiya və autentifikasiya.** Şəbəkələrarası ekran bütün subyektlərin tətbiqi səviyyədə əlavə olaraq identifikasiya və autentifikasiyasını təmin etməlidir. İnzibati,identifikasiya və autentifikasiya şəbəkələrarası ekran inzibatçının daxil olma təlabatı zamanı identifikasiya və autentifikasiyanı təmin etməlidir. Şəbəkə­lərarası ekran biometrik xarakteristikalar və ya xüsusi qurğular (jeton,kart, elektron açar) və müvəqqəti fəaliyyətdə parol üçün identifikasiya və autentifi­kasiya imkanı yaratmalıdır. Şəbəkələrarası ekran autentifikasiya zamanı identifi­kasi­ya­nın həqiqiliyi təsdiq olunmamış qeyri-identifikasiyalı subyektin müdaxilə­sinə mane olmalıdır. İnzibatçının göndərdiyi sorğunun uzaqlaşdırılması zamanı (qəbul olunmamış) identifikasiya və autentifikasiya informasiyanın aktiv və passiv saxlanılmasına davamlı olan metodlarla təmin olunmalıdır [3,7].

**İnzibatçılıq** :istifadənin sadəliyi.Çoxkomponentli şəbəkələrarası ekran öz komponentlərinin mərkəzləşdirilmiş idarə edilməsini təmin etməlidir.Həmçinin filtrlərin konfiqurasiyasına.bütün filtrlərin qarşılıqlı uyğunlaşdırılmasına nəzarət etməli,qeydiyyat informasiyasını analiz etməlidir.Şəbəkələrarası ekranların idarə olunması üçün qrafik interfeys nəzərdə tutulmalıdır.

**Tamlıq**. Şəbəkələrarası ekran həm yüklənir,həm də dinamik prosesdə təyin olunmuş alqoritmin informasiya hissəsinin nəzarətləri cəmi üzrə və öz proqramının tamlığına nəzarət vasitələrinə malik olmalıdır. Testləşdirmə. Şəbəkələrarası ekranda əlavə olaraq şəbəkələrarası ekranın idarə olunması üçün qrafiki interfeys və brandmauer komponentlərinin mərkəzləşdirilmiş idarə olunması prosesinin reqlamentli testləşdirilməsi imkanına şərait yaradılmalıdır. Test sənədləri şəbəkələrarası ekran və test nəticələri sınaqlarının izahı olmalıdır.

**Konstruktor (layihə ) sənədləşməsi** .Əlavə olaraq şəbəkələrarası ekranın ida­rə olunması üçün qrafiki interfeysin izahı olan sənədlər olmalıdır.

**İkinci sinif təhlükəsizlik şəbəkələrarası ekranlara əlavə tələbatlar.**

Şəbəkələrarası ekran əlavə olaraq aşağıdakıları təmin etməlidir [8].

-subyektlərin (obyektlərin) və ya müdafiə olunan şəbəkənin tətbiqi

funksiyalarının gizlədilməsi imkanı;

- şəbəkə ünvanlarının translasiyası imkanı.

Qeydiyyat. Əlavə olaraq şəbəkələrarası ekran aşağıdakıları təmin etməlidir:

-filtrləşmə qaydalarını pozmaq cəhdində distansion siqnalizasiya;

-tətbiqi səviyyədə sorğu olunan servislərin qeydiyyat və hesaba alınması;

- şəbəkələrarası ekranda hadisələrə proqramlaşdırılmış reaksiya.

**İnzibatçılıq.** Identifikasiya və autentifikasiya.Şəbəkələrarası ekran identifika­tor (kod) və müvəqqəti fəaliyyət parolu üzrə identifikasiya və autentifikasiya imkanını yaratmalıdır. Brandmauer identifikasiyalı subyekt və ya autentifikasiya zamanı identifikasiyanın həqiqiliyi təsdiq olunmamış subyektin daxil olmasına mane törətməlidir. Kənarlaşdırılmış inzibatçının daxil olma sorğusu zamanı identifikasiya və autentifikasiya informasiyanın aktiv və passiv tutulmasının dol­ğun metodu ilə təmin olunmalıdır.

**Tamlıq.** Şəbəkələrarası ekran həm yükləmə,həm də dinamiki prosesdə nəzarət cəmləri üzrə informasiya sahəsi və öz proqramının tamlığına nəzarət edən vasitələrə malik olmalıdır. Bərpa şəəkələrarası ekran brandmauerin xüsusiyyətlərinin əməli bərpasını təmin edən (vəsaitin nasazlıq və işdən imtinası zamanı) bərpaetmə prosedurasını nəzərdə tutmalıdır.

**Testləşdirmə.** Şəbəbkələrarası ekranda reqlament daxili testləşdirmə imkanı olmalıdır:

**-**filtrləşmə qaydalarının həyata kecirilməsi;

**-**qeydiyyat prosesi;

**-** sorğuların identifikasiya və autentifikasiyası;

**-**inzibatçının hərərəkətlərinin qeydiyyat prosesi;

**-**şəbəkələrarası ekranın informasiya və proqram hissəsinin tamlığı prosesinə

nəzarət

**-**bərpaetmə prosesi.

**Test sənədləşməsi.** Şəbəkələrarası ekranın test və sınaqlarının təsiri və testləşmənin nəticələri.

**Beşinci sinif təhlükəsizlikli şəbəkələrarası ekranlara tələbatlar.**

**Daxil olmanın idarə edilməsi**. Şəbəkələrarası ekran şəbəkə səviyyəsində filtrləşməni təmin etməlidir.Filtrləşmə üzrə qərar hər bir şəbəkə paketi üçün göndərənin və qəbul edənin şəbəkə ünvanından və ya digər evivalent atributlar əsasında olmasından asılı olmayaraq,hər bir şəbəkə paketi üçün qəbul oluna bilər [8].

**İnzibatçılıq:qeydiyyat**. Şəbəkələrarası ekran inzibatçının sistemə (sistemdən) giriş (çıxışının) qeydiyyatını,həmçinin,yüklənmə hadisəsi və sistemin və onun proqram əsasının inisializasiyasını təmin etməlidir.Sistemdən çıxışın qeydiyyatı brandmauerin aparat söndürülməsi zamanı yerinə yetirilmir.Qeydiyyat parametr­lərində aşağıdakılar göstərilməlidir:

-zaman,tarix və qeydiyyat aparılan hadisənin kodu;

-qeyd olunan hadiə cəhdinin nəticəsi uğurlu və ya uğursuz;

-qeyd olunan hadisə cəhdi zamanı şəbəkələrarası ekran inzibatçısının identifikatoru.

**Tamlıq**. Şəbəkələrarası ekran özünün proqram və informasiya sahəsinin tamlığına nəzarət vasitələrinə malik olmalıdır.Bərpa. Şəbəkələrarası ekran vəsa­it­lərin nasazlıq və işdən imtina zamanı bərpa prosesini nəzərdə tutmalıdır.

**Testləşdirmə.** Şəbəkələrarası ekranda reqlamentli testləşmə imkanı təmin olunmalıdır:

-filtrləşmə qaydalarının həyata keçirilməsi;

-inzibatçının identifikasiya və autentifikasiyası;

-inzibatçının fəaliyyətinin qeydiyyatı prosesi;

-şəbəkələrarası ekranın proqram və informasiya,sahəsinin tamlığına nəzarət

prosesi;

-bərpa proseduru.

**Şəbəkələrarası ekran inzibatçısının rəhbərliyi.** Sənəddə aşağıdakılar olma­lıdır:

-brandmauerin nəzarət altında olan funksiyalarının təfsilatı;

-şəbəkələrarası ekranın sazlanması və konfiqurasiyası üzrə rəhbərlik;

-brandmauerin startının təsviri və startın doğruluğunun yoxlanılması proseduru;

-bərpaetmə proseduru üzrə rəhbərlik/

**Test sənədləşməsi**. Şəbəkələrarası ekranın məruz qaldığı test və sınaqların təsviri və testləşmənin nəticələri olmalıdır. Konstrukto r(layihə) sənədləşməsi. Tərkibi:

-Şəbəkələrarası ekranın ümumi sxemi;

-Brandmauerin işinin ümumi təsviri;

-Filtrləşmə qaydalarının təsviri;

-Identifikasiya və autentifikasiya proses və vasitələrinin təsviri;

-Qeydiyyat vasitə və proseslərinin təsviri;

- Şəbəkələrarası ekranın proqram və informasiya sahəsinin tamlığına nəzarət vasitəsi və proseslərinin təsviri;

-Brandmauerin xüsusiyyətlərinin bərpa prosedurunun təsviri.

**1.21. Şəbəkələrarası qarşılıqlı təsir siyasətinin işlənib hazırlanması**

Şəbəkələrarası qarşılıqlı təsir siyasəti təşkilatda təhlükəsizlik siyasətinin elə hissəsidir ki o xarici mühitlə informasiya mübadiləsi təhlükəsizliyi tələbərinə cavab verir. Cari tələblər mütləq iki aspekti əks etməlidir [7]:

-şəbəkə servisinə daxil olma siyasəti;

-şəbəkələrarası ekranın işsiyasəti.

Şəbəkə servisinə daxil olma siyasəti kompyüter şəbəkəsinin təhlükəsizliyinin bütün mümkün servislərinin təqdim olunması,həmçinin də,istifadəsi qaydalarını müəyyən edir. Bu siyasət çərçivəsi daxilində uyğun olaraq bütün şəbəkə ekranı vasitəsilə təqdim olunan servislər mümkün ünvanlar verilməlidir;hər birservisin müştəriləri üçün. Bundan əlavə,nə zaman və hansı istifadəçinin hansı servis və kompyüterdən istifadə edə bilməsi qaydalarının təsviri də təqdim olunmalıdır. Ayrıca olaraq istifadəçi və kompyüterlərin autentifikasiya qaydaları da müəyyənləşdirilir Həm də təşkilatın qeyri-lokal şəbəkəsində istifadəçilərin iş şəraiti müəyyən ollunur.

Şəbəkələrarası ekranın iş siyasəti brandmauerin fəaliyyəti əsasında şəbəkələrarası qarşılıqlı təsirlərinin idarə olunmasının baza prinsipini təşkil edir. Bu iki prinsipidən biri seçilə bilər:

-açıq şəkildə icazə verilməyən hər bir şeu qadağan olunub;

-açıq şəkildə qadağan olunmayan hər bir şeyə icazə verilir.

Seçimdən asılı olaraq qərar təhlükəsizliyin xeyrinə şəbəkə servislərinin istifadə rahatlığının əleyhinə,həm də əksinə ola bilər. Birinci halda şəbəkələrarası ekran belə konfiqursiya oluna bilər ki,istənilən açıq şəkildə icazə verilməyən şəbəkələrarası qarşılıqlı təsirin qarşısnı alar.Nəzərə alsaq ki, belə yanaşma birmənalı olaraq üstünlük prinsipini minimuma endirir,o,təhlükəsizlik nöqteyi- nəzərində ən yaxşı hesab olunur. Burada inzibatçı unutqanlıq üzündən hansıs intiyaza icazələri saxlaya bilməz .Belə ki,onlar qəsdən deyilmədikdə belə qadağan olunacaqlar. Yolverilə bilən artıq servislər təhlükəsizliyin ziyanına istifadə oluna bilərlər. Bu da müxtəlif səhv və nöqsanlar ola bilən bağlı və mürəkkəb proqram təminatı üçün xrakterikdir. ”Açıq şəkildə icazə verilməyən hər bir şey qadağan olunub”prinsipi mahiyyət etibarı ilə naşılığın zərər verə biləcəyi faktının etirafıdır.

“Açıq şəkildə icazə verilməyən hər bir şey qadağan olunu”prinsipini seçərkən şəbəkələrarası ekran elə sazlanır ki, yalnız açıq şəkildə qadağan olunan şəbəkələrarası qarşılıqlı təsirləri bloklaşdırır. Bu halda istifadəçi tərəfindən şəbəkə sevislərindən istifadə rahatlığı artır,lakin şəbəkələrarası qarşılıqlı təsir təhlükəsizliyi azalır.İnzibatçı istifadəçi tərəfindən qadağan olunmuş bütün hərəkətləri nəzərə ala bilər. O, reaksiya vermı rejimindı işləməli olur. Şəbəkənin təhlükəsizliyinə mənfi təsir göstərən şəbəkələrarası fəaliyyət haqqında xəbərdarlıq etməli və onlrı qadağan etməlidir.

**1.22.Şəbəkələrrası ekranın qoşulma sxeminin müəyyənləşdirilməsi**

Şəbəkələrarası ekranların qoşulması üçün müxtəlif sxemlər var. Bunlar fəaliyyət şəraiti,həmçinin,brandmauerlərin şəbəkə interfeyslərinin miqdarından asılıdır.

Biz şəbəkə interfeysinə malik brandmauerlər həm təhlükəsizlik baxımından həm də konfuiqurasiya rahatlığı mövqeyindən kifayət qədər effektiv deyil. Onlar fiziki cəhətdən daxili və xarici şəbəkələrə sərhəd qoymur uyğun olaraq da şəbəkələrarası qarşılıqlı təsirin etibarlı müdafiəsini təmin edə bilmir [9,10]. Belə şəbəkələrarası ekran­ların sazlanması və onlarla bağlı maşurtlaşmanın sazlanması kifayət qədər mürək­kəb məsələdir. Onun dəyəri bir şəbəkə interfeysli brandmauerə dəyişilməsindən daha baha başa gəlir. Ona görə də yalnız iki və üç şəbəkə interfeysli şəbəkələrarası ekranlar qoşulmuş sxemlərə baxacağıq. Bu zaman təhlükəsiz lokal şəbəkəyə bağlı və açıq altşəbəkələrin məcmusu baxacağıq. Burada açıq altşəbəkə dedikdə poten­sial əks xrici şəbəkə tərəfindən tamamilə və ya qismən müdaxilə üçün açıq olan altşəbəkə nəzərdə tutulur. Açıq altşəbəkəyə məsələn ümumi müdaxilə mümkün olan WWW-FTP və SMTP serverləri,həmçinin,modem pulam terminal server daxil ola bilər.

Brandmauerin qoşulmasının bütün mümkn sxemləri arasında növbətilər tipik sayılır:

-lokal şəbəkənin vahid təhlükəsizlik sxemi;

-müdafiə olunan bağlı və mwdafiə olunmayan açıq altşəbəkələrlə sxem;

-bağlı və açıq altşəbəkələrin ayrılqda təhlükəsizlik sxemi.

Lokal şəbəkənin vahid təhlükəsizlik sxemi daha sadə həlldir.vBurada brandmauer bütövlükdə lokal şəbəkəni əks xarici şəbəkədən ekranlaşdırır. Maşurt­laşdırıcı və brandmauer arsıında bütün trafikin hərəkət etdiyi yeganə yol var. Adətən marşurtlaşdırcıı elə sazlanır ki, brandmauer yeganə kənardan görünən maşın olur .Lokal şəbəkəyə dxil oln açıq serverlər şəbəkələrarası ekranla qorunacaqlar. Lakin xarici şəbəkədən daxil ola bilən birləşmiş serverlər digər ünsürlərlə birlikdə şəbəkələrarası qarşılıqlı təsiir təhlükəsizliyini azaldır. Ona görə də cari brandmaueri qoşma sxemini məhz lokal şəbəkədə açıq serverlərin olmadığı halda və ya açıq serverlərin xarici şəbəkədən yalnız məhdud sayda istifadəçilər üçün daxil olma imkanı olduqda istifadə etmək olar.

Lokal şəbəkədaxlində ümumi müdaxilə olunabilən açıq serverlər olduqda onları açıq altşəbəkə kimi şəbəkələrarası ekrana qədər aparmaq məqsədəuyğundur. Cari üsul lokal şəbəkənin bağıı hissəsi üçün yüksək təhlükəsizliyə malikdir. Lakin,şəbəkələrarası ekrana qədər yerləşən açıq serverler üçün təhlükə­sizliyi aşağı səviyyədə təmin edir.

Bəzi brandmauerlər bu serverləri özlərində yerləşdirməyə imkan yaradırlar .Lakin, belə həll kompyüterin yüklənməsi vəbrnadmauerin özünün təhlükəsizliyi nöqteyi-nəzərindən çox da yaxşı həll deyil. Yuxarıda deyilənləri nəzərə alsaq belə qənaətə gəlmək olar ki, brandmauerin təhlükəsizliklə bağlı altşəbəkəyə birləşdi­rilməsi vətəhlükəsizliyi qorunmayan açıq altşəbəkəyə birləşdirilməsi yalnız açıq altşəbəkənin təhlükəsizliyinə yüksək tələbat olmadığı halllarda istifadə oluna bilər.

Açıq serverlərin təhlükəsizliyinin yüksək tələbat irəli sürüldüyü hallarda ayrılıqda bağlı və açıq təhlükəsizlikli altşəbəkə sxemlərindən istifadə etmək lazımdır. Belə sxem bir brandmauer üç şəbəkə interfeysi və ya iki brandmauer ikişəbəkə interfeysi əsasında qurlmalıdır [10]. Hər iki halda açıq və qapalı lokal şəbəkə altşəbəkələrinə daxil olma imkanı yalnız şəbəkələrarası ekran vaitəsilə mümkündür. Bu zaman açıq şəbəkəyə daxil olma imkanı qapalı altşəbəkəyə daxil olmağa imkaan vermir.

Sonuncu iki sxemdə şəbəkələrarası təhlükəsizliyinin daha böyük səviyyəsini iki brandmauerli sxem təmin edir ki, onlardan hər biri qapalı altşəbəkənin təhlü­kəsizliyinə ayrıca eşelon yaradır. Qorunan açıq altşəbəkə ekranlaşdırılan altşəbəkə kimi çıxış edir. Adətən ekranlaşdırılan altşəbəkə elə konfiqurasiya olunur ki,kompyüterə daxil olmanı əks xarici şəbəkəsindən həyata keçirir , həm də lokal şəbəkənin bağlı altşəbəkəsindən həyata keçirir. Lakin xarici şəbəkə və qapalı altşəbəkə arasında birbaşa informasiya paketi ilə mübadilə mümkün deyil.

Sistemin ekranlaşdırılmış altşəbəkə ilə hücumu zamanı heç olmasa,iki müstəqil müdafiə xəttini qırmaq lazımdır ki, bu da çox çətin məsələdir.Şəbəkələrarası ekranların vəziyyətlərinin monitorinqi vasitələri praktiki olaraq bu cəhdi qaçılmaz olaraq,aşkara çıxaracaqlar və sitemin inzibatçısı vaxtında icazəsiz daxil olma cəhdinin qarşısını almaq üçün lazımi tədbirıər görəcək.

Diqqət yetirmək lazımdır ki, uzaqlaşdırılmış (kənarlaşdırılmış) istifadəçilərin kommutasiya rabitə xətləri vasitəsilə qoşulmasının həm də təşkilatının apardığı təhlükəsizlik siyasəti ilə uyğunluğu da yoxlanılmalıdır .Bu məsələnin tipik həlli-lazımi funksional imkanlara malik kənarlaşdırılmış daxil olma serverini(terminal server) quraşdırılmasıdır. Məsələn, Annex şirkətinin Bay Networks terminal serveri. Terminal server bir neçə asinxron port və lokal şəbəkənin interfeysi ilə sistem təşkil edir. Asinxron port və lokal şəbəkə arasında informasiya mmübadiləsi yalnız xarici istifadəçinin uyğun autentifikasiyasından sonra həyata keçirilir. Terminal serverin qoşulması elə həyta keçirilməlidir ki,iş yalnız şəbəkələrarası ekranın vasitəsilə yerinə yetirilsin. Bu kənarlaşdırılmış istifadəçilərin təşkilatın informasiya vasitəlirindən istifadəsi zamanı lazıımi səviyyədə təhlükəsizlik əldə edilməsinə görə azımdır. Belə qoşulma terminal server açıq altşəbəkələrin tərkibinə daxil olduğunda mümkündür.

Bu zaman açıq və qapalı altşəbəkələrin ayrı-ayrı təhlükəsizlikli brandmauerlərinin qoşulma sxemlərindən istifadə olunur. Terminal serverin proqram təminatı kommutasiya kanalları vasitəsilə rabitə seanslarına nəzarət və inzibatçılq etmək imkanlarına malik olmalıdır.Müasir terminal serverlərinin idarəetmə modulları aşağıdakı funksiyaları yerinə yetirməklə müştərilərin daxil olmasını məhdudlaşdırır və serverin öz təhlükəsizliyini təmin etmək üçün kifayət qədər geniş imkanlara malikdir.

-PPP protokolu üzrə kənarlaşdırılmış daxil olma müraciətləri üçün lokal paroldan

istifadə olunması (həmçinin inzbatçının müdaxiləsi üçün);

-lokal şəbəkənin hansısa maşını ilə autentifikasiyaya sorğunun istifadəsi;

-xarici autentifikasiya vasitələrindən istifadə;

-terminal serverin portlarına daxil olma üçün nəzarət siyahısının tərtibi;

-terminal serverdən rabitə seanslarının protokolaşdırılması.

**1.23. Brandmauerin fəaliyyət parametrlərinin sazlanması**

Şəbəkələrarası ekran kompyüter həmçinin onda fəaliyyyət göstərən əməliyyat sitemi (ƏS) və xüsusi proqram təminatından ibarət proqram-aparat təhlükəsizlik kompleksindən ibarətdir. Qeyd etmək lazımdır ki ,bu xüsusi proqram təminatını çox vaxt brandmauer də adlandırırlar [14]. Kompyüterin brandmaueri kifayət qədər güclü və fiziki cəhətdən təhlükəsiz olmalıdır. Məsələn, Xüsusi kənarda yerləşən və qorunan ərazidə yerləşməlidir. Bundan başqa onun ƏS-nin yüklənməsindən icazəsizdaşıyıcılardan müdafiə vasitələri olmalıdır.

Brandmauerin əməliyyat sistemi bir sıra tələblərə cavab verməlidir:

-sistemin vasitələrinə daxil olmağa məhdudiyyət qoyan vasitələrin olması;

-təqdim olunan proqram interfeysindən yan ötərək kompyüter vasitələrinə daxil

olmağın qarşısını almaq;

-lokal şəbəkədən öz vasitələrinə üstünlük dərəcəsi ilə daxil olmanı qadağan

etmək;

-istənilən inzibati fəaliyyət monitorinqi(auditi)vasitələrinə malik olmaq.

Göstərilən tələbatlara OC UNİX ,həmçinin ,Microsoft Windows NT müxtəlif növləri cavab verir.Seçilmiş əməliyyat sistemi brandmaueri onun konfiqura­siya­sını kompyüterə quraşdırdıqdan sonra bütün şəbəkələrarası ekranın fəaliyyət parametrlərini sazlamağa başlamaq olar Bu proses növbəti mərhələdən ibarətdir:

-şəbəkələrarası ekranın iş qaydalarının işlənilməsi şəbəkələrarası qarşılıqlı fəaliyyət siyasətinə uyğun olmalı və qaydalar brandmauer interfeysində təsvir olunmalıdır;

-bu qaydaların ziddiyyətli olmamasının yoxlanılması;

-brandmauerin sazlanma parametrlərinin şəbəkələrarası qarşılıqlı fəaliyyət siyasəti ilə uyğun olmasının yoxlanılması.

Birinci mərhələdə formalaşdırılan şəbəkələrarası ekranın iş qaydaları bazası şəbəkələrarası qarşılıqlı fəaliyyət siyasətinin formalaşdırılmış təsviridir. Qaydaların komponentləri müdafiə olunan obyektlər,istfiadəçilər və servislərdir.

Müdafiə olunan obyektlərə bir şəbəkə interfeysiolan adi kompyüterlər şylüzlər (bir neçə şəbəkə interfeysi olan kompyüterlər), marşrutlaşdırıcılar, şəbəkələr idarəetmə sahələri daxil ola bilərlər. Müdafiə olunan bir obyekt şəbəkə ünvanı altşəbəkə maskası və.s kimi atributlar dəstinə malikdir. Bu atributlardan bir hissəsini əllə verməli, qalanları isə avtomatik olaraq informasiya bazasından, məsələn, NIS/NIS+, SNMP MIB, DNS götürmək olar. Obyektlərin tam təsvirinin vacib olduğuna diqqət vermək lazımdır, beləki, ekranlaşdırma qayda­larının düzgünnlüyününn şlyüzlər və marşurtlaşdırıcıların şəbəkə interfeyslərinin təyin olunduğu halda əmin SNMP-agentindən almaq olar [12].

Şəbəkələrarası ekranın iş qaydalarını təsvir edərkən istifadəçilər giriş adları ilə adlandırılır və qruplara bölünürlər .İstifadəçilər üçün icazə verilən başlanğıc və məqsədli şəbəkə ünvanları,tarix diapazonu ə iş müddəti,həmçinin,autentifikasiya sxemi və qaydası göstərilir.

İstifadə olunan servislər dəstinin müəyyənləşdirilməsi kifayət qədər TCP/IP servislər dəstinə malik brandmauer verilənlər bazası əsasında həyata keçirilir. Qeyri-standart servislər xüsusi atributlar vasitəsilə əl ilə verilə bilər. Müasir brandmauerlər bütün standart servislərin TCP/IP əvvəlcədən hazırlanmış təyinatlarına malikdirlər. Onlar dörd qrupa bölünürlər-TCP UDP RPC ICHP.

TCP sevislərinin tam nəzarət oluna bilən servislərdir. Belə ki,asan diaqnostika olunan virtual birləşmələr əsasında təqdim olunur və istifadə olunurlar.

UDP servisləri ənənəvi olaraq filtrləşmə üçün çətindirlər. Belə ki, virtual birləşmənin qurulma fazası mövcüd deyil. Müştəri və server arasında dialoq konteksti kimidir. Brandmuerin bu kontrksti özü hesablaya bilər. Şəbəkələrarası ekranı hər iki istiqamətdə kəsən bütün UDP paketlərini nəzərdən keçirir və sorğulara cavablar verir. Nəticədə deytaqram protokolu üçün virtual birləşmə analoqu adlanır. Belə birləşməənin bütün qeyri-leqal cəhdləri isə qurulmuş birləşmələrdə kənar deytaqrammalar kimi şəbəkələrarası qarşılıqlı fəaliyyət siyasətinə uyğun emal olunurlar.

RPC-servisləri istifadə olunan portlarda nömrələrin dəyişkən olduqları üçün filtrləşmə üçün mürəkkəbdirlər. Brandmauerlər RPC trafikinə nəzarət edir, PORT­MAP­PER funksiyasına sorğular üzrə çıxarır və cavablardan portların qeyd olunmuş nömrələrini üzə çıxarırlar.

İCMP protokolu İP protokolunun özü ilə birgə səhvlər haqqında informasiya yoxlama məlumatları göndərmək həmçinin şəbəkənin bütövlükdə test edilməsi üçün istifadə olunur. İCMP protokolu üçün portlar konsepsiyasınan isrifadə olunmur. Burada Servisin tipini göstərmək üçün 0-dan 255 qədər ədədlərdən istfiadə olunur ki,onlar da ünvanlarla birlikdə şəbəkələrarası qarşılıqlı fəaliyyətə nəzarətdə nəzərə alınlrlar.

Qaydalar bazası formalaşdıqdan sonra onun ziddiyyətliyi yoxlanılır. Bu xüsusi vacib məsələdir. Əsasən də mürəkkəb siyasətli şəbəkələrarası qarşılıqlı fəaliyəət konfiqurasiyali çoxkomponentli şəbəkələr üçün daha vacib imkanı olmadan çox saylı səhv və zəifliklərin yaranması qaçılmaz olardı. Formalaşmış qaydaların ziddiyyətliyinin yoxlanılması avtomatik yerinə yetirilir [7,15]. Üzə çıxmış qeyri-birmənalıqlar ziddiyyətli qaydaların redaktə olunması ilə aradan qaldırılır. Qaydaların ram müəyyənləşməsi və səhvlərin aradan qaldırılmasından sonra inzibatçı tərəfindən kompliyasiya və filtrlərin quraşdırılması üzrə əlavə hərəkətlər tələb oluna bilər. Qaydalar bazasının formalaşmasından sonra bir çox brandmauerlər yekun sazlanmanı avtomatik olaraq yerinə yetirirlər.

Brandmauerin sazlanma parametrlərinin şəbəkələrarası qarşılıqlı fəaliyyət siyasətinə uyğunluğununun yoxlanması şəbəkələrarası ekranın iş protokolunun analizi əsasında yerinə yetirilə bilər. Lakin bir yoxlamanın daha çox nəticəviliyi şəbəkənin Təhlükəsizliyinin xüsusi analizi sisteminin istifadəsi nəticəsində əldə oluna bilər.

Belə sistemlərin daha parlaq nümayəndəsi İnternet Security Systems şirkətinin İnternet Scanner Safesuite proqramı paketidir.

Bu paketə daxil olan Fire Wall Scanner altsistemi şəbəkələrarası ekranlar konfiqurasiyasında zəif yerlərin axtarışını təmin edir və onların korreksiyası üçün məsləhətləri təqdim edir. Zəif yerlərin axtarışı şəbəkələrarası ekranların müxtəlif tipli təhlükəsizliyinin pozulması cəhdlərinə reaksiyaların yoxlanılması əsasında həyata keçirilir. Bu zaman bütün şəbəkə servislərininəki qeyd olunur və onlara müraciət şəbəkəlrarası ekran vasitəsilə həyata keçirilir.Fire Wall Scanner şəbəkəində daimi olaraq yüksək şəkildə təhlükəsizliyi saxlamaq üçün şəbəkələr­rası ekranın bir hissəsini quraşdırmaq lazımdır.

Şəbəkələrarası ekranı quraşdırarkən yadda saxlamaq lazımdır ki, digər vasitələr kimi o da,inzibatçının və istifadəçilərim kobudluğundan qoruya bilmir. Mühafizə olunan şəbəkəyə icazəsiz daxil olma,məsələn,asan tapıla bilən parolun seçilməsi ilə baş vere bilər [16]. Ekranlaşdıran sistem,həmçinin,nəzarətdə olmayan rabitə kanalına müdafiiədən də qoruya bilmir. Əgər potensial rəqabətdə olan xarici şəbəkə arasında nəzarətdən kənarda qalmış kanal varsa,onda brandmauer ondan gələn həmlənin qarşısını ala bilmir. Bu həm də verilənəri ötürən telefon kanallarına da aiddir. Əgər modem şəbəkələrarası ekrandan yan keçərək mühafizə olunan şəbəkənin daxilinə qoşulmağa imkan verirsə,onda təhlükəsizlik pozulacaq. Burada təhlükəsiliyin əsas prinsipini yadda saxlamaq lazımdır-sistem onun ən zəif bəndinin təhlükəsizliyi qədər təhlükəsizdir. Ona görə də ekranlaşdırılan sistemin informasiya mübadiləsinin daxili və xarici şəbəkələr arasındakı buütün kanallarına nəzarət etməsi vacibdir.

**FƏSİL II. SİMMETRİK ŞİFRƏLƏMƏ ÜSULLARININ TƏT­BİQİ İLƏ**

**KOMPYUTER ŞƏBƏKƏLƏRINDƏ INFORMASIYA**

**MÜHAFIZƏSININ IŞLƏNMƏSI**

**2.1. AT-BAŞ şifrələməsi (sadə şifrələmə)**

İnformasiya təhlükəsizliyinin təmin olunmasında bir sı­ra üsul­­lar­dan istifadə olunur. Bunalara sadə şifrələmə, mü­rək­­kəb üsulla şifrələmə, əvəzətmə və yerdəyişmə üsu­luna gö­rə şif­rə­ləmə və s. aiddir.

Məlumatı göndərən və alan tərəflər onun üzərində yalnız on­la­ra məlum olan çevirmələri (şifrələmə və deşif­rə­ləmə əmə­liy­yat­­larını) aparır. Şifrələmə alqoritmi kənar şəxs­lərə məlum olmur. Bir çox mü­təxəssislər gizli yazını kripto­qra­fi­ya hesab et­mirlər. Kodlaşdırma dedikdə açıq mətnin ele­ment­­lərinin (hə­rf­­ləri­nin, sözlərinin, cüm­lə­­ləri­nin və s.) müəy­­yən kodlarla əvəz olun­­ması başa dü­şü­lür. Kod­laş­dır­manın iki əsas növündən is­­-ti­fa­də olunur: sim­vol (analoq) kodlaş­dır­ılması və rəqəm (diskret) kod­­laş­dı­rılması [3].

Simvol kodlaşdırması zamanı ilkin mətnin əlifbasının hər bir hərfi bu və ya digər əlifbanın digər hərfi ilə əvəz olu­nur (Cədvəl 2.1). Simvol kodlaşdırmasına nümunə olaraq, Mor­ze əlif­bası­nı, şifrələmənin əvəzetmə və yer­də­­yişmə üsul­­­­ları­nı gös­tər­mək olar.

Cədvəl 2.1. Simvol kodlaşdırılması



Buna sadə şifrələmə, yəni at-baş şifrələməsi üsulu da de­­yi­lir. İl­­-kin məlumat bu şifrələməyə görə sürüş­dürü­lə­rək sim­vol­lar cü­­­tü ilə əvəz olunur. Yəni, hər hansı Xi=Xn-i şək­lin­də təsvir et­mək olar.

**2.2. Yerdəyişmə üsulu ilə şifrələmə**

Yerdəyişmə üsulununda istifadə ed­iləcək şifrə­­lər za­ma­nı, simvolların ötürülmə ardıcıllığını dəyişir, ancaq, sim­­vol­ların öl­çü­­ləri də­yişdiril­mir. Sındırılması mümkün ol­ma­­­­yan şifrə yar­at­­-maq əs­lində çox sadədir [5]. Bunun üçün lazım olan üsul artıq bir neçə on il­lər­dir ki, məlumdur. Belə ki, açar kimi istənilən bit sətri gö­tü­­rülür. Bu sətrin uzunluğu verilmiş mətnin uzun­lu­ğu ilə üst-üstə düşür. Maraqlı budur ki, şəbəkədə bir dəfəlik ar­d­ı­­­cıl­lıqla ötür­mə probleminin həlli çox qədim tarixi olan kvant me­­xa­­­­­­­ni­ka­­­sından gəlir.

**İzafilik:** Birinci kriptoqrafik prinsip belədir: bütün şifrə­lən­miş materiallar müəyyən izafiliyə malik olma­lı­dır, başqa söz­lə mə­­lumatı anlamaq üçün o lazım olan in­for­masiyaya ma­­­­lik ol­ma­­lı­dır. Mə­lu­ma­tın əks şifrələməsi za­ma­nı qə­b­ul­edi­ci onun doğru­lu­ğu­nu analiz vasitələri, hətta sadə he­­s­ab­la­ma­lar apar­­maqla ay­dın et­mək im­ka­nı­na malik olma­lı­dır. İzafilik qə­bul­edi­­­­ci­­­ləri yan­lış məlu­mat­larla (tərki­bin­də zi­bil ol­an, ar­xiv­ləş­dir­­mə eh­­tiyyat nüs­­xəsinin hazır­lan­ma­sı, ba­zanın sıx­ıl­ması, kor­­lan­mış ba­zanın bərpası) aldat­ma­ğa ça­lı­­şan pis­niy­yət­lilərin həm­­lə­­lə­rinə qarşı durmaq üçün la­zım­dır.

**İkinci kriptoqrafik prinsip:** Əvvəlcə göndərilmış məl­u­mat­­­­ların təkrar göndərilməsi ilə mübarizənin zəruri olma­sı­dır. Uy­­ğun üsullardan birisi hər bir məlumata, ha­ra­dasa yal­nız 10 sani­­yə ərzində doğru olan “ştampın” əla­və olunmasıdır.

**2.2.1.** **Birqat yerdəyişmə şifrələməsi**

Birqat yerdəyişmə şifrələməsində yalnız sütun dəyiş­di­ri­lir. Bu şifrələmədə açar həm rəqəmlərdən, həm­ də açar söz­dən isti­fa­­də olunur [5]. Biz öz nümunəmizdə hər iki üsuldan is­ti­fadə edə­­­cə­yik. Məslən: “Səhər üçdə gələ­cəm” cümləsini şifrələyək (cəd­vəl 2.2).

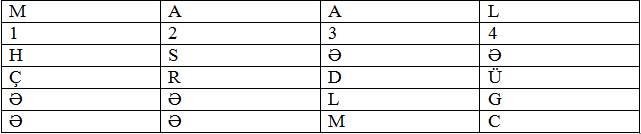
İlk olaraq məlumatımıza uyğun cədvəl qururuq və mə­lu­ma­tı­mı­zı cədvəldə yerləşdiririk. Sonra rəqəmləri ar­dı­­cıl­lıqla ya­zırıq. Yə­ni bizim açarımız rəqəmlə 2413, söz­­­lə AL­MA-dır və biz rə­qəm­li açarı cədvəldə ardıcıl olarıq yazı­rıq.

Cədvəl 2.2.

|  |  |  |  |
| --- | --- | --- | --- |
| A | L | M | A |
| 2 | 4 | 1 | 3 |
| S | Ə | H | Ə |
| R | Ü | Ç | D |
| Ə | G | Ə | L |
| Ə | C | Ə | M |

Növbəti cədvəldə açara görə sütunlarin yeri dəyiş­di­ri­lir və mə­­lumat şifrələnmiş olur. **Şifrələnmiş məlu­ma­tı­mız “HSƏ­Ə­ÇR­DÜƏƏL­­GƏƏMC” olur** (cədvəl 2.3).

Cədvəl 2.3.



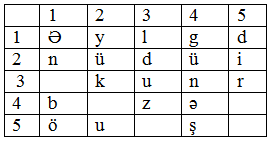
Deşifrələmə zamanı cədvəldə rəqəmlərin yazılma ar­dı­­­­cıl­lığı 2413 olur və məlumat deşifrələnir.

* + 1. **İki qat yerdəyişmə şifrələməsi**

Məxfi saxlamaq istədiyimiz məlumatın təhlükə­sizli­yi­ni tə­min etmək üçün həm sətirə, həm də sütuna görə şif­rə­lənmə apa­­­rıla bi­lər. Belə şifrələmə üsulu ikiqat yer­də­yiş­­mə adlanır. Yer­­­də­yiş­mə sütunlar və sətirlər üçün ayrı-ayrılıqda yerinə ye­ti­-rilir. Əv­vəl­cə cədvələ məlu­ma­tın mət­ni yazılır, sonra isə növbə ilə sü­tun­­­­ların yeri, daha son­ra isə sətirlərin yeri də­yiş­dirilir [8]. Şif-rənin açıl­ması (deşif­rə­lənməsi) zamanı yer­də­­yişmə qay­dası əks isti­qa­mət­­də tətbiq olunur. Yəni əvvəlcə sətirlər və sü­tunlar yer­də­yiş­mə ilə ilk vəziyyətə gətirilir, sonra isə mə­­lumat sütunlar üzrə oxu­­nur.

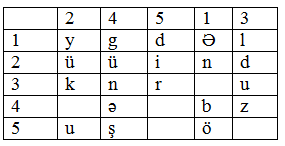
Yerdəyişmə variantlarının sayı 4x4 ölçülü cədvəl üçün 576, 5x5 ölçülü cədvəl üçün 14400 ədəd təşkil edir. Sadə birqat yerdəyişmədən fərqli olaraq ikiqat yer­də­yiş­mə­yə gö­rə ilkin mə­lu­matın şifrələnməsindən əvvəlcə sü­tun üz­rə, son­­ra isə sətr üzrə mə­lumatların yerdəyişmə prosesi baş ve­rir (cədvəl 2.4, 2.5). Bu­na misal olaraq birinci şif­rə­­ləmə cəd­və­lində açarlar ardıcıl­lığı­nın sütunlar üzrə dü­zəl­dilməsi apa­­rılır. İkinci mərhə­lə­də isə sətrlər

Cədvəl 2.4.

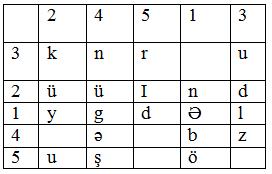


ardı­cıl­lı­ğı üz­rə nizam­lama aparılır və cədvəl 2.6-də isə həm sə­tir, həm də sütun elementlərinin yeri dəyişdirilir, belə­lik­lə açıq mətn şifrə­lə­nir. Açıq mətn: “Ən böyük ulduz Günəşdir”

Cədvəl 2.5.

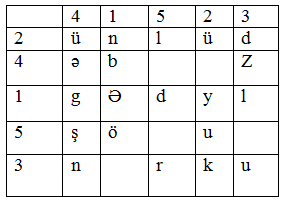


Cədvəl 2.6.



Cədvəl 2.7-də isə sütun və sətr element­lərinin ikinci dəfə yeri dəyişdirilir. Belə yerdəyişməyə ikiqat yerdəyişmə şifrələnməsi deyilir (cədvəl 2.8).

Cədvəl 2.7.



**Şifrələnmiş mətn:** ***ünlüd əb\_ \_z gƏdyl şö\_u\_ n\_rku***

Psütun=Psətir1xPsətir2x..... Psətirn.

logPsütun+logPsətir2+...+logPsətirn

log(1→2)=(NÜ)+(B\_)+(ƏY)+(ÖU)+(\_K)=2+8+0+6+7=23

log(1→3)=(ND)+(BZ)+(ƏL)+(Ö\_)+(\_u)=7+4+8+1+8=28

log(1→4)=(nü)+(bə)+( əg)+(öş)+(\_n)=2+1+1+0+7=11

log(1→5)=(nl)+(b\_)+(əd)+(ö\_)+(\_r)=6+8+4+1+7=26

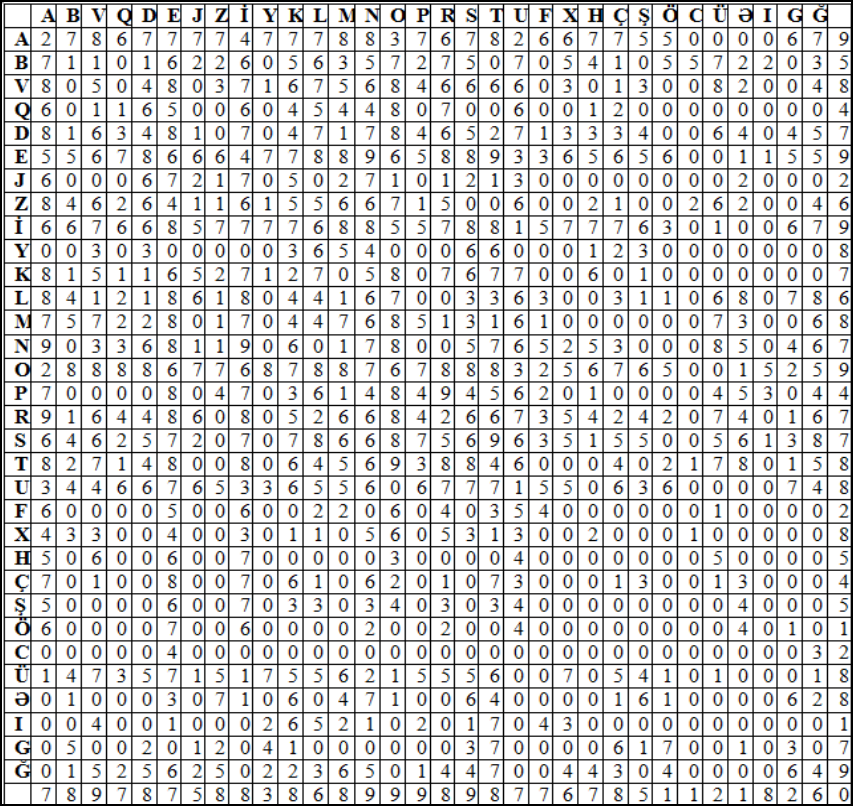
log(2→1)=(ün)+(\_b)+(yə)+(uö)+(k\_)=8+5+0+0+8=21

log(2→3)=(üd)+(\_z)+(yl)+(u\_)+(ku)=6+6+0+7+6=25

log(2→4)=(üü)+(\_ə)+(yg)+(uş)+(kn)=1+8+4+4+6=23

log(2→5)=(ül)+(\_\_)+(yd)+(u\_)+(kr)=6+0+0+7+5=18

Cədvəl 2.8.



log(3→1)=(dn)+(zb)+(lə)+(\_ö)+(u-)=6+2+0+6+7=21

log(3→2)=(dü)+(z\_)+(ly)+(\_u)+(uk)=5+8+6+8+7=34

log(3→4)=(dü)+(zə)+(lg)+(\_ş)+(un)=5+7+0+5+6=23

log(3→5)=(dl)+(z\_)+(ld)+(\_\_)+(ur)=1+8+7+0+7=23

log(4→1)=(ün)+(əb)+(gə)+(şö)+(n\_)=8+2+6+0+9=25

log(4→2)=(üü)+(ə\_)+(gy)+(şu)+(nk)=1+1+0+3+5=10

log(4→3)=(üd)+(əz)+(gl)+(ş\_)+(nu)=6+2+7+5+6=26

log(4→5)=(ül)+(ə\_)+(gd)+(ş\_)+(nr)=6+1+4+5+6=22

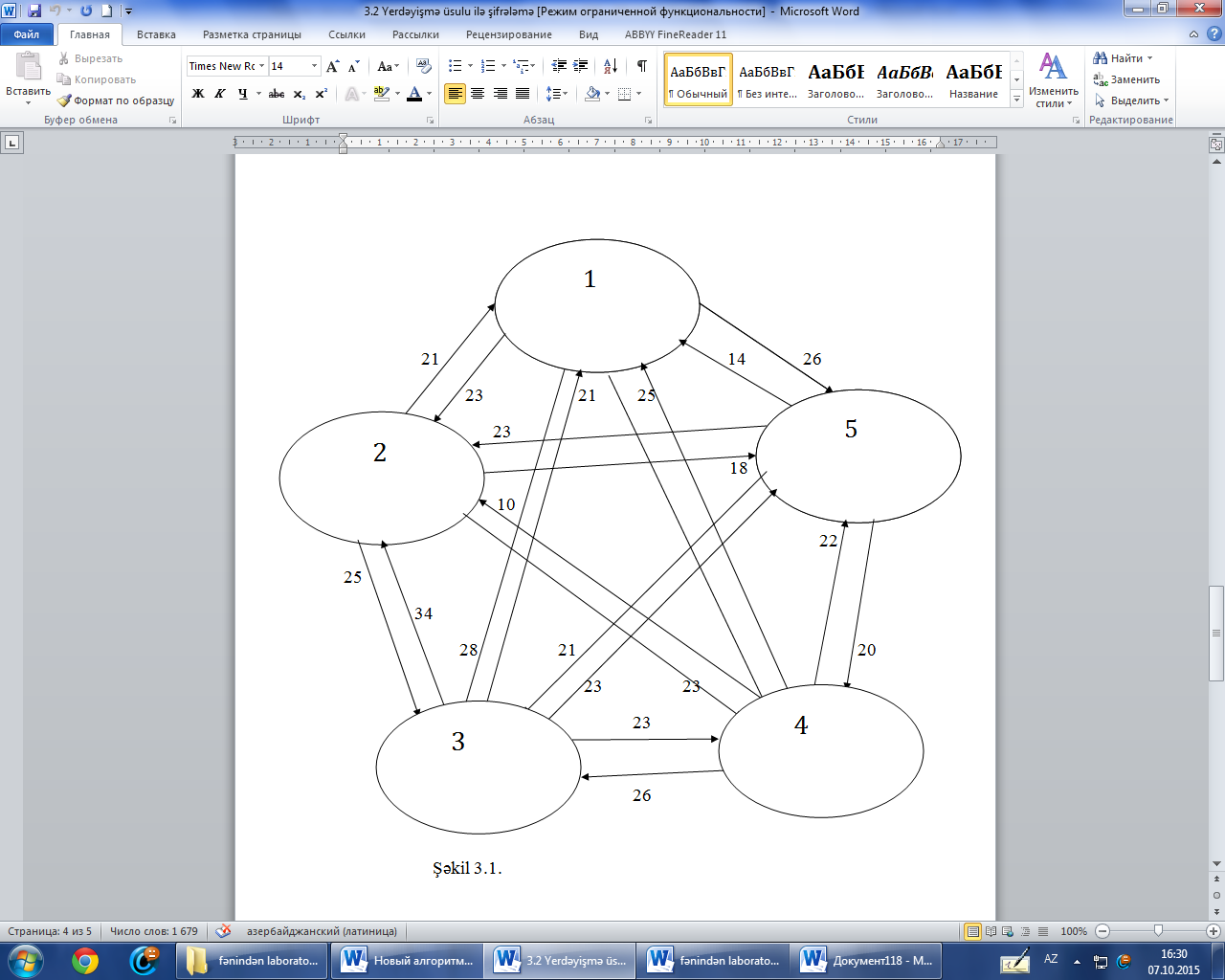
log(5→1)=(ln)+(\_b)+(də)+(\_ö)+(r\_)=0+5+0+1+8=14

log(5→2)=(lü)+(\_\_)+(dy)+(\_u)+(rk)=5+0+3+8+7=23

log(5→3)=(ld)+(\_z)+(dl)+(\_\_)+(ru)=7+6+1+0+7=21

log(5→4)=(lü)+(\_ə)+dg)+(\_ş)+(rn)=5+8+2+5+0=20

Log və cədvəl 2.8-ə əsasən şifrələmənin aşağıdakı sxe­mi­ni almaq olar şəkil 2.1.



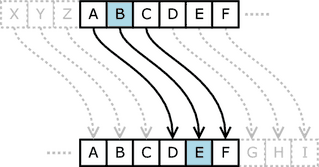
Şəkil 2.1. İkiqat yerdəyişmə üsulu ilə şifrələnmənin sxemi

Bu sxemdə bir sütundan digərinə keçən yol­ların sayı göstərilmişdir.

**2.3. Sezar şifrələməsi**

Sezar üsulu ilə şifrələmə qədim şifrələmə hesab olu­nur və bu­na görə hər bir simvol müəyyən sayadək öz ye­ri­ni di­gər bir sim­volla əvəz edir. Bu sadə əvəzetmə şifrə­lə­­mə­si he­sab olunur və məş­hur yunan imperatoru şə­rəfinə Yu­li Se­zar ad­landırılıb. Bu şifrə­ləməyə görə əlif­ba­nın hər bir sim­volu uyğun olaraq rəqəm şəklində nöm­rələnir və Se­zara gö­rə bu rəqəmlər üzərinə 1,3,5 əla­və etməklə şif­rə­­ləmə əmə­liy­­yatı aparılır. Əgər açıq mət­nin sim­vollarını X ilə işarə et­sək onda şifrələmə y=x+k(mod n) şəklində yazıl­mış olur. Bu­­rada k-açar sözü­­dür, n-əlifbanın sayı­dır. Daha aydın ət­raf­lı yazaq. Bizim eranın I əs­rin­də Yuli Sezar se­­na­ta gön­dər­diyi mək­tub­lar­dakı hərfləri əlif­ba­da 3 mövqe sü­rüş­­­­­­dürmə yo­lu ilə şif­rə­lə­yir­di. Belə ki, bu za­man mətnin hər bir hərfi əlif­­bada on­dan son­ra üçüncü möv­qe­də duran hərflə əvəz olu­­­­nur­du. Əgər hərf əlifbanın so­nun­da yerlə­şir­disə və on­dan son­­­­ra üç hərf yox idisə, on­da dairəvi prinsiplə əlif­banın əv­və­­­­­­li­nə ke­­­çir və sıranın növbəti hərfləri ki­mi oradakı hərf­­lər­­dən is­ti­­­­­fa­də olu­­nur­du. Aydındır ki, şifrə əvə­zet­mə üsul­la­rı sin­­finə da­­xil­dir.

Sezar şifrələməsi qədim şifrələmə üsullarından biri sa­yı­­lır və bu üsula görə hər bir simvol müəyyən mövqe, yə­ni müəyyən say­­­­da simvol qədər öz yerini digər bir sim­volla əvəz edir [14,16]. Bu şi­frələmədə əlif­banın hər bir simvolu uy­ğun olaraq rəqəm şək­­lin­­də nöm­rə­­lənir, Sezara görə bu rə­qəmlər üzərinə 1, 3 və ya­­xud 5 əla­­­­və etməklə şifrələmə əməliy­ya­tı aparılır. Əgər açıq mə­t­­­­­­­­nin sim­­­vollarını x ilə işarə etsək on­da şifrələmə *y=x+k(mod n)* şə­k­­­­lin­də ya­zıl­mış olur. Bunu sxematik olaraq aşa­ğıdakı kimi təs­­vir et­mək olar.



Sezar, məktublarındakı yazılarda hərfləri əlifba sırasına görə 3 mövqe sürüşdürürdü, məsələn "A" hərfi yerinə "D", "B" hərfi yerinə "E" istifadə edirdi (cədvəl 2.9). Olduqca sadə və hədəfinə çatan bu üsul o dövrün şərtləri üçün kafi olmuşdur.

Cədvəl 2.9.



Sezar şifrələməsini riyazi olaraq belə ifadə etmək olar;

*y=x+k (mod n).*

Burada y - şifrələnmiş məlumat, x - açıq məlumat ( şif­rə­lən­­mə­­miş məlumat), k-açar, n-simvolların sayıdır. Açar adə­­­tən tək ədədlər götürülür 3, 5, 7. Sezar sifrə­lə­mə­sinə aid bir nü­mumə gös­­­tərək. Məsələn; “ ***I GO TO SCHOOL***” cüm­lə­­si­ni Sezar şifrələməsi vasitəsilə şifrə­ləyək. *K=3, n=11*

I hərfi 9-cu sırada olduğuna görə 9-un üzərinə 3 əlavə edirik və I hərfi yerinə həmin hərfi L yazırıq (cədvəl 2.10).

I=9+3=12=L

G=7+3=10=J

O=15+3=18=R

T=20+3=23=W

O=15+3=18=R

S=19+3=21=V

C=3+3=6=F

H=8+3=11=K

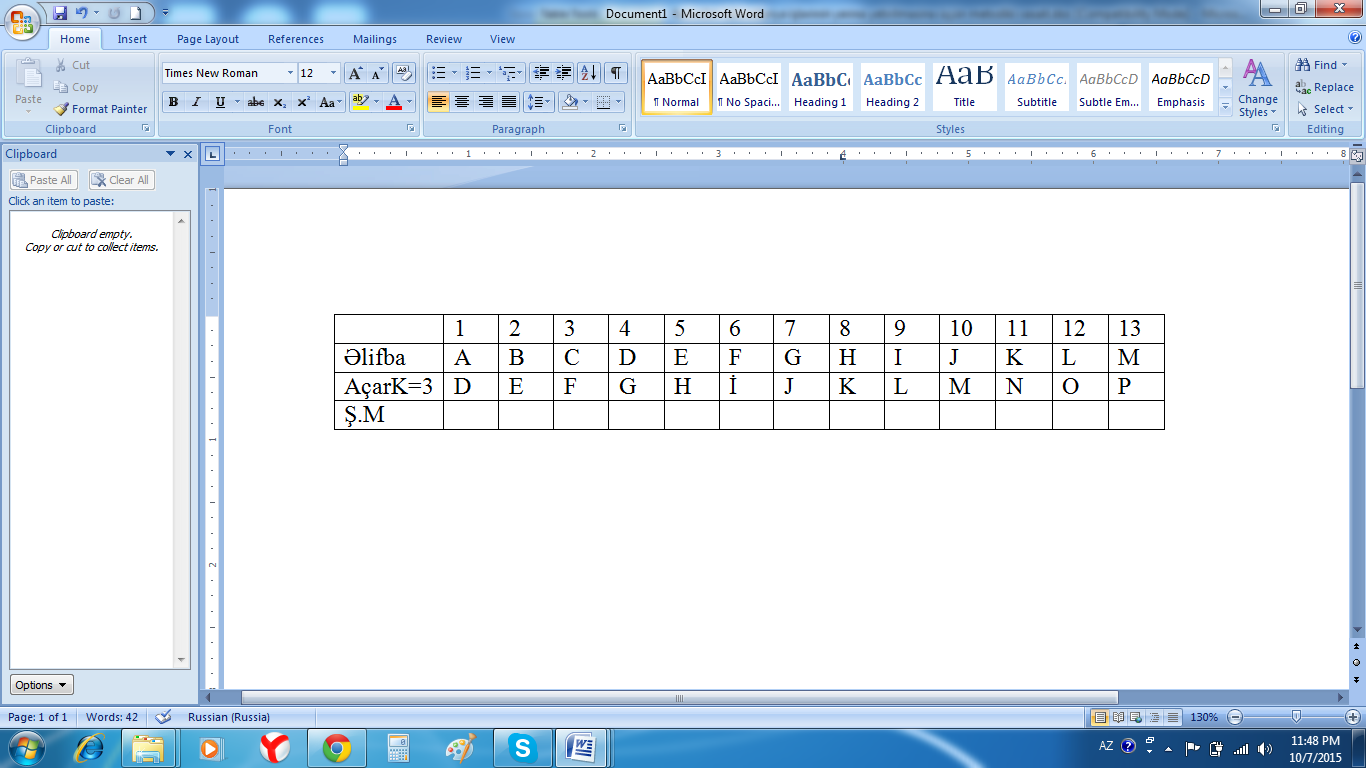
O=15+3=18=R

O=15+3=18=R

L=12+3=15=O

I GO TO SCHOOL L JR WR VFKRRO

Cədvəl 2.10.



Deşifrələmə apararkən bu əməliyyatların əksi apa­rı­lır. Yə­ni, L12-ci sırada olduğuna görə 12-dən açarımızı, yə­ni 3-ü çıxırıq və L hərfinin əvəzinə 12-3=9=I hərfini ya­zırıq.

L=12-3=9=I

J=10-3=7=G

R=18-3=15=O

W =23-3=20=T

R=18-3=15=O

V=22-3=19=S

F=6-3=3=C

K=11-3=8=H

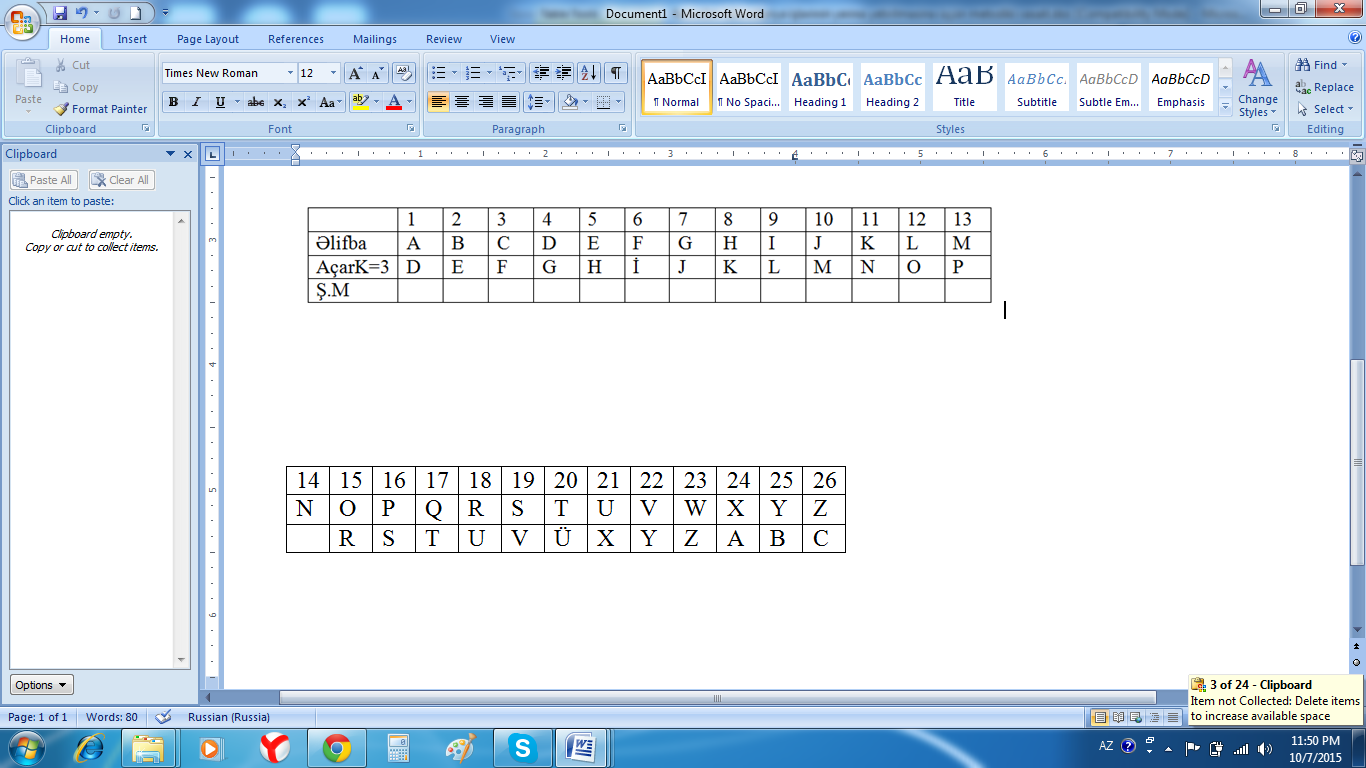
R=18-3=15=O

R=18-3=15=O

O=15-3=12=L

L JR WR VFKRRO I go to school

Cədvəl 2.11.



**2.4. Sehirli kvadrat şifrələməsi**

Orta əsrlərdə yerdəyişmə üsulu ilə şifrələmək üçün se­hirli kvad­ratlar tətbiq olunub. Sehirli kvadrat elə cəd­və­lə de­yi­lir ki, on­­ların xanalarına birdən başlayaraq kvad­ra­tın ölçü­sü­nə qədər ya­­­zılmış ədədlərin cəmi kvadratın hər bir dio­qa­nalı, sü­tun və sətri üzrə eyni olsun [19].

Şifrələnən mətn sehirli kvadratın xanalarına onların nöm­rələrinə uyğun yazılır. Əgər sonra belə cədvəlin tər­ki­­bini sətrlər üzrə yazsaq, onda ilk məlumatın şifrə­lən­miş mətnini ala­rıq. O vaxt­lar belə hesab edilirdi ki, sehirli kva­d­­rat üsulu ilə şifrələnən mətni təkcə şifrələnmə aça­rı yox, həm də sehirli kvadrat qo­ru­yur.

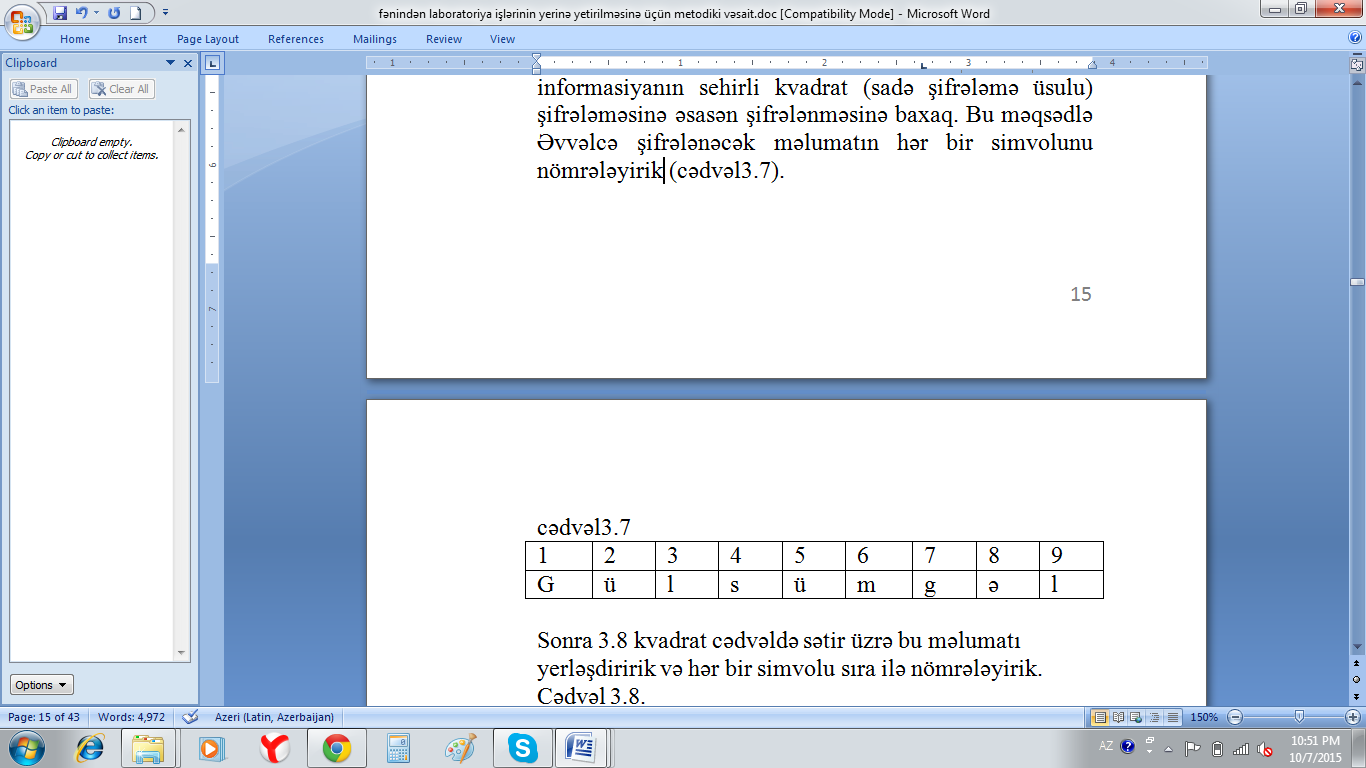
Sehrli kvadratlar həmişə riyaziyyatçıları və ümu­miy­yət­lə, əy­­­­­l­əncəli riyaziyyat həvəskarlarını maraq­lan­dır­mış­­dır. Se­hr­­li kva­­d­­­rat - bərabər sayda sətir və sütunlara bö­­lün­müş elə kva­d­ra­ta de­yilir ki, onun sətirləri, sütunları və diaqo­nal­la­rı üzrə yer­lə­şən müx­təlif ədədlərin cəmi ey­ni olsun.

Bütün belə mümkün sehrli kvadratların nəzəriyyəsi bu gü­­nü­müzədək hələ də tam şəkildə işlənilməmişdir. 2x2 ölçü­lü (yəni 2 sə­tir və 2 sütunu olan kvadrat) sehrli kva­drat yox­dur. 3x3 ölçülü sehr­li kvadratlar çoxdur. Ay­dın­dır ki, hər han­sı bir sehrli kvad­ra­tın öz mərkəzi ətrafında fır­lan­ma­sın­dan alınan kva­­drat da sehrli kva­d­­rat­­dır. Eləcə də, sehrli kva­d­­­ratın sə­tir­ləri­nin və ya sü­tun­ları­nın onun sim­metriya ox­la­rı­na nəzə­rən yer­də­yiş­­mə­si nəti­cə­sində də sehrli kvadrat alınır.

Nümunələrə keçək: 1-dən 9-a qədər ədədlərin əmələ gə­tir­diyi 3x3 ölçülü sehrli kvadratların sayı 8-dir.

Açıq məlumat “**Gülsüm gəl”** (sehirli kvadrat 3x3) olan in­for­masiyanın sehirli kvadrat (sadə şifrələmə üsu­­­­­­­­­lu) şifrə­lə­mə­sinə əsasən şifrələnməsinə baxaq. Bu məq­səd­­lə əvvəlcə şifrələnəcək məlumatın hər bir sim­vo­lu­nu nöm­­rə­­ləyirik (cədvəl 2.12).

Cədvəl 2.12.



Sonra 2.13 kvadrat cədvəldə sətir üzrə bu məlumatı yerləş­di­ri­rik və hər bir simvolu sıra ilə nömrələyirik.

Cədvəl 2.13.

|  |  |  |
| --- | --- | --- |
| 6 | 7 | 2 |
| 1 | 5 | 9 |
| 8 | 3 | 4 |

Şifrələmə zamanı ilk əvvəl məlumatımızı cədvəl 2.14- də­ki şəkildə yazırıq. Sonra sehirli kvadratı tətbiq edirik.

Cədvəl 2.14.

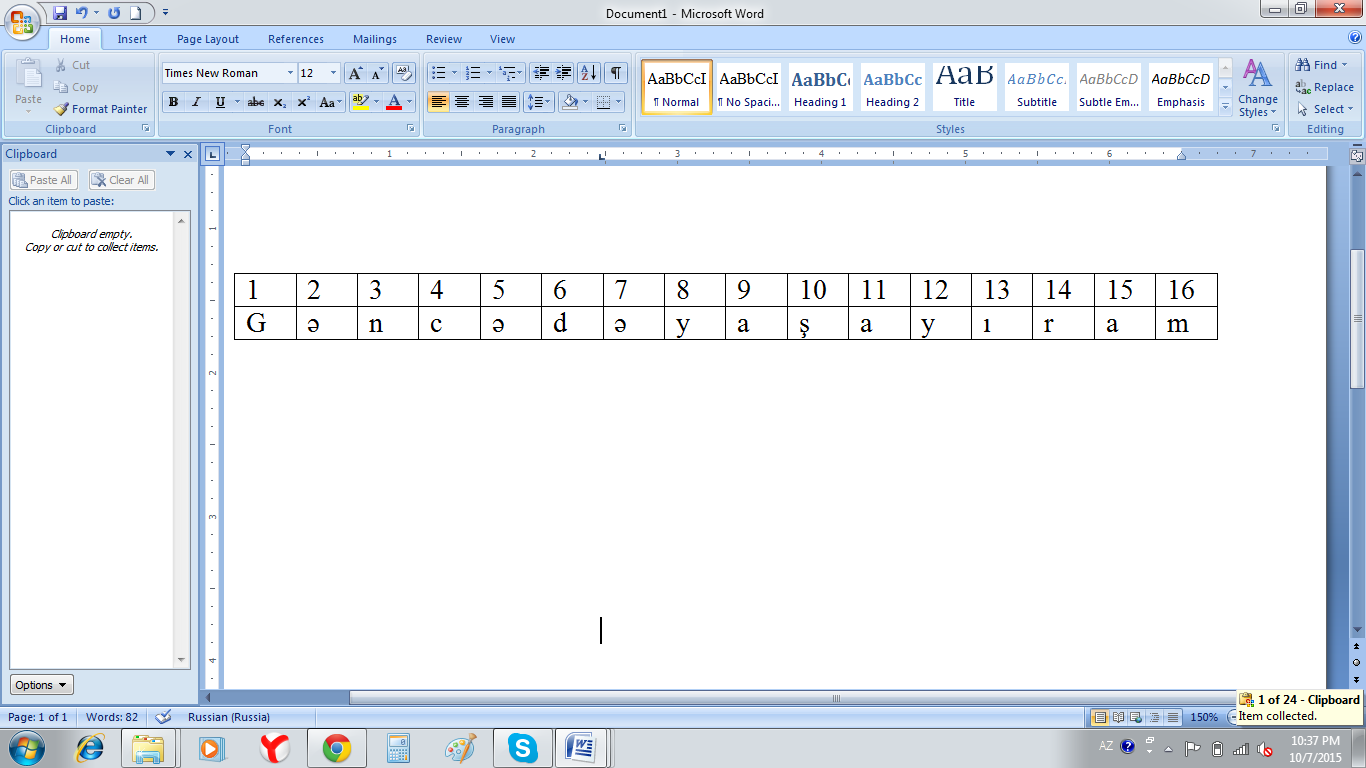
|  |  |  |
| --- | --- | --- |
| m | g | ü |
| g | ü | l |
| ə | l | s |

Mə­lu­­ma­tı­mız 9 simvoldan ibarət olduğu üçün sətir, sütun və dio­­­qa­nalların cəmi 15 olmalıdır (cədvəl 2.15).

Bunu  düsturu ilə müəyyən etmək olar.

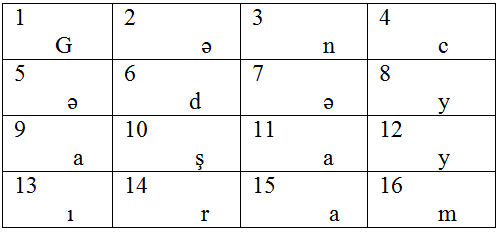
Açıq məlumat “**Gəncədə yaşayıram”** 4x4 sehirli kvadrat şifrələnməsinə baxaq. Cədvəl 2.15-də simvollarin nömrələnməsi verililmişdir.

Cədvəl 2.15.



Sehirli kvadrat tətbiq olduğu üçün cədvəl 2.16 alınır. Cədvəl 2.17-də isə məlumat şifrələnmiş halda olur. Cədvəl 2.18-də isə şifrələnmiş məlumatın sehirli kvadrata əsasən xanalara yerləş­di­ril­­məsi verilmişdir.

Cədvəl 2.16.



Cədvəl 2.17.

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 15 | 14 | 4 |
| 12 | 6 | 7 | 9 |
| 8 | 10 | 11 | 5 |
| 13 | 3 | 2 | 16 |

Cədvəl 2.18.

|  |  |  |  |
| --- | --- | --- | --- |
| G | a | r | c |
| y | d | ə | a |
| y | ş | a | ə |
| ı | n | ə | m |

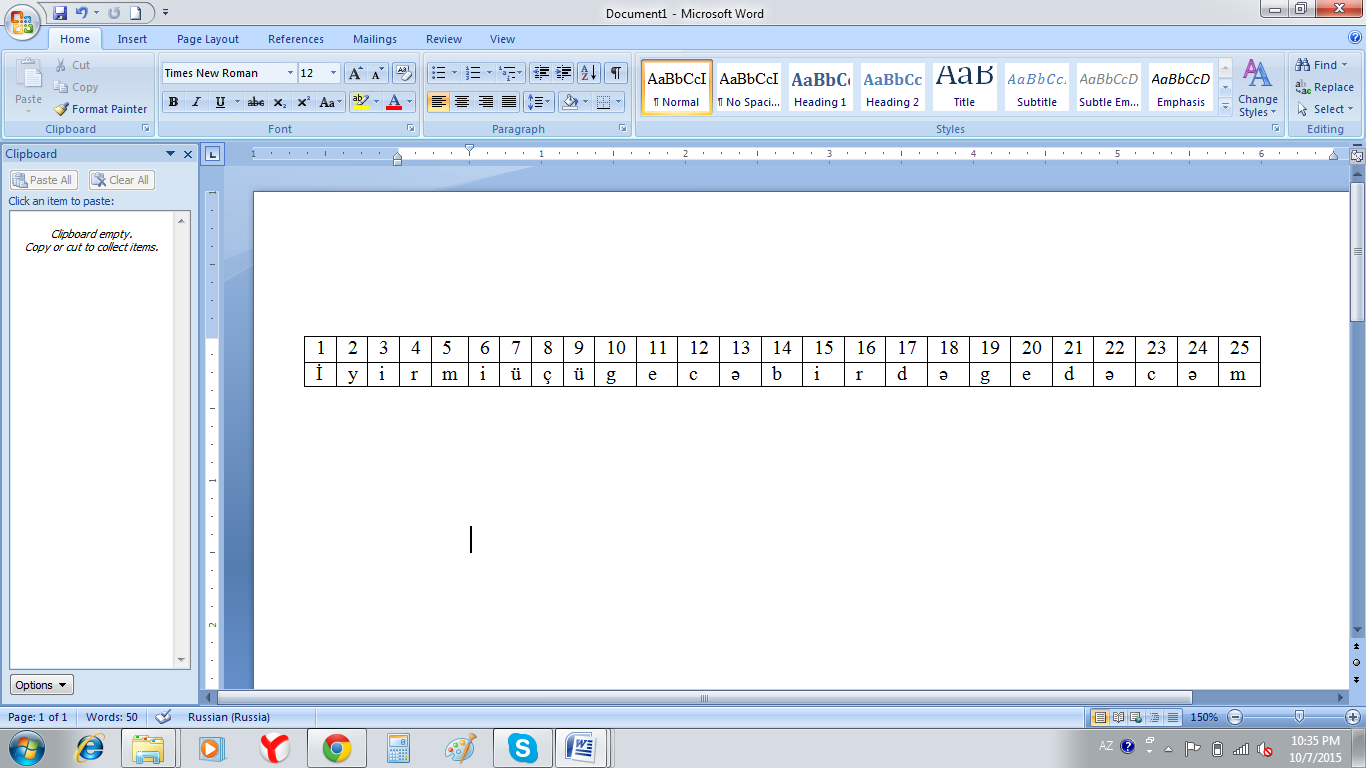
Kvadratın ölçüsünü artırdıqda mümkün sehrli kvad­rat­la­rın sa­­yı da sürətlə artır. Məsələn, müəyyən olun­muş­dur ki, 4x4 ölçülü sehr­li kvadratların sayı 880-dir. 5x5 öl­çülü sehrli kvad­ratların sa­yı isə 275 milyondan artıqdır.

Sehrli kvadratlara təkcə riyaziyyatçıların deyil, həm də təs­­­­vi­ri incəsənət, rəssamlıq kimi sahələrin ustalarının da əsər­­lərində rast gəlinir. Göründüyü kimi bu kvadrata 1-dən 16-ya­dək bütün na­tural ədədlər yazılmışdır. Sütun­lar­­da, sə­tir­lərdə və dia­qonal­lar­dakı ədədlərin cəmi 34-dür.

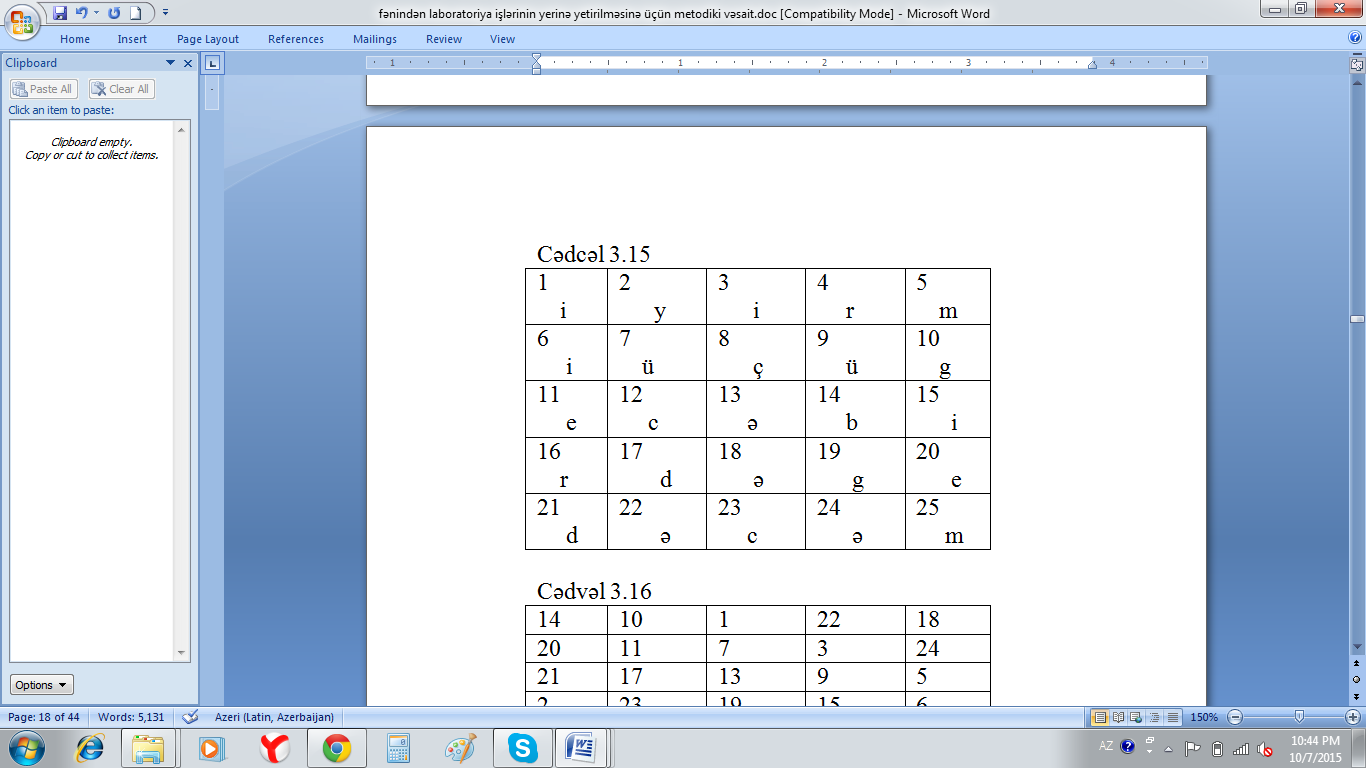
5x5-də şifrələmə zamanı kvadratın sətir, sütun və dio­qa­­nal­larının cəmi 65-ə bərabərdir.

Açıq məlumat “**İyirmi üçü gecə birdə gedəcəm”** (5x5) se­hir­li kvadratı ilə şifrələmə. Bu məlumatın şifrələnməsinə mi­sal olaraq aşağıdakı cədvəllərə baxaq (cədvəl 2.19, 2.20, 2.21, 2.22).

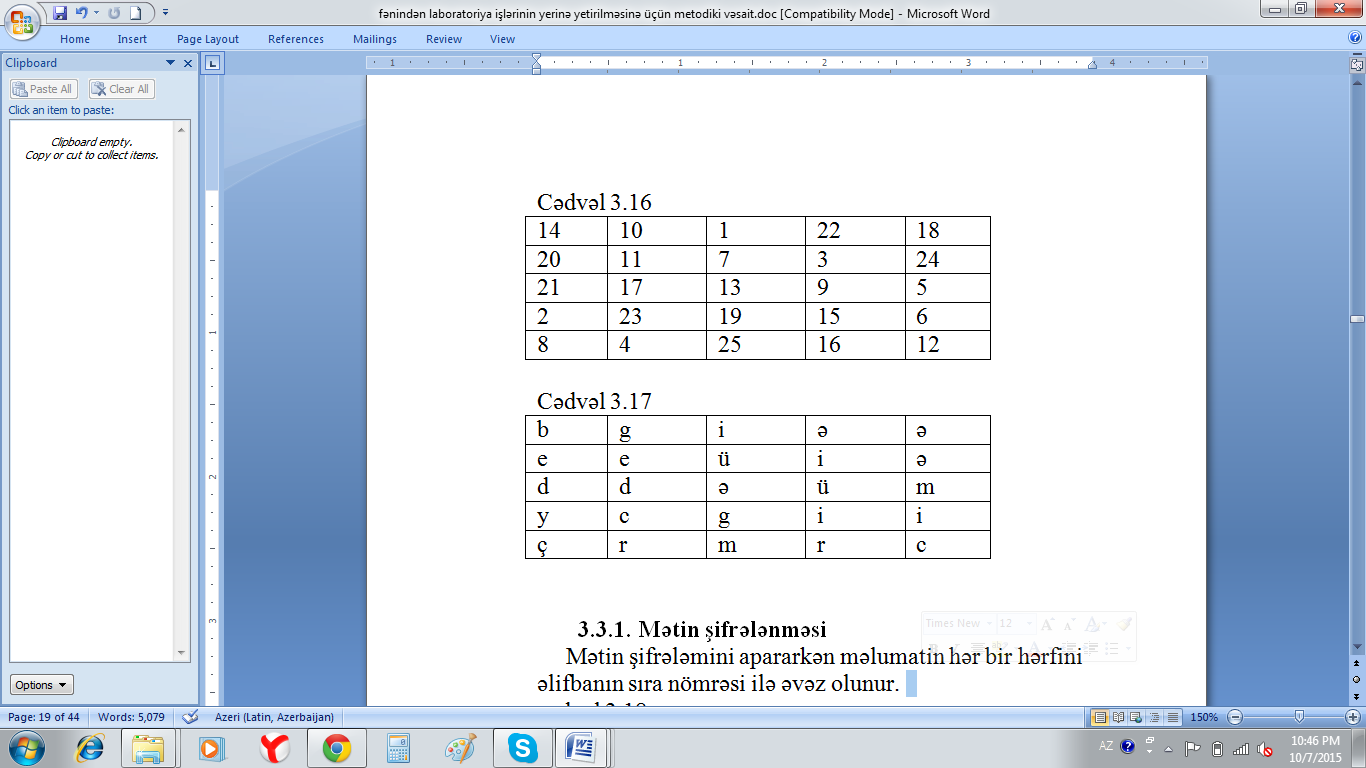
Cədvəl 2.19.



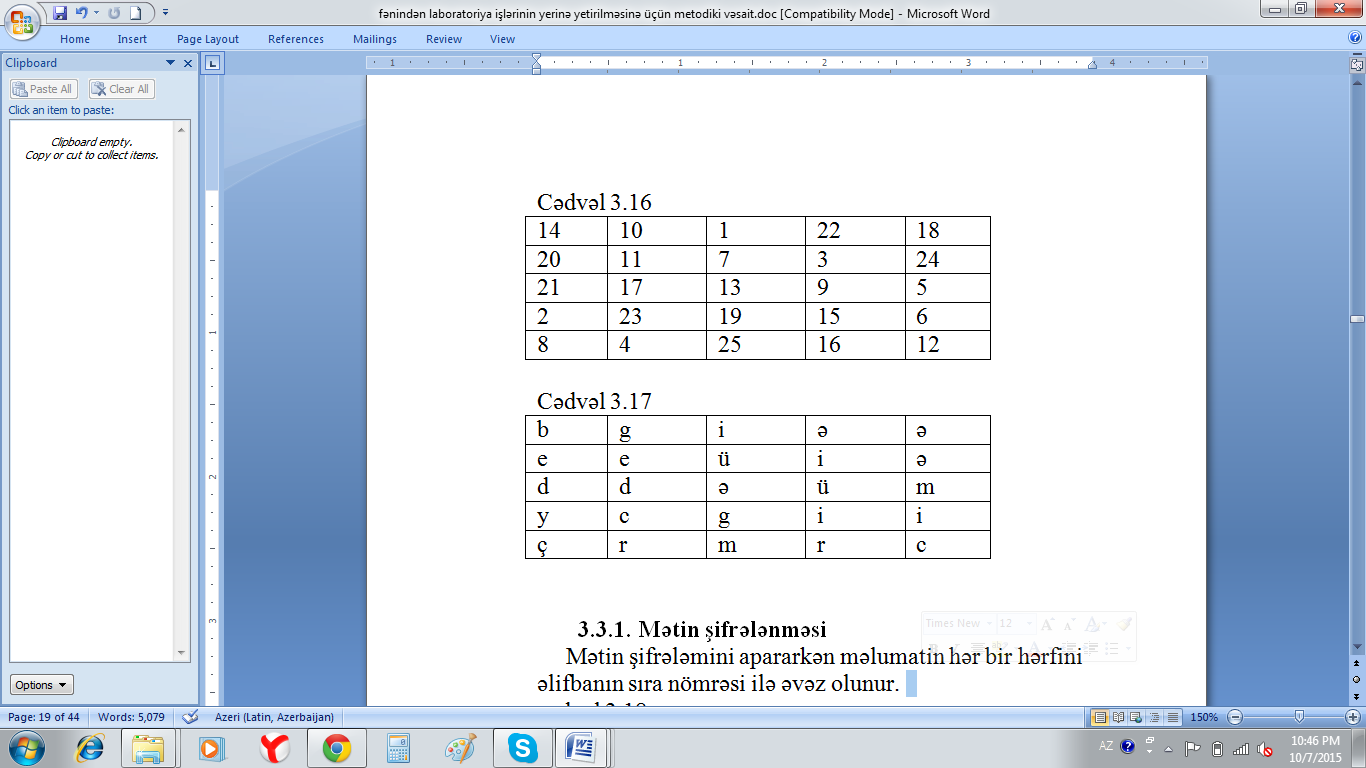
Cədvəl 2.20.



Cədvəl 2.21.



Cədvəl 2.22.

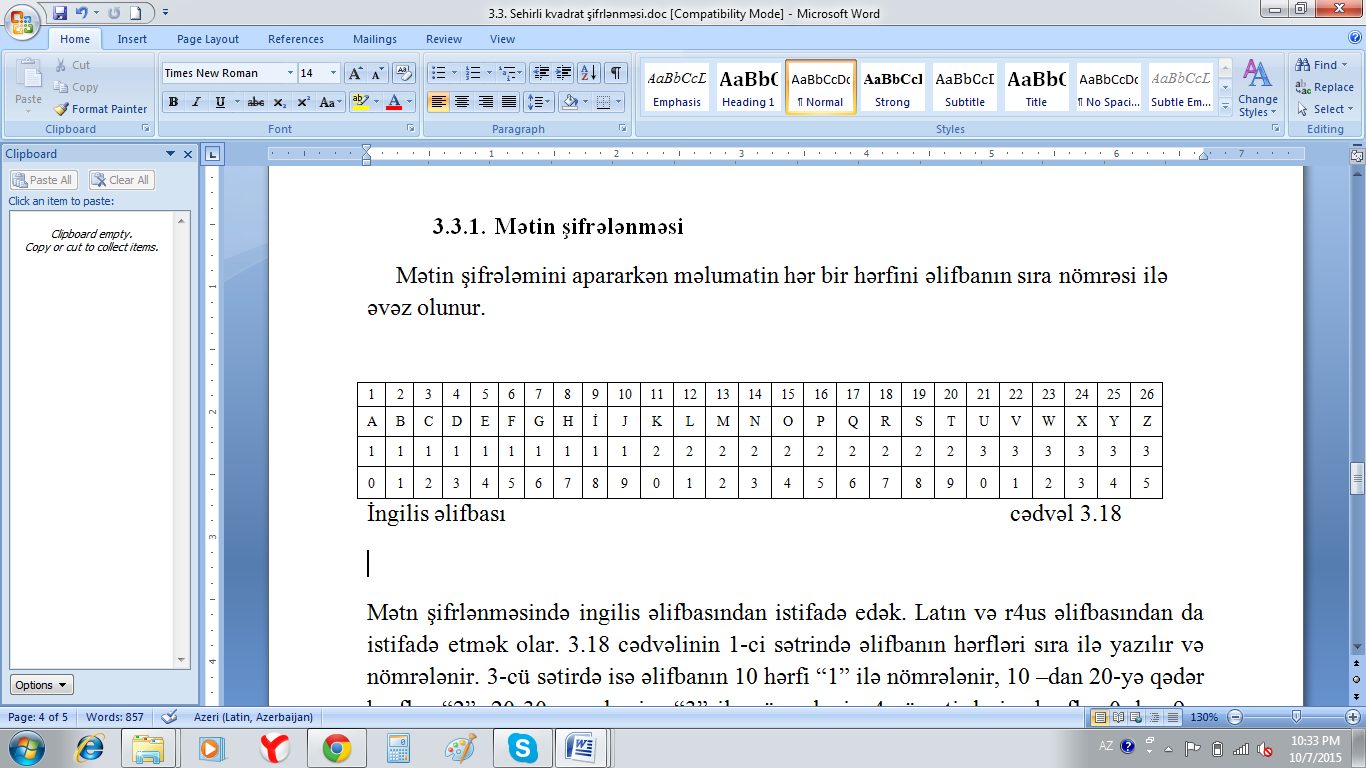


**2.4.1. Mətn şifrələnməsi**

Mətnin şifrələnməsini apararkən məlumatın hər bir hərfi əlifbanın sıra nömrəsi ilə əvəz olunur.

Mətn şifrələnməsində ingilis əlifbasından istifadə edək. La­tın və rus əlifbasından da istifadə etmək olar [20]. Cəd­və­l 2.23­-ün 1-ci sə­t­­­rində əlifbanın hərfləri sıra ilə ya­zı­­lır və nöm­rə­lə­nir. 3-cü sə­tirdə isə əlifbanın 10 hərfi “1” ilə nömrələnir, 10-dan 20-yə qə­­dər hərflər “2”, 20-30-a qədər isə “3” ilə nöm­­rələnir. 4-cü sə­tirdə isə hərflər 0-dan 9-a qədər nömrə­lə­nir. Məlumatı şifrə­ləmək üçün cəd­­­vəl­də hər şifrələnəcək rə­qə­­­min altında yerləşən rə­qəm­­lər (mi­sal üçün: H hərfinin al­tın­­­da 17, E hərfinin altında 14 və s.) ötürülərək ardıcıl yazıl­mış rəqəmlər yı­ğı­mı açıq mət­nin şif­rə­lən­­miş nömrəsi olur.

Cədvəl 2.23. İngilis əlifbası



Açıq məlumat: **“He learns English”**

H-17 E-14 L-21 E-14 A-10 R-27 N-23 S-28 E-14 N-23 G-16 L-21 I-18 S-28 H-17

“ He learn English’’-1714992114102723289914231621182817

**2.5.** **Qronsfeld üsulu ilə şifrələmə**

Bu üsul Sezar üsuluna uyğun olaraq mürəkkəb əvə­zetmə üsu­lu olub açarın modifikasiyasını özündə birləş­dirir. Bu üsu­­­la gö­rə açıq mətn açarın məzmununa uyğun olaraq rə­qəm­lə əvəz edi­lə­rək yazılır. Əgər açarın məz­mu­nu ilkin mət­­­nin məz­mu­nun­dan ki­çik olarsa onda aça­rın yazılması da­vam etdirilir və bu döv­rü olaraq təkrar edi­lir [17].

Qron­sfeld şifrələməsini yerinə yetirmək üçün açar söz­dən və əlifbanın hərflə­rinin sayına bərabər ölçüdə xü­susi şəkildə yara­dıl­mış kvadrat cədvəldən istifadə olu­nur.

Cədvəlin sətir və sütunları əlifbanın hərfləri ilə nöm­rə­­lə­nir və aşağıdakı kimi doldurulur:

* 1-ci sətir: əlifbanın N hərfi əvvəldən axıradək xa­na­lara ya­zı­lır.
* 2-ci sətir: ilk N-1 xanaya əlifbanın ikinci hər­fin­dən başlayaraq sonadək bütün hərfləri, N-ci xana­ya isə əlif­banın birinci hərfi yazılır.
* Sonuncu sətir: birinci xanaya əlifbanın N-ci hərfi və ikinci xanadan başlayaraq əlifbanın ilk N-1 hərfi ya­zı­lır.

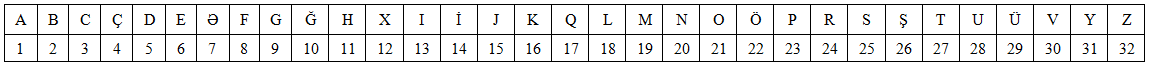
Şifrələmə zamanı ilkin mətn bir sətirdə, onun hərf­ləri­nin al­tın­­dan isə açar sözün hərfləri yazılır. Əgər açar sö­zün uzun­lu­ğun­­dan qısa olarsa, onda açar söz təkrar­lanır. İl­kin mətnin hərfi ona uyğun sütunla açar sözün onun al­­tın­da olan hərfinə uyğun sə­trin kəsişməsində duran hərflə əvəz olunur.

Qronsfeld şifrələməsində həm hərfə həm də rəqəmə görə şif­rə­­lən­mə aparılır.

Dediklərimizi ümumiləşdirsək Qronsfeld cədvəlini aşa­­ğı­da­kı ki­­mi təsvir edərək rəqəmə və hərfə görə şifrə­lən­­­mə apa­­ra bilə­rik:

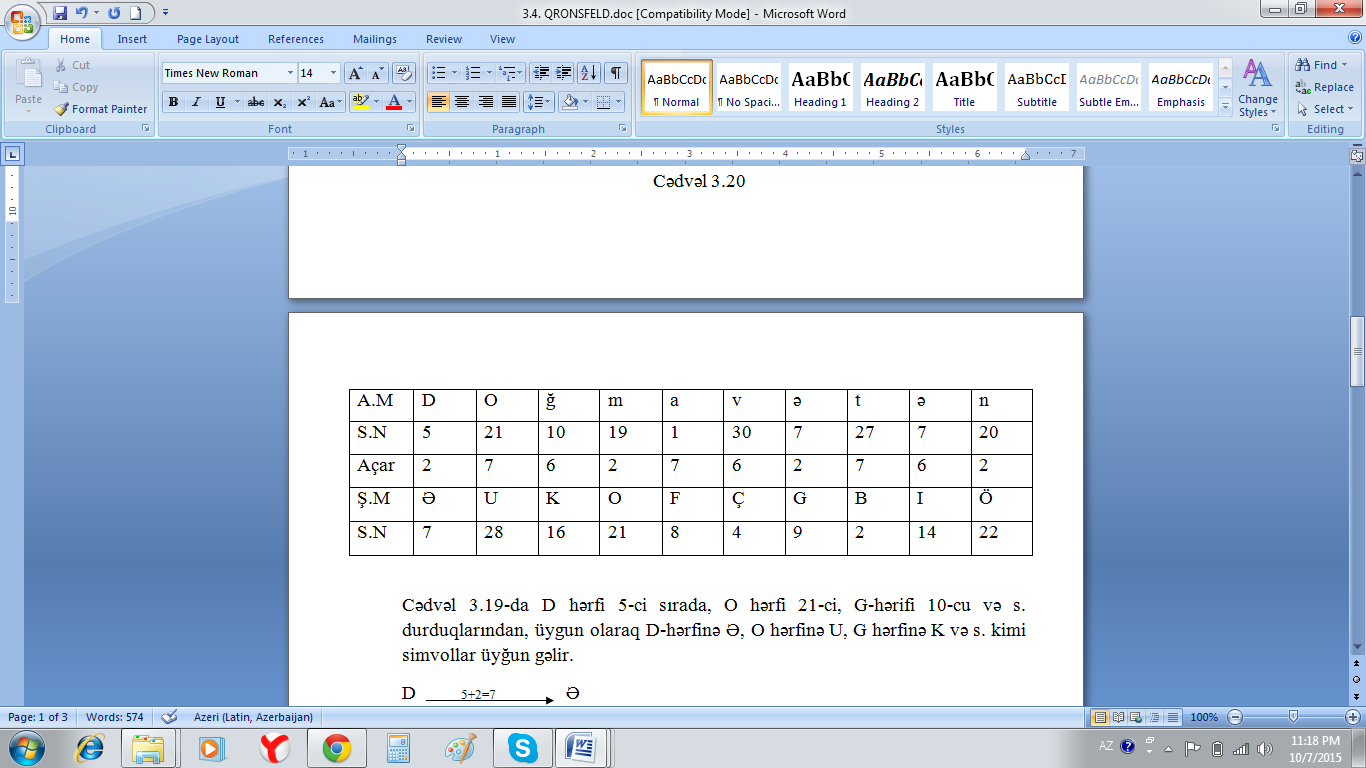
Şifrələmədə Azərbaycan əlifbasından istifadə edə­cə­yik ­(cədvəl 2.24).

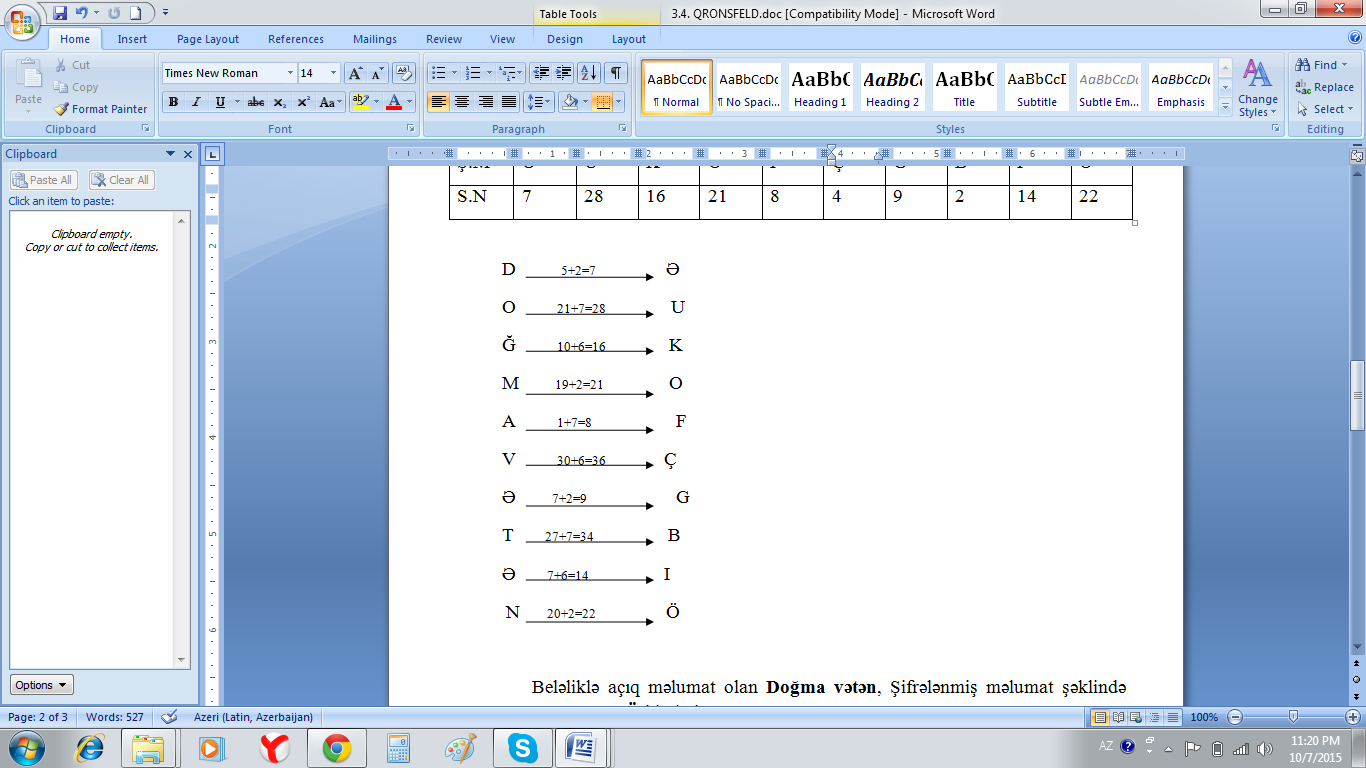
Cədvəl 2.24. Azərbaycan əlifbası



“Doğma vətən“ ifadəsini şifrələyək. Bunun üçün ilk əv­vəl aça­­rı seçək. Açarımız: **276**-dır. Yuxarıda qeyd olu­nan­la­ra əsa­sən cəd­vəl 2.25 alınır.

Cəd­vəl 2.25.





əlifbada 36 hərf olmadığından sürüsdürmə əlifbanın əvvəlinə qayıdır

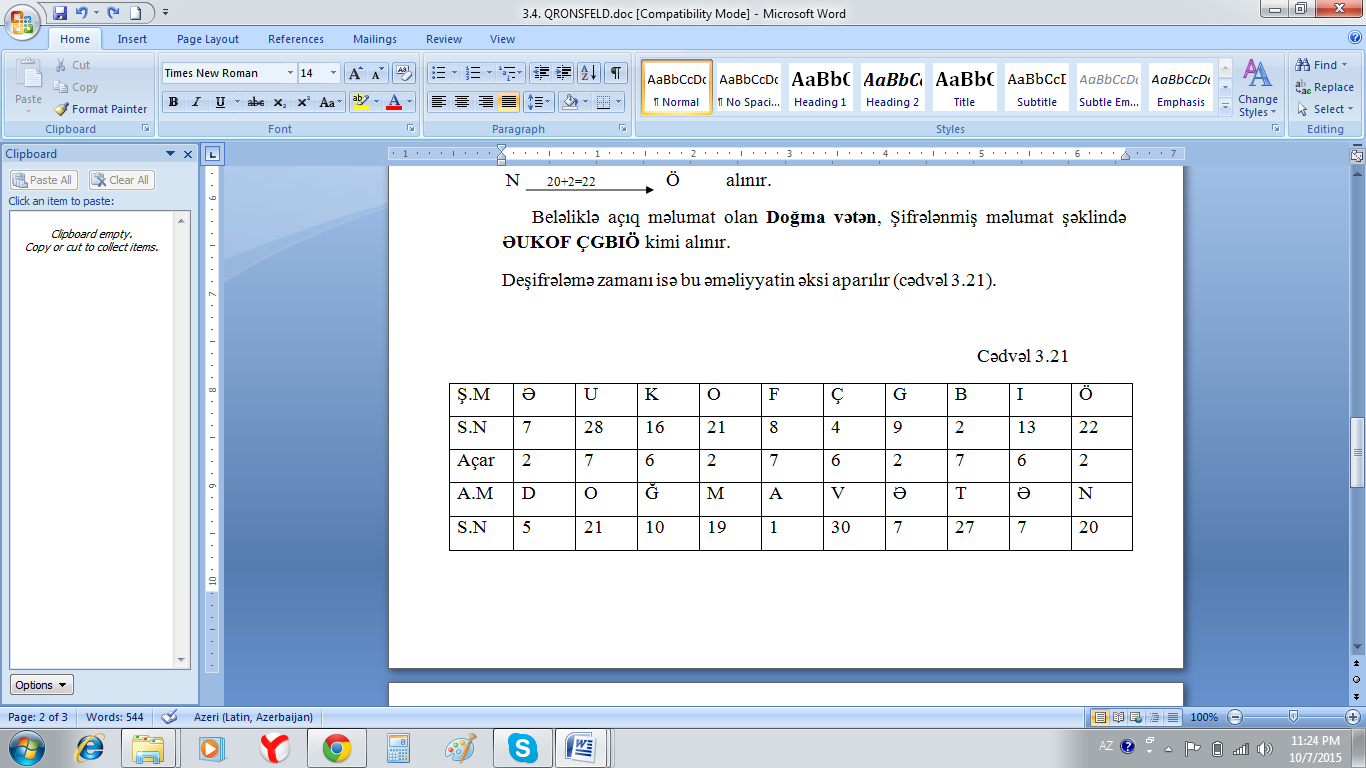
əlifbada 34 hərf olmadığından sürüsdürmə əlifbanın əvvəlinə qayıdır

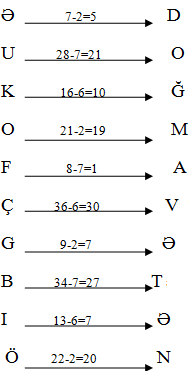
Bu cədvəldə D hərfi 5-ci sırada, O hərfi 21-ci, G-hərfi 10-cu və s. durduqlarından, uyğun ola­raq D-hərfinə Ə, O hərfinə U, G hərfinə K və s. ki­mi simvollar uyğun gə­lir. Be­lə­liklə “Doğ­ma və­tən” sözünün şifrələnməsi aşa­ğı­dakı ki­mi alınır.

Beləliklə açıq məlumat olan “**Doğma vətən**” Şifrə­lən­miş mə­lumat şəklində **“ƏUKOF ÇGBIÖ”** kimi alınır.

Deşifrələmə zamanı isə bu əməliyyatın əksi aparılır (cədvəl 2.26).

Cədvəl 2.26.





əlifbada 36 hərf olmadığından sürüsdürmə əlifbanın əvvəlinə qayıdır

əlifbada 34 hərf olmadığından sürüsdürmə əlifbanın əvvəlinə qayıdır

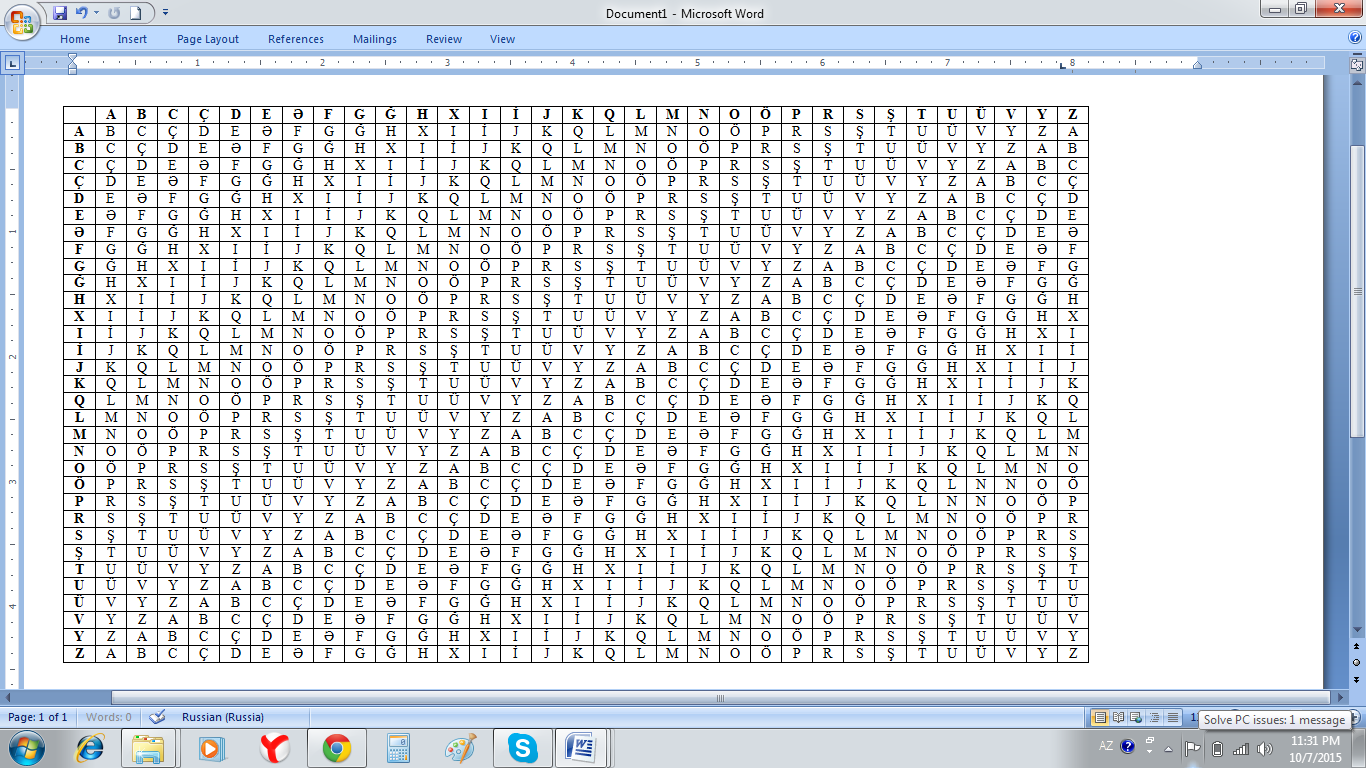
Deşifrələmə zamanı istifadə olunan əlifbaya baxılır. Ə hər­fi­nin sıra nömrəsindən çıxılır və alınan rəqəmin ye­rin­də duran hərf yazılır.

Beləliklə, şifrələnmiş məlumat **ƏUKOF ÇGBIÖ. DOĞMA VƏTƏN** açıq məlumat olur.

**2.6. VİJNER şifrələməsi**

Vijner cədvəli, kriptografiyada Vijner şifrələməsi üçün is­ti­fadə edilir və Fransız şifrəçisi Blaise də Vijner tə­­rəfindən ha­zır­lanmış bir cəd­vəldir [9]. Bu cədvəl şifrə üçün la­zım­lı hər bir hərfin han­­sı hərf ilə əvəzlənəcəyini gös­tərir. Hərflərin də­yiş­di­ril­­məsi üçün çox əlifba istifadə edi­lir. Hər hərfin söz­də­ki sırasına görə şif­rələmənin əlif­bası da dəyişir (cədvəl 2.27, cədvəl 2.28).

Cədvəl 2.27.



Vijner şifrələməsi Sezar şifrələməsinin inkişaf etdi­ril­miş ha­lı­dır. Sezar şifrələməsi zamanı hərflərin də­yiş­di­ril­mə­­si üçün yal­nız bir əlifbadan istifadə edilir, Vijner şif­rə­­­lə­mə­­sin­də isə birdən çox əlifbadan isti­fa­də edilir. Şif­rə­ləmə üçün bir açar se­çilir və bu aça­­­­­­ra görə hər hərf söz için­­də­ki sırasına gö­rə dəyi­şik bir əlifbası şif­rələnir. Açar­la bu şifrələmə Sezar şif­rələməsinə görə eyni asan­­­­lıq­la ye­­nə de­şifrə edilir.

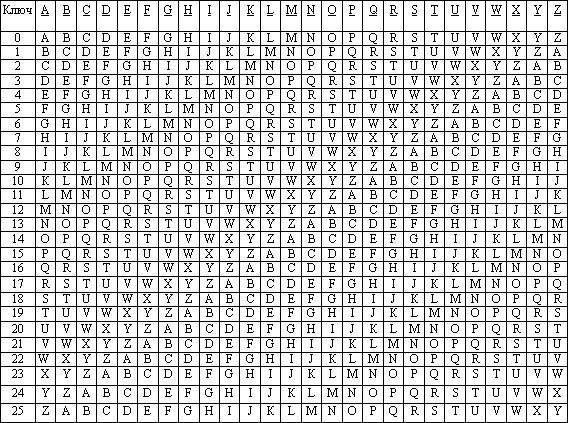
Vijner şifrələməsi uzun zaman etibarlı bir şifrələmə alqo­ri­tmi hesab edilib ("Le chiffre indéchiffrable", Türk­cə­­də: "deşifrə edi­lə bilməyən şifrə"). Seçilən bir söz şif­rə­ləmə üçün istifadə edilən əlif­banı təyin edir. Hər is­ti­fa­də edilən əlifbada hərflər Sezar şif­rə­ləməsində oldu­ğu ki­mi, əlifbadakı sırasından növbəti hərf ilə də­yişdirilir.

İlk olaraq 1854-ci ildə İngilis riyaziyyatçı Charles Bebbic Vijner şifrələməsini həll etdi. Bebbicin bu kəşfini heç açıq­la­ma­­ma­sına baxmayaraq, Prus polkovniki Frie­d­rich Kasiski 1863­-ci ildə öz deşifrələmə üsulunu açıqladı və bununla da bu üsu­lun ta­nın­masını təmin etdi.

Vijner cədvəlindən şifrələmə və deşifrələmə etmək üçün is­ti­fa­də olunur. Cədvəl iki cür olur: 1. açar məlu­mat­­lardan, yəni hərf­lər­­dən ibarət olmaqla (cəd­vəl 2.29, 2.30), 2. açar rə­qəm­lər­­dən ibarət olmaqla (cəd­vəl 2.31, 2.32).

Açar rəqəmlərdən ibarətdirsə yuxarı sətrdəki sim­vol­lar açıq mətnin simvolları yazılacaq. Sol tərəfdə isə açar bil­­di­rən və əlif­ba­­dakı hərflərin sayı qədər rəqəm­lər­dən iba­­rətdir. Əgər açar söz­lər­­­­dən ibarətdirsə yuxarı sə­tir­dəki sim­­­vollar açıq mətnin sim­vol­la­rı əvəz olunaraqyazı­la­caq. Sol tə­rəfdə şifrələmədə istifadə olu­­­nan açarın əlif­ba­sı dayanır. Deşifrələmə zamanı bu əmə­liy­ya­tın əksi aparılır.

Cədvəl 2.28.



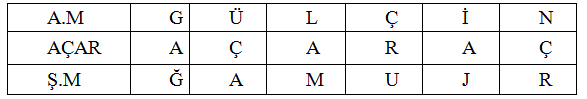
Mə­lu­ma­tın hərflə şifrələnməsinə aid misal.

A.M: GÜLÇİN

A.S: AÇAR

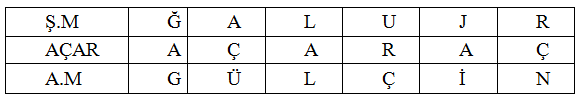
Ş.M: ĞAMUJR

Cədvəl 2.29. Məlumatın şifrələnməsi cədvəli.

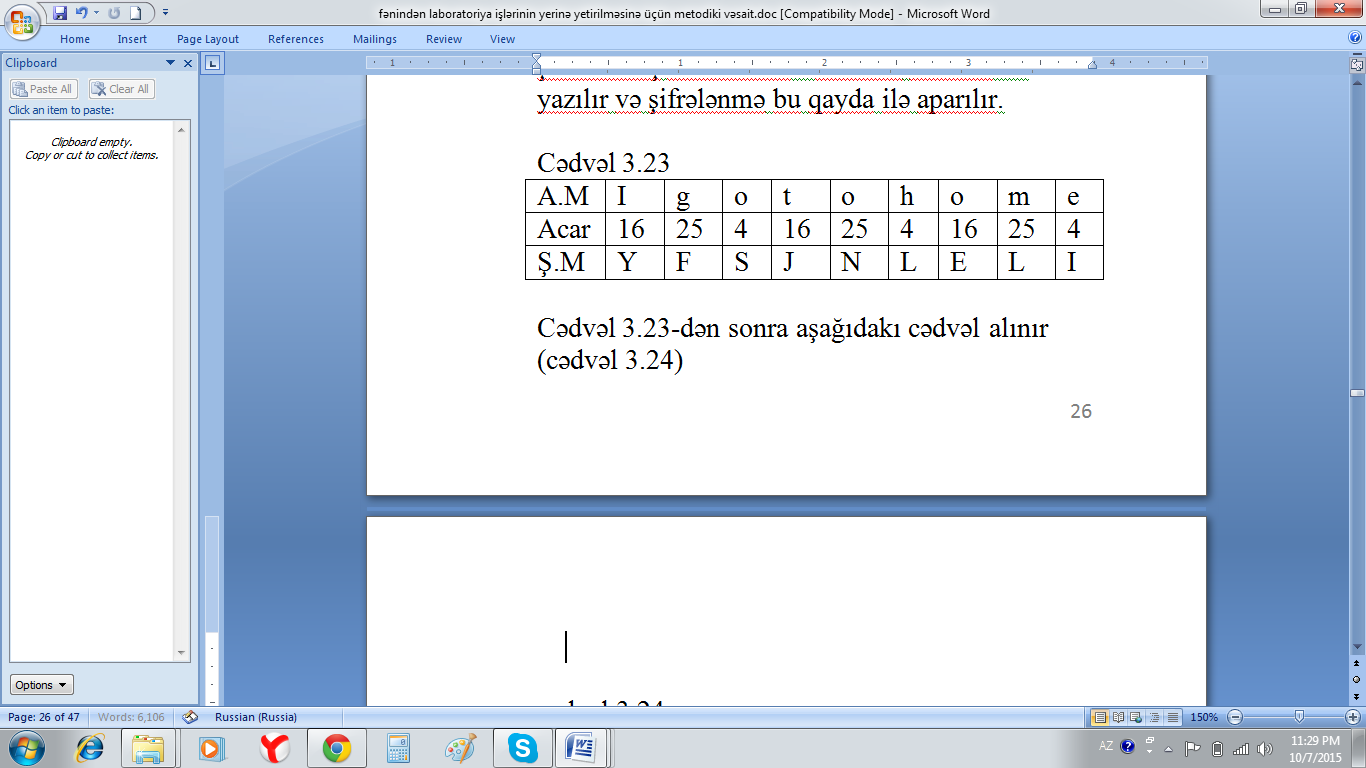


Burada da şifrələmə zamanı yuxarı sətrdə olan hərf ilə bi­rin­ci sütundakı hərf­lərin kəsişməsində olan hərf yazılır. Mə­sə­lən G hərfinin açarı A-dır. A hərfi ilə G hərfinin kə­siş­­­mə­sin­də Ğ hərfi durur və şifrələnmiş məlumatda G hər­­­­­­fi­nin əvəzinə Ğ yazılır və şifrələnmə bu qayda ilə apa­rı­lır.

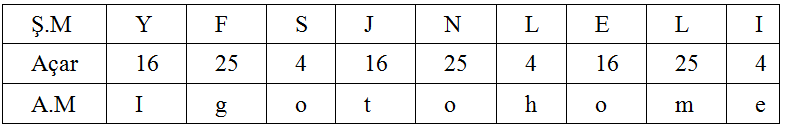
Cədvəl 2.30. Məlumatın deşifrələnməsi cədvəli



Cədvəl 2.31.



Cədvəl 2.32.

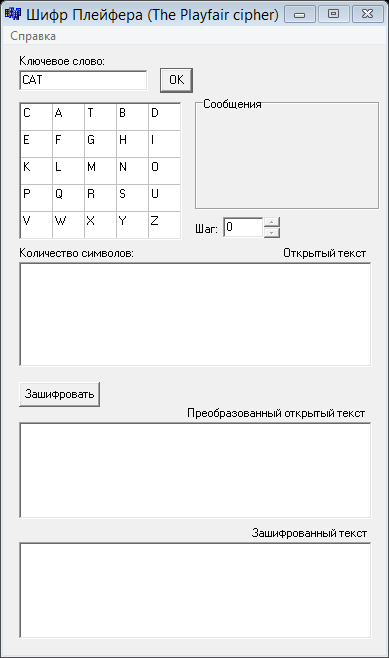


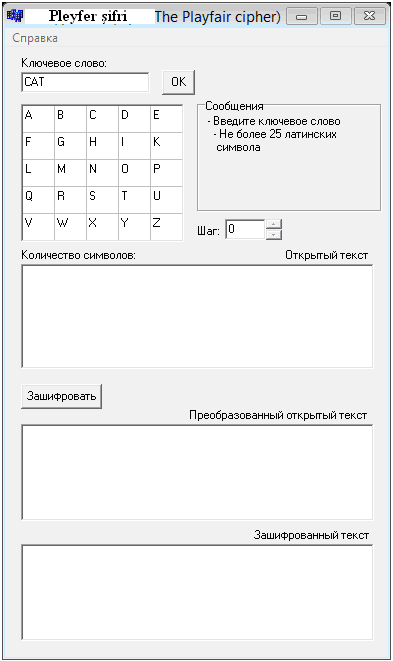
Vijner şifrələməsi üçün bir söz seçilir. Bu söz "AC­AR", şif­rə­lə­nəcək yazı isə "Vikipediya" ola bilər. Şif­­­rə­lə­mə üçün La­tın əlif­bası istifadə olunur. Açar söz olan "AC­AR" dörd hərfdən iba­­rət olduğu üçün parol da dörd əlifba istifadə edilir. İlk şif­rə­lə­mə, açar hərfi "A" olan bir Se­zar şifrələməsi olaraq başlayır. "A" əlif­­­-banın bi­rinci hər­fi olduğu üçün şifrələnəcək yazının ilk hərfi olan "v"-ni əlifbada bir hərf ötürməklə dəyişdirir. Şif­rə­ləmədə "v" hər­findən saymağa başlanılır. Bu şəkildə "v" birinci hərf olduğu üçün eyni qalır. Açar sözün ikinci hərfi "C" ola­caq. "C" Latın əlifbasının 3-cü hərfidir. Beləcə şifrə­lə­nə­cək yazının ikinci hərfi "i" üç hərf atlamaqla dəyiş­diri­lir. "i" hərfi birinci hərf ola­raq prezumpsiyası üzrə 3-cü hərf se­çilir. Birinci hərf "i" oldu­ğun­dan 3-cü hərfdə "k" olur. Be­ləcə "i" hərfi "k" ola­raq dəyiş­di­ri­­lir. Şifrələnəcək ya­zının 3-cü hərfi "k" da ey­ni şəkildə də­yiş­di­ri­lir. Açar sö­zün 3-cü hərfi "A" ol­du­ğu üçün "k" olduğu kimi qa­lar. Açar sözün dördüncü hər­fi "R" Latın əlifbasının 17-ci hər­fi­dir. Şifrələnəcək yazı­nın dördüncü hərfi "i" yenə ilk hərf olaraq 17-ci hərf müəy­yən edilir. Latın əlifbasında ilk hərf "i" kimi sa­yıl­­dığın­da 17-ci hərf "y" olur. İlk dörd hər­fin şifrə­lə­mə­si be­ləcə "vkky" olur. Eyni üsulla bütün söz şifrələnir.

**2.7. Pleyferə görə şifrələmə və onun əsası. Biqramlar**

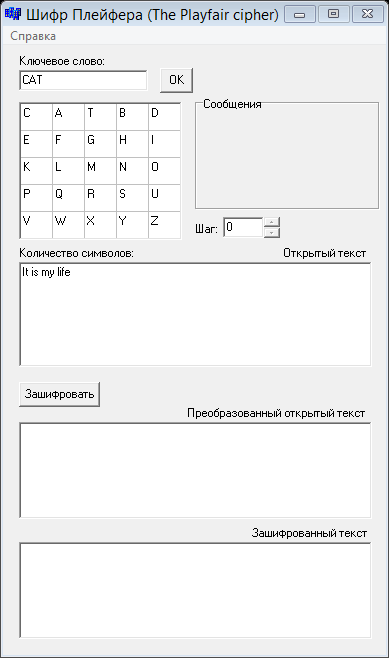
İlkin məlumatların simmetrik şifrələmə ilə təhlü­kə­­siz­li­­yi­ni tə­min etmək üçün istifadə olunan üsullardan biri də Pley­­­­ferə görə şif­rələmə hesab olunur. Bu şifrələmə 1854-cü ildə məşhur ingilis ali­­mi Çarli Pleyferin şərəfinə ad­lan­­­­­­­­­­dırıl­mış­dır. Pleyferə görə məlumatları şifrələmək üçün­ cədvəldən isti­fadə olunur. Cəd­vəlin ölçüləri kvadrat ol­­­­­­­duğuna görə bu­­na kvadratlar cədvəli və yaxud Pley­fe­rin kvadratlar cəd­vəli de­yilir [17,19]. Cəd­vəlin ölçüləri 5x5, 6x6 və s. şəklində təsvir edi­lir. Cəd­vəldə iki sim­vol­lar cüt­lü­­yün­­­dən eyni sim­­volla əvəz edilən sim­vol­lar cüt­lü­-yü­­nə biq­­­ramlar de­yi­lir. Bi­qra­ma­ya gö­rə hər bir əlif­ba­nın özünə məxsus müm­kün biq­ra­ma­lar çox­luğu vardır. İngi­­lis əlif­ba­sı üçün 26x26, Azərbaycan əlif­bası üçün 32x32, rus əlif­bası üçün 33x33 müm­kün hallardan iba­rət biqramlar alı­­nır. Misal, AB, BA, AS sim­vollar cütlüyün gös­tərmək olar. Pleyferə görə şif­­­rə­ləmə cədvəli ma­tris­dən iba­­rət olur və mat­ris faza və ya açar söz­lə­rin­dən iba­rət olur. Mat­­­risi ya­rat­maq üçün və şifrə­lə­mədən istifadə et­­mək üçün açar sözünə və açıq mətnin idarə edilməsi üçün 4 qay­­­d­aya əməl edil­mə­li­­dir.

1. Əgər iki simvol biqramından eynidirsə onda 1-ci sim­­voldan sonra “x” əlavə edirik, yenidən iki simvol cüt­lü­­yü təkrar şifrələnir və proses davam etdirilir. Bəzi hal­lar­da “x” əvəzinə “Q” simvolundan istifadə olunur.

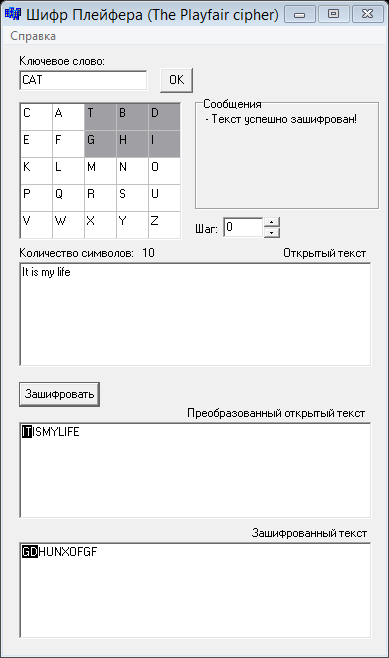




1. Əgər ilkin mətndə biqramın simvollarında eyni sim­vol­lara rast gəlinərsə, onda bu simvollar sağdan ən yu­xarı sü­­tun­da yer­ləşdirilir. Əgər simvol sətirdə sonun­cu­dursa on­da bu sətrin bi­rinci simvolu ilə əvəz edi­rik.

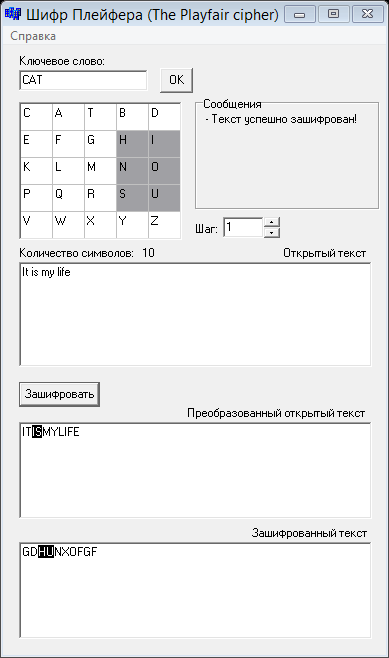


1. Əgər ilkin mətnin biqramlarının simvolları bir sü­tun­da rast­laşarsa o həmin sütunun altında yerləşən sim­vol­la əvəz edi­lir. Əgər simvol cədvəlin aşağı sütu­nun­da yer­­­ləşərsə on­­­da bu sü­tu­nun birinci simvolu ilə əvəz edi­lir.



1. Əgər ilkin mətnin biqramlarının simvolları müx­tə­lif sətir və sütunlarda yerləşərsə, onda həmin sətir­də yer­ləşən sim­­volla əvəz olunur. Məlumatı şifrədən azad et­­mək üçün bu prosesin əksinin tətbiq edilməsi ilə həyata keçirilir.

Növbəti biqramalara keçidi isə belə göstərə bilərik:

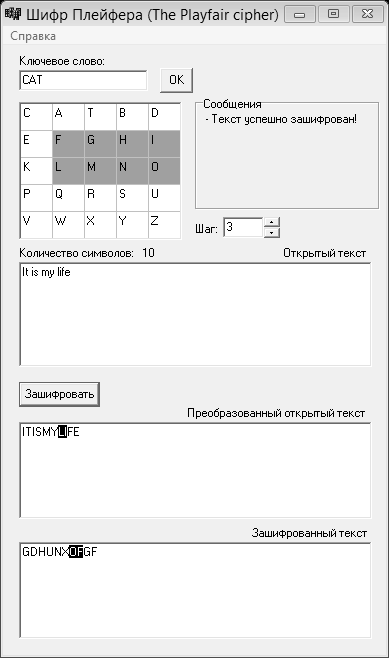
1-ci  
   
Əgər açar sözündə iki və daha çox eyni simvoldan istifadə olunursa, onda onlardan biri yazılır.

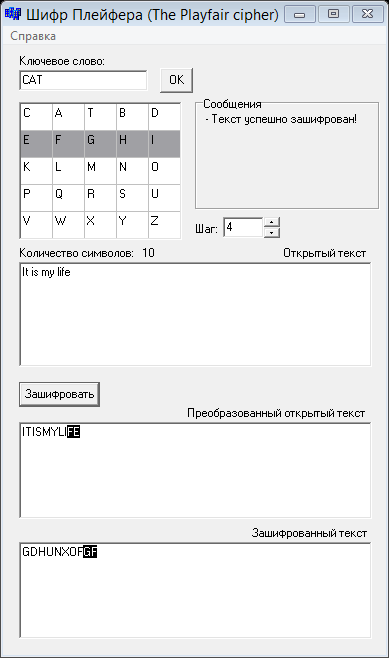
İlk öncə açar söz daxil edilir. Burada nəzərə almaq lazım­dır ki, açar sözunun tərkibində olan hərflər ingilis əlifbasının hərf­lə­ri olmalıdır. Bundan sonra simvollar açara uyğun düzülür (ilk açar sözü ya­zılır). Daha sonra açıq mətn daxil edilir.

Ondan sonra şifrələmək istədiyimiz mətni daxil edirik.

Proqram yazdığımız mətni böyük hərflərlə yazır və biqramlara ayırır, həmin biqramların yeri əlifbada göstə­ri­­lir.

2-ci  

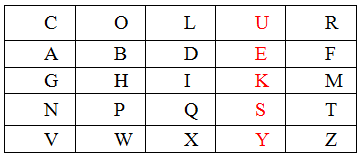

3-cü  


4-cü  


Pleyfer şifrələnməsi və ya Pleyfer kvadratı texniki ola­­raq əl ilə şifrələnən simmetrik üsuldur. Şifrələmə iki sim­­vollar cüt­lü­yü­nün (biqramı) eyni simvolla əvəz­lən­mə­si­nə əsas­lanır. Pleyfer şifrə­lə­mə­si sadə yerdəyişmə və əvə­zet­mə şifrələn­mə­­sinə nis­bə­tən bir qə­dər etibarlıdır. O tək­cə la­­­tın əlifbası üçün deyil həmdə 26x26=676 müm­kün hal­lar­dan ibarət biq­ram­larda aparıla bilər. Pley­­fer şif­rə­lə­məsi üçün 5x5 ölçülü matrislərdən istifadə edilir (ki­ril əlifbası üçün bu matrisin öl­çü­sü 4x8 olmalıdır). Mat­ris ya­­­­rat­maq üçün açar sözünə və dörd sadə qaydaya əməl et­­­mək la­zım­­dır. Açar matri­si­ni ya­rat­maq üçün bi­rin­­­­ci növ­­bə­də mat­ri­sin boş xa­na­larını açar sö­zün sim­­vol­­ları ilə dol­durmaq lazımdır (tək­­rar olu­­nan sim­vol­ları yaz­ma­­­maq şər­­tilə). Sonra matrisin qa­lan boş xa­­na­la­rı­­nı əlif­ba­­nın hə­r­f­­­­­­­­­lərilə doldururuq. Açar sözu ma­t­­­­­ri­sin yu­xa­rı sət­­rin­də sol­­­­dan sağa yazılır. Açar sözü 5x5 öl­çülü mat­ri­sə əlavə edil­­­­­miş söz şifrələmə üçün açar he­sab edilir.

Məsələn: Açar sözü olaraq **“COLOUR”** götürək (cədvəl 2.33 və 2.34).

Cədvəl 2.33.



Məlumatı şifrələmək üçün onu bir neçə biqrama böl­mək la­zım­­dır (biqram – iki simvoldan ibarət qrupdur). Bi­q­ramın iki sim­­­volu düzbucqlı matrisin künclərinə yer­ləş­­­dirilir. Bu və­ziyyətlərə uyğun küncləri təyin edirik və daha sonra aşa­ğı­dakı dörd qaydaya əməl edirik.

1. Əgər iki simvol eynidirsə onda birinci simvoldan son­­ra “X” əlavə edirik.

Məsələn:

Məlumat: **“MY FRIEND DIDN’T USE TO SMOKE”**

Məlumatı biqrama bölək: **“MY FR IE ND XD ID NT US ET OS MO KE”**

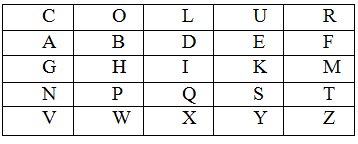
2) Əgər ilkin mətində biqramanın simvollarında eyni sim­­­­­­vola təsadüf edilərsə onda bu simvollar sağdan ən ya­xın sü­­­tun­la­ra yer­ləşdirilir. Əgər simvollar sətrdə sonun­cu­­­­­dur­lar­sa on­da bu sət­rin birinci simvolu ilə əvəz olu­nur­lar.

3) Əgər ilkin mətnin biqramının simvolları bir sü­tun­də rast­­­la­şar­sa o həmin sütunun altında simvolla əvəz edi­lir. Əgər sim­vol cəd­vəlin aşağı sütununda yerlə­şir­sə o bu sü­tu­­nun birinci sim­volu ilə əvəz olunur.

4) Əgər ilkin mətnin simvolları müxtəlif sətr və ya sü­tun­lar­da yerləşərlərsə onda onlar həmin sətrdə yerləşən sim­­vol­larla əvəz olunurlar, ancaq bu yerləşmələr düz­bu­caq­­lının digər künc­lə­ri­nə uyğun olaraq yerləşdirilməlidir.

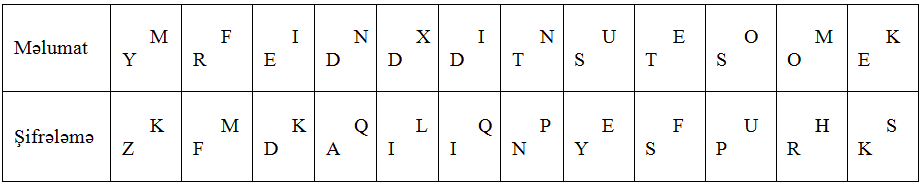
Məsələn: Açar sözü **“colour”**

Cədvəl 2.34.



Məlumat: **“MYFRIENDXDIDNTUSETOSMOKE”**

Cədvəl 2.35. Məlumatın şifrələnməsi

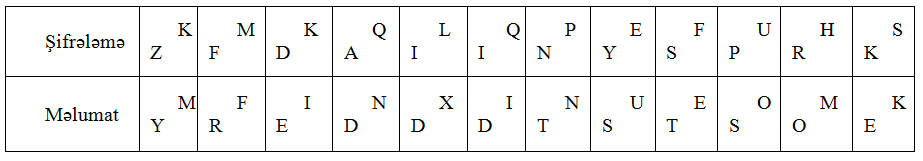


Şifrələnmiş məlumat: **“KZMFKDQALIQIPNEYFSUPHRSK”**

Deşifrələmə

Şifrələnmiş məlumat: **“KZMFKDQALIQIPNEYFSUPHRSK”**

Cədvəl 2.36. Məlumatın deşifrələnməsi



Məlumat: **“MYFRIENDXDIDNTUSETOSMOKE”**

Pleyfer şifrələməsini aparmaq üçün pleyfer proqra­mın­dan is­ti­­fadə olunur.

**III. ASİMMETRİK ŞİFRLƏMƏ ÜSULLARININ TƏTBİQİ İLƏ**

**KOMPYUTER ŞƏBƏKƏLƏRİNDƏ İNFORMASİYA**

**MÜHAFİZƏSİNİN İŞLƏNMƏSİ**

**3.1. Asimmetrik şifrələmə**

Evklidin, Ferminin, Eylerin, Qaussun, Çe­bı­ş­­­ev və Er­mi­­tin iş­ləri diafont tənlik­lərin həllində ağıl­lı və ki­fa­**­**yət qə­dər ef­fek­tiv al­­qo­­ritmləri, bərabər­siz­lik­lə­rin həl­li­nin ay**­**dın­­­­laş­dı­rıl­­masını, döv­­­rü üçün böyük sadə ədəd­lərin tər­­tibini, da­­ha yax­­şı yanaş­ma­­­­la­rın ta­pı­l­ma­sı­nı və s. özün­də cəm­ləş­di­rir. Son iki onillikdə, bi­rin­ci növ­­­­bə­də kripto­qra­­fi­­­­ya­nın tələ­blə­ri və EHM**-**in geniş yayıl­ma­sı sa­yə­sin­­də, ədəd­­lər nəzə­riy­yə­si­­nin al­­­qoritm məsələ­ləri üzrə təd­qi­qat­lar təla­tüm­lü dövrünü ya­şayır və kifa­yət qədər məh­sul­dar in­­­ki­şaf­da­dır [3,8].

Hesablama maşınları və elektron rabitə vasitələri in­san fəa­liy­­­­yə­tinin praktik olaraq bütün sahələrinə daxil ol­­muş­­lar. On­­­­larsız müa­sir kriptoqrafiya da ağla­sığ­maz­dır. Mə­tn­­­lərin şif­rə­lən­­­­­məsini və deşifrə olun­masını EHM­-in kö­­­­­mə­yi ilə ədəd­lərin em­alı pro­se­si kimi tə­səv­vür etmək, bu əmə­liy­yat­ları yerinə ye­ti­­r­­ən üs­ulları isə, külli miq­dar­da ədəd­lər üzə­rində müəyyən olun­­­muş bə­­zi fu­n­k­­siyalar ki­mi qəbul etmək olar. Bütün bunlar kr­ip­to­qr­a­f­iyada ədəd­­lər nəzəriyyəsi meto­dunun meydana çıx**­**ma­­sını tə­min edir.

Lakin, EHM-in imkanları müəyyən çərçivə daxilin­də­dir. Məh­­dud uzunluqlu blokda uzun rəqəmlər ardıcıl­lığı­nı bö­l­üş­­dü­r­üb yerləşdirmək və hər belə bir bloku ayrıca şif­­­­­­­rə­­ləmək laz­ım gəlir. Gələcəkdə biz belə he­sab edəcə­yik ki, bütün şif­rə­­lən­ən tam ədədlər müs­bət­dir­lər və ölçü­cə müəy­yən m ədəd­in­­dən (de­yək ki, texniki məh­du­diy­yət­­­­­lə) kiçikdirlər. Bu cür şərt şifrə­lə­mə pro­sesində alın­mış ədədləri də təmin etmə­li­dir. Bu, imkan ya­r­a­dır ki, bu və digər ədədləri z/mz çıxma həl­qəsinin ədədləri he­sab edək. Bu zaman şifrələnən funk­si­ya­­ya çıxma həl­qə­sinin qar­­­­­­şı­lıqlı eynimənalı inikası (təsviri) kimi baxmaq olar.

*f:z/mz→z/mz*

*f(x)* ədədi isə *x-*in şifrələnmiş halıdır.

Bu cür sadə şifrədə*k* fiksə edilmiş tam olduqda

*f:x→x+k­(mod­ m)*

uyğun gələn dəyişmə şifrəsidir. Belə şif­rə­dən hə­­lə Yuliy Sezar da istifadə etmişdir. Əlbəttə ki, *f***-**in hər bir təs­viri infor­ma­si­ya­nın etibarlı qorunması məq­sə­di­nə uyğun gəl­mir.

1978**-**ci ildə amerikalı R.Rivest, A.Şamir və L.Adli­man (R.L.Rivest, A.Shamir, L.Adliman) f funk­si­ya­­sının bir sıra üs­­tün­­­­­­­lüklərə malik nümunəsini təklif et­mişlər. Onun əsa­sın­da sis­­tem­in müəlliflərinin adlarının baş hərf­lə­ri ilə adlan­dı­rıl­­mış real is­tifadə olunan şifrələn­mə siste­mi**-**RSA sistemi qu­rul­­muş­dur. Bu funksiya belə­dir:

1. *f(x)* qiymətini hesablayan kifayət qədər sürətli alqo­ritm mövcuddur;
2. *f-1 (x)* əks funksiyasının qiymətini kifayət qədər sü­rət­lə he­sab­layan alqoritm mövcuddur;
3. *f(x)* funksiyası elə bir “sirrə” malikdir ki, onu bil­mək­­lə *f1(x)* qiy­mətini tez hesablamaq olar; əsk halda, *f-1 (x)* hesab­­lanma bax­ımından çətin həll olunan məsələyə çevrilir ki, bu öz həlli üçün o qədər çox vaxt tələb edir ki, *f***-**dən şifrə kimi istifadə edən şəxs üçün artıq şifrələnmiş məlumat öz ma­r­ağını itirir.

RSA sisteminə həsr olunmuş Massaçussis Texno­lo­gi­ya in­­s­ti­tut­unda məruzənin məqaləsi hələ nəşr olun­ma­mış məş­­­­­­­hur riya­zi­y­yatçı M.Qardnerə gön­də­ril­mişdir ki, o da 1977**-**ci ildə Scien­­ti­fik Amerikan jur­na­lında şif­rə­­­­­­­­­lə­mə­**­**nin bu siste­mi­nə həsr olunmuş mə­qalə nəşr et­dil­miş­dir. Qar­d­­**­**nerin mə­qalə­si­­­nin başlığı belə səs­lənir: “Açı­lışına mil­yon­­­­lar­­­la il tə­­l­əb olu­nan şifrənin yeni nö­vü”. Mə­hz bu mə­­-qalə RSA haq­qın­da mə­lu­­matın yayıl­ma­­­­­sın­da əhə­mi­y­yətli rol oyna­yıb, gen­iş qey­ri**-**mütə­xəs­sislər ordu­su­nun diq­qə­tini kripto­qraf­i­ya­­­ya cəlb etmiş və fak­tiki olaraq növ­bəti 20 il ər­zində bu sahənin kəskin in­ki**­­**şa­f­ına səbəb ol­muş­dur.

Nə­hayət, elmi kriptoqrafiyadan əvvəl son sözü daha yük**­**sək kripto­dözümlü, həmçinin, şifrələmə prosesini avto­­mat­­laş­­dır**­**ma­­ğa (mexanikləşdirmə mənasında) imkan ve­rən rotor kripto**­**sis­­tem­­ləri dedilər.

Belə sistemlərdən biri sonralar ABŞ**-**ın prezidenti olmuş To­­m­as Cef­ferson tərəfindən 1970**-**ci ildə kəşf olun­muş me­xa­­n­i­**­**ki ma­­şındır. Çoxhərifli yerdəyişmə rotor maşının kö­mə­yi ilə yer­i­­nə ye­­tirilir. Fırlanan rotorların qar­şılıqlı vəziy­yət­ləri­­nin var­ia­si­ya­ları ilə hər biri “ti­kil­mə” (deşilmə) yer­dəyiş­mə­si­ni hə**­**y­ata ke­çi­rir.

Rotor maşınlarının təcrübədə yayılması yalnız XX əsrin əv­­vəl­lərində olmuşdur. İlk təcrübi istifadə olunan ma­şın­lar­dan bi­ri 1917**-**ci ildə Edvard Xever tərəfindən ha­zır­lan­mış, Ar­tur Ki­rx tər­əfindən isə mükəm­məlləş­diril­miş al­man ma­şı­nı Enigma ol­­muş­dur. Rotor maşınların­dan ikin­ci dünya mü­ha­ribəsi il­lər­in**­**də aktiv istifadə olu­nur­du. Alman maşını Enig­­madan əlavə, həm­çi­nin, Siqa­ve (ABŞ), Turex (Böyük Britaniya), Red, Oran**­**ge və Pur­ple 2 (Yaponiya) qurğu­la­rın­dan da istifadə olunurdu. Ro­t­or sistemləri**-**formal krip­to­qra­fi­ya­nın zirvəsidir. Belə ki, çox möh­­kəm şifrələri kifayət qə­dər sadə həyata keçirir­di­lər. Rot­­or sis­­temlərin uğurlu kripto­hü­­cumu yalnız, 40**-**cı il­lərin əv­vəl­­­­­lərin**­**də EHM-in meydana çıxması ilə müm­kün oldu.

Elmi kriptoqrafiyanın (XX əsrin 30**-**60**-**cı illəri) əsas fərq­­ləndirici cəhəti**-**krip­todayanıqlılığı ciddi riyazi əsaslı kripto­sis­­­tem­lərin meydana çıxmasıdır. 30**-**cı illərin əv­vəl­­ləri­nə doğ­­­ru ri­ya­ziyyatın kriptologiyanın elmi əsası olan bölmələri tam for­­ma­laşdı: ehtimallar nəzəriyyəsi və ri­­ya­zi statistika, üm­u­mi cəbr, ədədlər nəzəriyyəsi, alqo­ritmlər nə­zəriyyəsi, in­­for­ma­si­ya nə­zə­ri­y­yəsi, kiber­ne­tika aktiv in­kişaf etməyə başladı. Klod Şen­­­­­­­­nonun “Giz­li (məxfi) sis­temlərdə rabitə nə­zə­riyyəsi” (1949) işi özü­nə­məx­sus böl­məyə çevrildi. Burada informasiyanın krip**­**to­­­­qra­­fik müda­fiəsi (təhlükə­siz­li­yi) prin­sip­ləri nəzə­riy­yəsi for**­­­**ma­­­­laş­dırıl­mış­dı. Şennon “pay­laş­dır­ma” (yayıl­ma) və “yer­­­­­­­­də­y­iş­**­**mə” an­la­yışlarını daxil et­miş və istə­ni­lən qədər da­­­ya­nıqlı krip­­**­**to­­sistemləri yaratmağın müm­­kün­­lü­yünü əsas­­­landırmışdır.

60**-**cı illərin aparıcı kriptoqrafik məktəbləri rotor krip­to**­­**sis­­tem­ləri ilə müqayisədə daha dözümlü blok şifrə­ləri­nin yar­ad**­**ıl­ma­sına gəlib çıxdılar. Bunların da praktiki isti­­fa­­də­si yalnız rə­qəm elektron qurğuları şəklində müm­kün­dür.

Kompyüter kriptoqrafiyasının (XX əsrin 70**-**ci illə­rin­dən eti­ba­rən) meydana çıxması kriptosistemlərin hə­yata ke­ç­­­i­­rilməsi üçün kifayət qədər səmərəli, yüksək sü­rətdə “əllə” və “me­xa­ni­ki” şifrələrdən bir neçə dəfə çox krip­to­da­yanıqlı şifr**­**ələr əl­də et­mə­yə imkan verən he­sab­lama va­si­tələrini tətbiq etməyə imkan ve­rdi.

Kriptosistemlərin birinci sinfi blok şifrələri olmuşdur. Bu­n­­­­**­**ların da istifadəsi güclü və kompakt hesablama vas­i­tə­­ləri­nin mey­dana gəlməsi ilə mümkün olub. 70**-**ci illərdə şif­rə­lə­mə­nin ame­­­­ri­­kan standartı DES (1978**-**ci ildə qəbul olu­nub) blok şifrə­ləri­nin əsasını təsvir etmişdir. Onun əsasında isə digər, daha da­ya­n­ı­qlı simmetrik kripto­sis­tem­­lər, o cüm­lə­dən ГОСТ 28147**-**89 stan­dart şifrəsi yara­dıl­mışdır [7].

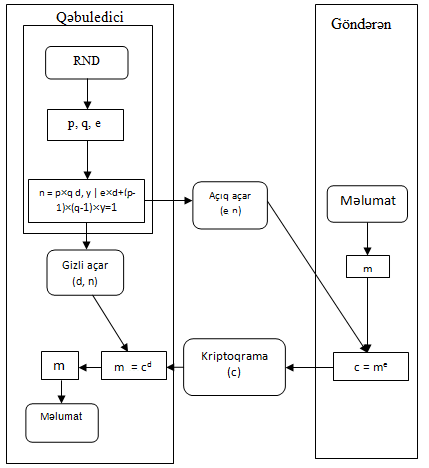
DES-in meydana çıxması ilə kriptoanaliz də zən­gin­ləş­miş­dir. Am­erikan alqori­t­minə həmlə etmək üçün krip­toan­a­liz­in bir neçə yeni növü (xətti, differensial və s.) yar­a­dıldı ki, bun­ların da prak­­tiki tətbiqi üçün yenə də böyük gücə malik hesablama sis­­tem­­ləri yaradılmalıdır.

70**-**ci illərin ortalarında müasir kriptoqrafiyada əsl part­­­­­­la­­yış baş verdi - tərəflər arasında məxfi açarın ötürül­mə­­­si­ni tə­ləb et­­mə­­­yən asimmetrik kriptosistemlər yara­dıl­­­­dı. Bu­­ra­da baş­­lanğıc nöqtə kimi 1976**-**ci ildə Uitfild Diffi və Martin Xell­man tərə­fin­dən “Müasir kripto­qrafi­ya­da ye­­­­­ni isti­­qa­mət­lər” baş­lığı altında çap olunmuş işlər gö­tü­rü­­­­­lür. Bu yazı­lar­da ilk dəfə olaraq şifrə­lən­miş infor­ma­si­­­ya­­­nın məxfi açarsız müb­a­­diləsi prin­si­pi for­ma­laş­­­dırı­lıb.

Müstəqil olaraq asimmetrik kriptosistem ideyasına Ralf Mer­kli də yanaşmışdır. Bir neçə il sonra Ron Ri­vest, Adi Şa­mir və Leonard Adleman təcrübi olaraq asim­me­t­rik krip­to­sistem olan RSA sistemini ixtira etmişlər. Onun da­­­ya­nıqlılığı böyük sadə ədəd­lərin vurulması (fak­to­riza­si­ya) problemi üzərində quru­lub. Asimmetrik krip­­toq­rafi­ya dərhal bir neçə yeni tətbiqi isti­qa­mət­ləri, xüsusilə elek­­­­­tron rəqəm imza (ERİ) və elektron pul sis­tem­lə­rini or­taya çıxarmışdır.

80**-**90**-**ci illərdə kriptoqrafiyanın tamamilə yeni isti­qa­mət­­**­**ləri meydana çıxdı: ehtimal şifrələmə, kvant kripto­qra­­­­­f­iya­sı və baş­qa­­ları. Onların təcrübi dəyərlərinin dərk edil­­­­­məsi hələ qar­şı**­**da­dır. Simmetrik kriptoqrafiyanın mü­kəm­­­­­­­­­­­məl­ləş­­diril­məsi məs**­**ə­­lə­si də aktual olaraq qalır. 80**-**90**-**cı illərdə Nef­eys­tel­ov şifrə­­ləri (SA­FER, RC6 və s.) iş­lə­nil­miş­dir. 2000**-**ci ildə isə açıq bey**­**nəl­xa­lq müsabiqə­dən son­ra ABŞ**-**ın yeni milli şifrə stan­­dartı **-** AES qəbul olun­­­du.

RSA kriptosisteminin ümumi görünüşü şəkil 3.1-də gös­tə­rilib.



Şəkil 3.1. RSA kriptosisteminin ümumi görünüşü

RSA sxeminin işinə baxsaq nümunədə şifrələnən ki­çik ədəd­dir. Kiçi­k ədədlər sadəliklə yerinə yetirilir (pra­k­ti­­ka­­da da­ha böyük ədədlər qəbul edilir).

Misal 1. *P=5, q = 11* olarsa, onda *n= 55.* Açıq açar ki­mi *7* ədə­di­ni se­çi­rik, bu halda bütün açıq açar alınır *( e = 7, n = 55).* Qap­alı aç­arı hesablayaq: *e x d + (p-1)* *x (q-1) x y = 1* əldə edirik *7 x d +40 x y = 1* alı­nır *d =23, y = -4* olarsa, bu halda qapalı açar ədədi olur (23, 55).

İx­tiyari istifadəçiyə kom­bi­na­­siyalı bit 1001112 gön­dər­mək istəyirik, onun ekvivalenti 3910. 39-un qüvvətinə açıq açar *e=7* yük­səl­dirik, *n=55*:(397mod 55)=19. 39 ədə­di şifrə­q­ramlı olur və əlaqə kanalına göndərilir. Qəbul edən gələn məlum­atı qüvvətə yüksəldir d=23: (1923mod 55)= 39. Çı­xış məlum­atı qaytarılır.

Misal: ABS məlumatını şifrələyərək və deşifrələyək. Mə­lu­­­matı 123 ədədi ardıcıllığı kimi təsvir edək (A-1,B-2,C-3):

* *p=5 və q=11* seçək (həqiqətdə ədədlər çox böyük ol­ma­lı­­dırlar).
* *n=5\*11=55,(p-1)\*(q-1)=40* hesablayırıq.
* E ədədini, məsələn, 7**-**yə bərabər seçmək olar.
* *(e\*7) mod 40=1* şərtindən d**-**ni tapırıq. Məsələn*, e=3.*

(3,55) açıq açarından istifadə edərək məlumatı şifrə­lə­yək:

* *C1=(13)mod 55 =1*
* *C2=(13)mod 55 =8*
* *C3=(13)mod 55 =27*

İndi isə *d=7* məxfi açarından istifadə edərək məlumatı de­şif­­r­ələ­yək:

* *M1=(17)mod 55 =1*
* *M2=(87)mod 55 =2097152mod 55 =2*
* *M3=(277)mod 55 = 10460353203 mod 55 =3*

Əgər ədədin sadə vuruqlara ayrılmasının effektiv me­tod­**­**la­rı mövcud olsaydı n ədədini p və ya q vuruqlarına ayı­r­ıb məx­­fi d aça­rını tapmaq olardı. Beləliklə, RSA al­qoritminin eti**­­**barlığı çə­tin həll olunan**-**praktik olaraq həll olun­mayan mə­­s­əl­ə**­**yəədə­din vuruqlara ayrılması mə­sə­ləsinə əsaslanıb, çün­­­ki hal**-**ha­z­ır­da vuruqlara ayır­ma­nın ef­­fektiv üs­ulu yox­dur.

* 1. **Əl Camal alqoritimi ilə şifrələmə**

Əl Camal asimmetrik sxemini təklif ed­­ib, bu şifrələmə sa­də ədəd modullarını qüvvətə yüksəltməkdə isti­fa­də edi­­­­­­­­lir. Bundan əvvəl bədniyyətlər hansısa çətin həll olan mə­­sə­lədə məl­um ədədi qüvvətə yüksəl­dir­dilər. Bu mə­lu­­­mat **diskret lo­q­a­rifma** problemi adını daşıyır.

**Açar seçimi mərhələsi:**

1. Sərbəst sadə ədəd seçilir P ( yetərli böyük )
2. Bu sadə ədəd üçün istənilən **təşkil edən element** (ing. pri­­mi­­­­­tivə root) **-** bu cür ədəd a, modulda təkrarən qüvvətə yük­­səl­mə hansı ki P(a1 mod p, a2 mod p,...), bütün se­çil­miş ədədlər da­­­­­­­xil olacaq 1-dən (p-1) qədər (mutləq 1-cə dəfə sərbəst niz­am­lı).
3. Təsadüfi ədədi sərbəst generasiya edir *x (0 <x <p)* - bu açıq aç­ardı.
4. Qiymət daxil olunur *b = ax* mod p kombinasiya (*a, p, b)* əl­də edənin açıq açarı kimi özünü ifadə edir.

**Şifrələmə mərhələsi:**

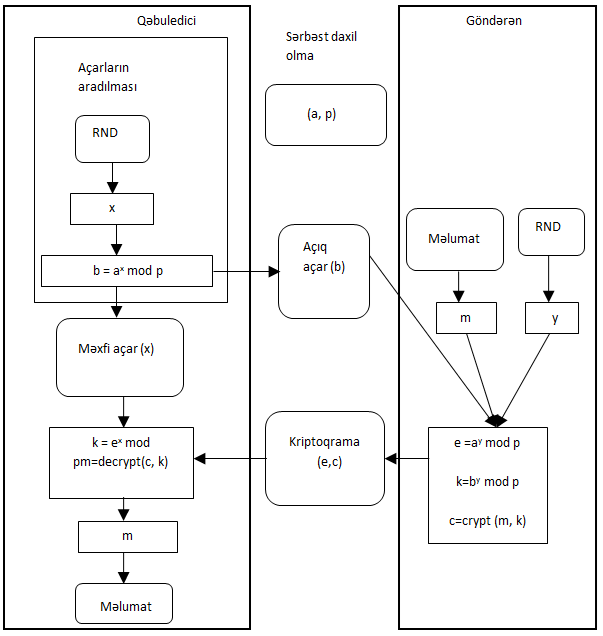
1. Göndərən sərbəst ədədi generasiya edir *y (0<y<p)*
2. Əvvəl şifroqram ədədi qoyulur *( ax mod p).*
3. Miqdarı hesablanır *k= (by mod p) = ((ax mod p)y modp).*
4. Məlumat realizasiyadan əvvəl qeyd olunur, göndərilən mə­lu­mat istənilən blok tipli şifrələmədə simmetrik açar kimi şif­rə­­­lə­nir.
5. Operativ yaddaşda və başqa yerdə *y və k* ədədi silinir, onlar təs­adüfən harasa düşə bilər.

**Deşifrələmə mərhələsi:**

1. Şifrələnmiş məlumatın gəlməsi əldə edən onu pa­ket­­lərə ayı­rır *( ay mod p)* və təzədən hesablayır *((ay mod p)x mod p)****-*** ri­ya­zi­yyat sübut edir ki, alınan ədəd k özünə bə­ra­bər ola­caq, hansı ki hesablanıb göndərilib, hazırki düs­tur ope­ran­dında x və y yerlərini dəyişmək olar.
2. *K* ayrılmanın daha çətin hissəsi simmetrik alqo­rit­m­də gə­lən bütün pakatləri deşifrə edir.
3. Əl Camal alqoritm sxemi şəkil 3.2**-**də göstərilib.

Diskret loqarifma problemi yaradır, sadə modul ədə­din qüv­­vətə yüksəltmədən sonra alınan nəticə həmin qüv­­­vətə yük­­­səlt­məyə əsaslanaraq müşahidə olunan vaxt tə­­­­­­­­yin edil­mə­­si müm­­kün deyil. Əl Camal sxemindən po­ten­siallı bəd­niy­yət *a, p, (ax mod p) və (ay mod p)* mə­lu­­­­­ma­­tını əldə edə bi­lər. Bircə çətin təyin edilən ədəd x və y “təmiz görünüşdə” müm­kün hesab məlumatın gös­tər­mir *k= (axy mod p),* hansı ki, şifrələr oxumaq üç­­ün la­zım­­­­dır.

Kriptodayanıqlı Əl Camal sxemi 512 bit p ədədi 56**-**bit­­li sim­metrik açara bərabərləşdirilir. Praktikada puzunluğu 768,1024 və 1536 qəbul edilir.



Şəkil 3.2. Əl**-**Camal kriptosistemləri

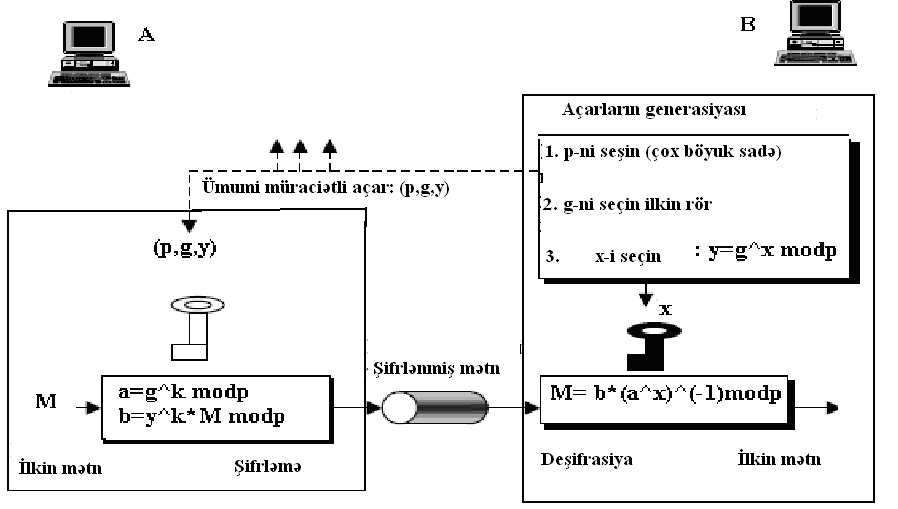
* + 1. **Şifrələmək**
  1. Tutaq ki *~M=5* məlumatının şifrələmək la­zım­dır.
  2. Açarların generasiyasının yerinə yetirək:
     1. Tutaq ki, *~p=11, g=2. ~x=8-* təsadüfi tam ədəd seçirik və bu *x* ədədi ~1 < x < p şərtini ödəyir.
     2. Hesablayaq, ~y= g^x\bmod{p}=2^8\bmod{11}=3.
     3. Beləliklə ~(p,g,y)=(11,2,3) üç açar açıq, ~x=8 açarı isə gizlin açardır.
  3. *1 < k < (p − 1)* şərtini ödəyən *k* təsadüfi tam ədədini seçirik. Tutaq ki, ~k=9.
  4. Hesablayaq ~a=g^k\bmod{p}=2^9 \bmod{11}=512 \bmod{11}=6.
  5. Hesablayaq, ~b=y^k M\bmod{p}=3^9 5 \bmod{11}=19683 \cdot 5 \bmod{11}=9.
  6. Alınan ədədlər cütlüyü ~(a,b)=(6,9) şifrələnmiş mətn adlanır.

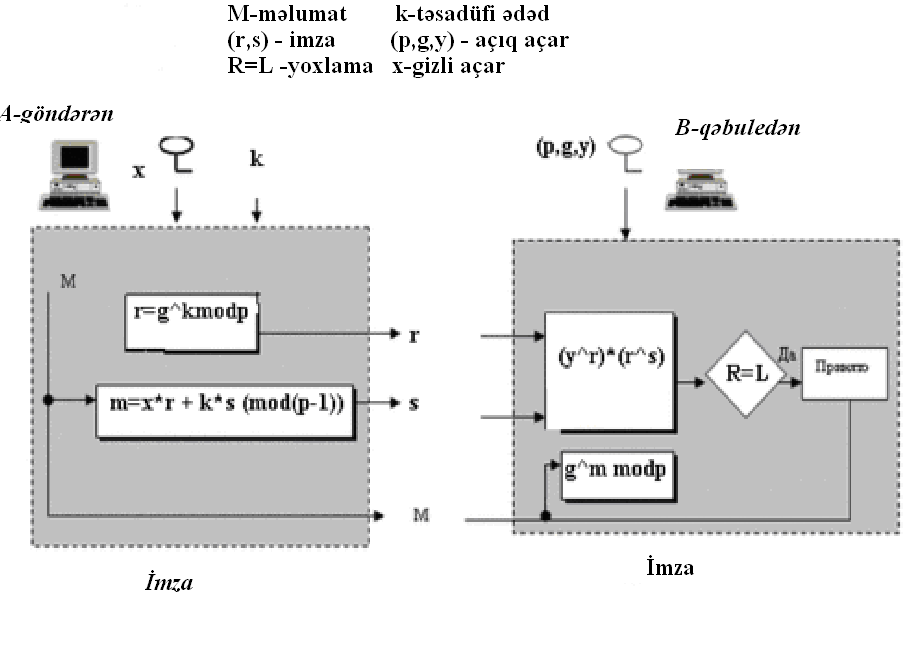
**3.2.2. Şifrədən azad etmək (deşifrə)**

* + 1. ~M=5 məlumatını almaq lazımdır. Bunun üçün şifrələnmiş mətn və gizlin açardan ~(a,b)=(6,9) və gizlin açar ~x=8 seçilir.

2.Verilmiş düstura görə M : ~M=b(a^x)^{-1}\bmod{p}=9(6^8)^{-1}\mod{11}=5

İlkin məlumat ~M=5 alınır.





### Məlumatın imzalanmasının Əl Camal alqoritmi ilə realizəsi

### prinsipi

### M məlumatı imzalamaq üçün :

### Məlumatlar daycestindən M : düsturu ilə hesablanır.

1. Təsadüfi **** ədədi seçilir və **** hesablanır
2. Evkilid alqoritminin köməyi ilə *s* ədəddi hesablanır ki, bu da:

**** şərtini ödəyir

1. **** məlumatında olan imza **** ədədlər cütlüyüdür.

### NƏTICƏ

Yerinə yetirilmiş dissertasiya işində qarşıya qoylmuş məqsədə nail olmaq üçün aparılan eimi-tədqiqat işləri haqqında aşağıdakı nəticələri söyləmək olar:

* kompyuter şəbəkələrində informasiya təhlükəsizliyi vasitələ­rinin tədqiq edilmişdir.
* kompyuter şəbəkələri və informasiya təhlükəsizliyi geniş tədqiq olunub, kompyuter sistemləri və şəbəkələrində təhlükələrin təsnifati aparılmış, kompyuter şəbəkələrində İnformasiya təhlükəsizliyinin əsas istiqamətləri muəyyənləşdirilmişdir.
* informasiyanın məxfiliyinin təmini və tamlığına nə­za­rət vasitələri araş­dırılmışdır.
* ənənəvi yanaşmadan fərqli olaraq, kompyuter şəbəkələrində təhlükəsizliyin təmini mədsədilə istifadə olunan üsul və vasitələrin tədqiqi aparılmış, bu vasitələr haqqında qıssa məlumatlar blokları hazırlanmışdır.
* bu bloklardan tədqiq olunan mövzu üzrə mühazirə və məşğələ dərslərində metodiki vəsast kimi istifadə etmək olar.
* şəbəkə perimetrinin, işçi stansiyalarının, həmlələri aşkarlayan sistemlərin məqsədi və məhdudiyyətləri, perimetrin mühafizəsi, kompyuter şəbəkələ­rində şəbəkələrarası ekranlar geniş tədqiq olunmuşdur.
* İsa Server 2004, İsa Server 2004-də yeniliklər, URLScan haqqında nəzəri və praktiki məsələlərə aydınlıq gətirilmiş, bütün səviyyələrdə mühafizənin təşkili kimi məsələlər həll edilmişdir.
* şəbəkəarası ekrandan keçən trafik, bütün trafikin yoxlanması, SSL trafikinin yoxlanması, hətta naqilsiz şəbəkələrin mühafizəsi problemləri, porblemlərin həlli yolları, İPSec–in icmalı, təhlükəsizlik sinfinə görə şəbəkəarası ekranlara tətbiq edilən əlavə tələbatlar kimi məsələlər araşdırılmışdır.
* simmetrik şifrələmə üsullarinin tət­biqi ilə kompyuter şəbəkələrində informasiya mühafizəsinin işlənməsi yerinə yetirilmişdir, praktiki misallarla hər bir üsulun tətbiqi ilə konkrekt misallar həll edilmişdir.

- asimmetrik şifrləmə üsullarinin tətbiqi ilə kompyuter şəbəkələrində informasiya mühafizəsinin işlənməsi məqsədilə ən geniş istifadə olunan Əl Camal alqoritimi ilə şifrələmə, şifrədən azad etmək (deşifrə) kimi məsələlər həll edilmişdir.

### ƏDƏBİYYAT

#### 1. Бирюков А.А. Информационная безопасность. Защита и нападение, М.: 2012, 474с.

#### 2. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии , М.: 2007, 550с.

#### 3. Фороузан Б.А. Криптография и безопасность сетей, М.: 2010, 784с.

#### 5. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: 2001, 368с.

6.Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002, 208 с.

7. Галатенко В. А. Стандарты информационной безо­пас­нос­ти. -М.: Интернет-университет информа­цион­­ных тех­но­логий, 2006., 264 с.

8. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети-анализ технологий и синтез решений. М.: ДМК Пресс, 2004, 616 с.

9.Гафнер В.В. Информационная безопасность: учеб. пос­о­бие. – Ростов на Дону: Феникс, 2010, 324 с.

10.Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.  Инфор­­мационная безопасность открытых систем. В 2-х томах

11. Том 1.-Угрозы, уязвимости, атаки и подходы к защите. -М.: Горячая линия – Теле­ком, 2006, 536 с.

12.Том 2.-Средства защиты в сетях.-М.: Горячая линия - Телеком,2008.,560 с.

13.Лепехин А. Н. Расследование преступлений против ин­фор­­мационной безо­­пасности. Теоретико-право­вые и прикладные аспекты. М.:Тесей, 2008, 176 с.

14.Лопатин В. Н. Информационная безопасность Рос­сии: Чел­овек, общество, государство Серия: Безо­пас­ность чел­о­века и общества. М.: 2000. - 428 с.

15.Малюк А.А. Теория защиты информации. - М.:Горя­чая линия - Телеком, 2012., 184 с.

16. Родичев Ю. Информационная безопасность: Нор­ма­­т­ив­но-правовые ас­пек­ты. СПб.: Питер, 2008.,272 с.

17.Петренко С. А., Курбатов В. А. Политики инфор­мац­ион­ной безо­пас­ности. - М.: Компания [АйТи](https://ru.wikipedia.org/wiki/%D0%90%D0%B9%D0%A2%D0%B8), 2006,400 с.

18.Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004,384 с.

19.Шаньгин В. Ф. Защита компьютерной информации. Эф­фек­тивные методы и средства. М.: ДМК Пресс, 2008.

20. Щербаков А. Ю. Современная компьютерная без­оп­ас­ность. Теоре­ти­ческие основы. Практические ас­пек­ты. - М.: Книжный мир, 2009, 352 с.

21. Борисов М. А. Особенности защиты персональных дан­ных в трудовых отно­­шениях. (Гриф УМО по доп­ол­­ни­тельному профессиональному образо­ва­нию) М.: Кни­ж­ный дом «ЛИБРОКОМ», 2013.,224 с.

22.Жданов О. Н., Чалкин В. А. Эллиптические кривые: Основы теории и крип­­­­то­­графические приложения. М.:Книжный дом «ЛИБРОКОМ», 2013,200 с..