UOT 623; 519.7

MƏTNLƏRİN ŞİFRLƏNMƏSİ ZAMANI TƏTBİQ OLUNAN ÜSULLARIN ƏSAS PRİNSİPLƏRİ

mayor Fərman Məmmədov
Silahlı Qüvvələrin Hərbi Akademiyası
E-mail: fermanmemmedov@gmail.com

Xülasə. Məqalədə klassik və müasir şifrləmə alqoritmləri haqqında qısa məlumat verilir, onların tətbiq prinsipləri misallar üzərində izah edilir və şifrləmə üsullarının mürəkkəblik dərəcəsi müzakirə olunur. Həmçinin mətnlərin müasir şifrləmə üsullarına dair son dövrdə mövzu ilə bağlı elmi ədəbiyyatda rast gəlinən alqoritmlər şərh edilir. Müasir kompüter texnologiyalarının imkanlarından çıxış edərək mətnlərin şifrlənməsi üçün yaradılacaq yeni üsulların hibrid xarakterli olması tövsiyə olunur.

Açar sözləri: klassik kriptoqrafiya, müasir kriptoqrafiya, alqoritm, simmetrik şifrləmə, mətn şifrləməsi, əvəzetmə şifrləri, birəlifbalı şifrlər, çoxəlifbalı şifrlər.

Giriş

Son illər informasiya-komunikasiya texnologiyalarının sürətli inkişafı informasiya təhlükəsizliyi problemləri ilə bağlı yeni məsələləri və yeni imkanları gündəmə gətirmişdir. Elm və texnikanın inkişafı, sosial proseslərin mürəkkəbləşməsi, məlumat həcminin çoxalması idarəetmənin effektivliyinin artırılmasına get-gedə daha yüksək tələblər irəli sürür. İdarəetmənin yaxşılaşdırılması üzrə imkanların genişlənməsi ilk növbədə idarəetmə elmi, informasiya texnologiyaları (İT), elektron hesablama texnikası və rabitə vasitələrinin intensiv inkişafı ilə bağlıdır [1].

İT mühitinin genişlənməsi, onun insan həyatının bütün sahələrinə daxil olması ilə nəticələnmişdir. İnternetin yayılması insanlar arasında məlumat mübadiləsinin artmasına, onların həyat fəaliyyətinin asanlaşdırılmasına, həmçinin idarəetmə prosesinin daha çevik həyata keçirilməsinə və s. geniş imkanlar yaradır. Hazırda İT-nin bu şəkildə yayılması Ordunun müvafiq qurumları, qərargahları, idarəetmə məntəqələri, eləcə də müasir silah sistemləri arasında məxfi əlaqənin təmin edilməsini prioritet məsələyə çevirir.

Həyatı asanlaşdıran informasiya mübadiləsi çox ciddi təhlükəsizlik boşluqlarının əmələ gəlməsinə səbəb olur. Ötürülən məlumatları icazəsiz əldə edərək onları öz maraqları çərçivəsində təhrif etməyə can atan qeyri-qanuni istifadəçilərin olması ehtimalı nəzərdə saxlanılmalıdır. Bu səbəbdən də məlumatın mövcud rabitə kanalları vasitəsilə ötürülməsi, eyni zamanda ötürülən məlumatı yalnız tələb olunan şəxslərin oxuya bilməsi zərurəti meydana gəlmişdir [2].

Müasir ordularda informasiyanın göndərilməsi, saxlanılması və emalı üçün İT-nin tətbiqinin gündən-günə bütün sahələrə yayılması kiber hücumçuların (bədniyyətlilərin) marağının daha da artmasına səbəb olur. Bir-biri ilə əlaqə saxlayan iki abonent arasındakı məlumatların üçüncü şəxs tərəfindən əldə olunması və dəyişdirilməsi gün keçdikcə adi hala çevrilir. Bu da öz növbəsində informasiya təhlükəsizliyi məsələsini gündəmə gətirir.

İnformasiya təhlükəsizliyi dedikdə, müxtəlif informasiya-kommunikasiya texnologiyaları, avadanlıqların və proqram təminatlarının birgə tətbiqindən meydana gələn mürəkkəb infrastrukturlarda məlumatların qorunması, emalı, fasiləsiz işinin təmin edilməsi, digər təhdidlərə qarşı mübarizə üsulları və müxtəlif mübarizə vasitələri başa düşülür. Təhlükəsizlik sisteminə cavabdehlik daşıyan qurumların kritik strukturlarına olan təhdidlər hər bir dövlətdə real xarakter daşıyır. Bu baxımdan təhlükəsizliyi təmin etmək üçün müxtəlif qoruma mexanizmləri işlənilmiş, yeni texnologiyalar, alqoritm və proqramlar hazırlanmışdır. Bu texnologiyalardan biri şifrləmədir (kriptoqrafiya).

İnformasiyanın şifrlənməsi və deşifrləmə

Məlum olduğu kimi, informasiyanın şifrlənməsi, icazəsi olmayan şəxslər tərəfindən onun istifadəsinin qarşısını alınması və məxfiliyin təmin edilməsi məsələləri ilə elmin xüsusi sahəsi – kriptologiya məşğul olur. Kriptologiya – informasiyanın çevrilməsi və başqa şəklə salınması (şifrlənməsi) ilə informasiyanın qorunması, eləcə də onların açılması üsullarını öyrənən elmdir [3]. Kriptoqrafik şifrləmə zamanı göndərilən və qorunması tələb olunan rəqəmli məlumat müəyyən açardan istifadə edilərək şifrləmə alqoritmləri vasitəsilə anlaşılmaz formaya salınır və göndərilir. Qəbul edən tərəf isə müvafiq deşifrləmə əməliyyatı ilə məlumatı bərpa edir.

Şifrləmə və deşifrləmə əməliyyatları, bir qayda olaraq, aşağıdakı şəkildə həyata keçirilir:

$$C = E_k(M), \quad (1)$$

$$M = D_k(C). \quad (2)$$

Burada, C – göndərilən şifrlənmiş kontenti (Cipher), M – məxfi məlumatın mətnini (Message), E və D – müvafiq olaraq şifrləmə (Encryption) və deşifrləmə (Decryption) alqoritmlərini, k – isə açar sözü (Key) ifadə edir.

Kriptoqrafik şifrləmə üsulları (alqoritmləri) istifadə olunan açarların növünə görə, adətən, simmetrik və asimmetrik olur [4, s.149]. Simmetrik alqoritmlər şifrləmə və deşifrləmə əməliyyatları zamanı yalnız bir açardan istifadə edilməklə həyata keçirilir, asimmetrik alqoritmlər isə iki açar vasitəsilə icra olunur.

Hesab edilir ki, şifrləmə alqoritmi maraqlı şəxslərin hamısına məlumdur, şifrlənmiş məlumatın açılması isə yalnız göndərən və alan tərəflərə məlum olan açar söz vasitəsilə həyata keçirilə bilər. Bu baxımdan, açar sözün tərəflərə çatdırılması məxfi məlumatların ötürülməsi ilə bağlı meydana çıxan problemlərdəndir. Qeyd etmək lazımdır ki, ümumi prinsipi (1) və (2) şəklində verilən şifrləmə – deşifrələmə prosesi müxtəlif alqoritmlərlə həyata keçirilir. Bu məqalədə şifrləmə alqoritmlərinin tarixinə nəzər salınır, onların inkişaf mərhələləri təhlil edilir, perspektiv imkanları ilə bağlı ideyalar şərh olunur.

Klassik kriptoqrafik metodlar

İnsanlar qədim zamanlardan bu günə kimi məlumatların gizli ötürülməsi məqsədilə müxtəlif metod və üsullardan istifadə etmişlər [5]. Həmin dövrün əksər şifrləmə üsulları yerdəyişmə və ya əvəzetmə prinsiplərinə əsaslanırdı. Klassik kriptoqrafik üsullar barədə R.M.Əliquliyev, Y.N.İmamverdiyev [3], V.Ə.Qasımov [4], C.E.Shannon [6] və başqalarının əsərlərində ətraflı məlumatlar verilir.

Məlum olan ən qədim şifrlərdən biri Sezar şifridir. Bir əlifbalı əvəzetmə şifrləri sinfinə aiddir. Burada ilkin mətnin hər bir hərfi əlifba sırasında ondan müəyyən olunmuş k sayda sonrakı mövqedə duran hərflə əvəz olunur. Əlifbanın sonuncu hərflərinin şifrlənməsi zamanı sıra əlifbanın əvvəlindən davam edir (Cədvəl 1).

Cədvəl 1
Sezar şifrinin Azərbaycan əlifbası ilə tətbiqi

A	B	C	Ç	D	E	Ə	F	G	Ğ	H	X	I	İ	J	K	Q	L	M	N	O	Ö	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

R	S	Ş	T	U	Ü	V	Y	Z	A	B	C	Ç	D	E	Ə	F	G	Ğ	H	...
23	24	25	26	27	28	29	30	31	0	1	2	3	4	5	6	7	8	9	10	...

Əlifbanın hərflərini nömrələməklə, şifrləmə və şifrin açılma qaydasını aşağıdakı kimi yazmaq olar:

$$y = (x + k) \bmod n\,, \tag{3}$$

$$x = \big(y + n\,(k \bmod n)\big) \bmod n\,. \tag{4}$$

Burada, x – açıq mətnin simvolunun nömrəsi, y – şifrlənmiş mətnin simvolunun nömrəsi, n – əlifbanın gücü (əlifbadakı hərflərin ümumi sayı), k – açardır (ikinci sıra hərflərinin birinci sıraya nəzərən neçə hərf sürüşməsinin sayıdır).

Məsələn, açar olaraq 3 ədədini götürək Azərbaycan əlifbası ilə şifrləmənin konkret halına baxaq. Bu zaman hər bir hərf əlifbada sıraca ondan 3 vahid sonrakı mövqedə duran hərflə əvəz olunacaq. Belə ki, "HƏRB" sözü "İĞTD" şəklində şifrlənəcək. İlkin sözü bərpa etmək üçün şifrin nömrələri tapılır və açarla fərqin yerləşdiyi mövqedəki hərf götürülür.

Sadə və primitiv olmasına görə müasir kriptoqrafiyada Sezar şifri çox zəif şifr hesab edilir [2]. Belə ki, hər bir mətn üçün mümkün şifrlənmiş mətnlərin sayı n-dir.

Klassik şifrləmə üsullarının növbəti nümunəsi XVI əsrdə yaşamış kriptoqrafik sistemlərin təkmilləşdirilməsi ilə məşğul olan diplomat Vijinerin adı ilə bağlıdır. O, şifrləmə üçün açar sözdən və əlifbanın hərflərinin sayına (n) bərabər ölçüdə xüsusi şəkildə yaradılmış kvadrat cədvəldən istifadə edirdi. Cədvəlin sətir və sütunları əlifbanın hərfləri ilə nömrələnir və aşağıdakı kimi doldurulur:

– I sətir: əlifbanın n hərfi əvvəldən axıradək xanalara yazılır;

– II sətir: ilk $n-1$ xanaya əlifbanın ikinci hərfdən başlayaraq sonadək bütün hərfləri, n-ci xanaya isə əlifbanın birinci hərfi yazılır;

– n-ci sətir: birinci xanaya əlifbanın n-ci hərfi və ikinci xanadan başlayaraq əlifbanın ilk $n-1$ hərfi yazılır.

Şifrləmə zamanı birinci sətirdə ilkin mətn, ikinci sətirdə onun altından isə açar sözün hərfləri yazılır. Açar sözün uzunluğu ilkin mətnin uzunluğundan qısa olarsa, onda açar söz təkrarlanır. Birinci sətir tərtib olunmuş cədvəlin sütununun, ikinci isə sətrinin göstəricisi olaraq qəbul edilir. Sətir və sütunun kəsişməsində duran hərf şifr kimi götürülür.

Azərbaycan əlifbası üçün Vijiner cədvəli aşağıdakı şəkildə olar (Cədvəl 2).

Cədvəl 2
Azərbaycan əlifbası üçün Vijiner cədvəli

	A	B	C	Ç	D	...	V	Y	Z
A	A	B	C	Ç	D	...	V	Y	Z
B	Z	B	C	Ç	D	...	Ü	V	Y
C	Y	Z	B	C	Ç	...	U	Ü	V
Ç	V	Y	Z	B	C	...	T	U	Ü
D	Ü	V	Y	Z	B	...	Ş	T	U
...	...	...	...	...	...	...	...	...	...
V	Ç	D	E	Ə	F	...	A	B	C
Y	C	Ç	D	E	Ə	...	Z	A	B
Z	B	C	Ç	D	E	...	Y	Z	A

Məsələn, "SİLAH" açar sözü ilə "KRİPTOQRAFİYA" mətni aşağıdakı şəkildə şifrlənir:

İlkin mətn	K	R	İ	P	T	O	Q	R	A	F	İ	Y	A
Açar sözü	S	İ	L	A	H	S	İ	L	A	H	S	İ	L
Şifrmətn	R	H	Ü	P	Q	Ü	Ç	Ə	A	V	Ö	L	L

Vijiner şifrinin başqa bir variantında ilkin mətn və açar sözün sıra nömrələri n moduluna görə toplanılır. Alınan ədədə uyğun simvol şifr kimi götürülür.

Vijiner şifrininin şifrləmə və deşifrləmə əməliyyatını (5) və (6) düsturları şəklində yazmaq olar:

$$C_i = (M_i + k_{(i \bmod m)}) \bmod n\,, \quad (5)$$

$$M_i = (C_i - k_{(i \bmod m)}) \bmod n\,. \quad (6)$$

Burada, C – göndərilən şifrlənmiş kontenti, M – məxfi məlumatın mətnini, k – açar sözü, m – açarın uzunluğunu, i – isə ilkin mətn, açar və şifrdə simvolların yerləşmə nömrəsini ifadə edir.

Vijiner şifri Sezar şifrinin təkmilləşdirilmiş forması hesab olunur. Çünki m = 1 olduğu zaman şifrləmə avtomatik olaraq Sezar qaydasına çevrilir.

Vijiner şifrinin digər bir modifikasiyasında isə açar qismində tərəflərin (göndərən və alan) hər ikisində olan müəyyən bir kitabın mətnindən fraqment istifadə olunur. Bu zaman fraqmentin uzunluğu şifrlənən məlumatın uzunluğuna bərabər götürülür. Qeyd olunmalıdır ki, göndərilən şifrlənmiş məlumatın əvvəlinə şifrləmə açarının kitabın hansı hissəsindən götürüldüyünü göstərən bir cüt ədəd əlavə edilir. Birinci ədəd kitabın səhifəsini, ikinci ədəd isə həmin səhifədə sətrin nömrəsini göstərir. O zaman açar müvafiq kitabın müəyyən olunmuş səhifəsi və səhifədəki sətri göstərən iki ədəddən ibarət olur.

Bu üsulun xüsusi halı kimi, "şeirə görə" şifrləmə üsulu da mövcuddur. Şifrləməni həyata keçirmək məqsədilə əvvəlcədən əlifbanın bütün hərfləri rast gəlinən uzun bir şeir götürülür və ya əzbərlənir. Məlumatın şifrlənməsi zamanı onun hər bir hərfi iki ədədlə əvəz olunur. Bu ədədlərin birincisi həmin hərfin rast gəlindiyi sətri, ikincisi isə sətirdəki sırasını göstərir [4, s.189].

Şifrləmə üsullarından biri də yunan yazıçısı Polibiyə məxsusdur. Onun şifri çoxəlifbalı əvəzetmə prinsipinə əsaslanır. Belə ki, yunan əlifbası əvvəlcə 5×5 ölçülü kvadrat cədvələ yazılır, sonra isə ilkin mətnin hər bir hərfi bu kvadratda tapılır və eyni sütunda ondan aşağıdakı sətirdə yerləşən hərflə əvəz olunur. Polibiy kvadratının Azərbaycan əlifbasına uyğunlaşdırılmış vəziyyəti aşağıdakı cədvəldə göstərilib (Cədvəl 3).

Cədvəl 3
Azərbaycan əlifbası ilə düzəldilmiş Polibiy cədvəli

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

Cədvəldə boş xanalar qalmasın deyə iki xanaya "I" və "İ", eləcə də "J" və K" hərfləri birlikdə yazılıb. Beləliklə, əlifbadakı hərflərin sayına görə cədvəl beş sətir və altı sütundan ibrət olub.

Azərbaycan əlifbasına uyğunlaşdırılmış Polibiy cədvəli ilə "HƏRB" sözünü şifrləsək "MIVF" və ya "MİVF" şəklində şifr əldə edilir. Deşifrləmə zamanı əlifba açar rolunu oynayan düzbucaqlının içinə yazıldıqdan sonra şifrin eyni sütunda, lakin bir ədəd yuxarıdakı sətirdən müvafiq hərflər götürülərək ilkin mətn bərpa olunur.

Polibiy cədvəlinə əsasən, şifrləmə zamanı, ilkin mətnin simvolları əlifba sırası boyunca müəyyən qədər sürüşdürülmüş olur. Bu zaman əlifbanın simvolları dəyişməz olaraq qaldığına görə tərəflər bir-birinə yalnız şifrələnmiş mətni və açar simvolu (sürüşmə addımını) da ötürə bilərlər.

Yunanlar və romalılar gizli əlaqə üçün şifrləmənin digər bir üsulu kimi əlifbanın hərfləri ilə doldurulmuş və nömrələnmiş Polibiy kvadratından istifadə edirdilər. Belə ki, əlifbanın hərfləri ilə doldurulmuş Polibiy kvadratının sətir və sütunları 1-dən 5-dək nömrələnir. Mətnin şifrlənməsi üçün onun hərfləri kvadratda tapılır və hərfin əvəzinə onun yerləşdiyi sətrin və sütunun nömrələr cütü yazılır.

Bu üsul da əvəzetmə şifrləri sinfinə aiddir. Şifrin açarı sütunları və sətirləri nömrələnmiş kvadrat hesab olunur. Şifr isə ilkin mətn hərflərinin mövqelərinə uyğun sətir və sütunların nömrələrindən düzəldilmiş ikirəqəmli ədədlərdən ibarət olur.

Məsələn, Azərbaycan əlifbası ilə düzəldilmiş, sətir və sütunları nömrələnmiş Polibiy cədvəlinə baxaq (Cədvəl 4).

Cədvəl 4

Azərbaycan əlifbası ilə düzəldilmiş və sətir və sütunları nömrələnmiş Polibiy cədvəli

	1	2	3	4	5	6
1	A	B	C	Ç	D	E
2	Ə	F	G	Ğ	H	X
3	I, İ	J, K	Q	L	M	N
4	O	Ö	P	R	S	Ş
5	T	U	Ü	V	Y	Z

Cədvələ əsasən, “KRİPTOQRAFİYA” sözünün şifrkodu “32 44 31 43 51 41 33 44 11 22 31 55 11” olar.

Müasir kriptoqrafik metodlar

Kompüter texnikasının yaranması və tətbiqi ilə əlaqədar ötən əsrin 70-ci illərindən başlayaraq kriptoqrafiya yeni mərhələyə qədəm qoydu. Belə ki, İT-nin meydana gəlməsi kompüterdən istifadə etməklə müasir kriptoqrafik metodların yaranması klassik “əllə” və ya mexaniki şifrləmə üsullarına nisbətən dəfələrlə yüksək kriptoqrafik davamlılığı və sürəti təmin etdi. Eyni zamanda, bütün sahələrdə olduğu kimi bu sahədə də sürətli inkişaf prosesi baş verdi. Nəzərə alsaq ki, zaman-zaman təklif olunan şifrləmə üsulları tətbiq sahəsindən və müasir İT texniki təminatın imkanlarından çıxış edərək özündən əvvəl mövcud olan üsulların çatışmayan cəhətlərinin aradan qaldırılmasına yönəldilmişdir, burada son illərdə dərc olunmuş müasir kriptoqrafik metodların təhlili ilə kifayətlənə bilərik.

S.Udepal və G.Upasnanın [7]-də təklif etdiyi şifrləmə üsulu ASCII cədvəlinə əsaslanır. İlkin mətnin ASCII cədvəlindəki qiymətləri götürülərək onlar arasında ən kiçik qiymət tapılır. İlkin mətnin ASCII qiymətlərinin hər biri ilə aralarındakı ən kiçik qiymət arasında modul əməliyyatı icra olunur. Alınan nəticələrdən hər hansı biri 16-dan böyük olarsa, onda həmin qiymətə 16 ilə modul əməliyyatı tətbiq edilir və həmin qiymətin ilkin mətndəki mövqeyi yaddaşda saxlanılır. Sonra 4 simvoldan ibarət açar generasiya olunur və açarın ASCII cədvəlindəki qiymətləri arasından ən kiçiyi götürülür. Bu dəfə açarın ASCII qiymətlərinin hər biri ilə ən kiçik qiymət arasında modul əməliyyatı icra olunur. Yekun açarı əldə etmək üçün ilkin mətnin modul əməliyyatı icra edilmiş qiymətləri ilə modul əməliyyatı icra edilmiş açar qiymətləri toplanılır. Növbəti addımda ilkin mətnin modul əməliyyatı icra edilmiş qiymətləri ilə yekun açarın qiymətləri cəmlənir. Əldə edilmiş qiymətlərin müvafiq ASCII simvolu şifr kimi götürülür. ASCII cədvəlindən əldə edilmiş nəticəyə uyğun simvol götürülür.

Şifrlənmiş mətni deşifrləmək üçün proses aşağıdakı qaydada yerinə yetirilir:

Şifr daxil edilir və mini-şifr tapılır. Şifr və mini-şifrin ASCII cədvəlindəki qiymətləri götürülür. Yekun açarın ASCII cədvəlindəki qiymətləri tapılır və onların arasından ən kiçiyi götürülür. Şifr və yekun açarın ASCII qiymətləri arasındakı fərq tapılır və yaddaşda saxlanılan mövqedəki qiymətin üzərinə 16 əlavə edilir. Mini-şifr fərqlə toplanılaraq ilkin mətnin ASCII cədvəlindəki qiymətləri əldə olunur. Həmin qiymətlərə uyğun simvollar götürülərək ilkin mətn əldə edilir.

A.B.Paşayev tərəfindən [2]-də təklif olunan metodda latın və kiril əlifbalarının böyük və kiçik hərfləri, Azərbaycan əlifbasının ingilis əlifbasında olmayan hərfləri, eləcə də durğu işarələrindən (klaviaturada mövcud ola simvollardan) ibarət 178 element saxlayan simvoltipli massiv əlifba kimi tərtib olunur. Bir qayda olaraq, şifrləmək və deşifrləmək üçün istifadə olunan açar sözün uzunluğu şifrlənən

mətnin uzunluğundan kiçik götürülür. Mətn və açar sözün simvollarının massivdəki elementlərinə uyğun olaraq, indeksləri ardıcıllıqla tapılır və toplanılır. Alınan ədəd 178-dən kiçikdirsə, massivdə uyğun indeksə malik element, əks halda isə alınan ədəddən 178 çıxılaraq fərqə uyğun indeksə malik element şifr kimi götürülür. Mətnin hər bir sonrakı simvolunu şifrləmək üçün açar sözün növbəti simvolundan istifadə edilir və bu proses açar sözün sonuncu simvoluna qədər davam edir. Mətnin şifrlənməsini davam etdirmək üçün yenidən açar sözün birinci simvoluna müraciət edilir və proses mətnin sonuncu simvolunadək dövri olaraq davam etdirilir. Nəticədə, şifrlənmiş simvollar ardıcıllığı əldə edilir.

Şifrlənmiş mətni deşifrləmək üçün proses əksinə yerinə yetirilir:

– şifrlənmiş mətndəki və açar sözdə iştirak edən simvolların massivdəki elementlərə uyğun indeksləri tapılır;

– şifrlənmiş sözdə iştirak edən simvolun massivdəki elementə uyğun indeksi açar sözdə iştirak edən simvolun massivdəki elementə uyğun indeksindən böyükdürsə, indekslər çıxılır;

– fərq mənfi ədəddirsə, onun üzərinə 178 əlavə olunur;

– alınan ədəd açar sözdəki simvolun massivdəki elementə uyğun indeksindən çıxılır.

Bu proses açar sözün sonuncu simvoluna qədər davam edir. Şifrlənmiş mətnin hər bir sonrakı simvolunu deşifrləmək üçün isə açar sözün ilk simvolundan başlanılır və nəticədə ilkin mətn alınır.

A.B.Paşayevin digər məqaləsində [2]-də təklif olunan alqoritmin açarları tam sayma qaydası və tezliklərin analizi metodlarının tətbiq edərək kriptoanalizi çətinləşdirmək məqsədilə onun bir modifikasiyası verilir və nəticədə alınan alqoritmin mürəkkəbliyi qiymətləndirilir [8]. Bu məqsədlə əlifbanın istənilən simvollarından düzəldilmiş və yalnız sonunda bir boşluq olan simvollar ardıcıllığı "mətn-əlavə" şəklində götürülür. Şifrləmə alqoritminin modifikasiyası əsas mətnə müəyyən "parazit" mətn-əlavələrin daxil edilməsini nəzərdə tutur. Bu əlavələr elə daxil olunur ki, deşifrləmə zamanı onları asanlıqla silmək mümkün olsun. Əlavənin yerindən asılı olaraq, "parazit" simvolların sayı müəyyən həddə müəyyənləşdirilən natural ədədlərlə ifadə olunur. Daha sonra [2]-də təklif olunan alqoritmə müvafiq olaraq şifrləmə həyata keçirilir. Beləliklə, başlanğıc mətn mənasına görə onunla heç bir əlaqəsi olmayan təsadüfi əlavələrlə tamamlanır.

Deşifrləmə zamanı [2]-dəki alqoritmin tətbiqi ilə məlumatın ilkin deşifrlənməsi həyata keçirilir. Sonra isə, birinci mövqedən başlayaraq, hər bir təknömrəli mövqelərdə duran bütün əlavələr silinir.

Z.Alqad tərəfindən təklif olunan metodda rəngli şəkilin piksellərinin mövqelərinə (sətir, sütun və kanal nömrəsi) əsasən, şifrləmə məsələsinə baxılır [9]. Bunun üçün əvvəlcə məxfi şəkil seçilir. Mətnin hər hərfi üçün: ASCII cədvəlinə uyğun olan qiymət əldə edilir, şəkildə ilk rast gəlinən kodun mövqeyi götürülür və mövqenin müvafiq qiymətləri şifr kimi kod matrisinə yığılır.

Deşifrləmə əməliyyatı zamanı kod matrisində olan mövqe məlumatları oxunaraq şəkildəki piksellərə uyğun simvollar vasitəsilə mətn bərpa edilir.

S.E.Ghrare, H.A.Barghi və N.R.Madi [10]-da şifrlənmiş gizli simmetrik açara əsasən, yeni şifrləmə metodu təklif edir. Belə ki, açar ilkin mətnə əsasən, generasiya olunur və şifrin içərisində gizlədilərək qarşı tərəfə göndərilir. Bu metodla açarın qarşı tərəfə çatdırılması problemi həll olunur. Açarın generasiyası üçün əvvəlcə ilkin mətn iki yerə bölünərək K_1 və K_2-yə mənimsədilir. Açarlar bir-birləri vasitəsilə şifrlənir və alınan nəticədə yekun açar K əldə edilir. K ilkin mətnin yarısına bərabər olur. İlkin mətn şifrlənir və şifrin içərisində gizlədilir. Qarşı tərəf əvvəlcə şifrmətndən açarı ayırır və deşifrləmə əməliyyatını apararaq ilkin mətni əldə edir. Şifrləmə və deşifrləmə əməliyyatı aşağıdakı qayda da yerinə yetirilir:

$$C = E(K, M) = (M + K) \bmod 26\,, \tag{7}$$

$$M = D(K, C) = (M - K) \bmod 26\,. \tag{8}$$

Burada, C – göndərilən şifrlənmiş kontenti, M – məxfi məlumatın mətnini, E və D – uyğun olaraq şifrləmə və deşifrləmə alqoritmlərini, K – isə açar sözü ifadə edir.

V.K.Mittal və M.Mukhija 2019-cu ildə Vijiner şifrinin modifikasiya olunmuş variantı təklif etmişlər [11].

Burada, əlifbanın hərflərinin sayına bərabər ölçüdə yaradılmış klassik kvadrat cədvəldən istifadə edilmir. Əvəzində mətndəki boşluqların da şifrlənməsi üçün xüsusi simvol əlavə edilərək əlifba təkmilləşdirilir və cədvəl yalnız səkkiz sətirdən ibarət olur. Əlavə olaraq, cədvəldəki sətirlər birdən səkkizədək, sütunlar isə sıfırdan $(n-1)$-dək nömrələnir. Burada, n – təkmilləşmiş əlifbanın gücüdür. Şifrləmə zamanı sətirdən mətnin və açarın uyğun simvollarının sütundakı nömrələri tapılaraq n moduluna görə toplanılır. Hər bir simvol üçün növbəti sətirdən istifadə edilir və sonuncu sətirdən sonra mətnin sonunadək şifrləmə bitənədək sətirlər dövri olaraq təkrarlanır. Deşifrləmə zamanı isə hər sətirdən şifrin və açar sözün uyğun simvolunun sütundakı nömrələri tapılaraq n moduluna görə çıxılır və mətn əldə edilir.

Nəticə

Mətnlərin kriptoqrafik mühafizə məsələsi ilə bağlı irəli sürülən tələblər və informasiya texnologiyalarının imkanlarından asılı olaraq şifrləmənin müxtəlif aspektlərinə diqqət yetirilmişdir.

Bu aspektlər sırasında birinci yerdə şifrləmə alqoritmi dayanır. Sezar alqoritmi və onun sadə analoqları simvolların eyni qədər sürüşdürülməsi ilə həyata keçirilirdi və mümkün şifrləmə variantlarının sayı əlifbanın gücü ilə ekvivalent idi. Açar sözün uzunluğunun birdən çox olması mətnin şifrlənmiş variantlarının sayının əlifba gücünün faktorialı ilə hesablanmasına gətirdi. Əlifba ardıcıllığının dəyişdirilməsi şifrlənmiş variantlarının sayını kvadrata yüksəltdi. Lakin bütün bu şifrləmə üsulları kripto-hücumlara qarşı zəif dayanıqlılıq nümayiş etdirir. Belə ki, kripto-hücum təşkil edənlərin arsenalında əsasən aşağıdakı iki üsul mövcuddur: açarları tam sayma qaydası və tezliklərin analizi metodu. Müasir kompüter vasitələri isə çoxsaylı variantları məhdud müddətlərdə saya bilir. Ona görə də sonrakı mərhələlərdə şifrləmə üsulları sırasına blokla şifrləmə, şifrləmə zamanı əlifbaların dəyişdirilməsi, mətnlərə əlavələrin (parazit ifadələrin) daxil edilməsi və s. baş verdi.

Bunları nəzərə alaraq, hesab etmək olar ki, mətnlərin şifrlənməsi və müasir informasiya kanalları ilə ötürülməsi zamanı kripto-hücumlara qarşı dayanıqlığı təmin etmək üçün müxtəlif yanaşmaları özündə əks etdirən hibrid şifrləmə üsulunun tətbiqi məqsədəuyğundur.

İstifadə edilmiş ədəbiyyat siyahısı

1. Baxışov, R. Hava Hücumundan Müdafiə bölmələrində idarəetmə sistemlərinin dayanıqlılığının artırılması üçün avtomatlaşdırılmış idarəetmə sistemlərinin effektivliyinin analizi // – Bakı: Hərbi bilik, – 2019. №2, – s. 33-39.

2. Paşayev, A.B. Mətn şifrləmənin bir metodu haqqında / A.B.Paşayev, E.N.Səbziyev, A.H.Həsənov [və b.] // – Bakı: Milli Təhlükəsizlik və Hərbi Elmlər, – 2016. №2(2), – s. 123-128.

3. Əliquliyev, R.M. Kriptoqrafiyanın əsasları / R.M.Əliquliyev, Y.N.İmamverdiyev. – Bakı: "İnformasiya texnologiyaları" nəşriyyatı, – 2006. – 688 s.

4. Qasımov, V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik / V.Ə.Qasımov. – Bakı: MTN Nəşriyyat-Poliqrafiya Mərkəzi, – 2009. – 340 s.

5. Həsənov, A. Hərbi rabitə vasitələri haqqında məlumat / A.Həsənov. – Bakı: Hərbi Nəşriyyat, – 2015. – 280 s.

6. Shannon, C.E. Communication theory of secrecy systems: [Electronic resource]. – February 5, 2020. URL: https://bit.ly/3blCEhV

7. Udepal, S., Upasna, G. An ASCII value based text data encryption System: [Electronic resource]. // International Journal of Scientific and Research Publications, – November 2013. Volume 3, Issue 11, – 04.02.2020. URL: https://bit.ly/3aq27Wg

8. Paşayev, A.B. Bir modifikasiya olunmuş şifrləmə metodu ilə şifrlənmiş mətnin deşifrlənmə çətinliyinin qiymətləndirilməsi / A.B.Paşayev, E.N.Səbziyev, A.H.Həsənov [və b.] // Milli Təhlükəsizlik və Hərbi Elmlər, – 2016. № 3(2), – s. 22-26.

9. Alqad, Z. A New Approach for Data Cryptography / Z.Alqad, M.Oraiqat, H.Almujafet [et. al] // International Journal of Computer Science and Mobile Computing, – September 2019. Vol.8, Issue 9, – p. 30-48.

10. Ghrare, S.E., Barghi, H.A., Madi, N.R. New Text Encryption Method Based on Hidden Encrypted Symmetric Key // ACIT 2018, – Ceske Budejovice, Czech Republic, – June 1-3, – 2018, – p. 240-244.

11. Mittal, V.K, Mukhija, M. Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique // International Journal of Trend in Scientific Research and Development (IJTSRD), – August 2019. Volume 3, Issue 5, – p. 1936-1939.

Аннотация

Основные принципы реализации методов шифрования текста

Фарман Мамедов

В статье даётся краткий обзор классических и современных алгоритмов шифрования, изъясняется на примерах принципы их применения и обсуждается степень сложности методов шифрования. А также изложены алгоритмы встречающиеся в последнее время в научной литературе про современные алгоритмы кодирования текстов. Используя возможности современных компьютерных технологий, рекомендуется при создании новых методов гибридное текстовое шифрование.

Ключевые слова: классическая криптография, современная криптография, алгоритм, симметричное шифрование, шифрование текста, шифры замены, одноалфавитное шифры, многоалфавитное шифры.

Abstract

Basic principles of implementation methods of text encryption

Farman Mammadov

The article provides a brief overview of classical and modern encryption algorithms, explains their application principles, and discusses the degree of complexity of encryption methods. There is also an overview of modern algorithms for the decoding of texts that have been used recently in scientific literature. It is recommended that new methods for encrypting texts should be made by hybrid methods using modern computer technologies.

Keywords: classical cryptography, modern cryptography, algorithm, symmetric encryption, text encryption, subtitution ciphers, monoalphabetic ciphers, multialphabetic ciphers.

Məqalə redaksiyaya daxil olmuşdur: 10.02.2020
Təkrar işlənməyə göndərilmişdir: 15.02.2020
Çapa qəbul edilmişdir: 20.02.2020