**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**

**Sərbəst iş №1**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

**Fənn:** “ Veb sistemləri və texnologiyaları ”

**Mövzu:** Məlumatların şifrələnmə metodları

**Qrup:** 2441a

**Tələbə:** Abbasov Həsən

**Müəllim:** Heydərzadə Nübar

**BAKI 2024**

İnformasiya təhlükəsizliyinin əsas istiqamətləri olan informasiy Axınla şifrləmə üsulları qammalaşdırmanın bir növüdür və açıq mətni bit-bit şifrmətnə çevirir anın gizliliyinin, tamlığının təmin olunması və xidmət göstərməkdən imtina edilməsi hallarının qarşısının alınması üçün müxtəlif üsul və vasitələrdən istifadə olunur və zəruri tədbirlər görülür. Lakin bütün bunlara baxmayaraq, sistemdə mümkün boşluqlardan, buraxılan səhvlərdən istifadə edən hakerlər, rəqiblər, bədniyyətli şəxslər bəzən informasiyaya giriş əldə edə bilirlər.

Bu halda məxfi informasiyanın məzmununun kənar şəxslər tərəfindən oxunmasının qarşısını almaq üçün atılan ciddi addımlardan biri də informasiyanın mənasının və məzmunun gizlədilməsi, yəni şifrlənməsi üsullarının tətbiqindən ibarətdir.

*Kriptoqrafiya*– məlumatların məzmununu gizlətmək, icazəsiz istifadəsinin və ya gizli dəyişdirilməsinin qarşısını almaq məqsədilə onların çevrilməsi prinsiplərini, üsul və vasitələrini öyrənən elm sahəsidir. Kriptoqrafiya dedikdə istənilən formada olan, o cümlədən disk qurğularında saxlanılan və ya kompüterdə emal olunan, eləcə də rabitə kanalları vasitəsilə ötürülən informasiyanın məzmununun gizlədilməsi üsulları məcmusu başa düşülür.

Kriptoqrafik şifrləmə üsullarını (alqoritmlərini) aşağıdakı əlamətlərə görə təsnif etmək olar:

* *istifadə olunan açarların növünə görə*: simmetrik şifrləmə üsulları və asimmetrik şifrləmə üsulları.
* *şifrləmə alqoritminə görə*: əvəzetmə üsulları, qammalaşdırma üsulları, yerdəyişmə üsulları, kombinasiya (kompozisiya) edilmiş üsullar.
* *şifrləmə ardıcıllığına görə*: bloklarla şifrləmə və axınla şifrləmə.

**Simmetrik (biraçarlı) şifrləmə üsulları**

Gizli açarlı kriptoqrafik şifrləmə sistemlərinin ən vacib elementi gizli açarın ötürülməsi üçün “ciddi qorunan kanal”ın olmasıdır. Şəkildən göründüyü kimi, gizli açarlı kriptoqrafik sistemə əsasən, məlumatı göndərən şəxs gizli şifrləmə açarını və alqoritmini istifadə etməklə açıq məlumatı şifrləyir və göndərilməsi nəzərdə tutulan şəxsə ötürür.

Şifrləyici

Şifri açan

İlkin

məlumat (*T*)

*Göndərən tərəf*

Şifrlənmiş məlumat (*S)*

*Alan*

*tərəf*

İlkin

məlumat (*T*)

Açar (*K*)

Açar (*K*)

*Rabitə kanalı*

Simmetrik kriptoqrafik sistemlərin ümumi sxemi

Qorunan kanal

Rəqib, kriptoanalitik, bədniyyətli şəxs

Açar generatoru

Məlumatları göndərən və alan tərəflərin hər ikisinin eyni bir açardan istifadə etməsi faktını vurğulamaq üçün, adətən, gizli açarlı şifrləmə üsullarını *bir açarlı* və ya *si-metrik şifrləmə sistemləri* adlandırırlar.

Simmetrik şifrləmə üsullarının əsas çatışmazlığı ondan ibarətdir ki, gizli açar həm göndərənə, həm də alana məlum olmalıdır. Bu, o deməkdir ki, simmetrik kriptoqrafik sistemdən istifadəyə başlamazdan əvvəl hər iki (göndərən və alan) tərəf gizli açarı mütləq bilməlidir. Bu baxımdan burada, əlavə olaraq, açarın gizli (ciddi qorunan) kanalla digər tərəfə göndərilməsi problemi yaranır. Açarın ötürülməsi elə həyata keçirilməlidir ki, potensial rəqib (bədniyyətli şəxs) onu əldə edə (tuta) bilməsin.

Digər çatışmazlıq kimi, alan tərəf əlində olan şifrlənmiş və açıq mətnlərə görə bu məlumatı hər hansı konkret şəxsdən (göndərəndən) aldığını sübut edə bilməməsini, eləcə də hər hansı məlumatı və onun şifrmətnini generasiya edərək başqasından aldığını iddia etmək imkanının mümkünlüyünü göstərmək olar. Belə ki, o, əlində olan məxfi açarla digər tərəfdən asılı olmadan analoji məlumatı generasiya edə, şifrləyə və şifri aça bilər.

**Asimmetrik (ikiaçarlı) şifrləmə üsulları**

İki açarın istifadə olunması səbəbindən bu sistemləri *ikiaçarlı*, şifrləmə və şifrin açılması üçün istifadə olunan açarların müxtəlif olması səbəbindən isə onları *asimmetrik* kriptoqrafik sistemlər adlandırırlar.

Şifrləyici

Şifri açan

İlkin

məlumat (*T*)

*Göndərən tərəf*

Şifrlənmiş məlumat (*S)*

*Alan*

*tərəf*

İlkin

məlumat (*T*)

Açıq açar (*ke*)

*Rabitə kanalı*

Asimmetrik kriptoqrafik sistemlərin ümumi sxemi

Rəqib, kriptoanalitik, bədniyyətli şəxs

Açar generatoru

Gizli açar (*kd*)

Qeyd olunmalıdır ki, effektivliyə və davamlılığa görə asimmetrik şifrləmə üsullarına nisbətən simmetrik şifrləmə üsulları üstünlüyə malikdir. Belə ki, eyni uzunluqlu açara görə simmetrik şifrləmə üsulları asimmetrik şifrləmə üsulları ilə müqayisədə daha sürətlə işləyir və məxfiliyi daha yüksək təmin edir.

**Əvəzetmə üsulları**

Əvəzetmə üsulları özündə açıq mətnin fraqmentlərinin (ayrı-ayrı simvollarının və ya bloklarının) şifrmətndə başqa simvollarla və bloklarla əvəz edilməsinə əsaslanır.

Ən sadə əvəzetmə üsulu *birəlifbalı əvəzetmə üsuludur*. Bu üsulu çox vaxt *sadə əvəzetmə* adlandırırlar.

Əvəzetmə üsullarına bariz nümunə kimi Sezar şifrini göstərmək olar. Bu şifrə əsasən açıq mətnin hər bir hərfi əlifbada ondan bir neçə (məsələn, 3) mövqe sonra dayanan hərflə dəyişdirilir. Bu zaman əlifba dairəvi yazılmış hesab olunur, yəni mətndə əlifbanın sonuncu hərfləri rast gəlindikdə dairəvi prinsiplə əlifbanın əvvəlində olan hərflərlə əvəz olunur. Məsələn, Sezar şifrinə əsasən (sürüşmə – 3) “kriptoqrafiya” sözü “mtqşvrotçhqbç” şifrinə çevrilir.

Davamlılığı zəif olduğundan sadə əvəzetmə şifrləri hazırda istifadə olunmur. Belə şifrlərin sındırılması ayrı-ayrı simvolların və onların kombinasiyalarının rast gəlinmə tezliklərinin statistik təhlilinə əsaslanır. Belə ki, istənilən dildə müxtəlif hərflərin, onların iki, üç və ya daha çox sayda kombinasiyalarının mətndə təkrarlanmaları xarakterik xüsusiyyətlərə malikdir. Ona görə də aydındır ki, sadə əvəzetmə şifrləməsi zamanı şifrmətndə şifrlənmiş simvolların təkrarlanması açıq mətndə olan təkrarlanmalar ilə üst-üstə düşür. Bu isə şifri çox asanlıqla açmağa imkan verir.

Əvəzetmə şifrlərinin davamlılığını yüksəltmək məqsədilə çoxəlifbalı əvəzetmə üsulundan istifadə olunur. Çoxəlifbalı əvəzetmə prosedurasında əvəzetmələr (əlifbalar) çoxluğu və bu çoxluqların tətbiq olunması ardıcıllığını müəyyən edən paylama funksiyası istifadə olunur. Belə ki, hər hansı simvolun şifrlənməsi zamanı o, şifrləmə açarı və paylama funksiyasının qiyməti ilə müəyyən edilən əlifbadan simvol ilə əvəz edilir.

Çoxəlifbalı əvəzetmə üsulunun xüsusi halı kimi Vijiner şifrini göstərmək olar. Bu üsulda şifrləmə açarı *m* ədəddən ibarət çoxluq seçilir: *k*=(*k1*, *k2*,…, *km*). *T*=(*t1*, *t2*,…, *tn*) açıq mətninin *S*=(s*1*, *s2*,…, *sn*) şifrmətninə çevrilməsi üçün ümumiləşdirilmiş Sezar şifrindən istifadə olunur:

*si*=(*ti*+*ki*) mod *N*.

Burada *N* – əlifbanın simvollarının sayıdır. Açarın bütün *m* simvolu istifadə olunub qurtardıqdan sonra (*m*+1)-ci simvol qismində dairəvi prinsip üzrə açarın birinci simvolu (*k1*) götürülür. Faktiki olaraq, açar qismində ilkin açarın simvollarının dövri təkrarlanması şəklində formalaşan sonsuz *k1*, *k2*,…, *km*, *k1*, *k2*,…, *km*,... ardıcıllığı istifadə olunur. Belə ardıcıllığı *qamma ardıcıllıq* adlandırırlar. Qamma ardıcıllığın formalaşdırılması (qammalaşdırma) üsullarına növbəti paraqrafda baxılacaqdır.

Çoxəlifbalı əvəzetmə şifrini də sındırmaq kifayət qədər asan olsa da sadə əvəzetmə şifrinə nisbətən bir qədər çətindir.

**Qammalaşdırma üsulları**

*Qammalaşdırma* – ilkin mətnin simvollarının müəyyən qaydada formalaşdırılmış psevdotəsadüfi simvollar ardıcıllığı ilə əlifbanın gücünə (simvollarının sayına) bərabər modulla toplanması yolu ilə çevrilməsini özündə ehtiva edir.

Qammalaşdırma üsulunu, formal olaraq, çoxəlifbalı əvəzetmə üsulları sinfinə aid etmək olar. Lakin reallaşdırılmasının və formal təsvir olunmasının asanlığı baxımından qammalaşdırma üsulu geniş istifadə olunur və ona görə də onları ayrı sinfə ayırırlar.

Qammalaşdırma üsulunun mahiyyəti aşağıdakından ibarətdir. Məxfi *k* açarının köməyi ilə *g1*, *g2*,…, *gi*,... simvollar ardıcıllığı generasiya olunur. Bu ardıcıllıq qamma adlanır. Şifrləmə zamanı qamma *T*=(*t1*, *t2*,…, *tn*) açıq mətni ilə üst-üstə qoyulur. Şifrmətnin simvolları açıq mətnin və qammanın uyğun simvolları üzərində aparılmış tərsi olan əməliyyatın köməyi ilə alınır:

*si*=*ti*∙*gi* , *i*=1,2,...

Tərsi olan əməliyyat qismində əlifbanın gücünə (hərflərinin sayına – *N*) bərabər modulla toplama

*si*=(*ti*+*ki*) mod N

əməliyyatından istifadə olunur.

Qammalaşdırmaya əsaslanmış şifrləmə sistemlərinin davamlılığı qammanın xarakteristikalarından – onun uzunluğundan və qammanın simvollarının rast gəlinməsi ehtimallarının paylanmasının müntəzəmliyindən asılıdır.

Bərabər ehtimallı təsadüfi sonsuz qamma ilə qammalaşdırma üsulu daha davamlı hesab olunur. Bu üsullar zəruri olan aşağıdakı üç şərti ödəməlidirlər:

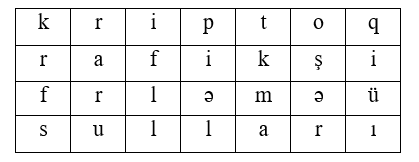
* qammanın bütün simvolları tam təsadüfidir və qammada bərabər ehtimalla rast gəlinirlər;
* qammanın uzunluğu açıq mətnin uzunluğuna bərabərdir və ya ondan uzundur:
* hər bir açar (qamma) yalnız bir mətnin şifrlənməsi üçün istifadə olunur və sonra məhv edilir.

Belə şifr prinsip etibarı ilə sındırıla bilməz, yəni mütləq davamlı olur. Lakin mütləq davamlı şifrlərin tətbiqi çox da rahat olmadığından praktikada, demək olar ki, istifadə olunmurlar. Adətən, qamma ya təsbit edilmiş uzunluqlu açar ardıcıllığının dövri təkrarlanması yolu ilə alınır, ya da hər hansı qayda ilə (məsələn, psevdotəsadüfi ədədlərin generatorunun köməyi ilə) generasiya olunur.

**Yerdəyişmə üsulları**

Yerdəyişmə üsulları şifrləmə zamanı müəyyən olunmuş qaydada açıq mətnin simvollarının yerini dəyişir. Bu, o deməkdir ki, şifrləmə açarının uzunluğu şifrlənən (ilkin) mətnin uzunluğuna bərabər olmalıdır. Məxfi açardan yerdəyişmə üsullarında istifadə üçün əlverişli olan şifrləmə açarını almaq üçün bir sıra üsullar mövcuddur. Belə üsullardan birinin köməyi ilə marşrut yerdəyişməsi adlanan şifrləmə üsulu formalaşdırılır. Bu üsul vasitəsilə şifrmətni almaq üçün açıq mətni hər hansı həndəsi fiqura (məsələn, düzbucaqlıya) müəyyən trayektoriya ilə yazır, sonra isə onu başqa trayektoriya ilə köçürürlər.

Üsulu əyani nümayiş etdirmək üçün aşağıdakı nümunəyə baxaq. Tutaq ki, “kriptoqrafik şifrləmə üsulları” mətnini şifrləmək lazımdır. Onda probelləri nəzərə almadan bu mətni 4x7 ölçülü düzbucaqlı cədvələ sətirlərlə soldan sağa doğru yazaq.



Şifrmətni almaq üçün bu cədvəldən hərfləri sütunlarla yuxarıdan aşağı hərəkət etməklə yazmaq lazımdır. Onda aşağıdakı mətn alınar: “krfsraruifllpiəltkmaoşərqiüı”.

Davamlığının zəif olması baxımından yerdəyişmə şifrləri müasir şifrləmə sistemlərində yalnız digər şifrləmə üsulları ilə kombinasiyada istifadə olunurlar.

**Axınla şifrləmə üsulları**

Əgər şifrləmə zamanı ilkin mətnin simvolları hər hansı müəyyən alqoritmə uyğun olaraq şifrmətnin müvafiq simvollarına ardıcıl şəkildə çevrilirsə, onda belə sistem axınla şifrləmə sistemi adlanır.

Axınla şifrləmə üsulları qammalaşdırmanın bir növüdür və açıq mətni bit-bit şifrmətnə çevirir. Axınla şifrləmə alqoritmlərində şifrləmə vahidi bir bit-dir. Şifrləmənin nəticəsi əvvəl şifrlənmiş axından asılı olmur. Axınla şifrləmə alqoritmləri axınların ötürülməsi sistemlərində, yəni informasiyanın ötürülməsinin ixtiyari vaxtda başlaması və sona çatması, eləcə də təsadüfən qırılması mümkün olan sistemlərdə tətbiq olunur.

Sistemin davamlılığı açar ardıcıllığının daxili strukturundan tam asılıdır. Əgər generator kiçik dövrə malik ardıcıllıq verirsə, onda davamlılıq yüksək olmur.

**Bloklarla şifrləmə üsulları**

Bloklarla şifrləmə zamanı ilkin mətn bloklara (uzunluğu təsbit olunmuş hissələrə) bölünür, şifrləmə alqoritmi blokları ardıcıl şəkildə, bloklara daxil olan simvolların hamısını isə eyni zamanda şifrləyir. Belə ki, bloklarla şifrləmə üsulları ilkin mətnin bloklarının tərsi olmayan çevrilmələri ailəsini təşkil edir. Bloklarla şifrləmə üsulu, faktiki olaraq, blokun əlifbası çərçivəsində əvəzetmə üsulundan ibarətdir. Bu çevirmə bloklarla şifrləmə rejimindən asılı olaraq birəlifbalı və ya çoxəlifbalı ola bilər.

Bloklarla şifrləmə sistemlərində şifrləmə vahidi bir neçə baytdan (4-dən 32-yə qədər) ibarət olur. Blokun şifrlənməsinin nəticəsi həmin blokun bütün ilkin baytlarından asılı olur.

Bloklarla şifrləmə üsullarının əvəzetmə üsullarının xüsusi halı olmasına baxmayaraq, aşağıdakı səbəblərdən onlara ayrıca baxılır. Əvvəla, informasiyanın ötürülməsi sistemlərində istifadə olunan simmetrik şifrlərin əksəriyyəti bloklarla şifrləmə üsullarıdır. İkincisi, adi əvəzetmə üsullarından fərqli olaraq, bloklarla şifrləmə üsullarını alqoritmik şəkildə təsvir etmək çox rahatdır.

Bloklarla şifrləmə üsullarına qoyulan əsas tələbləri aşağıdakı kimi formalaşdırmaq olar:

* bloklar kataloqunun tərtib edilməsi və saxlanılmasını çətinləşdirmək məqsədilə onların uzunluğunun kifayət qədər böyük (64 və ya ondan böyük) olması;
* kənar şəxslər tərəfindən açarların seçilməsi imkanlarını aradan qaldırmaq məqsədilə açarlar fəzasının kifayət qədər böyük olması;
* ilkin və şifrlənmiş mətnlərin uyğunluğuna əsasən ilkin mətnin və ya açarın müəyyən edilməsinin analitik və ya statistik üsullarının reallaşdırılmasının mümkün qədər qarşısının alınması üçün ilkin və şifrlənmiş mətnlər arasında əlaqələrin mürəkkəb olması.

Bloklarla şifrləmə üsullarının ciddi çatışmazlıqlarından biri ondan ibarətdir ki, açıq mətnin bir-birinin eyni olan blokları şifrmətndə də bir-birinin eyni olan bloklara çevrilir. Aydındır ki, bu amil bloklarla şifrləmə üsulunun davamlılığını aşağı salır. Belə ki, əgər rəqibin əlinə uyğun şifrmətnlə birlikdə ilkin mətnin nümunəsi düşərsə, onda o, analoji blokları olan şifrmətnləri asanlıqla hissə-hissə aça bilər.

Belə çatışmazlığın aradan qaldırılması üçün blokların qarışdırılması rejimindən istifadə olunur. Bu rejimdə növbəti blokun şifrlənməsi zamanı açıq mətnin əvvəlki blokları da istifadə olunur. Məsələn, açıq mətnin cari bloku şifrmətnin əvvəlki bloku ilə iki moduluna görə bitlərlə toplanır və sonra nəticəyə şifrləmə alqoritmi tətbiq edilir. Burada ilkin blok qismində ya yalnız sıfırlardan ibarət blok, ya da təsadüfi seçilən blok istifadə olunur. İkinci halda təsadüfi blok şifrmətnə əlavə edilir.

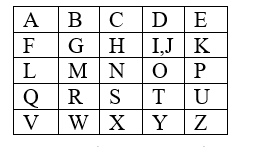
**Sadə şifrləmə üsullarının nümunələri**

*Polibiy kvadratı.* Eramızdan əvvəl ikinci əsrdə yunan yazıcısı və tarixçisi Polibiy 5x5 ölçülü kvadrat şifrləmə cədvəli icad etmişdi. Bu cədvəl ixtiyari əlifba ilə (məsələn, yunan əlifbasının 24 hərfi və bir boş yer; iki “i” və “j” hərflərini bir xanada yazmaq şərti ilə latın əlifbasının 26 hərfi) doldurulur.

Mətnin şifrlənməsi üçün onun hər bir hərfi kvadrat cədvəldə tapılır və bu hərfin əvəzinə cədvəldə ondan aşağıdakı sətirdə eyni sütunda yerləşən hərf yazılır. Hərf sonuncu sətirdə yerləşərsə, onun əvəzinə həmin sütunda birinci sətirdə yerləşən hərf götürülür. Şifrləmə üsulu əvəzetmə sinfinə aiddir.

Şifrin açarı: kvadratın ölçüsü və əlifba.

Məsələn, latın əlifbası üçün

****

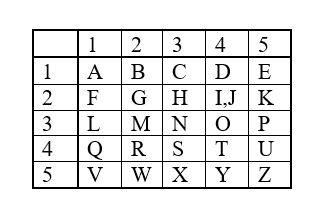
kvadratını götürsək, “KRİPTOQRAFİYA” sözünün şifr kodu “PWOUTVWFODF” olar.

*Nömrələnmiş kvadrat.* Yunanlar və romalılar gizli əlaqə üçün əlifbanın hərfləri ilə ardıcıl doldurulmuş və nömrələnmiş Polibiy kvadratından istifadə edirdilər. Belə ki, əlifbanın hərfləri ilə doldurulmuş Polibiy kvadratının sətirləri və sütunları 1-dən 5-dək nömrələnir.

Mətnin şifrlənməsi üçün onun hərfləri kvadratda tapılır və hərfin əvəzinə onun yerləşdiyi sətrin və sütunun nömrələri cütü yazılır. Bu üsul əvəzetmə şifrləri sinfinə aiddir.

Şifrin açarı: sütunları və sətirləri nömrələnmiş kvadrat.

Məsələn, latın əlifbası üçün düzəldilmiş

****

kvadrata əsasən “KRİPTOQRAFİYA” sözünün şifrkodu “25 42 24 35 44 34 41 42 11 21 24 54 11” olar.

*Sezar şifri.* Bizim eranın I əsrində Yuli Sezar senata göndərdiyi məktubları hərfləri əlifbada 3 mövqe sürüşdürmə yolu ilə şifrləyirdi. 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, şifr əvəzetmə üsulları sinfinə daxildir.

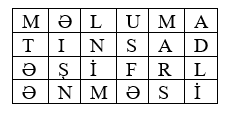
Şifrin açarı: əlifba və sürüşmə.

Məsələn, latın əlifbası üçün Sezar “VENI VEDI VICI” (Gəldim, gördüm, qalib gəldim) ifadəsini əlifbada 3 hərf sağa sürüşdürməklə “YHQL YHGL YLFL” kimi şifrləmişdi.

*Sütunların (sətirlərin) transpozisiyası.* Məlumatın şifrlənməsi üçün hərflərinin yerdəyişməsi üçün sadə *M*x*N* ölçülü şifrləmə cədvəlindən istifadə edilir. Burada *M* – cədvəlin sətirlərinin sayı, *N* isə sütunlarının sayıdır. Şifrləmə üçün məlumat cədvəlin içərisinə sətirlərlə (və ya sütunlarla) yazılır və sütunlarla (və ya sətirlərlə) oxuyurlar. Beləliklə, ilkin məlumatın hərfləri yerlərini dəyişmiş olur.

Şifrləmənin açarı: cədvəlin ölçüsü.

Məsələn, “MƏLUMATIN SADƏ ŞİFRLƏNMƏSİ” cümləsini 4x6 ölçülü cədvəl vasitəsilə aşağıdakı kimi şifrləmək olar. Məlumat cədvələ sətirlərlə yazılır:



Belə cədvəldə yazılmış məlumatı sütunlarla oxuduqda “MTƏƏƏIŞNLNİMUSFƏMARSADLİ” şifri alınar.