**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**



**Sərbəst iş №1**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

**Mövzu:** “məlumatların şifrələnmə metodları”

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

**Qrup:** 2441a

**Tələbə: Əlibabayev İsmayıl**

**Müəllim: Heydərzadə Nübar**

**BAKI 2024**

XX əsrin 70-ci illərinə kimi verilənlərin şifrələnməsi üsullarının yaradılması və öyrənilməsi ilə məşğul olan elm sahəsi və praktiki fəaliyyət kriptoqrafiya adlanırdı. İndiki zamanda elmin, texnikanın və praktiki fəaliyyətin bu sahəsi yaradıcılıq ilə əlaqəlidir, informasiyanın müdafiə sisteminin kriptoqrafik təhlilini və tətbiqini həyata keçirir.

**ŞİFRƏLƏMƏ**

Şifrləmə dedikdə açıq mətn adlanan M başlanğıc məlumatının şifrələnmiş mətn (və ya şifrmətn) adlanan Mı formasına çevrilməsi başa düşülür. Nəzərə almaq lazımdır ki, əks çevirməni həyata keçirmək üçün açar adlanan əlavə informasiyaya malik olmaq lazımdır. Bəzi istifadəçilər şifrələməni kodlaşdırma ilə səhv salırlar. Əslində bu proseslər arasında hiss olunacaq dərəcədə fərq vardır. Kodlaşdırmada da başlanğıc məlumatın başqa bir formaya çevrilməsi prosesi yerinə yetirilir, amma bu çevrilmədə məqsəd informasiyanın əlverişli ötürülməsi və ya əlverişli təhlil edilməsidir. Məsələn, xüsusi hazırlanmış mətn ikilik kod ilə kodlanır (yəni hər bir simvol 1 və 0 –ların ardıcıllığı ilə əks olunur). Məqsəd bu informasiyanı Elektron Hesablama Maşınında rahat təhlil etmək, lazım gəldikdə yaddaşda saxlamaqdır, çünki elektrik impulsları ardıcıllığı ilə əks olunan informasiyanı kabel vasitəsilə ötürmək rahat və əlverişlidir. Şifrələmənin məqsədi isə başqadır. Mətn ona görə şifrələnir ki, şifrəni açmaq üçün açara malik olmayan kənar şəxs (daha doğrusu pisniyyətli insan) şifrələnmiş mətni oxuya bilməsin (hətta mətn haqqında müəyyən məlumata malik olsa da belə).

Beləliklə, şifrələmə informasiyanın konfidensiallığını təmin edən alətdir. Şifrələmə alqoritmi iki böyük qrupa bölünür:

1.Simmetrik (ənənəvi şifrələmə);

2.Açıq açarla şifrələmə.

**SİMMETRİK ŞİFRƏLƏMƏ**

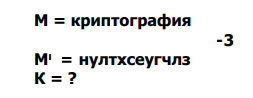
Şifrələmənin simmetrik alqoritmində bir K açarından istifadə olunur. Açar məlumatı şifrələmək və sonrakı mərhələdə şifrədən çıxarmaq (deşifrə) üçün istifadə edilir. Deməli, məlumatı göndərən və qəbul edən həmin açara malik olmalıdır. Öndə söylənənləri sxem şəkilində belə yazmaq olar:



Burada E – şifrələmə funksiyasıdır (encrypt), D - isə deşifrələmə funksiyasıdır (decrypt), hər iki funksiya bir yerdə K açarından istifadə edir. Tarixə nəzər salsaq görərik ki, şifrələmə birinci yaranmışdır. Bununla yanaşı XX əsrin ortalarına kimi bu üsul şifrələmənin yeganə üsulu sayılırdı. Simmetrik alqoritm indiki zamanda geniş istifadə olunur. Simmetrik alqoritm üç sinifə bölünür: 1. Dayaqlıq alqoritmi; 2.Başqasının yerinə qoyulma alqoritmi; 3.Həm dayaqlıq, həm də ki, başqasının yerinə qoyulma alqoritmi (EHM-da informasiyanın mühafizə edilməsi üçün müasir dövrdə hazırlanan bütün alqoritmlər praktiki olaraq bu sinifə aiddirlər).

**DAYAQLIQ ALQORİTMİ**

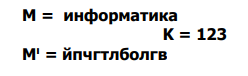
Şifrələmənin dayaqlıq alqoritmi aşağıdakı prinsipə uyğun işləyir: baçlanğıc məlumatın hər bir siqnalı (və ya simvollar ardıcıllığı) digər simvol ilə (və ya digər simvolların ardıcıllığı ilə) əvəz olunur (dəyişdirilir). Konkret nümunələrə baxaq. Sezar şifri. Ən qədim və ən sadə dayaqlıq şifri Qay Yuliy Sezar tərəfindən istifadə edilən şifr sayılır. Burada başlanğıc məlumatın hər bir şifrələnən hərfi özündən üç mövqe sonra duran hərflə əvəz olunur.



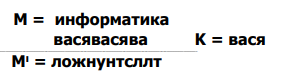
Y.Sezar şifrinin xüsusiyyəti onun açarının olmamasıdır. 3 ədədi açar kimi istifadə edilə bilməz, çünki o məlumat göndərən tərəfindən seçilmir, sadəcə olaraq hərfin yerindən tərpədilməsi üçün istifadə edilir. Qeyd etmək lazımdır ki, Y.Sezarın rəhbərliyi dövründə göstərilən hal şifrin asanlığı sayılmırdı. İndiki zamanda informasiyanın şifrələnməsi və deşifrələnməsi prosesi o qədər mürəkkəbləşdirilmişdir ki, lazım olan əməliyyatların əl ilə həyata keçirilməsi mümkün deyil. Bu məqsədlə proqram təminatından istifadə edilir və bu işlə məşğul olan şəxs lazım gəldikdə tamamilə şifrələmə alqoritmini bərpa edə bilir. Kriptoqrafik proqram təminatı geniş kütlə üçün nəzərdə tutulmayanda bu qayda-qanun pozula bilər. Məsələn, elektron səsvermə sistemlərində, hökumət əlaqə xətlərində istifadə olunan üsuldan imtina olunanda və s. nümunə kimi göstərilə bilər. Təcrübə göstərir ki, bədniyyətli insanlar kriptoqrafik müdafiə sistemini sındırmaqla proqrama daxil ola bilir, istifadə olunan alqoritmləri təhlil edirlər.

Qronsfeld şifrəsi.

Yuli Sezarın şifrəsinin modifikasiya olunmuş halını nəzərdən keçirək. Açar kimi fiksə olunmuş uzunluğa malik rəqəmlər ardıcıllığından istifadə edilir. Əgər açarın üzunluğu mətnin uzunluğundan qısadırsa, ardıcıllığın hər bir rəqəmi açıq mətnin bir simvolu ilə yazılır və bu halda açar dövrü olaraq təkrarlanır. Nümunə kimi “информатика” sözünü “123” açarı ilə şifrələyək.



Cari şifr (Şifr Jül Vernin “Janqada” romanında oxuculara təqdim edilmişdi) çoxəlifbalı şifrəyə (və ya mürəkkəb dəyişən şifrəyə) aiddir. Çoxəlifbalı şifrədə açıq mətnin 1-ci simvolu çoxəlifbalı şifrənin köməyilə şifrələnir. Burada 1-ci simvolun açarı K1, 2-ci simvolun açarı K2 və s. n-ci simvolun açarı Kn, n+1 –ci simvolun açarı isə yenidən K1 olacaqdır. n istifadə edilən əlifbaların (və ya sadə dəyişən şifrələrin) sayıdır. Öndə verilmiş nümunədə n=3. Çoxəlifbalı şifrənin xüsusiyyətlərindən biri Qronsfeld şifrəsinin yaxşı formada nümayiş olunmasıdır. Qronsfeld şifrəsinin müəyyən çətışmazlıqları da vardır ki, onlarda Qronsfeld şifrəsinin modifikasiya edilməsi ilə aradan qaldırılmışdır, yəni açar kimi rəqəmlərdən deyil, hərflər ardıcıllığından istifadə olunmasıdır. Açıq mətndəki hərflərin sıra nömrəsi onların altında yazılmış açarın hərfləri ilə üst-üstə yığılır və nətəcədə şifrələnmiş mətnin hərflərinin sıra nömrəsi alınır.



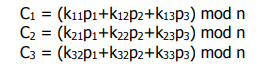
Öndə araşdırılmış Sezar və Qronsfeld şifrələrinin “toplanma” mexanizmi (rəqəmlərlə və ya hərflərlə) başqa şriflərdə də istifadə olunur. Belə şifrələrin xüsusiyyəti ondan ibarətdir ki, şifrə açarın bərpa edilməsinə imkan verir (əgər açıq və şifrələnmiş mətn məlumdursa). Bu əks əlaqə əməliyyatı ilə, yəni “toplanma” – “çıxılma” ilə yerinə yetirilir. Beləliklə, əgər pisniyyətli insan (düşmən) açıq mətnə malikdirsə və bu mətnə uyğun şifrəni bilirsə, onda o açara sahib ola bilər və açardan istifadə etməklə digər şifrələnmiş mətnlərin də şifrəsini açmağa cəhd göstərə bilər. Belə bir üsul məlum açıq mətnlə yerinə yetirilən kriptoanaliz adlanır. Təcrübə göstərir ki, Qronsfeld şifrəsi ilə şifrələnmiş mətn bu üsulun qarşısında acizdir. Bəzən düşmənləri ən çox yayılmış üsulla aldadırlar, yəni qəsddən düşmənin aça biləcəyi şifrəyə uyğun mətni şifrələyir və kanal vasitəsilə ötürürlər. Bundan xəbərsiz pisniyyətli insan göndərilmiş mətni şifrədən azad edir və yalanlardan ibarət olan mətni məqsədi üçün istifadə edir. Nəticədə şifrədən azad olmuş mənasiz söz yığımına sahib olur. Belə şifrələmədən Böyük Vətən Müharibəsində (1941-1945-ci illərdə) geniş istifadə edilirdi.

**Çoxhərfli şifrələmə.**

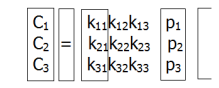
Dayaqlıq şifrələnməsində qeyd olundu ki, şifrələmə zamanı ilkin məlumatın hər bir simvolu deyil, simvollar qrupu şifrələnir. Nəzərə almaq lazımdır ki, bu zaman şifrələnəcək simvollar qrupu başqa bir qrupun simvolları ilə şifrələnir. Belə şifrələnmə çoxhərfli şifrələmə adlanır. Çoxhərfli şifrələməni aydınlaşdırmaq üçün Pleyfeyer şifrələnməsini araşdıraq. Şifrələmə zamanı şifrələmə vahidi kimi biqrammadan (hərf cütlüyü) istifadə edilir ki, burada da bir hərf cütlüyü digər hərf cütlüyü ilə əvəz olunur. Şifrələmə ingilis əlifbası üçün nəzərdə tutulmuşdur. Açar kimi istifadə edilən kod cümləsi (ibarəsi) 5x5 kvadrat çərçivənin birinci hücrəsinə yazılır (təkrarlanan hərflər buraxılır). Sonra isə çərçivənin birinci hicrəsinə yazılmış hərflərdən başqa yerdə qalan bütün hərflər kvadratın çərçivəsinə əlifba sirası ilə yazılır (daha doğrusu çərçivə doldurulur). Nəzərə almaq lazımdır ki, I və J hərfləri eyni hərf kimi qəbul olunur. Çərçivəni açar sözü olan MONARCHY sözü ilə dolduraq.



İlkin mətn biqramma bölünür. Əgər açıq mətndə iki eyni hərf bir biqramm əmələ gətirirsə, onda onlar arasında X simvolu qoyulur (məsələn, BALLOON BALXLOON kimi şifrələnir). Əgər biqramm bir sətirdən (sütundan) ibarətdirsə, onda dövrü yerdəyişməni nəzərə almaqla onlar birinci (aşağıdakı) qonşu sətir ilə yerlərini dəyişirlər. Nümunədə OR NM kimi, OP isə HV kimi şifrələnir. Əgər biqrammın hərfləri müxtəlif sətirlərdə və sütunlarda yerləşirlərsə, onda hər bir hərf cütlüyü sətirin və sütunun kəsişdiyi hücrədə yerləşən ikinci hərf ilə əvəz olunur. Məsələn, BE CI kimi, OS isə AP kimi şifrələnir. Deməli, INFORMATION sözü GAPHMORSFAAW kmi şifrələnəcək. Carı şifrə ilkin mətnin statistik xüsusiyyətini saxlayır, yəni tezlik biqramm cədvəlini dil üçün qurmaq olur və bu zaman şifrələnmiş mətnin biqramm tezliyini təhlil etmək mümkün olur. Digər tərəfdən ingilis dilində 26 hərfin olduğunu nəzərə alsaq, onda biqramm 262 = 676 olacaq. Bu baxımdan məsələ mürəkkəbləşir, şifrələnən mətnin həcminin artması nəticəsində çəkilən zəhmət uçuruma gedir. Digər maraqlı çoxhərfli şifrələməyə nümunə kimi Hill şifrini göstərmək olar. Şifrə m əmsallı m xətti bərabərliklərdən ibarətdir. Şifrə açiq mətnin hər bir m hərfini şifrələnmiş m hərfi ilə əvəz edir. Məsələn, m=3 olduqda aşağıdakı bərabərlik sistemini əldə edirik (burada n - əlifbanın gücüdür).



Şifrələmə açarı K əmsallı matrisa olacaqdır, amma şifrələməni vektorun tərtibi kimi təqdim etmək olar. Şifrələmə vektorunun tərtibi açıq mətnin hərflərinin ardıcıllıq nömrələrindən tərtib edilmişdir (birinci hərf 0 nömrəsinə malikdir). Onda K açar matrisası belə olacaqdır:



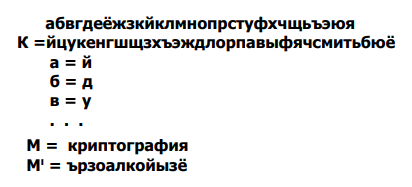
Şifrələnmiş mətni deşifrə etmək üçün matrisanı k əmsalına əks olan k-1 əmsalına vurmaq lazımdır. Hill şifri ilkin məlumatın simvollar tezliyini yaxşı mühafizə etsədə (gizli saxlayır) məşhur açıq mətn kriptotəhlilinə zəif cavab verir. Sistem xəttidir, odur ki düşmənə şifrəni açmaq üçün m3 cüt qədər “aşıq mətn – deşifrə olunmuş mətn” əməliyyatını həyata keçirmək lazımdır. Cari şifrə üçün daha effektli kriptotəhlil üsulu seçilmiş açıq mətnlə kriptotəhlil üsuludur.

**Birdəfəlik bloknot.**

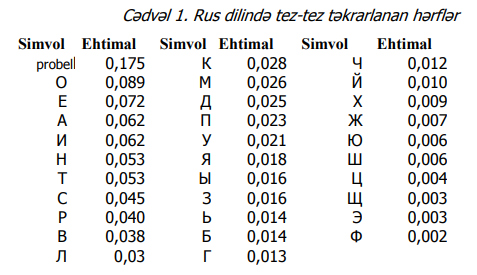
Qeyd etmək lazımdır ki, öndə baxılan bütün şifrələmə üsulları klassik alqoritmlərlə şifrələməyə aiddirlər və elm və texnikanın kompütersiz dövrlərində istifadə olunmuşdur. İstifadə olunan hər bir alqoritm müəyyən növ kriptotəhlil ilə bağlı olmuşdur. İndiki zamanda yeni şifrələmə üsullarından istifadə olunur ki, onları “sındırmaq” həddindən artıq çətindir. Şifrə Vernama şifrəsi adlanır (bəzi ədəbiyyatlarda onu birdəfəlik bloknot da adlandırırlar). Vernama şifrəsində açıq mətn onun ölçüsü ilə uyğun gələn mütləq təsadüfi açarla üst-üstə qoyulur. Sonra açar ləğv edilir (yəni digər mətnlərin şifrələnməsində istifadə olunmur). Şifrənin mütləq kriptodavamlığı Klod Şennon tərəfindən sübut olunmuşdur. Təcrübədə birdəfəlik bloknotdan təsadüfi hallarda istifadə olunur (əsasən yüksək səviyyəli məlumatları şifrələyəndə ondan istifadə edilir). Digər tərəfdən bloknotun hazırlanması çox baha başa gəlir. Bununla yanaşı şifrə açarının şəxsə təqdim edilməsi şəxs ilə təkbə-tək görüş zamanı yerinə yetirilməlidir.

**Çoxəlifbali şifr (sadə dəyişməklə alinan şifr).**

Dayaqlıq şifrələrindən geniş yayılmışıdır. Burada əlifbanın hər bir simvoluna digər əlifbanın bəzi simvolu uyğun gəlir. Şifrələmə zamanı açıq mətndəki hər bir simvol uyğun digər simvol ilə əvəzlənir. Şifrə açar kimi hazırlanmış cədvəldən istifadə olunur. Başqa sözlə, şifrələnmiş mətnə açar əlifbada yeri dəyişdirilmiş simvollardır.



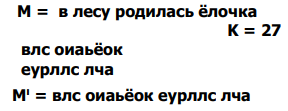
Göstərilən nümunədə aşarların sayı yerdəyişmədə iştirak edən hərflərin sayına, yəni 33-ə bərabərdir. Əgər milyon kompüter milyon mümkün açarların sayını yoxlasaydı, bütün variantların yoxlanmasına milyon il lazım gələcəkdi. Deməli, monəlifbalı şifrə seçim üsulu ilə açarın seçilməsinə imkan vermir, şifrənin sındırılması isə mümkün deyil. Amma cari şifrə sadə şəkildə kriptoanalız aparmağa imkan verir. Kriptotəhlil hər bir simvolun hesablanması və həmin simvolun rast gəlinmə tezliyi ilə yerinə yetirilir. Kifayət qədər uzun məlumat (4 - 5 tərtibli cümlə) üçün bu informasiya kifayətdir, əlifbanın hərflərinin cədvələ uyğun təkrarlanması ilə onu tutuşdurmaq olar. Məlumdur ki, bütün dillərdə istifadə olunan sözlərdə əlifba simvolların təkrarlanması mövcuddur, məsələn, rus dilində “O” hərfi daha tez-tez təkrarlanır, nəin ki, “Ф” hərfi. Bunu aşağıdakı cədvəldə aydın müşahidə etmək mümkündür.



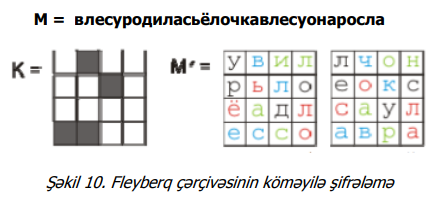
İngilis dilində aparılmış araşdırmalar göstərir ki, ən çox the artikulundan istifadə edilir. Beləliklə, monoəlifba şifrəsi aparılan kriptoanalizə zəif müqavimət göstərir. Bu baxımdan düşmənə məqsədyönlü açar axtarmaq lazım deyil, açar şifrəni araşdıran zaman özü-özünə bərpa olunacaq.Öndə yazılanlardan aydın olur ki, Q.Y.Sezarın şifrəsi də monoəlifbalı idi.

**BAŞQASININ YERİNƏ QOYULMA ALQORİTMİ**

Bu alqoritmdə açıq mətnin simvolları açarın müəyyən etdiyi simvollar ardıcıllığı ilə dəyişdirilir (başqasının yerinə qoyulur). Bunu nümunədə aydınlaşdıraq. Açıq mətnin simvolları soldan sağa deyil, yuxarıdan aşağı başqasının yerinə qoyulur və nəzərə alınır ki, sütunun hündürlüyü məhduddur. Nəticə sətir kimi alınır.



Şifrə açarın seçilməsi ilə bağlıdır (açar kimi sütunun hündürlüyü iştirak edir) və istənilən halda açar məlumatın uzunluğundan çox ola bilməz. Fleyberq çərçivəsinə başqa bir nümunədə baxaq. Şifrə açar kvadrat çərçivədir və çərçivənin yanları cüt sayda hücrələrdən ibarətdir. Hücrələrin dörddə biri (çərək) aşağıdakı prinsiplə kəsilir: əgər bəzi hücrə kəsilmişsə, onda həmin hücrə kəsilə bilməz, çünki o hücrə çərçivənin 900 , 1800 və 2700 dönməsində hüdudu aşır. Mətni şifrələmək üçün kəsiklə olan çərçivə cızıqlanmış kvadratın üzərinə qoyulur, sonra isə mətnin hərfləri kəsiklərə yazılır. Bütün kəsiklər dolduqdan sonra çərçivə 900 döndərilir. Çərçivənin dolma prinsipinə görə kəsiklər bu zaman dolmamış hücrələrin yerinə olacaqdır. Kəsiklərə mətnin davamı yazılır, yenidən çərçivə döndərilir və prosedur bir dəfə də təkrar olunur. Əgər mətn bir kvadrata yerləşməmişsə, onda eyni qayda ilə növbəti doldurulur. Sonuncu kvadratın boş qalmış hücrələri təsadüfi simvollar ilə doldurulur.



Fleyberq şifrəsi hamı tərəfindən (sözsüz ki uçaqlar nəzərdə tutulur) sevilə-sevilə oxunan mahnıdan istifadə etməklə hazırlanmış açıq mətnin kriptotəhlilinə o qədər də tutarlı səviyyədə cavab verə bilmədi (nəzərə almaq lazımdır ki, ikilik əlifba üçün bu əlaqə müəyyən qədər azdır, amma təbii-dil əlifbaları üçün belə söyləmək düzgün deyil).

**DES alqoritmi.**

Uzun müddət ən məşhur simmetrik şifrələmə alqoritmi DES (Data Encrypting Standart) sayılırdı (alqoritm 1977-ci ildən istifadə edilməyə başlanmışdır). Alqoritm Faystel şifrəsinin struktur bazasına söykənir. Alqoritm 64 bitlik bloka və 56 bitlik açara malikdir. F raundun funksiyası səkkiz S-matris adlanan toplumdan bəhrələnir. Hər bir matris 4 sətirdən ibarətdir, hər bir sətir isə 0-dan 15-ə qədər rəqəmlərin (uyğun olaraq 16 sütundan) yerdəyişməsindən ibarətdir. Matrislər sərt verilmişdir. Hər bir matris 6 bitlik girişə malikdir və 4 bitlik nəticə verir. Girş kəmiyyətinin birinci və axırıncı biti matrisin sətirini, yerdə qalan dördü isə sütunlarını əks etdirir. Hesablamada ikilik say sistemindən istifadə olunur, sətirlərin və sütunların kəsişməsi çevrilmənin nəticəsi olacaqdır. Burada F çevrilməsi aşağıdakıları özündə əks etdirir:

1. 32 bitlik Ri bloku bəzi (bir para) 16 biti xüsusi cədvəlin köməyindən istifadə etməklə, təkrarlamaq yolu ilə 48 bitə kimi genişləndirilir.

2.Alınmış nəticə XOR əməliyyatının köməyilə 48 bitlik Ki altaçarından istifadə etməklə cəmlənir (üst-üstə yığılır).

3.Cəmlənmənin nəticəsi 8 altıbitlik bloka bölünür və onlardan hər biri uyğun S –matrisinin köməyilə yaradılır.

4.Nəticədə alınmış 32-bitlik blok dayaqlıq alqoritmində sərt verilmiş yerdəyişməyə məruz qalır.

Uzun müddət ərzində DES ABŞ-ın federal standartı olmuşdur. Alqoritm lazımı formada “sürətli axın effektini” nümayiş etdirir (açıq mətnin bir bitinin və ya açarının dəyişməsi şifrələnmiş mətnin çoxlu sayda bitlərinin dəyişməsinə səbəb olur) və uzun illər boyu şifrənin sındırılması cəhdinə qarşı mətanətlə dura bilmişdir. Digər tərəfdən uzunluğu 56 bit olan açar məhsuldarlığı böyük sürətlə artan EHM-lərin tələblərini tutarlı səviyyədə ödəmədiyi üçün 1997-ci ildə yeni alqoritmin yaradılması üçün müsabiqə elan olundu. Müsabiqənin şərti belə idi: yaradılacaq alqoritm ən azı 15-20 il müddətində kriptostandartlara lazımı səviyyədə qulluq göstərməlidir.

**AES alqoritmi.**

Müsabiqənin qalibi 2000-ci ildə müəyyən olundu – qalıb Belçika şifri RIJNDAEL elan olundu. Bir müddət sonra şifrə AES (Advanced Enecryption Standard) adlandırılır. Şifrə qeyristandart blok şifrəsidir və Feyştel şəbəkəsindən istifadə etmir. Hər bir giriş bloku ikiölçülü bayt massivi kimi təqdim edilir (blokun ölçüsündən asılı olaraq 4x4, 4x6 və ya 4x8 kimi müxtəlif şəkildə göstərilə bilər). Blokun ölçüsündən və açarın uzunluğundan asılı olaraq alqoritm 10-dan 14-ə kimi raundlardan ibarətdir və hər bir raundda bəzi dəyişikliklər həyata keçirilir (ya asılı olmayan sütunlar üzərində, ya asılı olmayan sətirlər üzərində, ya da ki, cədvəldə olan baytlar üzərində). Öndə sadalanan şifrələrlə yanaşı indiki zamanda IDEA, Blowfish, RC5, CAST-128 simmetrik şifrələrindən də istifadə olunur.