**Açıq açarla şifrələmə metodları. Elektron rəqəmsal imza**

**AÇIQ AÇARLA ŞİFRƏLƏMƏ ALQORİTMİ**

Açıq açarla şifrələmə alqoritmində hər bir istifadəçi bir cüt açara malikdir və bu açarlar bir-birilə bəzi asılılıqlarla bağlıdırlar. Açarlarda bu xüsusiyyətlər vardır: *bir açarla şifrələnən mətn, bir cüt açarla şifrələnən mətn*. Bir açarı *gizli (bağlı) açar* adlandırırlar. İstifadəşi özünə məxsus gizli açarı etbarlı bir yerdə gizlətməlidir və onu heç kimə etibar etməməlidir. İkinci açar *açıq açar* adlanır və istifadəçi bu açar barədə hamını məlumatlandırmalıdır.

Əgər A istifadəçi B istifadəçiyə şifrələnmiş məlumat göndərmək istəyirsə, onda o həmin məlumatı B açarı ilə şifrələyir. Bundan sonra mətni heç kim (hətta A özü də) oxuya bilməz (B-dən başqa), çünki mətni şifrədən çıxarmaq üçün mütləq ikinci açar - gizli açar lazımdır.

Şifrələmə sxemi aşağıdakı kimidir:

**Mı = E (M, Kaçıq)**

**M = D (M, Kbağlı)**

burada E – şifrələmə funksiyası (encrypt), D – deşifrələmə funklsiyası (decrypt), Kaçıq və Kbağlı – uyğun olaraq məlumatı qəbul edənin açıq və bağlı (gizli) açarları.

Açıq açarla şifrələmə üsulu Diffi və Helmana məxsusdur (1976-cı il). Buna baxmayaraq onlar konkret alqoritm təklif edə bilmədilər, amma alqoritmin ödəyə biləcəyi prinsipləri və şərtləri formalaşdıra bildilər.

|  |  |
| --- | --- |
| http://www.oloommagazine.com/Images/Articles/2009/3&4/1001.gif  *Uitfild Deffi* | http://www.rudata.ru/w/images/d/d4/Martin-Hellman.jpg  *Martin Hellman* |

Bu şərtlərə aşağıdakılar aiddir:

1.Açarlar cütlüyünün (açıq və bağlı) generasiya prosesi hesablama çətinliyi yaratmamalıdır;

2.Mətnin şifrələnmə prosesi, yəni E (M, Kaçıq) və deşifrələnmə prosesi D (M, Kbağlı) hesablama çətinlikləri yaratmamalıdır;

3.Düşmənin Kbağlı açarı haqqında məlumatı olmamalıdır (əgər onda Kaçıq açarı haqqında məlumat olsada belə);

4.Düşmən **Mı** şifrələnmiş mətnə və Kaçıq açara malikolsada belə, açıq **M** mətnini hesablama imkanı olmamalıdır.

Beləliklə, şifrələmə və deşifrələmə istənilən ardıcıllıqla yerinə yetirilsə də, belə etmək də mümkündür: mətni bağlı açarla şifrələməli, açıq açarla şifrədən çıxarmalı.

***RSA alqoritmi***.

RSA açıq açarla şifrələmə alqoritmlərindən biridir. Alqoritm 1977-ci ildə Rivest, Şamir və Adleman tərəfindən yaradılmışdır. Alqoritm 20 il ərzində ən populyar sayılmış və açıq açarla istifadə olunan alqoritmlər içərisində praktiki olaraq ən çox istifadə ediləni olmuşdur.

RSA ikilik mətnlərin şifrələnməsi üçün istifadə edilir. Açıq mətn bloklara bölünür və hər bir blok **M** ikilik ədədi kimi götürülür. Bu zaman M<n şərti ödənilməlidir (n=*pq*, burada *p* və *q* iki böyük təsadüfi sadə ədədlərdir).

Açıq və bağlı açarlar RSA alqoritmində bir-birilə əlaqəlidirlər, yəni bir açarın şifrələnməsi o biri açarın şifrədən çıxarılmasına səbəbdir.

Alqoritmin çatışmazlığı əməliyyatı aşağı sürətlə yerinə yetirməsidir. RSA alqoritmində şifrələmə və deşifrələmə əməliyyatları çox böyük tərtibli çox böyük ədədlərin qüvvətə yüksəldilməsi ilə yerinə yetirilir, bu isə öz növbəsində əməliyyatı yerinə yetirmək üçün həcmli resursların olmasını tələb edir.

Bu baxımdan təcrübədə ən çox iki alqoritmin kombinasiyasından istifadə olunur. Məlumat simmetrik alqotmin köməyilə şifrələnir (məsələn, AES), bu zaman hər dəfə təsadüfi açar generasiya olunur. Təsadüfi açar açıq açarla şifrələnir (məsələn, RSA alqoritmi ilə) və məlumat ilə birlikdə göndərilir. Belə hibrid sxem şifrələmə/deşifrələmə əməliyyatının sürətini təmin etməklə yanaşı onun etibarlığını da artırır.

|  |  |  |
| --- | --- | --- |
| *http://hardware.localhost.nl/pictures/2001-2003/schrotthall/people/ron_rivest.jpg*  *Ronald Rivest* | *http://www.webplanetnews.ru/images/prw_170x_of_1d319009dca27d74d2f3c9a18284892b.jpg*  *Adi Şamir* | *http://amturing.acm.org/images/adleman-1(1).jpg*  *Л. M. Адлеман* |

|  |
| --- |
| *Ronald Linn Rivest* (ingiliscə Ronald Linn Rivest: 1947-ci ildə Skenektadi ştatının Hyu-York şəhərində anadan olmuşdur) kriptoqrafiya sahəsində amerika mütəxəssisidir. “Elektrotexnika və kompüter elmləri” fakultəsinin “Kompüter elmləri sahəsində Endri və Ernı Viterbi adına layiq görülmüş professor”udur. “Hesablama nəzəriyyəsi” laboratoriyasının üzvü və “Kritoqrafiya və informasiya təhlükəsizliyi” qrupunun lideridir.  *Adi Şamir* (6 iyul 1952-ci ildə Tel-Aviv şəhərində anadan olmuşdur) məşhur İsrail kriptotəhlilçisi, hesablama sistemləri nəzəriyyəsi sahəsində alim, Veysman adına institutda “İnformatika və tətbiqi riyaziyyat” sahəsində professor, Alan Türinq adına mükafatın laureatı.  *Leonard Maks Adleman* (ingiliscə Leonard Adleman-Eydelmen: 31 dekabr 1945-ci ildə anadan olmuşdur) kompüter elmləri sahəsində amerika alimi-nəzəriyyəçisi, Cənubi Kaliforniya Universitetinin kompüter elmləri və molekulyar biologiya üzrə professoru. RSA şifrələmə sisteminin və DNK-hesablamanın həmmüəllifidir. |
| ***AÇIQLAMA****: RSA* (Rivest, Shamir və Adleman soyadlarının abbreviaturasıdır) - böyük tam ədədlərin faktorlaşdırılması məsələlərinin çətinliklə hesablanmasına əsaslanan açıq açarlı kriptoqrafik alqoritmdir. RSA şifrələmə və rəqəmsal yazılar üçün ilk kriptosistemidir. Alqoritm böyük sayda kriptoəlavələrdə istifadə olunur. 1976-cı ilin noyabr ayında Uitfild Diffi və Martin Hellman tərəfindən çap edilmiş “Kriptoqrafiyada yeni istiqamət” məqaləsi kriptoqrafik sistemlər barədə təsəvvürü alt-üst etdi və nəticədə yeni istiqamətin – açıq açarlı kriptoqrafiyanın əsası qoyuldu. Sonralar işlənib təkmilləşdirilmiş Diffi-Hellman alqoritmi müdafiə olunmayan kanaldan istifadə edən hər iki tərəfə ümumi gizli açar əldə etməyə imkan verdi. Amma yaradılmış yeni alqoritm autentifukasiya problemini həll edə bilmədi. Çap olunmuş məqaləni dərindən təhlil edən Massasuçest Texnologiya İnstitutunun alimləri Ronald Rivest, Adi Şamir və Leonard Maks Adleman belə nəticəyə gəldilər ki, U.Diffi və M.Hellman tərəfindən təklif olunan açıq açarlı kriptoqrafik sistemi araşdırmaq üçün mütləq riyazi funksiya tapılmalıdır. 40 yaxın variant araşdırıldıqdan sonra alimlər belə qərara gəldilər ki, araşdırma nəticəsində alınmış funksiyanı RSA adlandırsınlar.  1977-ci ildə “Scientific AmericanScientific American” jurnalında Ronald Rivestin icazəsi ilə kriptosistemi aydınlaşdıran ilk məqalə çap edilir. Oxuculara şifrələnmiş alqoritmə malik olan, aşağıda verilmiş rəqəmlər çoxluğundan istifadə etməklə ingilis dilində olan bir cümlənin şifrəsini açmaq təklif olunur.  9686 1477 8829 7431  0816 3569 8962 1829  9613 1409 0575 9874  2982 3147 8013 9451  7546 2225 9991 6951  2514 6622 3919 5781  2206 4355 1245 2093  5708 8839 9055 5154  Ronald Rivestin elan edir ki, verilmiş kodu açmaq üçün 40 kvadrillion il lazımdır. Təxminən 15 il sonra, 1993-cü ilin sentyabr ayında tapmacanın həll olunmasına start verilir. Bir müddət sonra “başsındıran” tapılır. Tapmacada bu sözlər yazılmışdı: “[THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE](https://ru.wikipedia.org/w/index.php?title=THE_MAGIC_WORDS_ARE_SQUEAMISH_OSSIFRAGE&action=edit&redlink=1)”- “Sehirli söz - hər şeydən iyrənən quzuqapan, yırtıcı quş”. Mükafata layiq görülən şəxs müəyyən məbləğdə olan pulu proqram təminatının yaradılması fonduna təmənnasız hədiyyə edir. 1982-ci ildə Ronald Rivest, Adi Şamir və Leonard Adleman RSA şirkətini yaradırlar. 1989-cu ildə DES simmetrik şifrəsi ilə birlikdə yaradılmış alqoritm İnternetdə də istifadə olunmağa başlanılır. 1990-cı ildə ABŞ-ın Müdafiə Nazirliyi hərbi işlərdə alqoritmdən istifadə edir. 1997-ci ildə, Hökumət Əlaqələri Mərkəzində işləyən ingilis riyaziyyatçısı Klifford Koks RSA oxşar olan kriptosistemi hazırlayır. Qeyd etmək lazımdır ki, İnternet sistemində RSA alqoritmindən geniş istifadə olunur. Aşağıdakı şəkildə simmetrik şifrələmə sxemi verilmişdir. |

**ELEKTRON RƏQƏMSAL İMZA**

Qeyd edildi ki, çoxlu sayda açıq açarlı şifrələmə alqoritmləri bir-birini əvəz edə biləcək açarlar cütlüyü ilə işləyirlər, yəni bu açarlardan birinin şifrələdiyi mətni digər açar deşifrə etməyə imkan verəcəkdir.

Konfidensiallıq məqsədi ilə mətn məlumatı qəbul edənin açıq açarı ilə şifrələnir.

Məlumatın informasiyanı göndərənin baqlı (gizli) açarla şifrələndiyi halı nəzərdən keçirək. Bu halda həmin mətni kim istəsə şifrədən azad edə bilər, çünki bu halda açıq açar hamıya əlçatandır. Digər tərəfdən məlumatı alan əmin ola bilər ki, məlumatın həqiqi müəllifi məlumatı göndərəndir, yəni bağlı açarın sahibidir, çünki başqa bir şəxs bağlı açarı yarada bilməzdi.

Beləliklə, məlumatın həqiqiliyi (autentikliyi) yaranır. Hüquqi baxımdan məlumatın müəllifi ondan imtina edə bilməz (apellyasiya verə bilməz).

Bu ideya *elektron rəqəmsal imza* konsepsiyasının yaranmasına səbəb oldu.

***Rəqəmsal imzalar.***

Rəqəmsal imzalar informasiyanın həqiqiliyinə nəzarət etmək üçün elektron formada istifadə edilən güclü alətdir. Rəqəmsal imza elektron verilənlərin tamlığını təmin edir, verilənlərin aktuallığını müəyyən etməklə yanaşı müəlliflik hüququnu da təsdiqləyir. Rəqəmsal imza verilənlərin imzalanması üçün yaradılmış informasiya obyektidir və bu verilənlərin tamlığına və mötəbərliliyinə əmin olmağa imkan verir.

Elektron imza faylda baş verə biləcək xətaların qarşının alınması üçün təhlükəsizliyi müəyyənləşdirən elektron işarəsidir. Elektron işarə faylı yaradanı yoxlamağa və müəyyən etməyə imkan verir. Elektron işarə fayla rəqəmsal imza əlavə edildikdən sonra onda baş vermiş dəyişikliyi müəyyən edir.

Elektron imzanın müxtəlif növləri mövcuddur.

1.*Birləşdirilmiş elektron imza*. Birləşdirilmiş elektron imza yaradılan zaman elektron imzanın yeni faylı yaradılır və bu faylın daxilinə imzalanacaq faylın verilənləri yerləşdiriılir. Bu proses hazırlanmış sənədin konvertə (zərfə) qoyulduqdan sonra zərfin (konvertin) möhürlənməsinə bənzəyir. Sənədi konvertdən çıxaran zaman onun möhürləndiyinə əmin olmaq lazımdır. Birləşdirilmış elektron imzanın üstünlüyünə imzalanmış sənədin sonrakı mərhələdə istifadəsi zamanı *manipulyasiya* (yeni-latın dilində manus - əl, pellere – itələmək, vurmaq, hərəkətə gətirmək sözlərindən törəmədir) olunmasının sadəliyini aid etmək olar. Yəni həmin sənədin üzünü çıxarmaq, harasa göndərmək və s. əməliyyatları yerinə yetirmək olar.

2.*Ayrılmış elektron imza*. Ayrılmış imza yaradan zaman imza faylı ayrıca imzalanmış fayldan yaradılır, bu zaman imzalanmış fayl heç cür dəyişikliyə uğramır. İmzanı yoxlamaq üçün elektron imzalı fayldan istifadə etmək lazımdır. Ayrılmış elektron imzanın çatışmazlığı imzalanmış informasiyanın bir neşə fayl (imzalanmış fayl kimi və ya bir və ya bir neçə imzalı fayl şəkilində) şəkilində saxlanılmasıdır. Sonuncu vəziyyət imzanın qəbul edilməsini çətinləşdirir, çünki istənilən manipulyasiya əməliyyatında verilənlərin surətinin çəkilməsi və asılı olmayan faylların ötürülməsi tələb edilir.

3.*Verilənlərin daxilində elektron imza*. Belə şəkildə imzanın tətbiq edilməsi istifadə olunan əlavələrdən asılıdır (məsələn, elektron imza Microsoft Word və ya Acrobat Reader sənədinin daxilində olarkən). Əgər elektron imza yaradılmış əlavədən kənardadırsa, onda verilənlərin müəyyən hissəsininn doğruluğunu yoxlamaq çətinlik yaradacaqdır.

Elektron imzadan müxtəlif sahələrdə istifadə etmək olar:

* Elektron imzadan elektron sənəddə məsulliyyət daşıyan imza kimi istifadə etmək olar (ya fərd şəxsən sənədi imzalayır, ya da ki, sənəd olan kağıza öz möhürünü vurur);
* Elektron imza proqramda, ya da ayrı modullarda istifadə edilir. Bu zaman kompüter istifadəçisi bu tip proqramları ya İnternetdən yükləyir, ya da ki, bu proqramları etibarlı və məlum mənbəədən alır.

Dəftərxana və ya müxtəlif şirkətlərin katibliyi ilə işgüzar yazışmaların aparılması zamanı elektron imza bəzən “zərf” rolunu oynayır, yəni bir tərəfdə göndərilən məktub elektron imza ilə “möhürlənir”, digər tərəfdə isə alınmış məktub “açılır”. Bu zaman hər iki halda verilənlərin toxunulmazlığı və həqiqiliyi öncədən yoxlanılır.

***Elektron imza***

Elektron imza məlumatı öhdəliklə əlaqələndirmək və ya məlumatın həqiqiliyini müəyyən etmək məqsədi ilə iştirakçı tərəfindən yerinə yetirilmiş və ya qəbul edilmiş, elektron vasitələrlə realizə olunmuş istənilən simvol və ya prosesdir. Elektron imzanın əsas funksiyası, adi imza kimi, müəllifin identifikasiyasıdır. Kağız sənəd dövriyyəsində olduğu kimi, elektron imzanın varlığı hələ sənədin həqiqiliyinə dəlalət etmir. Elektron imzalar ailəsinə rəqəm imzası texnologiyası, müəyyən biometrik verilənlər əsasında identifikasiyanı aparmağa imkan verən texnologiyalar (barmaq izləri, səsin tembri, göz tor damarlarının yerləşmə şəkli, əl imzası zamanı xətlərin xronometrajı və başqa biometrik amillər), həmçinin əsasında müxtəlif ***smart-kartların*** və digər aparat açarlarının istifadəsi dayanan texnologiyalar aid edilir. Sadalanan bütün texnologiyalar (smart-kartlar istina olmaqla) - şəxsiyyəti identifikasiya etmə texnologiyalarıdır.

|  |  |
| --- | --- |
| ***AÇIQLAMA***: Daxilinə çip quraşdırılmış avtomatlardırılmış kart alman mühəndisi Helmut Qrettrup və onun həmkarı Yurgen Deslof tərəfindən 1968-ci ildə icad olunmuşdur. Karta patent isə1982-ci ildə verilmişdir. Kartlarin ilk kütləvi istifadəsi 1983-cü ildə Fransada, telefon danışıqları pulunun ödənilməsi üçün istifadə edilir. Fransız ixtiraçısı Ronald Morono 1974-cü ildə yaddaş kartına patent alır. 1977-ci ildə isə Bull şirkətinin əməkdaşı Mişel Uqon ilk dəfə olaraq daxilinə mikroprosessor yerləşdirilmiş smatr-kartı ixtira edir. 1978-ci ildə M.Uqon özüproqramlanan birçipli mikrokompüterə (СПОМ - самопрограммируемый одночипный микрокомпьютер) patent alır. Üç il sonra edilmiş ixtiraya əsaslanaraq qurulmuş CP8 çipi Motorola şirkəti tərəfindən istehsal olunur. Bu ərəfədə Honeywell Bull şirkəti smart-kartla bağlı mikroprosessorlara 1200-ə yaxın patentə sahib olur. Şirkət sonrakı illərdə şirkəti ilə əməkdaşlığa başlayır və yeni quruluşa malik smart-kartların istehsalını yerinə yetirir. Debet kartlı texnologiyanın kütləvi istehsalı 1992-ci ildə tamamlanır. Debet kartlı texnologiya istifadəyə çox asan idi, kart sahibi kartı terminala daxil etdikdən sonra ona məxsus PIN-kodu yığır və lazım olan əməliyyatı yerinə yetirirdi.  Smart-kart texnologiyasına əsaslanan elektron pul sistemi 1990-cı illərin ortasına kimi Avropada geniş istifadə edilir. Bununla yanaşı smart-kartdan Almaniyada (Geldkarte), Avstriyada (Quick), Belçikada (Proton), Fransada (Moneo), Nidelandiyada (), İsveçrədə (Cash), Norveçdə (Mondex), İsveçdə (Cash), Finlyandiyada (Avant), Böyük Britaniyada (Mondex), Danimarkada (Danmønt) və Portuqaliyada (Porta-moedas Multibanco) istifadə olunurdu.   |  | | --- | | http://www.ljplus.ru/img/p/l/plesetsk/th_zhurnal.lib.ru_radwi_s_sergej_korolew.jpgHelmut Qrettrup (almanca Helmut Gröttrup; 1916 - 1981) alman mühəndis-raketçisi, idarəetmə sistemləri üzrə mütə-xəssis, alman raket mütəxəsislərinin rəh-bəri. Elektron çiplərinin köməyilə müştərilərə aid verilənlərin identifika-siya edilməsi sahəsinə öz tövhələrini vermişdir. Müasir informasiya tex-nologyalarında mütəxəs-sisin ideyalarından geniş istifadə olunur. |   Smart-kartların geniş istifadəsi 1990-cı ilə təsadüf edir. Bu əsasən GSM mobil telefonlarında smart-kartın iş prinsipinə əsaslanan SIM-kartlardan istifadə ilə bağlı idi. 1993-cü ildə Beynəlxalq Ödəmə Sistemləri və Europay smart-kartdan kredit və debet hesablarının ödənilməsində istifadə olunması barədə müştərək işə başlayırlar. İlk EMV (Europay, MasterCard, Visa) standartı 1994-cü ildə istehsal olunur. Texniki xarakteristikaları təkmilləşdərilmiş EMV 1998-ci ildən ustehsal olunmağa başlayır.    Rolan Moreno (fransızca Roland Moreno) kredit kartlarında və mobil telefonların SIM-kartında istifadə olunan elektron yaddaş kartının – smart-kartın ixtiraçısı. |

 Sənədlərin imza ilə müəllifləşdirilməsi  çoxdan məlumdur. İstənilən sənəd yalnız onda müəllifin imzası (möhürü) olduqda hüquqi qüvvəyə minir. İstənilən imza sənədin müəllifinin kim olduğunu dəqiq göstərir, sənədi imzalayanın sənəddə qeyd olunmuş məlumatla razı olması haqqında şəhadət verir, göndərənin başqa sənədi deyil, məhz göndərdiyi sənədi imzaladığını təsdiq edir, sənədin ilkin mətninin sonrakı dəyişiklik və təhriflərdən mühafizəsinə zəmanət verir.

Real elektron imza sistemlərinin fəaliyyəti hüquqi, təşkilati və proqram-texniki təminat tələb edir. Hüquqi təminatda elektron imzaya hüquqi qüvvə verən hüquqi aktların qəbul edilməsi aiddir. Təşkilati təminat istifadəçilərin müəyyən sertifikasiya mərkəzlərində qeydiyyatını, istifadəçi və sertifikasiya mərkəzi arasında bir-birinə verilmiş açıq açarlara görə cavabdehlik haqqında sənədlərin rəsmiləşdirilməsini əhatə edir. Proqram-texniki təminata elektron imzanın formalaşdırılmasını, yoxlanmasını, açarların generasiyasını və saxlanmasını, işlənmiş sənədləri və onların imzalarını saxlayan verilənlər bazasının saxlanmasını və s. təmin edən bütün proqram və aparat vasitələri daxildir.

Plastik kart ***bankomat*** və ***POS terminalları*** üçün əsas informasiya daşıyıcısı olduğu üçün həmişə saxtakarların, oğruların diqqət mərkəzindədir. Ona görə belə kartları buraxmazdan öncə təhlükəsizlik məsələləri dərindən işlənilməlidir.

|  |  |  |
| --- | --- | --- |
| ***AÇIQLAMA***: *Bankomat* ingiliscə Automated teller machine sözündən yaranmadır, bəzən ATM, bəzən dəbank avtomatı kimi oxunur. Bankomat proqram-texniki komnleks olub ödəmə kartından istifadə etməklə nağd pulun avtomatlaşdırılmış şəklildə alınması və verilməsi üçün istifadə edilir. Bununla yanaşı bankomatdan istifadə etməklə (ödəmə kartı ilə və ya onsuz) digər əməliyyatları da (məhsulun dəyərinin ödənilməsi, xidmətlərə görə pulun ödənilməsi, uyğun əməliyyatların yerinə yetirilməsini təsdiqləyən sənədlərin tərtib olunması və s.) yerinə yetirmək mümkündür. Bankomatın prototipi 1939-cu ildə amerikalı alim Lüter Corc Cimçiyan tərəfindən icad olunmuşdur.  İlk hazırlanmış qurğu pulu tələbediciyə nağd şəkildə verirdi, amma alınmış pulun dəyərini ümumi hesabdan silə bilmirdi. İlk icad olunmuş qurğu ABŞ–da sınanılır. Lazımı nəticə əldə edilmədiyi üçün bank qurğudan istifadəni imtina edir. 30 ildən sonra alim yenidən qurğunu təkmilləşdirir və 1960-cı illərin axırlarında yenidən istifadəyə təklif edir. İlk bankomat 27 iyun 1967-ci ildə London şəhərinin şimal hissəsindəki Enfild rayonundakı bankların birində qurulur (bankomat Automated Teller Machine (ATM) adlandlrılmışdı). Qurğunun yaradıcısı şotlandıyalı Con Şepard-Barron idi. Qurğu De La Rue şirkətinin sifarişi əsasında yaradılmışdı. Şirkət dünyanın 150-dən çox ölkəsi üçün kağız pulun hazırlanmasında istifadə olunan qiymətli kağız istehsal edirdi. Con Şepard-Barronun hazırladığı qurğu pul tələb edən şəxsin hesabında nə qədər pulun olmasını yoxlaya bilmədiyi üçün bankirlərin rəğbətini qazana bilmir və ixtiraçı onu digər məqsəd üçün - şokalad satışı üçün təkmilləşdirir. 1966-cı ildə şotlandiyalı mühəndis Ceyms Qudfellou gizli 4 rəqəmli kod ilə mühafizə edilən koda patent alır (Patent bürosu koda “PIN-kod” adı altında identifikasiya nömrəsi verir). O dövrdən başlayaraq PIN-kod bank hesablarında geniş istifadə olunmağa başlanılır.  Bankomatların istifadəsi tədricən həyata keçirdi. 1971-ci ildə amerikanın 35 bankında bankomatlardan istifadə edilir. Amerikada bankomatların hər yerə quraşdırılması ilə məşğul olan Citibank bankıdır (bu hadisə 1972-ci ilə təsadüf edir).  01dc6370557008b90dcf5af0d5cad791  *İlk hazınlanmış bankomat*  1972-ci ildə Böyük Britaniyada Lloyds bankı IBM şirkəti tərəfindən icad olunmuş Cash-Point adlı ilk on-layn bankomatlarını işə salır. Bankomatlar vauçerin yerinə maqnit zolaqlı plastik kartları qəbul edirdi. Telekommunikasiyanın sürətli inkişafı Amerikada, Vaşınqton ştatında, bir neçə yüz bankın Exchenge adı altında birləşməsinə səbəb olur. Bu ərəfədə (1972-1975-ci illər) istifadə olunan bankomatlar nəin ki, pulun verilməsini, həmçinin onun qəbulunuda həyata keçirə bilirdi.  Rusiyada ilk bankomat 1991-ci ildə istifadə olunmuşdur. Hesablamalar göstərir ki, 2011-ci ildə dünyada 2,4 milyon bankomatdan istifadə olunurdu. Təxmini hesablanmışdır ki, 2017-ci ildə bu rəqəm 3,4 milyona çatacaqdır.   |  |  | | --- | --- | | http://mignews.com.ua/modules/news/images/articles/changing/2167201_480_320.jpg  *Con Şepard-Barron* | http://www.bzi.ro/public/upload/photos/116/James-Goodfellow_966f558b08.jpg  *Ceyms Qudfellou* |   Nəşr edilmiş məqalərinin birində qeyd edilir ki, 2012-ci ildə Yaponiyanın The Ogaki Kyoritsu Bankında müştərinin övucunun şəkilini dəstəkləməklə işləyən bankomat istifadəyə verilmişdir. |

|  |
| --- |
| ***AÇIQLAMA***: *POS – terminal* (ingiliscə Point Of Sale sözündən yaranmadır və *satış nöqtəsi* anlamını verir) – plastik kartların köməyilə pulun ödənilməsindən ötrü yaradılmış elektron proqram-texniki qurğudur. Pos-terminal tərkibində çip olan kartları, maqnit zolaqlı və kontaktsız kartları, həmçinin kontaktsız toxunma prinsipi ilə işləyən kartları da qəbul edir. Bəzən Pos-terminal kimi xəzinədarın (kassirin) iş yerində quraşdırılmış proqram-aparat kompleksi də nəzərdə tutulur. POS-terminal istifadəçi ilə qarşılıqlı interfeysə malikdir. Bundan istifadə edən alıcı alacağı məhsul haqqında (onun qiyməti, istifadə müddəti, istehsal tarixi və s.) məlumat əldə edə bilir. POS-terminal müəyyən kassa proqramına uyğun satıla bilər.    http://img.bugun.com.tr/newsFiles/1/0/0/1/1/1/0/1/0/0/1/1/0/0/0/0/1/1/0/1/file/1287706_1117720.jpg  *Pos terminal* |

Elektron rəqəmsal imza əllə çəkilən imzanın elektron ekvivalentidir. Elektron rəqəmsal imza nəinki informasiya göndərənin əsilliyinin müəyyən olunmasına, həm də məlumatın tamlığının qorunmasına xidmət edir.

İnformasiya göndərənin əsilliyinin müəyyən olunması üçün, elektron rəqəmsal imzadan istifadə zamanı bağlı və açıq açarlar tətbiq olunur. Proses asimmetrik şifrələnməyə oxşayır, amma bu halda bağlı açar şifrələmək üçün, açıq açar isə şifrəni açmaq üçün istifadə olunur.

***Elektron rəqəmsal imzanın*** tətbiq olunma alqoritmi bir sıra əməliyyatlardan ibarətdir.

İki qoşa açar yaradılır:

* 1.Açıq və bağlı;
* 2.Açıq açar bu işdə maraqlı olan tərəfə (sənədi qəbul edən, imzalanmış tərəf) ötürülür;
* 3.Göndərən informasiyanı bağlı açarın köməyilə şifrələyir və onu əlaqə kanalı vasitəsilə qəbul edənə ötürür;
* 4.Qəbul edən göndərilən informasiyanı açıq açarın köməyilə şifrədən azad edir.

Açıq açarla şifrələnmiş informasiyanın yalnız bağlı açarın köməyilə açılması elektron rəqəmsal imzanın məğzidir.

Nəzərə almaq lazımdır ki, elektron rəqəmsal imzaların əsasını xeş-funksiya təşkil edir.

Xeş-funksiya - yəni (H) funksiya məlumatın girişində (M) ixtiyari uzunluğu qəbul edir, amma çıxışda isə H(M) fiksə olunmuş uzunluğa malik qiymət alır. Bu M məlumatın *xeşi* və ya *profili* adlanır.

|  |
| --- |
| ***AÇIQLAMA:*** *Hashing* (bəzən *Xeşləmə* də adlandırılır) ixtiyarı uzunluğa malik olan giriş verilənlər massivinin müəyyən alqoritm ilə qeyd edilmiş uzunluqlu çıxış bitlər sətrinə çevrilməsidir. Belə çevrilməni həmçinin Xeş – funksiya və ya bağlama funksiyası da adlandırırlar. Funksiyanın nəticəsini Xeş, Xeş-kod, Xeş-cəm və ya əlaqə məlumatı (ingiliscə message digest) adlandırırlar. Müxtəlif xüsusiyyətə malik xeş alqoritmləri mövcuddur. 1953-cü ildə Donald Ervin Knut ilk dəfə sistem xeşləmə ideyasını təklif edir və bundan istifadəni IBM əməkdaşlarına məsləhət bilir. Sonrakı illərdə bu ideya ilə digər alimlər də məşğul olur və bu sahəyə öz tövhələrini verirlər.  http://www.mjhsbnn.com/nich-studentwork/nich-studentwork/fall_2012/athlete/brown/images/640_don-knuth-colour.jpg  Donald Ervin Knut (ingiliscə Donald Ervin Knuth) 10 yanvar 1938-ci ildə Viskonsin ştatının Miluoki şəhərində anadan olmuşdur, amerika alimidir, müxtəlif ölkələrdəki (o cümlədən Sankt-Peterburqdakı Dövlət Universitetinin) Universitetlərin, Stenford Universitetinin professorudur. Proqramlaşdırma sahəsində mühazirələr oxuyur (19 monoqrafiyanın, 160-dan çox elmi məqalənin, çoxlu sayda məşhur proqram texnologiyasının müəllifidir), yeni nəsil alimlərin yetişməsinə öz tövhələrini verir. Alim alqoritmin əsaslarına və hesablama riyaziyyatı üsullarına aid dünya şöhrətli, tanınmış seriya kitablar müəllifidir. D.E.Knut masaüstü TEX və METAFONT nəşriyyat sisteminin yaradıcısıdır. |

Bunlarla yanaşı kriptoqrafiyada (əsasəndə elektron rəqəmsal imzada) aşağıdakı xüsusiyyətlərə malik olan funksiyalardan da istifadə olunur:

1.*Birtərəflilik*. İstənilən xeş üçün *h-ı* praktiki olaraq hesablamaq mümkün deyil və ya x elə seçmək lazımdır ki, H(X) = h bərabərliyi yerinə yetsin.

2.*Birinci üslub kolliziyaya görə dayanaqlıq*. İstənilən məlumat üçün *x-ı* praktiki olaraq hesablamaq mümkün deyil və ya başqa bir *y* məlumat seçmək lazımdır ki, H(x)=H(y).

3.*İkinci üslub kolliziyaya görə dayanaqlıq*. *x* və *y* müxtəlif məlumatları üçün elə cütlük seçmək lazımdır ki, praktiki olaraq hesablamaq mümkün olmasın və ya bunlar üçün H(x)=H(y).

Xeş funksiyanın dayanıqlıq kriptoqrafik xüsusiyyəti elektron rəqəmsal imzanın etbarlığını təmin etməlidir. Doğurdan da, orijinal məlumatın heç olmasa bir simvolu dəyişilərsə, onun xeş funksiyası (bu səbəbdən Elektron Rəqəmsal İmza da) dəyişəcəkdir, digər tərəfdən bu xeş funksiya ilə başqa bir məlumatı seçmək mümkün olmayacaqdır.

Elektron imza elektron formada olan verilənlər blokudur, digər verilənlərlə (elektron sənəd, proqram faylları və s.) məntiqi əlaqəli olur və həmin verilənlərin müəllifini birqiymətli *identifikasiya* etməyə imkan verir.

Rəqəmsal imza elektron imzanın növlərindən biridir, müəllifin identifikasiyasından savayı bir neçə əlavə funksiyanı həyata keçirir. Rəqəmsal imza adətən asimmetrik kriptoqrafiyaya əsaslanır.

*Rəqəmsal imza* konkret məlumata (mətnə, fayla və ya ixtiyari uzunluqlu istənilən bitlər yığınına) əlavə olunan və aşağıdakı funksiyaları təmin etməyə imkan verən sabit uzunluqlu informasiya blokudur:

* məlumatın müəllifinin identifikasiyası və autentifikasiyası;
* məlumatın tamlığına nəzarət;
* məlumatın müəllifliyindən imtinanın qeyri-mümkünlüyünə zəmanət.

Məlumatın rəqəmsal imzası məlumatın özündən və imzalayanın gizli açarından asılıdır. Rəqəmsal imza iki alqoritm ilə realizə edilir: rəqəmsal imzanın yaradılması alqoritmi və rəqəmsal imzanın yoxlanılması alqoritmi. Rəqəmsal imza alqoritmlərinə misal olaraq RSA, DSA, ECDSA, ElGamal, Şnorr, QOST R 34.10-2001 və s. alqoritmlərini göstərmək olar.

**Rəqəmsal imzanın iş prinsipi.** Açıq açarlı kriptoqrafiya əsasında rəqəmsal imzanın iş prinsipinə baxaq. Tutaq ki, hər hansı **A** istifadəçisi müəyyən məlumatı imzalamalıdır. Bunun üçün o, heş-

Heş-funksiya

Şifrləmə

İmzalayanın gizli açarı

**Şəkil 4. İmzanın yaradılması**

funksiyanın köməyi ilə bu məlumatın heş-kodunu hesablayır və onu özünün gizli açarı ilə

şifrləyir. Şifrlənmiş heş-kod məlumata əlavə edilir. Beləliklə, məlumatın rəqəmsal imzası alınır. İmzanın yaradılması şəkil 4-də göstərilib.

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 birləşdirilmiş şifrlənmiş heş-kodu **A** istifadəçisinin açıq açarı ilə deşifrə edir və alınmış deşifrə edilmiş heş-kodu özünün yaratdığı heş-kodla müqayisə edir. Onlar üst-üstə düşürlərsə, imza həqiqi hesab olunur. Əks halda imza rədd olunur. Gizli açar yalnız **A** istifadəçisinə məxsus olduğundan aydındır ki, məlumatı da yalnız o imzalaya bilərdi. İmzanın yoxlanması şəkil 5-də göstərilib.

Heş-

funksiya

Deşifrləmə

Müqayisə

İmzalayanın

açıq açarı

**Şəkil 5. İmzanın yoxlanması**