NAZİM VERDİYEV
Azərbaycan Texnologiya Universiteti
Gəncə şəh. Ş.İ.Xətai küçəsi 103
nazimganja@mail.ru

HÜRUFİ KRİPTOQRAFİYASI İLƏ ELEKTRON İMZA TEXNOLOGİYALARI ARASINDA BƏNZƏYIŞ

Xülasə

Hürufilik təlimi Qurana istinadən sözə böyük dəyər verir, çünki söz hərflərdən, hərflər isə səslərdən ibarətdir. Hürufilərin əqidəsinə görə hər şey hərflərin məcmusudur. Hərflərin müqəddəsləşdirilməsi hürufiliyin əsas ideyasını təşkil edir.Ərəb əlifbasında hərflərin ədədi ekvivalentləri vardır və ona əbcəd deyilir, yəni hər bir hərfə müəyyən ədəd uyğundur, məsələn, əlif - 1, vav - 6, mim – 40, ra - 200 və s. Hərflərin hər biri ədədi ekvivalentlə yanaşı həm də özünə məxsus unikal koda malikdir. Unikal kod müəyyən hesablamalar nəticəsində alınır. Hesablamalar kiçik əbcəd, böyük əbcəd, törəmə əbcəd və birləşmiş (yekun, cəm) əbcəd olmaqla hər bir hərf üzrə aparılır. Hesablamalarda bölmə və toplama əməliyyatlarından istifadə olunur. Bölmə əməliyyatı mənazil, bürcət, səyarət və çəyarət adlanan ədədlərə bölünməklə aparılır. Mənazil - ədədin 28-ə, bürcət - 12-yə, səyarət - 7-ə, çəyarət isə ədədin 4-ə bölünməsindən alınan qalıq deməkdir. Həmin qalıqlar toplanaraq təkrar olunmayan qalıqların cəmini yaradır ki, bu da hərfin unikal kodu anlamına gəlir. Unikal kodlar yüksək səviyyəli mürəkkəb hesablamaların tərkibinə daxil olur və bu mərhələdə alınan ədədlər fəlsəfi-dini fikirlərin gizlədilməsi və açılışında istifadə edilir. Hərflərin unikal kodları elektron imza texnologiyasında istifadə olunan simmetrik və asimmetrik şifrələmə alqoritminin iş prinsipinə bənzəyir.

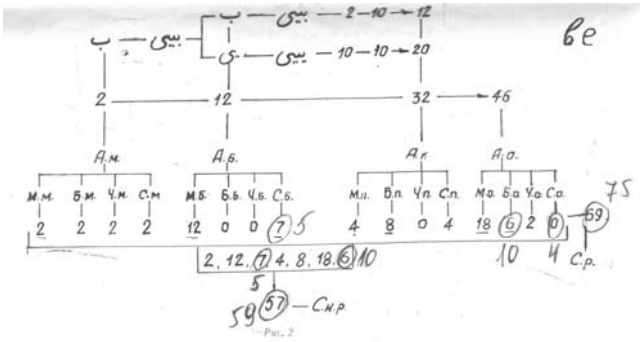
Simmetrik şifrələmə məna baxımından ərəb-fars hərflərinin unikal kodu ilə oxşarlıq təşkil edir, yəni hər bir hərfə məxsus unikal kod bütün aparıcı hürufi mütəxəssislərinə (sistemin bütün iştirakçılarına) məlum idi, unikal kodun alınması üsulu isə məna baxımından asimmetrik (RSA) şifrələmə ilə oxşarlıq təşkil edir. Unikal kodun alınması (hesablanması) üsulu hətta RSA alqoritmindən mürəkkəb və kodun sındırıla bilməməsi baxımından ondan daha üstündür.

Açar sözlər: hürufilik təlimi, gizli yazılar (kriptoqrafiya), elektron imza, simmetrik və asimmetrik imza, RSA alqoritmi, informasiya texnologiyaları

Hürufilik təliminin dəqiq elmi mahiyyəti ilə bağlı əsərlərə böyük ehtiyac olmasına baxmayaraq bu sahədə ciddi qıtlıq yaşanır. Hürufiliklə məşğul olan mütəxəssislər bildirirlər ki, onlar özlərinin anlayacağı gizli yazılardan (kriptoqrafiyadan, şifrələmədən) istifadə edərək təlimlərini dövrün təqiblərindən qoruyurdular. Nədir bu gizli yazılar, haradadır onlar?

Hürufilik təliminə görə hərflər, ədədlər müqəddəsdirlər və onlar təbiətin, varlığın əsası kimi qəbul olunur. Bu təlimin müddəaları Qurana istinad edir. Müqəddəs kitabda qeyd edilir ki, ilk olaraq səs, sonra isə söz yaranmışdır. Sözlər hərflər vasitəsilə ifadə olunduğundan hərflər Tanrının bütün təzahürlərini əks etdirən müqəddəs kəlamlardır, kəlam və söz isə Haqq tərəfindən nazil olan bir işarədir, çünki Tanrının insana bəxş etdiyi söz bilgi xəzinəsi və insan kamalının göstəricisidir. Hürufilərin əqidəsinə görə hər şey hərflərin məcmusudur. Hərflərin müqəddəsləşdirilməsi hürufiliyin əsas ideyasını təşkil edir. Bu fikirlərin təsdiqi kimi əlavə olaraq aşağıdakıları misal göstərmək olar: Kəlam (söz) qiyafəsində təcəlli edən Tanrı özünü hərflərdə görüntülədi. Yəni yaradıcı olan hərfdir [5,səh.42]. Bu səbəbdən hurufîlik danışan insanı Tanrılaşdırırdı. Hurufîlikdə məqsəd insandır və insanın açıqlanması Tanrını da açıqlamaqdır. Hurufîliyə görə hərflər insan üzündə də görünür. Hurufîlər "əlif hərfini buruna, burnun iki tərəfını iki "lam" hərfinə və gözləri "he" hərfinə bənzədərək insanın üzündə "Allah"

yazılmış olduğunu söyləyirdilər. Bunları yazmaq bu gün çox asandır, amma dünən ifadə etmək heç də asan deyildi. Məsələn, ən tanınmış şairlərimizdən Nəsimî hurufîydi; bu səbəbdən dərisi soyularaq öldürülmüşdü... [5,səh.45-46]. Hürufi hərəkatının qurucusu və öndəri Şihabəddin Fəzlullah Astrabadi Hurufînin (Nəiminin) (1339?-1394) [6] otuz iki yaşında ikən qurduğu firqə (partiya) əvvəlcə Təbriz və İstanbulda, sonra isə qısa zamanda İranın hər tərəfinə yayıldı. Hürufi firqəsinin hərf və say nəzəriyyəsinin əsasını bir sistem olaraq ortaya qoyan əsərlərin başında Fəzlullah Hurufînin "Cavidannamə" adlı əsəri gəlir. Lakin Nəiminin dini görüşləri Şəriətə müxalif olduğundan boynu vurularaq qətl edilmişdir [7]. Nəimidən öncə də İslam alimləri hərflərin müqəddəsliyi üzərində çox düşünmüşdülər. Məsələn, Əndəlüslü Mühyiddin Ərəbi (1165-1240) hərflərə böyük önəm verərək Fütuhati Məkkiyyə adlı kitab yazmışdı [5,səh.48].Respublikamızda hürufi təliminin elmi şəkildə öyrənilməsi məqsədilə yazılmış yeganə əsər Əhməd Elbrusun "Poetika və riyaziyyat" adlı rus dilində yazılmış və 1979-cu ildə "Elm" nəşriyyatı tərəfindən buraxılan kitabıdır. Bu kitabın çox ciddi qüsurlarının olmasını bir kənara qoysaq (bax: [4]) və onu hürufi təliminin elmi əsasları kimi qəbul etsək, o zaman çox qəribə və heyrətamiz bir hadisənin şahidi olarıq. Söhbət hürufi təliminin gizli yazılarını özündə ehtiva edən riyazi aparat ilə elektron imza texnologiyalarının oxşarlığından, bənzərliyindən gedir. Bir-birindən əsrlərlə aralı olan bu iki texnologiya eyniyyət təşkil etmir, lakin mahiyyət baxımından onların hazırlanma texnologiyası bənzərdirlər. Hürufi kriptoqrafiyasında hesablamalar sadə hesab əməlləri üzərində qurulmuşdur və xüsusi bir mürəkkəbliyi yoxdur. Burada xüsusi əhəmiyyət kəsb edən cəhət hesablamaların nəticələrindən istifadə məsələsidir. Həmin məsələnin izahına keçməzdən əvvəl hürufi hesablamalarının fəlsəfəsi ilə tanış olmaq lazım gəlir. Ərəb əlifbasında hərflərin ədədi ekvivalentlərinin olmasına əbcəd deyilir, yəni hər bir hərfə müəyyən ədəd uyğundur, məsələn, əlif - 1, vav - 6, mim – 40, ra - 200 və s. Adı xatırlanan kitabda verilmiş əsas hesablamalar hər bir hərf üzrə kiçik əbcəd, böyük əbcəd, törəmə əbcəd və birləşmiş (yekun, cəm) əbcəd olmaqla ədədlər üzərində aparılır. Hesablamalarda bölmə və toplama əməliyyatlarından istifadə olunur. Bölmə əməliyyatı nəticəsində mənazil, bürcət, səyarət və çəyarət adlanan qalıqların tapılması əməliyyatı aparılır. Mənazil - ədədin 28-ə, bürcət - 12-yə, səyarət - 7-ə, çəyarət isə ədədin 4-ə bölünməsindən alınan qalıq deməkdir. Kitabda verilmiş hesablamalardan biri nümunə olaraq aşağıda təqdim edilir.



Qeyd edək ki, kitab rus dilində olduğundan kiçik, böyük, törəmə və birləşmiş (yekun) terminləri müvafiq olaraq burada **м** (*малый*), **б** (*большой*), **п** (*производный*), **о** (*объединенный*) şəklində göstərilir. Məsələn, $\mathbf{М_м}$ – kiçik mənazil, $\mathbf{Б_б}$ – böyük bürcət, $\mathbf{С_п}$ – törəmə səyarət, $\mathbf{Ч_о}$ – birləşmiş çəyarət deməkdir. Şəkildə verilmiş hesablamaların necə aparılmasını öyrənək.

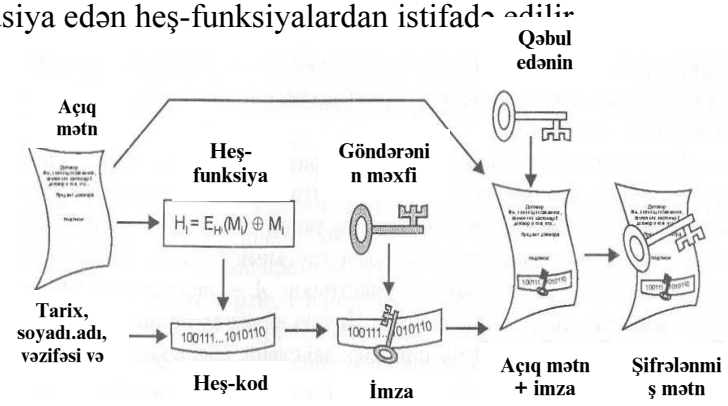
Əvvəla şəkildən görünür ki, bəzi ədədlər üzərində düzəlişlər edilmişdir. Onları izah edək. Məsələn, 12 ədədi 7-ə bölündükdə qalıq 7 deyil, 5 olmalıdır (12-1*7=5); 46 ədədi 12-ə bölündükdə qalıq 6 deyil, 10 olmalıdır (46-3*12=10); 46 ədədi 7-ə bölündükdə qalıq 0 deyil, 4 olmalıdır (46-6*7=4). Yekunda alınan ədəd (57, əslində isə 59) təkrar olunmayan qalıqların

cəmidir. Bu əməliyyat bütün hərflər üzrə aparılır (bu tip hesablamalar haqqında geniş məlumatlar [4]-də öz əksini tapmışdır). Yekunda alınan və qalıqların toplanmasından alınan cəmlər sonra daha mürəkkəb hesablamaların tərkibinə daxil olur və bu yeni mərhələdə alınan ədədlər fəlsəfi-dini fikirlərin gizlədilməsi və açılışında istifadə edilir. Hesablamalarda təkrar olunmayan qalıqların cəmi anlayışı məhz elektron imza texnologiyasında istifadə olunan RSA alqoritminin iş prinsipinə bənzəyir. Əgər belə demək mümkünsə, hürufi kriptoqrafiya texnologiyası müasir RSA alqoritmindən də mürəkkəbdir. Bu bənzəyişin mahiyyətini izah etmək üçün əvvəlcə elektron imza və RSA alqoritmi ilə tanış olmaq lazımdır. Bu məqsədlə ədəbiyyat siyahısında göstərilən 2 və 3-cü mənbələrə müraciət edək.

Elektron imza həyatımıza daxil olmuş elektron informasiya texnologiyaları vasitəsilə həyata keçirilən qeyri-adi imzadır. Bu imzanı kompüterə müəyyən simvollar, rəqəmlər (informasiya) dəstinin daxil edilməsi kimi qəbul etmək olar. İnformasiya əksər hallarda plastik kart şəklində hazırlanır və kompüterə qoşulan xüsusi qurğu vasitəsilə daxil edilir, yəni hər bir fiziki və ya hüquqi şəxs təkrar olunmayan nadir (unikal) koda malik olur. Bu imza hüquqi qüvvəyə malikdir, uzaq məsafədən sənədlərin, müqavilələrin imzalanmasında istifadə olunur, vaxta və maliyyəyə qənaət etməyə imkan verir, rahat, asan və təhlükəsizdir. Elektron imza elektron sənədi saxtalaşdırmaqdan qoruyur. Ondan müxtəlif hüquqi məsələlərin həllində istifadə olunur, məsələn, elektron sənəd dövriyyəsində, parlament seçkilərinə səsvermədə və s.

Ümumiyyətlə, elektron (rəqəmsal) imzada iki cür şifrələmədən istifadə olunur – simmetrik və asimmetrik şifrələmədən. Simmetrik şifrələmə üsulunda eyni bir açar həm məlumatı şifrələmək, həm də deşifrələmək üçün istifadə olunur. Asimmetrik (açıq açarlı) kriptoqrafik sistemlərdə hər bir iştirakçı bir-birindən riyazi asılı olan iki müxtəlif açarlardan istifadə edir. Açarlardan biri (məxfi və ya gizli açar) yalnız sahibinə məlumdur və tam məxfi saxlanılır, ikinci açar açıqdır, yəni sistemin bütün iştirakçılarına məlumdur. Gizli açar deşifrləmək üçün, açıq açar isə şifrələmək üçün istifadə olunur. Açıq açara görə uyğun məxfi açarın tapılması çox böyük həcmdə hesablama əməliyyatlarının aparılmasını tələb edir. Bu isə hesablama texnikasının indiki səviyyəsində praktiki olaraq qeyri-mümkündür. Açıq açar məlumatın elektron imzasını yaratmaq, məxfi açar isə məlumatın elektron imzasını yoxlamaq üçün istifadə olunur.

Bütövlüyə nəzarət üçün kriptoqrafik heş-funksiyalardan istifadə edilir. Heş-funksiya, adətən, müəyyən alqoritm şəklində realizə edilir. Bu alqoritm ixtiyari uzunluqlu məlumat üçün sabit uzunluqlu heş-kodu hesablamağa imkan verir. Təcrübədə 128 bit və daha artıq uzunluqda heş-kodu generasiya edən heş-funksiyalardan istifadə edilir.



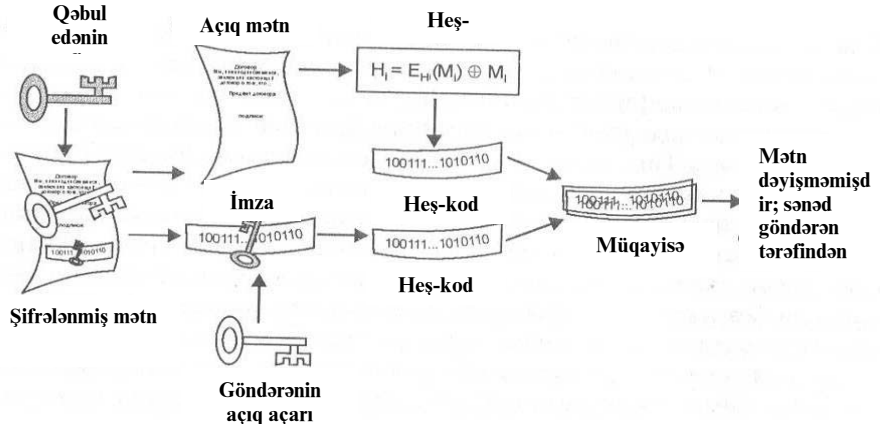
Elektron imzanın yaradılması prosesi

Heş-funksiyanın xassələri elədir ki, onun köməyi ilə alınan heş-kod məlumatla «möhkəm» bağlı olur. Məlumatın hətta bir biti dəyişdikdə belə heş-kodun bitlərinin yarısı dəyişir. Heş-

funksiyaya misal olaraq MD2, MD4, MD5, RİPEMİD, SHA1 və s. alqoritmlərini göstərmək olar.

Misal. «1234567890» sətri üçün SHA1 heş-funksiya alqoritminin hesabladığı heş-kod 16-lıq say sistemində 01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A simvollar ardıcılığıdır, yəni 40 simvoldan ibarət sabit uzunluqdur.

Sistemin istənilən iştirakçısı imzalanmış sənədi aldıqda A istifadəçisinin imzasını yoxlaya bilər. Bunun üçün o, heş-funksiyanın köməyi ilə alınmış məlumatın heş-kodunu yaradır. Sonra məlumata qoşulu olan şifrələnmiş heş-kodu A istifadəçisinin açıq açarı ilə deşifrə edir və alınmış deşifrə edilmiş heş-kodu özünün yaratdığı heş-kodla müqayisə edir. Onlar eynidirsə, imza həqiqi hesab edilir. Əks halda imza rədd edilir. Gizli açar yalnız A istifadəçisinə məxsus olduğundan aydındır ki, məlumatı da yalnız o imzalaya bilərdi.



Sənədin əsliliyinin yoxlanılması prosesi

Asimmetrik şifrələmə alqoritminə misal olaraq RSA, ElGamal, Şnorr alqoritmlərini göstərmək olar. Alqoritmin adı onu yaradan müəlliflərin soyadlarının ilk hərflərindən ibarətdir - R.**Ri**vest, A.**S**hamir, L.**A**dleman. Bu alqoritmi onlar Massaçusets Texnologiya İnstitutunda birgə işləyərkən 1977-ci ildə təklif etmişlər.

RSA alqoritmi aşağıdakı kimi işləyir:

1. İki kifayət qədər böyük sadə p və q ədədləri seçilir.
2. Onların $n=p*q$ hasili hesablanır.
3. Eyler funksiyası adlanan $\varphi(n)$=(p-1)*(q-1) funksiya hesablanır.
4. Elə d ədədi seçilir ki, (e*d-1) ədədi $\varphi(n)$-ə bölünsün.
5. $1<e<\varphi(n)$ şərtini ödəyən elə bir e ədədi müəyyən edilir ki, edmod(p-1)*(q-1)=1 olsun.
6. **{*e,n*}** cütü açıq açar, **{*d,n*}** cütü isə gizli (məxfi) açar adlanır.

Bundan sonra $\{e,n\}$ məlum açarı ilə məlumatı şifrələmək üçün şifrələnən mətn bloklara bölünür və onların hər biri (məsələn, i nömrəli blok) $M(i) \le n-1$ ədədləri şəklində təsvir edilə bilər.

Mətni M(i) ədədlər ardıcıllığı kimi aşağıdakı ifadə ilə şifrələmək lazımdır:

$$C(i) = M(i)^e \bmod(n)$$

Bu məlumatı deşifrələmək üçün **{*d,n*}** məxfi açarından istifadə etmək lazımdır. Bunun üçün aşağıdakı ifadədən istifadə edilir:

$$M(i) = C(i)^d \bmod(n)$$

Nəticədə M(i) ədədlər çoxluğu alınacaq ki, bu da ilkin mətn olacaqdır.

Misal. «QİDA» sözünü RSA alqoritmi ilə şifrələyək. Hesabatlar sadə olsun deyə kiçik ədədlərdən istifadə edək.

1. p=3 və q=11 ədədlərini seçək.

2. $n=p*q$ =3*11=33
3. $\varphi(n)=(p-1)*(q-1)$=2*10=20
4. ($e*d-1$) ədədi 20-yə bölünən olmalıdır. Odur ki, məsələn, d=3 ədədini seçirik.
5. $1<e<\varphi(n)$ şərtini ödəyən ədədi seçirik. Bu ədəd qismində istənilən elə bir ədəd seçilir ki, $e*3mod(20)$=1 bərabərliyi ödənilsin. Bu ədəd e=7 ədədidir, çünki (3*7-1) ədədi 20-yə bölünür.
6. Şifrələnən məlumatı *0...32* diapozonunda tam ədədlər ardıcıllığı kimi qəbul edək. Əlifba sırasında Q hərfi 17 rəqəmi ilə, İ hərfi 14, D hərfi 5, A hərfi isə 1 rəqəmi ilə ifadə olunur. Bu qayda ilə QİDA sözünü 17,14,5,1 kimi təsvir etmək olar. Məlumatı açıq açardan, yəni {*7,33*} cütündən istifadə etməklə şifrələyək:

$C_1 = 17^7 \bmod(33) = 410338673 \bmod(33) = 8$, yəni 410338673/33=12434505 +qalıq 8

$C_2 = 14^7 \bmod(33) = 105413504 \bmod(33) = 20$, yəni 105413504/33=12434505 +qalıq 20

$C_3 = 5^7 \bmod(33) = 78125 \bmod(33) = 14$, yəni 78125/33=2367 +qalıq 14

$C_4 = 1^7 \bmod(33) = 1 \bmod(33) = 1$

Şifrləmədən sonra {*8,20,14,1*} məlumatını deşifrə etməyə cəhd edək. Bunun üçün məxfi hesab edilən {*3,33*} açarından istifadə edilir.

$M_1 = 8^3 \bmod(33) = 512 \bmod(33) = 17$, yəni 512/33=15+qalıq 17

$M_2 = 20^3 \bmod(33) = 8000 \bmod(33) = 14$, yəni 8000/33=242+qalıq 14

$M_3 = 14^3 \bmod(33) = 2744 \bmod(33) = 5$, yəni 2744/33=83+qalıq 5

$M_4 = 1^3 \bmod(33) = 1 \bmod(33) = 1$

Beləliklə {17*,14,5,1*} ədədlərini əlifba sırasında axtardıqda şifrələnən sözün QİDA olduğu məlum olur.

Elektron imza texnologiyaları haqqında müəyyən bilik əldə etdikdən sonra hürufi kriptoqrafiyası ilə elektron imzanın simmetrik və asimmetrik (RSA) texnologiyalarını müqayisə etmək olar. Simmetrik şifrələmə ilə ərəb-fars hərflərinin təkrar olunmayan qalıqlarının cəmi (bunu şərti olaraq hərflərin unikal kodu da adlandırmaq olar) mənaca üst-üstə düşür, yəni hər bir hərfə məxsus unikal kod bütün hürufi müridlərinə, aparıcı mütəxəssislərə (sistemin bütün iştirakçılarına) məlum idi. Bunu açıq açar termini ilə də müqayisə etmək olar. Unikal kodun alınması üsulu isə, yəni qalıqlar əsasında digər informasiyanın alınması məna baxımından asimmetrik (RSA) şifrələmə ilə üst-üstə düşür. Ədəbiyyat siyahısında 1-ci kitabın 106 və 107-ci səhifələrində verilmiş açar-şifrələri məxfi (gizli) açar termini ilə müqayisə etmək doğru olardı. Hərflərə məsxus unikal kodun alınması (hesablanması) üsulunu RSA alqoritmi ilə müqayisə etdikdə belə nəticəyə gəlmək olur ki, hürufi kriptoqrafiyası hətta RSA alqoritmindən də üstündür.

XIV əsrdə İranda yaranan hürufi kriptoqrafiyası Azərbaycan, Hindistan, İraq, Suriya, Türkiyə, Balkanların güneyi Şərqi Avropada yayılan ilk ciddi elmi şifrələmə sistemi olsa da dünya elmində özünün layiqli qiymətini almamışdır. Hürufi kriptoqrafiyası XX əsr Qərb dünyasının elektron imza texnologiyasına bənzərliyi ilə onu 600 il qabaqlamış kimi görünür, lakin bu iki bilik sahəsi indiyə qədər müqayisə edilməmişdir. Bu günün informasiya texnologiyaları hürufilik dövrünə təsadüf etmiş olsaydı, elektron imza texnologiyaları bəlkə də Şərq elminin məhsulu kimi tarix səhnəsində qalardı. Hər halda aparılan müqayisədən də məlum olur ki, hürufi təlimi dəqiq riyazi əsaslar üzərində qurulmuş elə möhtəşəm bir təlimdir ki, mükəmməl kriptoqrafik sistemə malikdir və dini, fəlsəfi, estetik dünyagörüşü kimi onun öyrənilməyə haqqı vardır.

Ədəbiyyat

1. Ахмед Эльбрус. Поэтика и математика. Баку, Издательство «Элм», 1979
2. Чернышев Ю.Н. Информационные технологии в экономике. Учебное пособие. М., 2008
3. Verdiyev N.D. İnformasiya iqtisadiyyatı. Dərs vəsaiti. Gəncə, 2012
4. Verdiyev N.D. Hürufizmin riyazi əsasları. "Filologiya məsələləri"jurnalı, №8, 2019
5. Soner Yalçın Asistan. Beyaz müslümanların büyük sırrı. İstanbul, 2006
6. Kevser Yalçın. Hurufilik ve Sayıların Önemi - https://groups.google.com
7. Hüsamettin Aksu Hurufilik - https://insanveevren.wordpress.com/

Вердиев Назим Давуд оглы

Сходство между хуруфитской криптографией и технологиями электронной подписи

Резюме

Согласно Корану хуруфитское вероучение придает слову большое значение, потому, что слова состоят из букв, а буквы из звуков. По убеждению хуруфитов всё что есть это совокупность букв. Священность букв составляет основную идею хуруфизма.

В арабской азбуке каждая буква имеет свой числовой эквивалент и это называется абджад, т.е. каждой букве соответствует определенное конкретное число, например, алиф - 1, вав – 6, мим – 40, ра – 200 и т.д. Буквы помимо числовых эквивалентов также имеет свой уникальный код. Уникальный код получается в результате определенных вычислений. Вычисления проводятся по каждой букве по так называемому малому абджаду, большому абджаду, производному абджаду и объединенному абджаду. В вычислениях используется арифметические операции деления и сложения. Операция деления производится делением по так называемым маназиль, бурджат, саярат и чаярат. Маназиль – остаток от деления данного числа на 28, бурджат – на 12, саярат – на 7, чаярат – на 4. Все остатки суммируясь образуют совокупность неповторяющихся разделений, и это называется уникальным кодом. Уникальные коды входят в состав сложных вычислений высшего уровня и числа полученные на этом этапе используются для скрытия и раскрытия религиозно-философских мыслей. Уникальные коды букв аналогичны принципу работы симметричного и асимметричного алгоритмов шифрования, используемые в технологии электронной подписи. По своему смыслу симметричное шифрование составляет схожесть с уникальными кодами арабо-персидских букв. Уникальный код, свойственный каждой букве были известны всем ведущим хуруфитским специалистам (участникам всей системы), а способ получения уникального кода по своему смыслу составляет схожесть с асимметричным шифрованием (RSA). Способ получения (вычисления) уникального кода является более сложным по сравнению с алгоритмом RSA, а с точки зрения невозможности взлома кода превосходит его.

***Ключевые слова**: хуруфитское вероучение, тайные записи (криптография), электронная подпись, симметричная и асимметричная подпись, алгоритм RSA, информационные технологии.*

Verdiyev Nazim Davud

Similarity between hurufi cryptography and electronic signature technologies

Summary

The teaching of the hurufism is highly valued by the Qur'an because the word consists of letters and letters consists of voices. According to the hyparites, everything is a collection of letters. The sanctification of letters consists the basic idea of the right.

In the Arabic alphabet letters have numerical equivalents and are called “abjad”. Each letter corresponds to a certain number, eg: alif – 1, vav – 6, mim – 40, ra – 200 and so on. Each of the letters has a unique equivalent of its numerical equivalence. The unique code is taken as a result of certain calculations. The calculations are carried out on each letter, with a small intention, a great abstraction, a derivatical anomaly, and a combined (final, total) abjad. The calculations use division and subtraction. Section operation is carried out by division into numbers, called manazil, burjat, sayarat and chayarat.

Unique codes are included in high level complicated calculations and the numbers obtained at this stage are used to hide and unlock philosophical ideas. Symmetric encryption is similar to the unique code of the Arabic-Persian letters, meaning that the unique code for each letter is known to all leading experts (all system members) and the method of obtaining a unique code is similar to asymmetric (RSA) encryption. The method of getting a unique code is even more complicated than the (RSA) algorithm and the code is superior to it.

Keywords: bases of hurufism, secret writings (cryptoqraphy), electronic signature, symmetrical and asymmetrical signature, RSA algorithm, information technologies.

Redaksiyaya daxil olma tarixi: 07.05.2019
Çapa qəbul olunma tarixi: 08.06.2019
Texnika üzrə fəlsəfə doktoru, dosent Hacıyev Rövşən tərəfindən çapa tövsiyə olunmuşdur