**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**

**Sərbəst iş №4**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

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

**Mövzu:** “Məlumatların şifrələnmə metodları”

**Qrup:** 2441a

**Tələbə:** Həsənli İlkin

**Müəllim:** Heydərzadə Nübar

**BAKI 2024**

**Məlumatların şifrələnmə metodları**

İnformasiya təhlükəsizliyinin əsas istiqamətləri olan “Axınla şifrləmə” üsulları qammalaşdırmanın bir növüdür və açıq mətni bit-bit şifrmətnə çevirir. İnformasiyanın gizliliyinin, tamlığının təmin olunması və təhrif 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:

* **İstifadə 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 kanalın olmasıdır. Aşağıda göstərilən şəkildən göründüyü kimi, məlumatı göndərən şəxs gizli şifrləmə açarından və alqoritmini istifadə etməklə açıq məlumatı əvvəlcədən şifrləyir. Bundan sonra isə 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

Məlumatı göndərən tərəflə, o məlumatı alan tərəf eyni açardan istifadə edir. Buna görə də bu üsula **Bir-açarlı** və ya **Simmetrik şifrələmə sistemi** deyilir.

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 **asimmetrik şifrələmə sistemi** 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*)

Bu üsulda 2 açardan istifadə olunur. Açarlardan biri **açıq**, digəri isə **gizli** açardır. Açıq açar adından məlum olduğu kimi hər kəsə açıqdır. Ondan məlumatı şifrələmək üçün istifadə olunur. Gizli açar isə yalnız məlumatı alan tərəfə verilir. Gizli açar vasitəsilə şifrələnmiş məlumatın şifri açılır. İki açardan istifadə olunması daha təhlükəsizdir. Buna görə də Asimmetrik üsul Simmetrik üsula nisbətən daha çox istifadə olunur.

**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.

**Qammalaşdırma üsulları**

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

**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.

**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.