AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİYASI
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

Əliquliyev R.M., İmamverdiyev Y.N.

RƏQƏM İMZASI TEXNOLOGİYASI

Bakı –«Elm» - 2003

ISBN 5–8066–1608–8

Əliquliyev R.M., İmamverdiyev Y.N.

Rəqəm imzası texnologiyası

Vəsaitdə rəqəm imzası texnologiyasının əsasları və açıq açarlar infrastrukturunun əsas anlayışları şərh olunur. Mövcud rəqəm imzası sxemləri və onların riyazi əsasları, sxemlərin təhlükəsizliyi məsələləri, sxemlərə olan əsas təhlükələr və hücumlar araşdırılır.

Rəqəm imzası texnologiyasının praktik tətbiqinin elmi-nəzəri problemləri, standartlaşdırma və sertifikasiya məsələləri izah olunur, rəqəm imzasının intellektual kartlarda realizasiyası və konkret əməliyyat sistemində tətbiqi nəzərdən keçirilir.

Kompüter şəbəkələrində informasiya təhlükəsizliyi sahəsində ixtisaslaşan tələbələr və aspirantlar üçün nəzərdə tutulmuşdur. Vəsaitdən kompüter sistemləri və şəbəkələrinin istifadəçiləri də yararlana bilərlər.

Açar sözlər: imza, rəqəm imzası, açar, autentifikasiya, açıq açarlar infrastrukturu, tamlıq, təhlükə, heş-funksiya, rəqəm sertifikatı, hücum, standart, açarların idarə olunması.

Vəsait AMEA İnformasiya Texnologiyaları İnstitutu Elmi şurasının qərarı ilə çapa məsləhət görülmüşdür.

Giriş

XX əsrin ikinci yarısından başlayan və əhəmiyyəti XXI əsrdə daha da güclənəcək hesablama texnikası və telekommunikasiya sahəsində elmi-texniki inqilabın da arasında olduğu bir sıra vacib ictimai inkişaf amillərinin təsiri ilə bəşəriyyət öz inkişafının yeni tarixi mərhələsinə – informasiya cəmiyyəti mərhələsinə qədəm qoymuşdur. Bu cəmiyyətdə istehsalın əsas məhsulu informasiya və biliklərdir. İnformasiya-kommunikasiya texnologiyaları informasiya cəmiyyətinin formalaşmasına təsir edən ən mühüm amillərdən biridir. Onların inqilabi təsiri insanların həyat tərzində, onların təhsilində və işində, həmçinin hökumət və vətəndaş cəmiyyətinin qarşılıqlı əlaqəsində özünü biruzə verir. İnformasiya-kommunikasiya texnologiyaları sürətlə dünya iqtisadiyyatının inkişafının həyati vacib stimuluna çevrilir. İnformasiya-kommunikasiya texnologiyalarının sürətli inkişafı və geniş yayılması, qlobalizasiya prosesləri bəşəriyyətin inkişafı üçün geniş imkanlar yaratmaqla yanaşı, bir sıra problemlər də meydana çıxarmışdır. Bu problemlərdən biri də aktuallığını indi hamının etiraf etdiyi elektron mühitdə informasiya təhlükəsizliyinin təmin olunması məsələsidir [1]. Elektron mühitdə elə qarşılıqlı əlaqə aləti tələb olunur ki, istifadəçilər informasiyanı bir-birinə səhih ötürə bilsinlər, elektron kanallarla aldıqları bu və ya digər informasiyanın mənbəyini dəqiq təyin edə bilsinlər, informasiyanın mənbəyi isə öz müəllifliyini inkar edə bilməsin. Bir-birinə etibar etməyən (inanmayan) tərəflər halında bu problem xüsusilə kəskindir. Bu halda təhlükələrin mənbəyi yalnız üçüncü tərəf (düşmən) yox, qarşılıqlı təsirin həyata keçirildiyi tərəflərdən biri və ya bir neçəsi də ola bilər.

Bu məqsədlər üçün rəqəm imzası (Rİ) mexanizminin istifadəsi qoyulan bütün bu tələbləri yerinə yetirməyə imkan verir. Rəqəm imzası texnologiyasının tətbiqi məlumatın müəllifini– mənsub olduğu mənbəni (istifadəçi, server, proses və s.) birqiymətli təyin etməyə, göndərilən məlumatın elə

keçməsi, modifikasiyası və saxtalaşdırılmasını aşkara çıxarmağa imkan verir. Təbii olaraq məlumat dedikdə, təkcə elektron poçtla göndərilən məktub deyil, ümumiyyətlə şəbəkədə ötürülən bütün növ verilənlər nəzərdə tutulur.

İnformasiya texnologiyalarının inkişafı tarixindən məlumdur ki, artıq XX əsrin 70-ci illərinin əvvəllərinə yaradılmış ilk böyük kompüter şəbəkələrində informasiyanın kağızsız emalına, sənədlərin elektron mübadiləsinə başlıca maneələrdən biri əl imzasının elektron (rəqəm) variantının olmaması idi. Bu zərurətdən həmin onilliyin sonlarına doğru rəqəm imzası texnologiyası irəli sürüldü. Rəqəm imzası texnologiyası XX əsrin 80-90-cı illərindən etibarən bank sistemlərində, elektron kommersiya sistemlərində, istifadəçilərin autentifikasiyası sistemlərində, sənədlərin müəllifliyinin təsdiqi sistemlərində və başqa sahələrdə geniş tətbiq olunur. Məsələn, müasir ödəniş sistemlərində bütün proses əvvəldən axıra elektron (rəqəm) formasında baş verir [2]. Bu zaman təhlükəsizliyin təmin olunması və həqiqiliyin təsdiqi üçün (göndərilən elektron sənədlərin konfidensiallığı, informasiya mübadiləsi iştirakçılarının autentifikasiyası) şifrləmə və rəqəm imzası geniş istifadə olunur. Rəqəm imzasının istifadəsi aşağıdakılara imkan verir:

- müqavilələrin rəsmiləşdirilməsi və sənədlərin mübadiləsinə sərf olunan vaxtı əhəmiyyətli dərəcədə azaltmağa;
- sənədlərin hazırlanması, çatdırılması, uçotu və saxlanması prosedurunu təkmilləşdirməyə və ucuzlaşdırmağa;
- sənədin səhihliyinə zəmanət verməyə;
- informasiya mübadiləsinin konfidensiallığının yüksəldilməsi sayəsində maliyyə itgiləri riskini minimumlaşdırmağa;
- sənədlərin mübadiləsinin korporativ sistemini qurmağa və s.;

Real rəqəm imzası sistemlərinin fəaliyyəti hüquqi, təşkilati və proqram-texniki təminat tələb edir. Hüquqi təminata rəqəm

imzasına hüquqi qüvvə verən hüquqi aktların qəbul edilməsi aiddir. Təşkilati təminat istifadəçilərin müəyyən sertifikasiya mərkəzlərində qeydiyyatını, istifadəçi ilə sertifikasiya mərkəzi arasında (və ya iki istifadəçi arasında) bir-birinə verilmiş açıq açarlara görə cavabdehlik haqqında sənədlərin rəsmiləşdirilməsini əhatə edir. Proqram-texniki təminata rəqəm imzasının formalaşdırılmasını, yoxlanmasını, açarların generasiyasını və saxlanmasını, imzalanmış sənədləri və onların imzalarını saxlayan verilənlər bazasının saxlanmasını və s. təmin edən bütün proqram və aparat vasitələri daxildir.

Rəqəm imzası texnologiyası sahəsində intensiv elmi araşdırmalar XX əsrin 70-ci illərindən başlanmışdır. Bu illər ərzində rəqəm imzası texnologiyasının nəzəri əsasları işlənmiş, o, kriptoqrafiya çərçivəsində bir elmi istiqamət kimi formalaşmış, rəqəm imzası texnologiyasının istifadəsi sahəsində münasibətləri tənzimləmək məqsədilə bir sıra ölkələrdə, beynəlxalq birlik və təşkilatlarda normativ-hüquqi sənədlər, standartlar, rəqəm imzası vasitələrinin sertifikasiya qaydaları işlənib hazırlanmışdır. Rəqəm imzası texnologiyası getdikcə təkmilləşməkdə, daha geniş tətbiq dairəsi qazanmaqda, elm və texnologiya qarşısında daha mürəkkəb məsələlər qoymaqdadır.

Təqdim olunan bu vəsaitin məqsədi sürətlə inkişaf edən bu elmi istiqamətin əsaslarını şərh etmək, gələcək elmi-praktiki tədqiqatların istiqamətini müəyyənləşdirməkdə tədqiqatçılara kömək etməkdir.

1. Rəqəm imzasının mahiyyəti

1.1. Elektron imza və rəqəm imzası

Artıq "elektron imza", "elektron rəqəm imzası", "rəqəm imzası" kimi terminlər dilimizdə vətəndaşlıq hüququ qazanmaqdadır. Bu terminlərə aydınıq gətirmək lazımdır.

Texnologiya ingilis dilli mühitdə yaranaraq formalaşmışdır. İngilis dilli ədəbiyyatda əsas etibarı ilə "electronic signature" və "digital signature" terminləri işlədilir. Nadir hallarda, əsasən digər dillərdən ingilis dilinə tərcümə olunmuş yazılarda "digital electronic signature", "electronic digital signature" terminlərinə də təsadüf etmək olar. Zənnimizcə, "electronic signature" və "digital signature" terminlərinin tərcüməsi olan "elektron imza" və "rəqəm imzası" terminləri üzərində dayanmaq daha düzgün olardı.

"Elektron imza" və "rəqəm imzası" terminlərinin mühüm fərqləri var. 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. Bu tərif verilən imzanın həyata keçirilməsi üçün seçilmiş konkret daşıyıcı və ya metoda deyil, imzanın ənənəvi hüquqi aspektinə əsaslanır. 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 ilə yanaşı hal-hazırda müəyyən biometrik verilənlər əsasında identifikasiyanı aparmağa imkan verən texnologiyalar [7] (barmaq izləri, səsin tembri, göz toru damarlarının yerləşmə şəkli, əl imzası zamanı xətlərin xronometrajı və başqa biometrik amillər, perspektivdə DNK), həmçinin əsasında müxtəlif smart-kartların və digər aparat açarlarının istifadəsi dayanan texnologiyalar aid edilir. Sadalanan bütün texnologiyalar (smart-kartlar istisna

olmaqla)- şəxsiyyəti identifikasiya etmə texnologiyalarıdır. Bu texnologiyalardan hər birinin üstünlükləri və nöqsanları var.

Rəqəm imzası elektron imzanın bir növüdür və identifikasiya funksiyası ilə eyni vaxtda elektron sənədin həqiqiliyinin yoxlanması funksiyasını (autentifikasiyasını) da həyata keçirir. İSO 7498-2 standartına [69] uyğun olaraq, rəqəm imzası verilənlər blokunun kriptoqrafik çevrilməsi nəticəsində alınan verilənlərdir və onlar bu blokun tamlığına və mənbənin həqiqiliyinə əmin olmağa imkan verir, həmçinin sənədi alan tərəfin hərəkətlərindən mühafizəni təmin edir. Beləliklə, rəqəm imzası aşağıdakılara imkan verir:

- imzalayanın identifikasiyası;
- məlumatın identifikasiyası;
- imzadan boyun qaçırmama;
- məlumatın tamlığı.

Rəqəm imzasının bu imkanları elmi-metodik vəsaitdə ətraflı araşdırılacaq. Qeyd edək ki, rəqəm imzası anlayışını əl imzasının rəqəmləşdirilmiş forması ilə əlaqələndirmək düzgün deyil.

Rəqəm imzası müəyyən texnologiyaya bağlıdır, elektron imza isə texnologiyadan asılı deyil. Bu sahədəki beynəlxalq normativ aktların əksəriyyəti texnoloji neytrallığı gözləmək prinsipindən çıxış edərək "elektron imza" anlayışından istifadə edir. İndi məhz hansı elektron imza texnologiyasının gələcəkdə dominant olaçağını əvvəlcədən söyləmək mümkün deyil. Müasir proqram və elektron vasitələri elə sürətlə inkişaf edir ki, hər hansı varianta üstünlük vermək olduqca risklidir.

1.2. Elektron sənədə mümkün təhlükələr

Müasir dünyada sənədlərin elektron formasının və onların emal üsullarının geniş yayılması ilə əlaqədar elektron sənədlərin həqiqiliyinin və müəllifinin müəyyənləşdirilməsi problemi xüsusilə aktual olaraq meydana çıxır. Elektron sənəd ənənəvi sənəddən hər şeydən əvvəl fiziki deyil, məntiqi təbiətə malik olması ilə fərqlənir. Bu isə öz növbəsində sənədin

xassəsinin daşıyıcının xassəsindən ayrılmasına səbəb olur ki, bu da müxtəlif əqdlərin, o cümlədən müqavilələrin bağlanmasında əl imzası, möhür, bank və bankın mühafizə elementləri kimi ənənəvi rekvizitlərin tətbiqini qeyri-mümkün edir.

İnformasiyanın ötürülməsi zamanı birlikdə və ya ayrılıqda aşağıdakılar təmin olunmalıdır [1, 4, 10]:

1. Konfidensiallıq (məxfilik)- bədniyyətlinin ötürülən məlumatın məzmununu bilmək imkanı olmamalıdır;
2. Autentiklik (həqiqilik)- iki anlayışı əhatə edir:
   - tamlıq- məlumat təsadüfi və qəsdli dəyişilmədən mühafizə olunmalıdır;
   - göndərənin identifikasiyası (müəllifliyin yoxlanması)- alanın məlumatı kimin göndərdiyini yoxlamaq imkanı olmalıdır.

İnformasiya təhlükəsizliyinin təmin olunması nəzəriyyəsinə uyğun olaraq əvvəlcə elektron sənədlərə olan əsas təhlükələrə nəzər salaq. Elektron sənədlərin mübadiləsi zamanı bədniyyətli əməllərin aşağıdakı növləri mövcuddur [8]:

3. *İmtina:* Həqiqətdə sənədi göndərməsinə baxmayaraq abonent *A* bildirir ki, o, abonent *B*-yə sənədi göndərməyib. Bu tip təhlükələrdən mühafizə üçün elektron (və ya rəqəm) imzadan istifadə edilir.
4. *Modifikasiya:* Abonent *B* məlumatı dəyişdirir və iddia *edir* ki, məlumatı məhz bu şəkildə abonent *A*-dan almışdır.
5. *Əvəzetmə*: Abonent *B* özü sənədi formalaşdırır və onu abonent *A*-dan aldığını iddia edir.
6. *Fəal ələkeçirmə:* Pozucu (şəbəkəyə qoşularaq) sənədləri (faylları) icazəsiz ələ keçirir və onlarda dəyişiklik edir.
7. *Maskarad*: Abonent *C* abonent *A*-nın adından sənəd göndərir. Modifikasiyadan, əvəzetmədən, dəyişiklik etməkdən və maskaraddan mühafizə üçün rəqəm imzasından istifadə edilir.
8. *Təkrar:* Abonent *C* əvvəllər abonent *A*-nın abonent *B*-yə göndərdiyi sənədi təkrar *B*-yə göndərir. Təkrar tipli

təhlükələrdən ən yaxşı mühafizə imitoəlavələrin istifadəsi və daxil olan məlumatların uçotudur.

Autentifikasiya alqoritminin və texnologiyasının seçilməsi zamanı bədniyyətli əməllərin yuxarıda sadalanmış bütün növlərindən etibarlı müdafiəni nəzərdə tutmaq lazımdır. Klassik (biraçarlı) kriptoqrafiya çərçivəsində təhlükələrin bütün bu növlərindən müdafiə olunmaq çətindir, çünki məxfi açara malik tərəflərdən hansının bədniyyətli əməli törətdiyini müəyyən etmək qeyri-mümkündür. İkiaçarlı kriptoqrafiyaya əsaslanan sxemlər daha səmərəlidir.

1.3. İmzanın funksiyaları

İmzanın sənədlərin avtorizasiyası vasitəsi kimi istifadəsi çoxdan məlumdur. İstənilən sənəd yalnız onda müəllifin imzası (möhürü) olduqda hüquqi qüvvə qazanır. İstənilən imza- istər adi, istərsə də rəqəm imzası həmişə ən azı aşağıdakı funksiyaları yerinə yetirir [3, 4, 13]:

- sənədin müəllifinin kim olduğunu dəqiq göstərir (avtorizasiya funksiyası);
- sənədi imzalayanın sənəddə qeyd olunmuş məlumatla razı olması haqqında şəhadət verir (prosedur funksiyası). İmzalayan şəxs imzaladığı sənəddən boyun qaçıra bilməz;
- göndərənin başqa sənədi deyil, məhz göndərdiyi sənədi imzaladığını təsdiq edir. Başqa sözlə, ona başqa və ya oxşar sənədi zorla qəbul etdirmək olmaz, çünki onda orjinalın imzalanmış surəti var;
- sənədin ilkin mətninin sonrakı dəyişiklik və təhriflərdən mühafizəsinə zəmanət verir.

Qeyd edək ki, birinci iki funksiya sənədin nəzərdə tutulduğu şəxsin maraqlarını, üçüncü isə imzalayanın maraqlarını müdafiə edir. Bütün bu hallarda imzanın autentiklik (əsllik, həqiqilik) adlanan xassəsi, yəni autentifikasiyanı həyata keçirmək xassəsi "işləyir". Bu xassə, imzanın altında durduğu sənədə də keçir.

Autentifikasiya termini ümumi halda informasiya qarşılıqlı əlaqəsinin bütün aspektlərinə: rabitə seansına, tərəflərə, ötürülən məlumatlara və s. aid edilir. Məlumatların autentifikasiyası həm kommersiya, həm də məxfi (gizli) rabitə sistemlərinin abonentləri üçün həyati əhəmiyyətli amildir. Autentifikasiya qəbul edən və ya ola bilsin arbitr tərəfindən mövcud autentifikasiya protokolu (qaydası) çərçivəsində verilən məlumatın sanksiyalı (qanuni) göndərən tərəfindən göndərildiyi və bu zaman onun dəyişdirilmədiyi faktının müəyyən edilməsidir [3, 38].

Qeyd edək ki, tərəflər bir-birinə inandıqda tərəflərin autentifikasiyasını simmetrik şifrləmə çərçivəsində autentifikasiya kodu mexanizmi vasitəsilə həll etmək mümkündür. Lakin bir-birinə inanmayan tərəflər üçün ümumi məxfi açar əsasında tərəflərin autentifikasiyasını aparmaq mümkün deyil. Bu problemin həllinin əsas mexanizmi rəqəm imzasıdır.

Elektron məlumatların autentifikasiya metodlarının əksəriyyəti bu və ya digər kriptoqrafik metodlara əsaslanır. Elektron məlumatların belə autentifikasiya metodları çoxdan məlum olsalar da, yalnız kriptoqrafiyada yeni istiqamətin meydana çıxması ilə rəqəm imzasına qoyulan bütün tələbləri ödəməyə başladılar. Kriptoqrafiyada yeni istiqamət açıq açarlı kriptosistem anlayışının daxil edilməsi ilə əlaqədardır [59, 5, 8, 10, 21, 19, 30, 37].

1.4. Kriptoqrafiyada yeni istiqamət

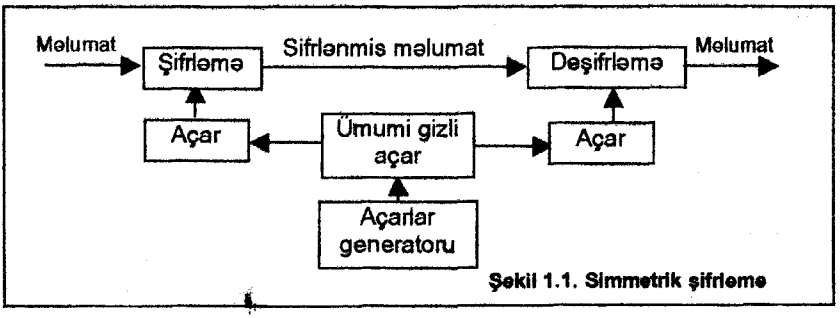
İnformasiyanın məxfiliyinin təmini və tamlığına nəzarət üçün ən güclü vasitələrdən biri kriptoqrafiyadır [1, 13, 20, 21, 33, 22]. Kriptoqrafiya bir çox cəhətlərdən informasiyanın mühafizəsinin proqram-texniki vasitələri arasında mərkəzi yer tutur. Onlardan bir çoxunun realizə olunması üçün kriptoqrafiya bünövrə rolunu oynayır, bəzən də yeganə müdafiə vasitəsi olur. Məsələn, fiziki müdafiəsi olduqca çətin

olan portativ kompüterlər üçün yalnız kriptoqrafiya hətta oğurlanma halında da məxfiliyə təminat verir.

Kriptoqrafiyanın əhəmiyyəti verilənlərin məxfiliyinin təmin olunması çərçivəsindən çox uzaqlara çıxır. İnformasiyanın ötürülməsi və emalının avtomatlaşdırılması artdıqca və informasiya axınları intensivləşdikcə kriptoqrafiyanın metodları böyük əhəmiyyət qazanırlar. Kriptoqrafiyanın müasir tətbiqlərinin bəzi istiqamətlərini sadalayaq:

1. İcazəsiz oxunmaqdan mühafizə (informasiyanın konfidensiallığının (məxfiliyinin) təmini);
2. Yalan məlumatların (qəsdən və ya bilməyərəkdən) yeridilməsindən mühafizə;
3. Qanuni istifadəçilərin identifikasiyası;
4. İnformasiyanın tamlığına nəzarət;
5. İnformasiyanın autentifikasiyası;
6. Rəqəm imzası;
7. Gizli elektron səsvermə sistemləri;
8. Elektron püşkatma;
9. Məlumatın qəbulu faktından imtinadan mühafizə;
10. Müqavilələrin eyni zamanda imzalanması;
11. Sənədlərin və qiymətli kağızların saxtalaşdırılmasından mühafizə.

Şifrləmənin simmetrik və qeyri-simmetrik adlanan iki əsas üsulu fərqləndirilir [3, 4]. Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmə, həm də deşifrləmə üçün istifadə olunur. Olduqca səmərəli (sürətli və etibarlı) simmetrik şifrləmə metodları mövcuddur [3, 10, 35].



Şəkil 1.1. Simmetrik şifrləmə

Şəkil 1.1. simmetrik şifrləmənin iş prinsipini illüstrasiya edir. Simmetrik şifrləmənin bir sıra nöqsanları var:

– məlumatın müəllifliyindən boyun qaçırmamanın təmini;
– açarların autentifikasiyası;
– açarların göndərilməsi (paylanması);

Simmetrik şifrləmə məlumatın müəllifliyindən boyun qaçırmamanı təmin edə bilməz. Simmetrik şifrləmədə məxfi açar həm göndərənə, həm də alana məlum olmalıdır. Məlumatı alan şəxs şifrlənmiş və deşifrlənmiş məlumatın varlığı əsasında bu məlumatı konkret göndərəndən aldığını sübut edə bilməz. Çünki belə məlumatı o özü də generasiya edə bilər.

Açarların autentifikasiyası dedikdə, məxfi açarın qanuni göndərənə (məsələn, açarları paylama mərkəzinə) mənsub olduğuna əmin olmağa imkan verən prosedurun aparılması nəzərdə tutulur.

Simmetrik şifrləmənin ən mühüm nöqsanı açarların mühafizəli kanalla göndərilməsini tələb etməsidir. Açarların paylanması məsələsi çox mühümdür, çünki açarların seansdan (rabitə) seansa və ya müəyyən həcmdə informasiya ötürüldükdən sonra dəyişdirilməsi adi tələblərdən biridir.

Əgər kriptosistem *N* istifadəçini şəbəkədə birləşdirirsə, istifadəçilər arasında ən azı *N(N-1)/2* açar paylanmalıdır. *N*-in kifayət qədər böyük qiymətlərində bu problemə çevrilir, çünki paylanacaq açarların sayı kvadratik qanunla artır. Bu məsələnin həlli üçün mühafizəli kanalın istismarının çox mürəkkəb və bahalı olduğunu nəzərə alan bir neçə struktur həllindən istifadə olunur. Onlardan biri açarların açıq paylanması sistemidir.

Açarların açıq paylanması ilk iki problemi həll edir, yəni məlumatın müəllifliyindən boyun qaçırmamanı təmin edir və məxfi açarların paylanmasını mühafizəli kanal olmadan həyata keçirməyə imkan verir, lakin autentifikasiyanın zəruriliyi qalır. Açarlar açıq kanalla ötürülür.

Açarların açıq paylanması üçün ilk alqoritm U. Diffi və M. Hellman tərəfindən "Kriptoqrafiyada yeni istiqamət" adlanan məqalədə [59] təklif olunmuşdur. Onun yerinə yetirilməsi üçün

tərəflər böyük sadə ədədin qiyməti p və multiplikativ qrupun doğuranı a barədə sözləşməlidirlər. k ümumi açarının hazırlanması üçün onlar təsadüfi $x, 1 \le x \le p-2$ və $y, 1 \le y \le p-2$ sadə ədədlərini generasiya etməlidirlər. Bundan sonra tərəflər (A və B) aşağıdakı protokola uyğun olaraq məlumat mübadiləsi etməlidirlər:

(1) $A \to B : a^x \bmod p$,

(2) $B \to A : a^y \bmod p$

Axtarılan ümumi açar $k=\left(a^y\right)^x=\left(a^x\right)^y \bmod p$ düsturu ilə hesablanacaq.

Misal. $p=97$, $a=5$ olsun. Tutaq ki, birinci istifadəçi $x=36$, ikinci istifadəçi isə $y=58$ seçir. Birinci istifadəçi ikinciyə $a^x \bmod p = 5^{36} \bmod 97 = 50 \bmod 97$, ikinci istifadəçi isə birinciyə $a^y \bmod p = 5^{58} \bmod 97 = 44 \bmod 97$ göndərir. Ümumi k açarı istifadəçilər tərəfindən uyğun olaraq belə hesablanır:

(1) $k=(a^y)^x \bmod p = 44^{36} \bmod 97 = 75$

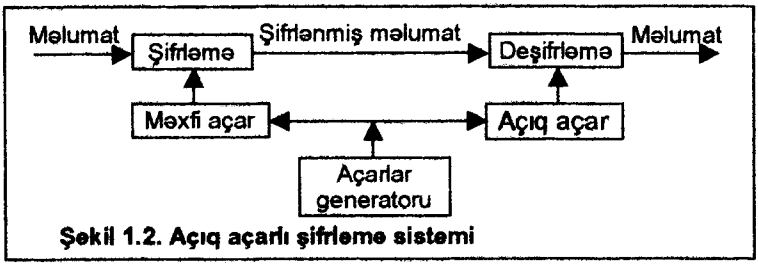
(2) $k=(a^x)^y \bmod p = 50^{58} \bmod 97 = 75$

Praktik cəhətdən davamlı kriptosistemlərin qurulması üçün iki yanaşma mövcuddur. Birinci halda kriptosistem qurulur və sonra onun sındırılmasının çətin məsələ olduğu göstərilir. İkinci halda isə müəyyən çətin məsələ seçilir və sındırılması bu məsələnin həllinə ekvivalent olan kriptosistem qurulur. İlk dəfə U.Diffi və M.Hellman [59] çətin məsələlər sinfindən kriptosistem qurmaq üçün istifadə etmişlər.

Açıq açarlı şifrləmə sistemlərində hər bir abonentin iki müxtəlif, lakin bir-birindən riyazi asılı olan açarı olur. Onlardan biri tam məxfidir və şifrləmə üçün istifadə olunur, ikincisi isə açıqdır, yəni bütün abonentlərə verilə (sahibinin ünvanı ilə birlikdə nəşr oluna) bilər və deşifrləmə üçün istifadə olunur. Açıq açara görə məxfi açarı hesablamaq qeyri-mümkündür. Açıq açarlı sistem elə qurulub ki, açıq açarla şifrlənmiş məlumat yalnız məxfi açarla açıla bilər və tərsinə. Beləliklə, açarlar bir-birinə qarşılıqlı tərsdirlər. Qeyd olunduğu kimi, sistemin hər bir abonenti özünün açarlar cütünə malikdir. Bu açarları o özü yaradır (generasiya edir), buna görə məxfi açar

həqiqətən yalnız onun özünə məxsus olur. Bu zaman o, məxfi açarı məxfi sənədlərin saxlanmasına qoyulan tələblərə uyğun olaraq saxlamalıdır. Açıq açara isə sistemin bütün istifadəçilərinin girişi var (ola bilər).

Açıq açarlı şifrləmənin iş prinsipi şəkil 1.2.-də göstərilib.



Şəkil 1.2. Açıq açarlı şifrləmə sistemi

Açıq açarlı şifrləmənin əsas çatışmayan cəhəti şifrləmə/deşifrləmə sürətinin aşağı olmasıdır. Buna görə də onlar çox vaxt simmetrik metodlarla birgə işlədilir.

1.5. Rəqəm imzası və ona qoyulan tələblər

Ümumi halda rəqəm imzası konkret məlumata (mətnə, fayla və ya istənilən uzunluqlu ixtiyari bitlər yığınına) əlavə olunan və aşağıdakıları təmin eiməyə imkan verən qeyd olunmuş (sabit) uzunluqlu informasiya blokudur [3, 32, 24, 69]:

- ilkin məlumatın autentikliyinin məlumatın mənbəyinin həqiqiliyinin yoxlanması yolu ilə təsdiqi (informasiyanın sahibinin, müəllifinin, göndərənin autentifikasiyası imkanı);
- məlumatın tamlığının təsdiqi (sanksiyasız dəyişilmələrin yoxluğu);
- məlumatın müəllifliyindən imtinanın qeyri-mümkünlüyünə zəmanət;

Məlumatın rəqəm imzası məlumatın özündən və yalnız imzalayan subyektə məlum olan məxfi açardan asılıdır. Bu zaman nəzərdə tutulur ki:

- rəqəm imzası asanlıqla yoxlanılan olmalıdır;

- imzanı yoxlamaq işini hər bir kəs məxfi açara müraciət etmədən həyata keçirə bilməlidir;
- İmzalayan şəxsin müəyyən məlumatı imzalama faktından boyun qaçırması və ya imzanı saxtalaşdırmaq cəhdi ilə bağlı mübahisəli vəziyyət yarandıqda, üçüncü tərəfin mübahisəni həll etmək imkanı olmalıdır.

Bu kontekstdə "imza" terminin işlənməsi onunla əsaslandırılır ki, rəqəm imzası kağız sənəddəki əl imzası ilə bir sıra ümumiliklərə malikdir. Əl imzası da yuxarıda sadalanan üç funksiyanı yerinə yetirir. Əl imzası ilə rəqəm imzası arasında mühüm fərqlər də mövcuddur. Bu fərqlər aşağıdakı cədvəldə əks etdirilib [3]:

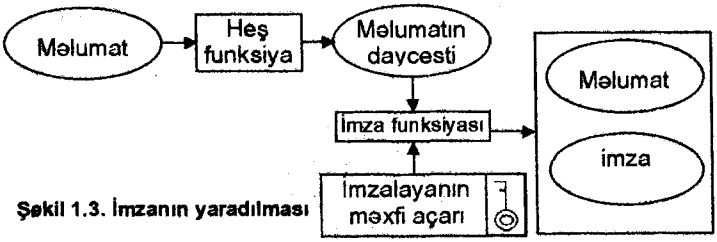
Əl imzası	Rəqəm imzası
İmzalanan mətndən asılı deyil, həmişə eynidir.	İmzalanan mətndən asılıdır, praktik olaraq həmişə müxtəlifdir.
İmzalayan şəxslə ayrılmaz əlaqədədir, onun psixofiziki xassələri ilə birqiymətli təyin olunur, itirilə bilməz.	İmzalayan şəxsə məxsus olan məxfi açarla müəyyən olunur, sahibi tərəfindən itirilə bilər.
Daşıyıcıdan (kağızdan) ayrılmazdır, buna görə də sənədin hər nüsxəsi ayrıca imzalanır.	Sənəddən asanlıqla ayrılır, buna görə də onun bütün nüsxələri üçün həqiqidir.
Realizə olunmaq üçün əlavə mexanizmlər tələb etmir.	İmzanın hesablanması və yoxlanması üçün əlavə mexanizmlər tələb edir.
Xidmət edən infrastruktur yaradılmasını tələb etmir.	Açıq açar sertifikatlarının etibar olunan infrastrukturunun yaradılmasını tələb edir.

1.6. Rəqəm imzasının iş prinsipi

Açıq açarlı şifrləmə sistemi əsasında rəqəm imzasının iş prinsipinə baxaq. Tutaq ki, hər hansı *A* abonenti müəyyən məlumatı imzalamalıdır. Bunun üçün o, aşağıdakı ardıcıllıqla hərəkət edir:

1. Heş-funksiya adlanan xüsusi riyazi funksiyanın köməyi ilə bu məlumatın heş-qiymətini (daycestini) hesablayır;
2. Məlumatın heş-qiymətini (daycestini) özünün məxfi açarı ilə şifrləyir;
3. Şifrlənmiş heş-qiymət (daycest) məlumata birləşdirilir və məlumatın rəqəm imzası olur.

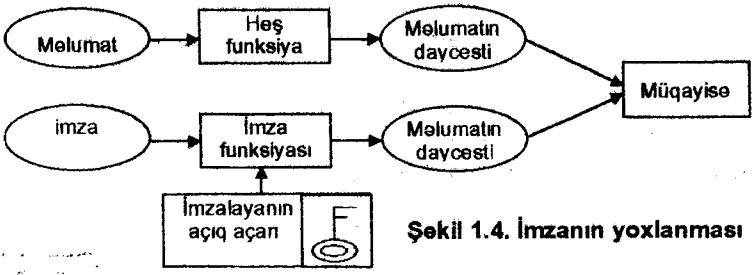
Heş-funksiyanın xassəsi elədir ki, onun köməyi ilə alınan daycest məlumatla "möhkəm" bağlıdır -məlumatın bir biti dəyişdirildikdə belə, heş-funksiyanın qiyməti dəyişir. İmzanın yaradılması sxemi şəkil 1.3.–də göstərilib.



Şəkil 1.3. İmzanın yaradılması

Bundan sonra sistemin istənilən iştirakçısı imzalanmış sənədi aldıqda *A* abonentinin imzasını aşağıdakı ardıcıllıqla yoxlaya bilər:

1. Alınmış məlumatın heş-qiymətini (daycestini) heş-funksiyanın köməyi ilə hesablayır;
2. Sonra məlumata birləşdirilmiş şifrlənmiş heş-qiyməti (daycesti) *A* abonentinin açıq açarı ilə deşifrə edir;
3. Alınmış deşifrə edilmiş heş-qiyməti özünün hesabladığı heş-qiymətlə (daycestlə) müqayisə edir;
4. Onlar üst-üstə düşürlərsə, imza həqiqi hesab olunur. Əks halda məlumat rədd olunur.



Şəkil 1.4. İmzanın yoxlanması

Məxfi açar yalnız *A* abonentinə məxsus olduğundan aydındır ki, məlumatı da yalnız o imzalaya bilərdi. İmzanın yoxlanması sxemi şəkil 1.4.–də göstərilib.

Təsvir olunan rəqəm imzası variantında sistemin istənilən istifadəçisi istənilən sənədin altındakı imzanı yoxlamaq imkanına malikdir. Rəqəm imzası sxeminin başqa variantında məlumatı yalnız ünvanlandığı abonent deşifrə edə və rəqəm imzasını yoxlaya bilər. Belə sistemlərdə məlumat seans açarı ilə simmmetrik açarlı kriptosistemin köməyi ilə şifrlənir.

1.7. Rəqəm imzası və adi imza

Asanlıqla görmək olar ki, açıq açarlı şifrləmə sisteminin əsasında rəqəm imzası adi imzanın sadalanan bütün üç funksiyasını tamamilə yerinə yetirir.

Rəqəm imzasının yerinə yetirdiyi mühafizə xidmətləri nöqteyi-nəzərindən adi imza ilə müqayisəli təhlilini verək.

Sənədin tamlığının mühafizəsi. Adi imza (imza və möhür) halında sənəd imzalandıqdan sonra dəyişdirilə bilər (məsələn, bir neçə sıfır artırıla bilər). Rəqəm imzası ilə imzalanmış elektron sənədi isə dəyişdirmək mümkün deyil, çünki sənədin məzmunu sənədin daycesti vasitəsi ilə imzanın özünə "daxil edilir".

İmzanın saxtalaşdırılması. Adi imzanı saxtalaşdırmaq üçün tələb olunan avadanlıq və onun qiyməti çoxları üçün əlçatandır. Hesablama texnikasının və üsullarının indiki inkişaf səviyyəsi üçün mütəxəsislərin tövsiyə etdiyi açarların uzunluğunu gözləmək halında rəqəm imzasını saxtalaşdırmaq üçün bir neçə yüz milyon dollarlıq xüsusi super kompüter və 300-500 il vaxt tələb olunur. Açarların uzunluğu iki dəfə artırılsa, avadanlığın qiyməti və imzanın axtarılması vaxtı kəskin artar.

Konfidensiallıq. Adi imza ilə imzalanmış sənəd, əlinə düşdüyü istənilən şəxs tərəfindən oxuna bilər. Rəqəm imzası

halında, yalnız sənədin ünvanlandığı şəxs tərəfindən oxunması rejimi nəzərdə tutula bilər.

Rəqəm imzasının yerinə yetirdiyi əsas funksiya-autentifikasiya (həqiqiliyin təsdiqi) funksiyası nöqteyi nəzərindən elektron imzanın digər növləri ilə müqayisəsi də maraqlıdır.

Subyekt öz həqiqiliyini aşağıdakı mahiyyətlərdən ən azı birini təqdim etməklə təsdiq edə bilər:

- bildiyi nəyi isə (parol, şəxsi identifikator, kriptoqrafik açar və s.);
- sahib olduğu nəyi isə (fərdi kart və ya analoji təyinatlı başqa qurğu);
- onun özünün hissəsi olan nəyi isə (səs, barmaqların izi və ya başqa biometrik xarakteristikalar);

Paylanmış sistemlərdə proseslər və verilənlər autentifikasiya olunuqda, kriptoqrafik metodlar ön plana çıxır, əslində onlara alternativ yoxdur.

Autentifikasiya üçün biometrik metodlar da tətbiq olunurlar. Biometrik metodlar obyektin müəyyən unikal bioloji parametrlərinin obyektin həqiqiliyini müəyyən etmək məqsədi ilə ölçülməsinə əsaslanıb. Hazırda məlum olan biometrik metodların etibarlılığı 99%-dir, halların 1 faizində imtina mümkündür. Biometrik qurğunun praktik etibarlılığı qanuni istifadəçiyə icazə verməkdən imtinaların (səhv imtina) və qeyri-qanuni istifadəçilərə girişin verilməsi (səhv giriş) sayına görə qiymətləndirilir.

Biometrik metodlardan əl imzasının tanınması metoduna ötəri nəzər salaq. Faksimil imzanın tanınmasının sadə üsulu etibarlı nəticə almağa imkan vermir. İmzanın cari variantının etalonla müqayisəsi yaramır, çünki tanınmada dəyişkənliyin (variabelliyin) nəzərə alınması zərurəti imzanın saxtalaşdırılması üçün əl yeri qoyur. Məsələnin həlli üçün cari imzanın koordinatlarının izlənməsi ilə yanaşı təzyiq, imzalama vaxtı və sürəti kimi dinamik xarakteristikaların daha mürəkkəb analizi metodu tətbiq olunur. Lakin dinamik xarakteristikaların analizi də tam zəmanət vermir. Girişə icazədən səhv imtina

mümkündür, bundan başqa imzanın sanksiyasız təkrar yaradılması və saxtalaşdırılması ehtimalı da istisna edilmir.

Sandia kompaniyasının laboratoriyası bir sıra kommersiya biometrik autentifikasiya qurğularının səmərəliliyinin tədqiqatını aparmışdır. Müxtəlif tanınma metodlarının etibarlılığı haqqında verilənlər aşağıdakı cədvəldə əks olunub [39]:

Texnika	**Səhvlərin faizi**
Səsin tanınması (Alpha metodu)	3%
Səsin tanınması (ECCO metodu)	2%
Əl imzasının dinamikası	2%
Gözün tor qişasının skanerdən keçirilməsi	0,4%
Əlin həndəsəsi	0,1%
Barmaqların izi	9% səhv imtina, səhv icazə yoxdur

Göründüyü kimi biometrik metodlar kifayət qədər yüksək səhv faizinə malikdirlər və dəqiq autentifikasiyaya zəmanət vermirlər. Rəqəm imzası da bir sıra nöqsanlara malikdir. Onlardan biri qiymətdir.

Rəqəm imzası mürəkkəb və bahadır, çox zaman ötürmə sürətinin aşağı düşməsinə səbəb olur. Elektron imzanın digər növləri ilə müqayisədə, fəaliyyət üçün zəruri infrastrukturun dəyəri xüsusi ilə yüksəkdir.

Aydındır ki, rəqəm imzasının ən böyük üstünlüyü sənədin təhlükəsizliyini və göndərənin identifikasiyası imkanını təmin etməsidir. Tərəflər sənədin göndərilməsindən alınmasınadək keçən vaxt ərzində sənədin tamlığının pozulmadığına əmin ola bilərlər.

2. Rəqəm imzası sxemləri

2.1. Rəqəm İmzası sxemləri və onların qurulması

Rəqəm imzası sxemləri. Rəqəm imzası sxemi aşağıdakılardan ibarətdir [3]:

- təhlükəsizlik parametri; bu parametr kimi imzanın uzunluğu, imzalanan məlumatların uzunluğu və s. götürülə bilər;
- ilkin məlumatlar fəzası;
- məxfi informasiyanı dəyişdirmədən baxılan sxemdə alına bilən imzaların maksimal sayı;
- açarların generasiyası alqoritmi;
- imzanı yaratma alqoritmi;
- imzanı yoxlama alqoritmi.

Göründüyü kimi, rəqəm imzası sxemini realizə etmək üçün iki alqoritm zəruridir:

1. Rəqəm imzasının yaradılması alqoritmi;
2. Rəqəm imzasının yoxlanması alqoritmi.

Bu alqoritmlərə qoyulan başlıca tələblər məxfi açardan istifadə etmədən imzanı yaratmaq imkanının istisna olunması və hər hansı gizli informasiyanı bilmədən imzanı yoxlamaq imkanına zəmanət verilməsidir.

Rəqəm imzası sxeminin etibarlığı aşağıdakı üç məsələnin çətinliyi ilə müəyyən olunur:

- imzanın saxtalaşdırılması, yəni verilmiş sənədin altındakı imzanın qiymətinin məxfi açarın sahibi olmayan şəxs tərəfindən tapılması;
- imza məlumatının yaradılması, yəni imzanın verilmiş qiymətinə bərabər imzaya malik heç olmasa bir məlumatın tapılması;
- məlumatın dəyişdirilməsi, yəni eyni imza qiymətinə malik iki müxtəlif məlumatın seçilməsi;

İmza sxemlərinin qurulması. Rəqəm imzası sxemlərinin qurulmasının müasir prinsipləri aşağıdakılardır:

- sistemin bütün istifadəçilərinin rəqəm imzasının hesablanması və yoxlanması eynidir və tam məlumdur, geniş məlum olan riyazi məsələlərə əsaslanır;
- rəqəm imzasını yoxlama açarlarının məxfi imzalama açarlarından hesablanması üsulları hamı üçün eynidir və yaxşı məlumdur, onların etibarlılığı da geniş məlum olan riyazi məsələlərə əsaslanır;
- imzalama üçün məxfi açarlar istifadəçinin özü tərəfindən təsadüfi olaraq bütün mümkün açarlar çoxluğundan seçilir;
- konkret rəqəm imzası alqoritminin davamlılığı hər hansı "məxfi" informasiya cəlb etmədən, yalnız məlum riyazi nəticələrin və potensial bədniyyətlinin hesablama gücləri haqqında sağlam fərziyyələrin əsasında qiymətləndirilə bilər.

Hal-hazırda rəqəm imzası sxemlərinin yaradılması üçün bir neçə prinsipial yanaşma təklif olunub. Onları üç qrupa bölmək olar:

- açıq açarlı şifrləmə sistemləri əsasında olan sxemlər;
- xüsusi hazırlanmış imzanı yaratma və yoxlama alqoritmlərinin əsasında olan sxemlər;
- simmetrik şifrləmə sistemləri əsasında olan sxemlər;

Rəqəm imzası sxemi yaratmaq üçün simmetrik şifrləmə sistemlərindən istifadə etmək olar [6, 26]. Bu halda məxfi açarla şifrlənmiş məlumatın özü imza rolunda çıxış edə bilər. Belə imzaların əsas çatışmayan cəhəti onların birdəfəlik olmasıdır, çünki hər bir yoxlamadan sonra məxfi açar məlum olur. Simmetrik şifrləmə sistemlərinin istifadəsi çərçivəsində bu vəziyyətdən yeganə çıxış yolu hər iki tərəfin inandığı vasitəçi funksiyasını yerinə yetirən inanılmış üçüncü tərəfin daxil edilməsidir. Bu halda bütün informasiya vasitəçidən keçməklə ötürülür, vasitəçi məlumatların bir abonentin açarından digərinin açarına yenidən şifrlənməsini həyata keçirir. Təbii olaraq, bu sxem olduqca əlverişsizdir.

Rəqəm imzası sxemi qurmaq üçün açıq açarlı şifrləmə sistemlərindən istifadə etmək ideyası məsələnin qoyuluşunun təməlindədir. Doğrudan da, tutaq ki, elə *(E, D)* çevirmələr cütü

var ki, birincisi açıq açardan, digəri isə məxfi açardan asılıdır. Məlumatın rəqəm imzası *S*-i hesablamaq üçün məxfi açarın sahibi *M* məlumatına ikinci çevirməni- *D* çevirməsini tətbiq edir: *S=D(M)*. Bu halda imzanı yalnız məxfi açarın sahibi hesablaya bilər, imzanın doğruluğunu- *E(S)=M* bərabərliyini isə istənilən şəxs yoxlaya bilər. *E* və *D* çevirmələrinə əsas tələblər bunlardır:

- bütün *M* məlumatları üçün *M=E(D(M))* bərabərliyinin ödənilməsi;
- verilmiş *M* məlumatı üçün məxfi açarı bilmədən *D(M)* qiymətini hesablamağın qeyri-mümkünlüyü.

Rəqəm imzasının hesablanması üçün təklif olunmuş bu üsulun fərqləndirici cəhəti imzalanan məlumatın özünün ötürülməsinin vacib olmamasıdır, çünki onu imzanın qiymətinə əsasən bərpa etmək mümkündür. Bununla əlaqədar olaraq, belə sistemləri mətni bərpa edən rəqəm imzası sistemləri adlandırırlar.

Aydındır ki, *(E, D)* çevirmələr cütü əsasında baxılan rəqəm imzası sxemi saxtalaşdırmanın qeyri-mümkünlüyü tələbini ödəyir, eyni zamanda imzalanmış məlumatın yaradılmasının qeyri-mümkünlüyü tələbini isə ödəmir.

Açıq açarlı şifrləmə sistemlərinin əsasında rəqəm imzası sxemlərinin qurulması üçün digər yanaşma açarsız heş-funksiyalardan istifadə etməkdir. Verilmiş *M* məlumatı üçün əvvəlcə heş-funksiyanın qiyməti *h(M)*, sonra isə imzanın qiyməti *S=D(h(M))* hesablanır. Aydındır ki, bu halda imzanın qiymətinə görə məlumatı bərpa etmək mümkün deyil. Buna görə məlumat ilə birgə imzanı da göndərmək lazımdır. Belə imzalar əlavəli rəqəm imzası adlandırılırlar [3, 71]. Qeyd edək ki, açarsız heş-funksiyaların istifadəsi ilə qurulan imza sistemləri rəqəm imzası üçün qoyulan bütün tələbləri ödəyir.

Praktikada daha geniş yayılmasını nəzərə alaraq biz əsasən açıq açarlı şifrləmə sistemləri əsasında olan sxemləri nəzərdən keçirəcəyik.

2.2. Rəqəm imzasının riyazi əsasları

Rəqəm imzasını realizə edən alqoritmlərdə istifadə olunan riyazi sxemlər biristiqamətli funksiyalara (one-way function) əsaslanır.

$F:X\to Y$ funksiyası istənilən $x\in X$ elementi üçün $f(x)$ asanlıqla hesablana bilirsə və bütün $y\in Y$ üçün $f(x)=y$ şərtini ödəyən x arqumentinin hesablanması polinomial həll olunmazdırsa, biristiqamətli adlanır.

Nəzəri olaraq, məlum $f(x)$ qiymətinə görə, növbə ilə x-in bütün mümkün qiymətlərini uyğun $f(x)$ qiyməti alınana qədər yoxlamaqla x-i həmişə tapmaq mümkündür. Lakin X çoxluğunun ölçüləri böyük olduqda belə yanaşma praktik olaraq həyata keçirilməzdir. Bu vaxta kimi biristiqamətli adına namizəd heç bir funksiya üçün onun həqiqətən də biristiqamətli olduğu isbat edilməyib.

Biristiqamətli funksiyalara ən sadə namizəd tam ədədlərin vurulmasıdır. Məlumdur ki, hətta çoxrəqəmli ədədlərin vurulması belə nisbətən asandır, ancaq hətta ən güclü kompüter də ixtiyarında olan ən yaxşı alqoritmlə təxminən yazılışlarının ölçüsü bərabər olan iki sadə ədədin hasilinə bərabər iki yüz rəqəmli onluq ədədi qəbul edilən vaxt ərzində vuruqlarına ayırmağa qadir deyil.

Biristiqamətli funksiya kimi Diffi və Hellman diskret qüvvətə yüksəltmə funksiyasını təklif etmişlər:

$$f(x)=a^x(\mathrm{mod}\ p)$$

burada x-tam ədəd, $1\le x\le p-1$, p k-bitlik sadə ədəddir. Həm də elə $a<p$ ədədi seçilir ki, onun qüvvətləri $\{1, 2, \ldots, p-1\}$ ədədlərinin hər hansı yerdəyişməsi olan p moduluna görə $\{a^1, a^2, \ldots, a^{p-1}\}$ ədədlərinin nizamlı düzülüşünü versin (belə a ədədi p moduluna görə ibtidai kök adlanır).

Hətta çox böyük p modulu üçün (məsələn, k=1024 olduqda) verilmiş x üçün bu funksiyanın qiymətini hesablamaq çox asandır. Buna inanmaq üçün a^{25} qüvvətinin hesablanmasına baxaq: $a^{25}=(((a^2\cdot a)^2)^2)^2\cdot a$. Bu bərabərlik göstərir ki, a^{25} qüvvətini cəmisi dörd kvadrata yüksəltmə və iki

vurma əməlinin köməyi ilə hesablamaq mümkündür. Qüvvət üstü x ədədinin uzunluğu L bit olarsa, L-dən $2L$-ə qədər sayda vurma və kvadrata yüksəltmə əməli tələb olunur.

Modula görə qüvvətə yüksəltməyə tərs məsələ diskret loqarifmləmə məsələsi adlanır: $a^x \equiv b \bmod n$ tənliyindən x-i tapmaq tələb olunur. Məsələn, $3^x \equiv 15 \pmod{17}$ tənliyindən $x=6$ tapmaq olar. Diskret loqarifmləmə məsələsinin həlli olmaya da bilər. Məsələn, $3^x \equiv 7 \pmod{13}$ tənliyinin həlli yoxdur. Diskret loqarifmləmə məsələsini böyük ədədlər üçün həll etmək olduqca çətindir.

Biristiqamətli funksiya şifrləmə funksiyası qismində istifadə oluna bilməz, çünki $f(x)$– etibarlı şifrlənmiş x məlumatı olsa da, heç kim, hətta qanuni istifadəçi də x-i bərpa edə bilməz. Bu problemi həll etmək üçün Diffi və Hellman məxfi girişli biristiqamətli funksiyalardan (one-way trapdoor function) istifadə etmək ideyasını irəli sürmüşlər [59].

k parametrindən asılı olan $f_k: X \to Y$ funksiyası aşağıdakı üç şərti ödədikdə məxfi girişli biristiqamətli funksiya adlanır:

1) *təyin* oblastından olan istənilən $x \in X$ üçün $y=f_k(x)$, $y \in Y$ qiymətini hesablamaq asandır;

2) k məlum olduqda ixtiyari $y \in Y$ üçün $x = f_k^{-1}(y)$, $x \in X$ qiymətini hesablamaq asandır;

3) bütün k–lar və bütün y–lər üçün k parametrini bilmədən $f_k^{-1}(y)$-i tapmaq hesablama cəhətdən mümkün deyil.

Məsələn, $E_k: X \to Y$ funksiyası $D_k: Y \to X$ tərs funksiyasına malikdirsə, ancaq tərs funksiyanı k sirrini bilmədən təkcə E_k-ya görə tapmaq mümkün deyilsə, məxfi girişli biristiqamətli funksiyadır.

Ən geniş yayılmış açıq açarlı kripitosistemlərdə əsasən aşağıdakı iki məxfi girişli biristiqamətli funksiyadan istifadə olunur:

– tam ədədlərin vuruqlara ayrılması məsələsi;

– diskret loqarifləmə məsələsi.

Diskret loqarifləmə məsələsinə bu qruplarda baxılır:

- sadə və ya genişlənmiş sonlu meydanın multiplikativ qrupu;
- sonlu meydan üzərində elliptik əyrilərin qrupları;
- sonlu meydan üzərində hiperelliptik əyrilərin yakobianı;
- sadə sonlu meydanda Lukas funksiyalarına əsaslanan qruplar;
- xəyali kvadratik meydanın siniflər qrupu.

2.3. RSA alqoritmi

Açıq açarlı şifrləmə sistemlərinə ilk konkret misal RSA adlanan sistemdir. Alqoritmin adı müəlliflərinin familiyalarının ilk hərflərindən ibarətdir. R. Rivest, A. Shamir, L.Adleman bu alqoritmi Massaçuset Texnologiya İnstitunda birgə işləri zamanı 1977-ci ildə təklif etmişlər [86].

RSA alqoritmi aşağıdakı kimi işləyir:

1. İki kifayət qədər böyük (100-200 və daha çox onluq rəqəmli) sadə p və q ədədləri seçilir;
2. Onların $n=pq$ hasili, həmçinin $\varphi(n)=(p-1)(q-1)$ (Eyler funksiyası) hesablanır;
3. $1<e<\varphi(n)$ şərtini ödəyən və $\varphi(n)$-lə qarşılıqlı sadə olan e ədədi seçilir;
4. $ed=1 \bmod \varphi(n)$ şərtini ödəyən d ədədi hesablanır;
5. (e, n) cütü məxfi açar, (d, n) cütü açıq açardır;
6. M məlumatının imzalanması proseduru- M ədədi n modulu üzrə e qüvvətinə yüksəldilir: $S=M^e \bmod n$.
7. M məlumatına uyğun S imzasının yoxlanması proseduru- S ədədi n modulu üzrə d qüvvətinə yüksəldilir: $M'=S^d \bmod n$. Əgər M'=M olarsa, M məlumatının d açıq açarını əvvəllər təqdim etmiş istifadəçi tərəfindən imzalandığı qəbul edilir.

p və q ədədlərini məhv etmək və ya məxfi açarla birlikdə saxlamaq lazımdır. n ədədinə modul, e ədədinə şifrləmə eksponenti, d-yə deşifrləmə eksponenti də deyirlər. (e, n) cütünü açıq açar, (d, n) cütünü məxfi açar kimi götürmək olardı.

(e,n) məxfi açarı ilə verilənləri şifrləmək üçün aşağıdakıları etmək lazımdır:

- Şifrlənən mətni bloklara bölmək, *i*-ci blok $m(i)=0,1,2,\ldots,n-1$ ədədi şəklində təsvir oluna bilər. Blokların sayı n-1 -dən çox olmamalıdır.
- $m(i)$ ədədlərinin ardıcıllığı şəklində təsvir olunan mətni $c(i)=(m(i)^e) \bmod n$ düsturu üzrə şifrləmək.

(d,n) açıq açarından istifadə edərək bu verilənləri deşifrləmək üçün, $m(i) = (c(i)^d) \bmod n$ hesablamaq zəruridir. Nəticədə ilkin mətnin hissələri olan $m(i)$ ədədləri çoxluğu alınacaq.

Nümunə üçün ABC məlumatını şifrləyək və deşifrləyək. Bunun üçün ABC məlumatını 123 ədədlər ardıcıllığı kimi təsvir edək (A-1, B-2, C-3).

1) $p=5$ və $q=11$ seçək (həqiqətdə ədədlər çox böyük olmalıdırlar).
2) $n=5*11=55$, $(p-1)*(q-1)=40$ hesablayırıq. e-ni, məsələn, 7-yə bərabər seçmək olar.
3) $(d*7) \bmod 40=1$ şərtindən d-ni tapırıq. Məsələn, $d=3$.

İndi {3,55} açıq açarından istifadə edərək məlumatı şifrləyək:

4) $C_1 = (1^3) \bmod 55 = 1$
5) $C_2 = (2^3) \bmod 55 = 8$
6) $C_3 = (3^3) \bmod 55 = 27$

İndi isə {7,55} məxfi açarından istifadə edərək məlumatı deşifrləyək:

7) $M_1 = (1^7) \bmod 55 = 1$
8) $M_2 = (8^7) \bmod 55 = 2097152 \bmod 55 = 2$
9) $M_3 = (27^7) \bmod 55 = 10460353203 \bmod 55 = 3$

RSA müəllifləri öz sistemlərinin işləmə prinsplərini izah edərkən ilkin mətn kimi

ITS ALL GREEC TO ME

frazasını seçmişlər. Bu mətni bir böyük ədədə çevirmək üçün sözlər arasındakı probeli-0, *A* hərfini-1, *B* hərfini-2, *C* hərfini-3, ..., *Z* hərfini isə 26 ilə kodlaşdırmış və hər simvolun təsviri üçün beş ikilik mərtəbə ayırmışlar. Nəticədə yuxarıdakı frazaya

M= 092019000112120007180505110020150013O5 ədədi uyğun olmuşdur.

Şifrləmə üçün müəlliflər e=9007 və n=1143816257578888676692357799614661201021896721242362562651842935706935245733897830597123563958705058989075147599290026879543541 seçmişlər.

Şifrləmədən sonra $c=M^e(\mathrm{mod}n)$=1993513149780510045231712274026064742320401705839146310370371740625971608948927504399096267258267501289355446135382376974802 6 ədədi alınmışdır. n ədədi təsadüfi şəkildə seçilmiş 64- və 65-rəqəmli sadə p və q ədədlərinin hasilidir.

RSA kriptosistemi ən müxtəlif proqram məhsullarında, müxtəlif platformalarda və müxtəlif sahələrdə istifadə olunur. Ondan Microsoft, Apple, Sun və Novel kimi məşhur firmalar öz əməliyyat sistemlərində də istifadə edirlər. Aparat ifasında RSA alqoritmi mühafizəli telefonlarda, Ethernet şəbəkə kartlarında, smart kartlarda tətbiq olunur, Zaxus (Racal) kriptoqrafik avadanlığında geniş istifadə olunur. Bundan başqa alqoritm Internetin bütün mühafizəli kommunikasiya protokollarının, o cümlədən S/MİME, SSL və S/WAN protokollarının tərkibinə daxildir. RSA kriptosistemi bir çox dünya standartlarının məsələn, SWIFT, ANSI X9.31 rDSA və amerikan bankları üçün X9.44 standartı layihəsinin, IEEE P1363 [68] və WAP WTLS [90] tövsiyələrinin tərkib hissəsidir.

2.3.1. RSA alqoritminin riyazi əsasları

RSA alqoritminin əsasında duran bəzi riyazi faktlara nəzər salaq.

a və b tam ədədləri n natural ədədinə bölündükdə alınan qalıqlar bərabərdirsə, a və b tam ədədləri n moduluna görə müqayisə olunan adlanırlar və bu simvolik olaraq belə yazılır:

$$a \equiv b(\mathrm{mod}\ n)$$

Buradan alınır ki, $a - b$ fərqi n ədədinə bölünür. Qalığı işarə etmək üçün çox vaxt mötərizəsiz yazılışdan istifadə edirlər:

$$b = a \bmod n.$$

Fermanın kiçik teoreminə görə p sadə ədəd, a isə tam ədəddirsə, onda $a^p \equiv a \pmod p$. Xüsusi halda $(a, p)=1$ olarsa, $a^{p-1} \equiv 1 \pmod p$ olar.

n natural ədədindən kiçik və onunla qarşılıqlı sadə olan müsbət tam ədədlərin sayına bərabər olan $\varphi(n)$ funksiyası Eyler funksiyası adlanır.

Eyler funksiyası üçün aşağıdakı münasibətlər doğrudur:

$\varphi(1)=1$

$\varphi(p^k)= p^{k-1}(p-1)$

$\varphi(ab)= \varphi(a)\varphi(b)$

burada p sadə ədəd, r, a, b- natural ədədlərdir və ƏBOB(a,b)=1. Qeyd edək ki, ƏBOB(a,b) əvəzinə (a,b) yazılışından da istifadə olunur. Bu xassələr n-in sadə vuruqlara ayrılışı məlum olduqda, $\varphi(n)$-i asanlıqla hesablamağa imkan verir. Məsələn, $\varphi(5)=5-1=4$; $\varphi(9)= \varphi(3^2)=3^{2-1}(3-1)=6$; $\varphi(45)=\varphi(5)\varphi(9)=24$.

Fermanın kiçik teoreminin mürəkkəb modullar üçün ümumiləşdirilməsi olan Eyler teoreminə görə, natural n ədədi ilə qarşılıqlı sadə olan ixtiyari a tam ədədi üçün $a^{\varphi(n)} \equiv 1 \pmod n$ doğrudur.

Əgər natural e ədədi $(e, \varphi(n))=1$ şərtini ödəyirsə, onda yeganə $d<\varphi(n)$ ədədi var ki, onun üçün

$$ed \equiv 1 \bmod \varphi(n)$$

müqayisəsi doğrudur.

Tutaq ki, $n=pq$, burada p və q -iki müxtəlif sadə ədəddir. Qeyd edək ki, bu halda $\varphi(n)= \varphi(pq)=(p-1)(q-1)$ olur.

d ədədinin tapıldığı bərabərliyə əsasən $ed = k\varphi(n)+1$ olar. Fermanın kiçik teoreminə görə istənilən tam M üçün $M^p \equiv M \pmod p$. Bu iki bərabərlikdən alınır:

$$S^d=(M^e)^d=M^{ed}=M^{k\varphi(n)+1}=M^{k(p-1)(q-1)+1}=M^{k\,p(q-1)}M^{-k\,q+k+1}=$$
$$=(M^p)^{k\,(q-1)}M^{k\,q+k+1} \equiv M^{k\,(q-1)}M^{k\,q+k+1} \equiv M \pmod p.$$

Analoji olaraq, göstərmək olar ki, $S^d \equiv M \bmod q$. p və q müxtəlif sadə ədədlər olduğundan, müqayisələrin məlum xassələri əsasında $S^d \equiv M \bmod pq = M \bmod n$.

2.3.2. RSA parametrlərinin seçilməsi

Məlumdur ki, RSA və asimmetrik alqoritmlərin davamlılığı bu növ alqoritmlərin əsasında dayanan biristiqamətli funksiyaların tərsinin tapılmasının çətinliyindən asılıdır. RSA halında $F(x)=x^y \bmod n$ biristiqamətli funksiyasının tərsinin tapılmasının çətinliyi n modulunun vuruqlara ayrılmasının çətinliyindən asılıdır. Bu yalnız fərziyyədir, çünki bu problemlərin ekvivalentliyinin isbatı hələlik məlum deyil. Əgər ədədin sadə vuruqlara ayrılmasının effektiv metodları mövcud olsaydı n ədədini p və q vuruqlarına ayırıb məxfi e açarını tapmaq olardı. Beləliklə, RSA alqoritminin etibarlılığı çətin həll olunan- praktik olaraq həll olunmayan məsələyə- ədədin vuruqlara ayrılması məsələsinə əsaslanıb. Bununla əlaqədar olaraq p və q ədədlərini elə seçmək lazımdır ki, n ədədinin vuruqlara ayrılması hesablama cəhətdən kifayət qədər çətin olsun.

Qeyd etmək lazımdır ki, məlum hücumlardan savayı RSA alqoritminin davamlılığı alqoritmin parametrlərinin səhv seçilməsi hesabına da aşağı düşə bilər. RSA alqoritminin məlum zəifliklərindən aşağıdakıları qeyd etmək olar:

1. p və q-nün qiymətlərinin səhv seçilməsi. p və q ədədləri sadə olmalıdırlar və məşhur sadə ədədlər cədvəllərinin heç birində təsadüf olunmamalıdırlar. Həmin ədədlər bir-birinə çox yaxın olmamalıdırlar. Əgər $(p-q)/2$ kiçikdirsə və $(p+q)/2$ ədədi $\sqrt{n}$-dən az fərqlənirsə, onda $(p+q)^2/4<n(p-q)^2/4$ olduqda bərabərliyin sol tərəfi tam kvadrat olar. n-nin faktorizasiyası zamanı $x>\sqrt{n}$ şərtini ödəyən bütün tam ədədləri $x^2-n=y^2$ bərabərliyini ödəyən qiymət tapılanadək sınayırıq. Onda $p=x+y$ və $q=x-y$ olacaq. Şərh olunmuş bu faktı, həmçinin p və q-nün səhv seçilməsinə əsaslanmış bir sıra digər hücumları nəzərə alaraq, p və q-nün seçilməsininin aşağıdakı şərtlərini formulə etmək olar:

1. Verilən ədədlər eyni uzunluqlu böyük sadə ədədlər olmalıdırlar, məsələn, əgər *n*-in uzunluğu 1024 bitdirsə, *p* və *q*-nün uzunluğu 512 bitə bərabər olmalıdır.
2. p və q bir-birindən olduqca çox fərqlənməməli və eyni zamanda bir-birinə çox da yaxın olmamalıdırlar;
3. p və q ədədləri elə olmalıdır ki, p-1 və q-1 ədədlərinin ƏBOB-i kiçik olsun; yaxşı olar ki, ƏBOB(p-1, q-1) = 2 olsun.
4. *p* və *q* ədədləri ciddi sadə ədəd olmalıdırlar. Əgər aşağıdakı şərtlər ödənirsə ədəd ciddi sadə ədəd adlanır:
   a. p-1 böyük sadə bölənə malik olmalıdır (onu *r* ilə işarə edək);
   b. p+1 böyük sadə bölənə malik olmalıdır;
   c. r-1 böyük sadə bölənə malik olmalıdır.

(a.) tələbi Pollard tərəfindən təklif olunmuş faktorizasiya alqoritminə [82] davam gətirmək zərurətindən irəli gəlir. *(b.)* tələbi də anoloji olaraq əsaslandırılır. Praktikada *(c.)* tələbinin ödənilməsi dövri hücumlara qarşı durmağa imkan verir.

Göstərilən şərtlərdən heç olmasa biri ödənilməsə, *n*-i sadə vuruqlarına ayırmaq üçün effektiv alqoritmlər var.

p, q və $\varphi(n)$ kəmiyyətindən birini bilərək, məxfi RSA açarını asanlıqla tapmaq olar. Həmçinin məlumdur ki, məxfi *d* deşifrləmə eksponentini bilərək, *n* modulunu ehtimali alqoritm vasitəsi ilə asanlıqla vuruqlara ayırmaq olar. Buradan alınır ki, şifrləmə üçün RSA sistemindən istifadə olunan şəbəkənin hər bir istifadəçisi özünün unikal moduluna malik olmalıdır. Doğrudan da, əgər şəbəkədə hamı üçün vahid *n* modulu istifadə olunursa, istənilən (e_i,d_i) cütünü bilərək *n*–i vuruqlara ayırmaq olar. Buna görə belə şəbəkədə istənilən istifadəçi istənilən digər istifadəçinin məxfi açarını tapa bilər. Bunu hətta *n* ədədini vuruqlara ayırmadan belə etmək olar [3].

2. Kiçik e eksponenti. Şifrləmə sürətini artırmaq məqsədi ilə praktikada kiçik şifrləmə eksponentindən istifadə olunur. *e* eksponentinin kiçik seçilməsi neqativ nəticələrə gətirib çıxara bilər. Məsələ ondadır ki, bu halda bir neçə istifadəçidə eyni *e* eksponenti ola bilər. Bu zaman həmin istifadəçilərə

göndərilmiş şifrlənmiş eyni məlumata (məsələn, sirkulyar məktub) görə həmin məlumatı deşifrləmək mümkündür.

3. Kiçik d eksponenti. Qeyd edək ki, kiçik deşifrləmə eksponenti seçmək də arzuolunmazdır, çünki *d*–ni sadə saf-çürük etmə ilə müəyyən etmək olar. Həmçinin, $d < \sqrt[4]{n}$ olduqda *d* eksponentini kəsilməz kəsrlərin köməyi ilə asanlıqla tapmaq olar.

Qeyd etmək lazımdır ki, hesablama texnikasının və ədədin vuruqlara ayrılması üsullarının inkişafı ilə əlaqədar olaraq vaxtaşırı açarın uzunluğuna verilən tələblər korrektə olunur. Hazırda RSA alqoritminin müəllifləri açarın uzunluğunu xüsusi şəxslər üçün 768 bit, kommersiya informasiyası üçün 1024 bit və xüsusi məxfi informasiya üçün 2048 bit məsləhət görürlər.

2.3.3. RSA alqoritminə hücumlar

1.RSA-nın açarsız oxunması metodu

Düşmənə açıq açar *(e,n)* və şifrmətn *C* məlumdur. İlkin mətn *M*-i tapmaq lazımdır.

Düşmən $C^{e^j} (\text{mod } n)=C$ bərabərliyini ödəyən *j* ədədini seçir, yəni düşmən elə keçirilmiş şifrmətnin açıq açarı ilə *j* dəfə şifrləməni yerinə yetirir: $(C^e)^e)^e...)^e (\text{mod } n)= C^{e^j} (\text{mod } n))$. Belə *j* taparaq, düşmən $C^{e^{j-1}} (\text{mod } n)$ hesablayır, yəni *j-1* dəfə şifrləmə əməliyyatını təkrarlayır –bu qiymət məhz *M* açıq mətnidir! Bu $C^{e^j} (\text{mod } n)=(C^{e^{j-1}} (\text{mod } n))^e=C$ bərabərliyindən alınır.

Misal. p =983, q =563, e = 49, M =123456.
$C=M^{49} (\text{mod } n) =1603$, $C^{497} (\text{mod } n) = 85978$, $C^{498} (\text{mod } n) =123456$, $C^{499} (\text{mod } n) =1603$.

2. Notariuslu sxemdə RSA imzasına hücum

Fərz edək ki, gəlib keçən sənədləri imzalayan elektron notarius var. *N* –notariusun imzalamaq istəmədiyi hər hansı açıq mətndir. Düşmənə notariusun açıq açarı *(e,n)* məlumdur. Düşmən notariusa bu *N* mətnini imzalatmaq istəyir.

Düşmən *N* ilə qarşılıqlı tərs olan hər hansı *x* təsadüfi ədədini generasiya edir və $y=x^e (\text{mod } n)$ hesablayır. Sonra

$M=yN$ qiymətini alır və onu imzalatmaq üçün notariusa verir. Notarius $M^d(\text{mod } n)=S$ imzalayır (çünki bu artıq N mətni deyil!). $S=M^d(\text{mod } n)=y^dN^d=(x^e)^dN^d=xN^d$ olduğundan S-i x-a bölməklə N^d-ni tapırıq: $N^d=Sx^{-1}(\text{mod } n)$.

Mühafizə üçün imzalama zamanı məlumata müəyyən təsadüfi ədəd (məsələn, zaman) əlavə etmək olar.

3. Seçilmiş şifrmətnə görə RSA imzasına hücum

C şifrmətni var. Düşmənə məlumatı göndərənin açıq açarı (e,n) məlumdur. İlkin M mətnini tapmaq lazımdır.

Düşmən hər hansı r: $r<n$, $(r,n)=1$ generasiya edir və $x=r^e(\text{mod } n)$ hesablayır. Sonra o $t=r^{-1}(\text{mod } n)$ və $y=xC(\text{mod } n)$ hesablayır və imzalamaq üçün göndərən şəxsə göndərir.

Göndərən, heç nədən şübhələnməyərək, y mətnini imzalayır: $w=y^d(\text{mod } n)$ və w-ni geriyə göndərir.

$$r=x^d\text{mod}n)=x^{-d}x^dC^d(\text{mod}n)=C^d=M$$

olduğu üçün düşmən $tw(\text{mod } n)=r^{-1}y^d(\text{mod}n)$ hesablayır.

Hücum bir qədər hipotetik xarakter daşıyır, buna baxmayaraq bir neçə vacib nəticə çıxarmağa imkan verir:

a) imzalamanı və şifrləməni müxtəlif açarlarla aparmaq lazımdır;
b) imza zamanı təsadüfi vektor əlavə etmək və ya heş-funksiyadan istifadə etmək lazımdır.

Bunlardan başqa, RSA-nın smart-kartlarda realizəsinə də tətbiq oluna bilən iki növ ekzotik hücumdan mühafizə problemi qarşıya çıxır [75]. Söhbət hesablamalara sərf olunan zamanın analizi və işlədilən gücün analizindən gedir. Bu hücumların əsasında mikroprosessorda yerinə yetirilən müxtəlif əməliyyatların fərqli vaxt tələb etməsi, həmçinin prosessorun müxtəlif güc işlətməsinə səbəb olması faktı durur. Alqoritmin zaman xarakteristikalarını (cavab vaxtını) və ya işlədilən gücü analiz edərək, müxtəlif əməliyyatların yerinə yetirilməsi mənzərəsini bərpa etmək olar.

2.3.4. RSA sxeminin təhlükəsizliyi

Vuruqlara ayırma ədədlər nəzəriyyəsinin ən qədim problemlərindən biridir. Açıq şifrləmənin ən geniş yayılmış sistemi RSA-nın davamlılığı və RSA əsasında rəqəm imzası sxeminin davamlılığı böyük tam ədədlərin faktorizasiyası (vuruqlara ayrılması) məsələsinin çətinliyinə əsaslanıb. Buna görə bu məsələ müasir kriptoqrafiyanın ən mühüm məsələlərindən biridir. Məşhurluğuna görə diskret loqarifmləmə məsələsindən üstündür və məşhur diskret loqarifmləmə alqoritmlərinin tərkib hissəsidir.

Hal-hazırda tam ədədlərin faktorizasiyası üçün kifayət qədər sürətli alqoritm yoxdur. Hazırda ən sürətli alqoritm ədədi meydanın qəfəsi metodudur (Number Field Sieve, NFS) [41, 79]. Bu metod 110 və daha çox mərtəbəli ədədlər üçün ən səmərəli metod hesab olunur. NFS tərəfindən sıxışdırılan alqoritmlər kvadratik qəfəs metodu (Quadtatic Sieve, QS) [79], elliptik əyrilər metodu [78], Pollardın Monte Karlo alqoritmi [82], kəsilməz kəsrlər alqoritmi, bölmə ilə sınaq (vuruqlara ayrılan ədədin kvadrat kökündən kiçik olan hər bir sadə ədədin sınanması) və s-dir.

Mövcud faktorizasiya alqoritmləri çətinliyinə (onların realizəsi üçün tələb olunan arifmetik əməliyyatların sayına) görə üç qrupa bölünürlər (c hər hansı sabiti işarə edir):

1. $O(n^c)$ arifmetik əməliyyat tələb edən eksponensial çətinlikli alqoritmlər;
2. $L(n)^{c+o(1)}$ arifmetik əməliyyat tələb edən subeksponensial çətinlikli alqoritmlər, burada $L(n) = e^{\sqrt{\ln n \ln\ln n}}$;
3. Çətinliyi $e^{((c\ o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3}}$ arifmetik əməliyyat olan ədədi meydanın qəfəsi metodu və onun sonrakı ümumiləşdirilmələri;

Faktorizasiya üsullarından praktikada ən çox işlədilən Pollard metodunun [82] ümumi sxemi aşağıdakından ibarətdir:

1. $f:Z_n \to Z_n$ funksiyası seçilir (adətən f funksiyası kimi - dərəcəsi 2-dən aşağı olmayan çoxhədli götürülür).
2. Təsadüfi olaraq $x_0 \in Z_n$ seçilir və x_1 , x_2,... qiymətləri $x_j=f(x_{j-1})$ mod n düsturu ilə hesablanaraq mərhələ 3-ün testi keçirilir.
3. $1< (x_j - x_k, n) <n$ şərti aşağıdakı qaydalardan biri üzrə seçilmiş j,k nömrələri üçün yoxlanır:
   1) $k<j$
   2) $j=2k$
   3) Əgər $j=2k$-dırsa, onda $k=2^h-1$.

Əgər bölən tapılmasa, növbəti j, k-ya keçilir.

Pollard metodunun çətinliyi $O(n^{1/4})$ evristik qiymətləndirməyə malikdir.

Vuruqlara ayırma metodlarının inkişafı məqsədi ilə RSA Data Security Inc 1991-ci ilin martında RSA Factoring Challenge (faktorizasiya üzrə RSA yarışı) proqramını elan etmişdir [61]. Yarış hər biri təxminən eyni uzunluqlu iki sadə ədədin hasilinə bərabər olan bir sıra çətin ədədlərin vuruqlara ayrılmasından ibarətdir. Yarış üçün 10 mərtəbə addımı ilə uzunluğu 100-bitdən 500-bitədək 42 ədəd seçilmişdir. RSA- 100, RSA-110, RSA-120 və RSA-129 kvadratik qəfəs metodunun köməyi ilə vuruqlara ayrılmışdır.

Məlumat üçün qeyd edək ki, beynəlxalq tədqiqatçılar qrupu 1999-cu ildə açarının uzunluğu 512 bit (155 onluq rəqəm) olan RSA şifrini açmağa müvəffəq olmuşlar. İnternet-tranzaksiyaların qorunması üçün, həmçinin kommersiya banklarının bir çoxunun şifrlərində məhz bu uzunluqda açardan istifadə olunur. ABŞ hökumətinin ixrac edilən proqram məmulatlarında istifadə edilməyə icazə verdiyi açarın uzunluğu da 512 bitə bərabərdir. 155 onluq rəqəmli ədədin iki sadə vuruğunun tapılması üzərində iş 11 müxtəlif coğrafi nöqtədə yerləşən, paralel işləyən 292 kompüterin resursları cəlb edilməklə 7 ay ərzində aparılmışdır. Bu kompüterlərin sırasına 175-400 MHs takt tezliyində işləyən 160 SGI və Sun işçi stansiyaları, 250 MHs tezliyində işləyən 8 Origin 2000 SGI kompüteri, 120 ədəd Pentium II (350-450MHs) prosessorlu

fərdi kompüter və 500 MHs tezliyində işləyən, Digital/Compaq istehsalı olan 4 prosessor daxil idi. Hesablama resurslarının ümumi sərfi 8 min MIPS-il olmuşdur.

Aşağıdakı cədvəldə ümumiləşdirilmiş ədədi qəfəs alqoritmindən istifadə etməklə tam ədədlərin vuruqlara ayrılması üçün tələb olunan hesablama gücü göstərilmişdir[39].

n-in ölçüsü (bitlərlə)	512	768	1024	1280	1536	2048
MIPS il	$3 \cdot 10^4$	$2 \cdot 10^8$	$3 \cdot 10^{11}$	$1 \cdot 10^{14}$	$3 \cdot 10^{16}$	$3 \cdot 10^{20}$

2.3.5. RSA sxeminin çətinlikləri

Qeyd olunduğu kimi, bütün asimmetrik şifrləmə metodlarına xas olan xüsusiyyət hesablamaların çoxrəqəmli ədədlərlə aparılması səbəbindən sürətlərinin simmetrik alqoritmlərlə müqayisədə olduqca aşağı olmasıdır. Qeyd etmək lazımdır ki, sonlu meydanlarda sürətli hesablama alqoritmlərinin işlənməsi hal-hazırda olduqca aktual məsələdir [29]. Böyük tam ədədlərlə hesab əməllərinin aparılması [27, 79]-də müzakirə olunur. Yalnız onu qeyd edək ki, böyük ədədi həmişə kiçik bloklara bölmək və hesablamaları bloklar üzərində aparmaq olar. Bunun üçün xüsusi proqramlar lazımdır. Hətta böyük tam ədədlərlə hesablamalar üçün xüsusi proqramlaşdırma dilləri yaradılmış və kifayət qədər geniş yayılmışdır. Onlardan sərbəst yayılan PARİ və UBASIC dillərini göstərmək olar.

RSA alqoritminin əhəmiyyəti az olmayan cəhəti hesablamaların həcmidir. Əgər uzunluğu k bit olan açar istifadə olunursa, onda açıq açar üzrə $O(k^2)$ əməliyyat, məxfi açar üzrə $O(k^3)$ əməliyyat, yeni açarların generasiyası üçün $O(k^4)$ əməliyyat tələb olunur. Açarın uzunluğunun artırılması imzanın yaradılması və yoxlanması zamanı hesablamaların artmasına, rəqəm imzasının uzunluğunun artmasına (RSA alqoritmində imzanın uzunluğu n ədədinin yazılışının uzunluğuna bərabərdir), açarların saxlanması üçün tələb olunan yaddaş həcminin artmasına səbəb olur. Məsələn,

açarın uzunluğunu 2 dəfə artırdıqda imzanın yoxlanması üzrə əməliyyatlar 4 dəfə, imzanın yaradılması üzrə hesablamaların həcmi 8 dəfə artır. Açarın uzunluğu artırıldıqda tələb olunan hesablama resurslarının əhəmiyyətli artması bütün mövcud məxfi girişli funksiyadan istifadə edən kriptoalqoritmlərə xasdır. Bundan başqa məxfi və açıq açarların saxlanması üçün tələb olunan yaddaşın həcmi artır. Yaddaş fərdi kompüterin adi istifadəçisi üçün kritik olmasa da, bir sıra hallarda əhəmiyyətli amildir, məsələn:

- məhdud hesablama imkanları olan istənilən qurğular üçün (smart-kart, mobil telefon və s.);
- kliyent sorğularının böyük həcmi ilə əhəmiyyətli dərəcədə yüklənən server komponentləri üçün.

Bundan başqa RSA sistemində açarların generasiyası zamanı p və q sadə ədədləri üçün kifayət qədər çox sayda əlavə çətin şərtləri yoxlamaq lazımdır. Bu şərtlərdən istənilən birinin yerinə yetirilməməsi bunu aşkar edən tərəfindən imzanın saxtalaşdırılmasını mümkün edir. Vacib sənədlərin imzalanması zamanı hətta nəzəri olaraq belə imkana yol vermək arzuolunmazdır. RSA metodunun bütün alqoritmik zəifliklərinə əlavə olaraq onun ABŞ patenti ilə qorunduğunu da qeyd etmək lazımdır. Yüz istifadəçi üçün lisenziyanın qiyməti 5000 dollardır.

2.3.6. Ədədlərin sadəliyi testləri

Böyuk sadə ədədlər praktik olaraq bütün asimmetrik şifrləmə sistemlərində, rəqəm imzası və açarların generasiyası sistemlərində istifadə olunur. Bu sistemlərin davamlılığı istifadə olunan sadə ədədlərin xassələrindən asılıdır. Beləliklə, sadə ədədlərin generasiyası məsələsi böyük praktik əhəmiyyətə malikdir.

Verilmiş uzunluqlu sadə ədədi qurmaq üçün praktikada əsasən verilmiş uzunluqlu təsadüfi natural ədəd seçilir və onun sadə olması yoxlanılır. Verilən ədədin sadə olmasını yoxlamaq üçün müxtəlif yanaşmalar mövcuddur.

Ədədlərin sadəliyinin yoxlanması qədim tarixə malikdir. Məsələn, $F_k = 2^{2^k}+1$, $k = 1, 2, \ldots$ Ferma ədədlərinin sadəliyinin yoxlanması düzgün çoxbucaqlıların xətkeş və pərgarın köməyi ilə qurulması məsələsi ilə əlaqədardır. Kriptoqrafik məqsədlər üçün çox böyük təsadüfi ədədləri yoxlamaq tələb olunur. N natural ədədinin sadəliyinin yoxlanması üçün ən sadə üsul sınaq bölmələri metodudur: $p = 2, 3, 5, 7, \ldots$ üçün $(p, N)>1$ şərtinin ödənməsi yoxlanır (burada (p, N) –p və N ədədlərinin ən böyük ortaq bölənidir). Bu alqoritm təkcə sadəliyi yoxlamır, N mürəkkəb olduqda qeyri-trivial böləni də tapır. Bu metod üçün tələb olunan əməliyyatların sayı N ədədinin kvadrat kökü tərtibindədir. Buna görə də 10^{30}–10^{40} tərtibindəki ədədlər üçün bu metod artıq tətbiq olunmazdır.

N-in sadəliyini müəyyən c sabiti üçün $O((\log N)^{(c*\ln \ln \ln N))}$ addıma yoxlayan Rumeli və Adlemanın alqoritmini də qeyd edək [42, 49]. Sadalanan testlər N ədədinin sadəliyinə *100%* qarantiya verir, yəni test çıxışda N ədədini sadə ədəd elan edirsə, bunu N ədədinin sadəliyinin ciddi riyazi isbatı hesab etmək olar. Ancaq bu testlər yerinə yetirilmə müddətinin böyük olmasına görə tətbiq olunmurlar.

Belə determinik testlərdən fərqli olaraq ədədlərin sadəliyini yoxlamaq üçün ehtimali testlər var. Tədqiq olunan ədəd üçün təsadüfi ədədlərlə bağlı müəyyən şərtlərin yerinə yetirilməsi yoxlanır. Əgər bu şərtlərdən hər hansı biri ödənmirsə, onda N mürəkkəb ədəddir. Əgər bütün şərtlər ödənirsə, onda müəyyən ehtimalla təsdiq etmək olar ki, N – sadə ədəddir. Nə qədər çox təsadüfi ədəd yoxlanılsa, bu ehtimal bir o qədər 1-ə yaxın olar. Adətən bu şərtlər Fermanın kiçik teoreminə əsaslanır. Fermanın kiçik teoreminə görə, əgər N sadə ədəddirsə, onda N–ə bölünməyən istənilən a ədədi üçün $a^{N-1} \equiv 1 (\mathrm{mod} N)$ müqayisəsi ödənir.

Əgər a-nın hər hansı qiymətində bu müqayisə ödənirsə, onda N mürəkkəb ədəddir. Müqayisənin ödənilməsini yoxlamaq çətinlik törətmir, əsas məsələ a-nın tapılmasıdır. a-nın zəruri qiymətini 2-dən başlayaraq bütün tam ədədləri ardıcıl

sınamaqla, yaxud $1<a<N$ parçasından təsadüfi şəkildə seçməklə tapmaq olar.

Ədədlər nəzəriyyəsinin klassik nəticəsi Çebışev teoreminə [14] görə *m* tam ədədindən kiçik müsbət sadə ədədlərin nisbi sayı $1/(\ln m)$-ə yaxındır. Məsələn, 10^{100}-dən kiçik sadə ədədlərin payı $1/(\ln 10^{100}) = 1/230$ yaxındır. Bu ədədlərin *90%*-i 10^{99} ilə 10^{100}arasında yerləşdiyindən, bu intervalda sadə ədədlərin nisbi sayı da *1/230* bərabərdir.

Buna görə, əgər təsadüfi olaraq *99* onluq rəqəmli ədəd, yəni 10^{99} -dan 10^{100}-dək olan intervalda ədəd seçilsə, onda ədəd təxminən *1/230* ehtimalı ilə sadə olacaq.

Beləliklə, biz təsadüfi olaraq tam müsbət tək ədəd seçsək və ardıcıl olaraq *x*, *x*+1, *x*+2, ... ədədlərinin sadəliyini yoxlasaq, orta hesabla sadə ədədlə ilk dəfə $\ln x$ nömrəli addımda qarşılaşarıq.

Təəssüf ki, bu yanaşma həmişə istəniləni vermir. Müqayisəni və $(a, N)=1$ şərtini ödəyən mürəkkəb ədədlər var. Belə ədədlər Karmaykl ədədləri adlanırlar. Məsələn, 561 belə ədəddir. Yalnız bu yaxınlarda belə ədədlər çoxluğunun sonsuz olduğu isbat edilmişdir [13].

Miller Fermanın kiçik teoreminin şərtini bir qədər gücləndirməyi təklif etmişdir [13]. Əgər *N* sadə ədəd və $N-1=2^s \cdot t$ -dirsə, burada *t* tək ədəddir, onda Fermanın kiçik teoreminə görə $(a, N)=1$ şərtini ödəyən hər bir *a* üçün

$$(a^m-1)(a^m+1)(a^{2m}+1)\cdot\ldots\cdot(a^{2^{s-1}}+1)=a^{N-1}-1$$

hasilindəki mötərizələrdən heç olmasa biri *N*-ə bölünür. Bu xassədən mürəkkəb ədədi sadə ədəddən fərqləndirmək üçün istifadə etmək olar.

Ciddi psevdosadə ədədin tərifini verək. Tutaq ki, *N* – tək ədəddir, $N-1 = d*2^s$, *d* – tək ədəddir. Əgər $a^d = 1 \pmod N$ və ya müəyyən r, $0<r<s$ üçün $a^{(d*2^r)} = -1 \pmod N$ olarsa, *N* ədədi *a* bazasına görə ciddi psevdosadə adlanır.

Ciddi psevdosadəliyi təsadüfi bazalar üzrə yoxlamağa əsaslanan ehtimali sadəlik testləri Selfric testi adlanır. Bu halda Karmaykl ədədlərinin analoqları (yəni ədədin özünü aşmayan

bütün təsadüfi bazalar üzrə ciddi psevdosadə olan ədədlər) yoxdur.

Ədədlərin sadəliyinin ehtimal testlərindən Solovey-Strassen, Lemann, Rabin-Miller və s. alqoritmlərini göstərmək olar [4, 41, 79].

a ədədinin sadəliyini yoxlamaq üçün ən sadə test olan Lemann alqoritminin addımlar ardıcıllığı belədir:

(1) *p* –dən kiçik təsadüfi *a* ədədi seçilir
(2) $a^{(p-1)/2} \bmod p$ hesablanır;
(3) Əgər $a^{(p-1)/2} \neq 1$ və yaxud $-1 (\bmod p)$ olarsa, *p* sadə ədəd deyil;
(4) Əgər $a^{(p-1)/2} \equiv 1$ və yaxud $-1 (\bmod p)$ olarsa, p ədədinin sadə ədəd olması ehtimalı $1/2$-dən böyük deyil.

Tutaq ki, yoxlama t dəfə aparılır. Əgər nəticə 1 və ya –1-ə bərabərdirsə, ancaq həmişə 1-ə bərabər deyilsə, onda p ədədi $\frac{1}{2^t}$ səhv ehtimalı ilə sadə ədəd olacaq.

[41]-də aşağıdakı praktik mülahizələr irəli sürülür:

n –bitlik təsadüfi p ədədi generasiya olunur;

(1) böyük və kiçik bitlər vahidə bərabar götürülür (böyük bitin vahid olması ədədin uzunluğuna, kiçik bitin vahid olması ədədin təkliyinə zəmanət verir);
(2) *p*-nin kiçik sadə ədədlərə– 3, 5, 7, 11 və s. bölünməsi yoxlanılır. Bir çox realizələrdə *p*-nin 256-dan kiçik bütün sadə ədədlərə bölünməsi yoxlanılır.
(3) Hər hansı təsadüfi *a* ədədi üçün Rabin-Miller testi yerinə yetirilir. Əgər *p* testdən keçirsə, başqa *a* ədədi generasiya olunur və yoxlama təkrarlanır. Hesablamaların sürətləndirilməsi üçün *a*-nın kiçik qiymətləri götürülür. Ən azı beş test aparılması məsləhət görülür.

2.4. Rabin sxemi

Rabin sxeminin [83,41] təhlükəsizliyi mürəkkəb ədədin moduluna görə kvadrat köklərin axtarışı məsələsinin çətinliyinə

əsaslanır. Məlumatlar fəzası qismində Z_n^* qrupu elementlərinin bütün kvadratları çoxluğu çıxış edir. M məlumatı üçün imza $h(m)$–dən n moduluna görə istənilən kvadrat kök qəbul edilir. Burada $h(m)$ heş-funksiyadır. M məlumatı üçün S imzasının yoxlanması $S^2 \equiv h(M) (\text{mod } n)$ müqayisəsinin yoxlanmasından ibarətdir. Bu sxemin Vilyams tərəfindən təklif olunmuş təkmilləşdirilmiş variantına nəzər salaq [41]:

$p \equiv 3 \ (\text{mod } 8)$, $q \equiv 7 \ (\text{mod } 8)$ sadə ədədləri seçilir və onların hasili $N=pq$ hesablanır. $k=1/2(1/4(p-1)(q-1)+1)$ düsturu ilə hesablanan k ədədi məxfi açar olacaq. Bundan başqa S kiçik tam ədədindən istifadə olunur ki, onun üçün $J(S, N)= -1$. N və S dərc olunurlar. Burada J- Yakobi simvoludur [14, 41]. Yakobi simvolu istənilən a tam ədədi və istənilən n tək ədədi üçün hesablana bilər, o, mürəkkəb modullar üçün Lejandr simvolunun [14] ümumiləşdirilməsidir və sadə $n>2$ ədədləri üçün Lejandr simvoluna bərabərdir:

$$\left(\frac{a}{n}\right) = \begin{cases} 1, \ a \text{ ədədi } n \text{ moduluna görə kvadratik çıxıqdırsa;} \\ 0, \ a \text{ ədədi } n \text{ - ə bölünürsə;} \\ -1, \text{ a ədədi } n \text{ moduluna görə kvadratik çıxıq deyilsə.} \end{cases}$$

Mürəkkəb n ədədi üçün Yakobi simvolu

$$J(a, n)=J(a, p_1) \cdot \ldots \cdot J(a, p_m)$$

düsturu ilə hesablanır, burada $p_1, \ldots p_m$ ədədləri n ədədinin sadə vuruqlarına ayrılışındakı sadə ədədlərdir. M məlumatının şifrlənməsi üçün $J(M, N)=J(M,N)=(-1)^{c_1}$ şərtini ödəyən c_1 hesablanır. Sonra $M^1=(s^{c_1} \cdot M) \text{mod } N$. $C=M'^2 \text{mod} N$, $c_2=M^1 \text{mod } 2$ hesablanır. Məlumat üçün son şifrlənmiş mətn (C, c_1, c_2) üçlüyüdür. Alan deşifrləmə üçün M''-i hesablayır:

$$C^k \equiv \pm M'' (\text{mod } N)$$

M''-in düzgün işarəsini c_2 müəyyən edir. Nəhayət,

$$M=(s^{c_1} \cdot (-1)^{c_1} \cdot M'') \text{mod } N$$

hesablanır.

Rabin-Vilyams sxeminin RSA sxemindən üstünlüyü ondan ibarətdir ki, bu sxemin ədədlərin vuruqlara ayrılması kimi təhlükəsiz olduğu isbat olunmuşdur.

2.5. Əl-Qamal imza sxemi

1984-cü ildə Tahir Əl-Qamal tərəfindən təklif olunmuş rəqəm imzası alqoritmi [60] irəliyə doğru böyük addım idi. Bu alqoritmdə *n* ədədinin əvəzinə xüsusi seçilmiş böyük sadə *p* ədədi götürülür. Belə seçim açarların uzunluğu 512 bit olduqda imzanın davamlılığını təxminən 1000 dəfə artırmağa imkan verir. Ancaq bu zaman rəqəm imzasının özünün uzunluğu 2 dəfə artaraq 1024 bit olur. Əl-Qamal sxemindən həm rəqəm imzası, həm də şifrləmə üçün istifadə etmək olar. Onun təhlükəsizliyi sonlu meydanda diskret loqarifmin hesablanmasının çətinliyinə əsaslanır.

Açarlar cütünü generasiya etmək üçün əvvəlcə *p* sadə ədədi və ondan kiçik iki *g* və *x* ədədləri seçilir, sonra $y=g^x \bmod p$ hesablanır. *y, g* və *p* açıq açardır. *g* və *p*-ni istifadəçilər qrupu üçün ümumi etmək olar. Məxfi açar *x* olacaq.

M məlumatını imzalamaq üçün əvvəlcə *p-1* ilə qarşılıqlı sadə olan təsadüfi *k* ədədi seçilir. Sonra $a=g^k \bmod p$ hesablanır və genişləndirilmiş Evklid alqoritminin [27] köməyi ilə $M=(xa+kb) \bmod (p-1)$ tənliyindən *b* tapılır. *a* və *b* ədədlər cütü imza olacaq. *k* təsadüfi qiyməti məxfi saxlanmalıdır. İmzanın yoxlanması üçün

$$y^a a^b \bmod p = g^M \bmod p$$

olduğuna əmin olmaq lazımdır.

Əl-Qamal sxeminin təsvirini aşağıdakı kimi cəmləşdirək:

Açıq açar:

p Sadə ədəd

g $< p$

y $= g^x \bmod p$

Məxfi açar:

x $< p$

İmzanın yaradılması:

k təsadüfi seçilir, p-1 ilə qarşılıqlı sadə ədəddir.

a (imza) = $g^k \bmod p$

b (imza), M=(xa+kb) mod (p-1) şərtini ödəyir.

İmzanın yoxlanması:

əgər $y^a a^b \bmod p = g^M \bmod p$ olarsa, imza düzgün hesab olunur.

İmzanın yoxlanmasının korrektliyi asanlıqla isbat edilir:

$$y^a a^b = (g^x)^a (g^k)^b = g^{xa} g^{kb} = g^{xa+kb} = g^M$$

Misal. p=11 və g=2 seçək. Məxfi açar x=8 olsun. y-i hesablayaq: $y = g^x \bmod p = 2^8 \bmod 11 = 3$.

Açıq açar y=3, g=2, p=11-dir. M=5-i imzalamaq üçün əvvəlcə təsadüfi k ədədini seçək: k=9. ƏBOB(k, p-1)= ƏBOB(9,10)=1 olduğu aydındır. $a = g^k \bmod p = 2^9 \bmod 11 = 6$ hesablayıb, genişləndirilmiş Evklid alqoritmi ilə $5 = (8*6+9*b) \bmod 10$ münasibətindən b-ni tapırıq. Buradan b=3 tapılır. İmza a=6, b=3 cütündən ibarətdir.

İmzanı yoxlamaq üçün

$y^a a^b \bmod p = g^M \bmod p$

$3^6 6^3 \bmod 11 = 2^5 \bmod 11$

olduğuna əmin olmaq lazımdır.

Hər bir Əl-Qamal imzası k-nın yeni qiymətini tələb edir, bu qiymət təsadüfi olaraq seçilməlidir. Əgər k məlum olsa, məxfi açar x-i

$$x = (M - ka)b^{-1} \bmod (p-1)$$

düsturu ilə hesablamaq mümkün olar. Əgər k-nın eyni qiyməti ilə şifrlənmiş və ya imzalanmış iki məlumat elə keçirilsə, hətta k-nın qiymətini bilmədən belə x-i hesablamaq mümkündür.

Əl-Qamal sxeminin bir çox variantları, məsələn, identifikasiya üçün, açarların mübadiləsi üçün, parolların həqiqiliyinin yoxlanması üçün və s. variantları mövcuddur. Onların əsasında

$$\alpha^A \beta^B \equiv \gamma^C \pmod p$$

müqayisəsinin yoxlanması durur. Burada (A,B,C) üçlüyü $\pm M$, $\pm b$, $\pm a$ ədədlərinin yerdəyişmələrinin biri ilə işarələrin müəyyən

seçimində üst-üstə düşür. Məsələn, $A=M$, $B=-a$ və $C=b$ olduqda ilkin Əl-Qamal sxemi alınır. ABŞ-ın [63] və Rusiyanın [16,17] ilk rəqəm imzası standartları bu ailədən olan imza sxemləri əsasında qurulmuşdur. Məsələn, ABŞ standartı DSS-də $A=M$, $B=a$ və $C=b$ qiymətləri, QOST R 34.10-94 Rusiya standartında isə $A=-M$, $B=b$ və $C=a$ qiymətlərindən istifadə olunur.

2.6. Şnorr sxemi

Alman kriptoqrafı K. P. Şnorrun təklif etdiyi rəqəm imzası və interaktiv identifikasiya sxemi [41, 88] bir sıra ölkələrin rəqəm imzası standartının əsasını təşkil etmişdir. Şnorr sxeminin təhlükəsizliyi də diskret loqarifmləmə məsələsinin çətinliyinə əsaslanır.

Açarlar cütünün generasiyası üçün əvvəlcə iki p və q sadə ədədləri seçilir, həm də q ədədi $p-1$-in vuruğudur. Sonra təsadüfi g tam ədədi seçilir və $a=g^{(p-1)/q} \bmod p$ hesablanır. Burada g ədədi p-1-dən kiçik istənilən ədəddir və onun üçün $g^{(p-1)/q} \bmod p > 1$ şərti ödənməlidir. Bu ədədlər açıq nəşr oluna bilərlər, həmçinin istifadəçilər qrupu tərəfindən də istifadə oluna bilərlər.

Konkret açarlar cütünü generasiya etmək üçün q-dən kiçik təsadüfi x ədədi seçilir. O, məxfi açar olacaq. Sonra açıq açar $y=a^x \bmod p$ düsturu ilə hesablanır.

İmzanın yaradılması:

(1) q-dən kiçik təsadüfi k ədədi seçilir və $r=a^k \bmod p$ hesablanır.

(2) M və r birləşdirilir və nəticə heşlənir: $e=H(M||r)$.

(3) $s=(k+xe) \bmod q$ hesablanır. e və s cütü imza olacaq.

İmzanın yoxlanması:

(4) $v=a^s y^{-e} \bmod p$ hesablanır.

(5) v və M birləşdirilərək heş-qiymət $e'=H(M||v)$ hesablanır.

(6) Əgər $e'=e$ bərabərliyi doğrudursa, imza həqiqi hesab olunur.

Doğrudan da, $v=a^s y^{-e}=a^{k+xe}(a^x)^{-e}=a^{k+xe}a^{-xe}=a^k=r$. Deməli, $H(M||v)=H(M||r)$ və $e'=e$.

Misal. (Süni kiçik parametrlərlə Şnorr sxemi)
Açarın generasiyası. p=129841 və q=541 sadə ədədlərini seçək. Burada $(p-1)/q$=240. Təsadüfi g=26346$\in Z_p^*$ ədədini seçərək a= 26346^{240} mod p=26 hesablayaq. $a\neq 1$ olduğu üçün Z_p^*-də tərtibi 541 olan yeganə dövri altqrup generasiya edir. Sonra məxfi açar x=423 seçək və $y=26^{423}$ mod p=115917 hesablayaq. Açıq açar (p=129841, q=541, a=26, y=115917) olacaq.
İmzanın generasiyası. Tutaq ki, M=11101101 məlumatını imzalamaq lazımdır. $1 \le k \le 540$ şərtini ödəyən təsadüfi k=327 ədədini seçək, $r=26^{327}$mod p=49375 və $e=H(M\,||r)$ =155 hesablayaq (bu misal üçün heş qiymət uydurmadır). Nəhayət, s=423·155+327 mod 541 = 431 hesablanır. M üçün imza (s=431, e=155) olacaq.
İmzanın yoxlanması. v =$26^{341}\cdot 115917^{-155}$mod =49375 və e'=H(M ||v)=155 hesablanır. e'=e olduğu üçün imza qəbul edilir.

Əl-Qamal tipli imza sxemlərində imzaların hesablanması və yoxlanması zamanı yerinə yetirilən ən mürəkkəb əməliyyat $g^z mod\ n$ diskret qüvvətə yüksəltmə əməlidir. Şnorr sxeminin Əl-Qamal sxemindən üstünlüyü y–in daha kiçik çoxluqdan (y–in uzunluğu 140-bit ətrafındadır) seçilməsidir. Bü diskret hesablamanın səmərəliliyini artırır. Bundan başqa qeyd edək ki, Şnorr sxemində e-nin hesablanması zamanı heş-funksiyanın istifadəsi və imzasının moduluna görə gətirilməsi imzanın uzunluğunu Əl-Qamal imzası ilə müqayisədə azaldır. İmzanın uzunluğu rəqəm imzası sxeminin səmərəliliyinin ən vacib göstəricilərindən biridir. Eyni təhlükəsizlik səviyyəsində Şnorr imzalarının uzunluğu RSA imzalarınkından kiçikdir. Məsələn, 140-bitlik q üçün imzanın uzunluğu 212-bitə bərabərdir və RSA imzasının uzunluğunun yarısından kiçikdir. Şnorr imzası Əl-Qamal imzalarından da xeyli qısadır.

2.7. DSA alqoritmi

DSA (Digital Signature Algorithm) rəqəm imzası alqoritmi 1991-ci ildə ABŞ-da Milli Standartlar və Texnologiya İnstitutu

(National Institute of Standards and Technology, NIST) tərəfindən rəqəm imzası standartında (Digital Signature Standard) istifadə etmək üçün təklif olunmuşdur [63], Şnorr (Schnorr) və Əl-Qamal imza alqoritmlərinin bir variantıdır. Alqoritm aşağıdakı parametrlərdən istifadə edir:

Açıq açar:

p Uzunluğu 512-dən 64 bit addımı ilə 1024 bitə qədər olan sadə ədəd

q p-1 -in 160-bitlik sadə vuruğu

g $=h^{(p-1)/q}$ mod p, burada h ədədi p-1-dən kiçik istənilən ədəddir və onun üçün $h^{(p-1)/q}$ mod p >1 ödənməlidir.

y $= g^x$ mod p (p bitlik ədəd)

Məxfi açar:

x < q (160-bitlik ədəd)

İmza:

k Təsadüfi seçilir, q-dən kiçikdir.

r (imza) = $(g^k$mod p) mod q

s (imza $=(k^{-1}(H(m)+xr))$ mod q

Yoxlama:

w $= s^{-1}$ mod q

u_1 $= (H(m)\cdot w)$ mod q

u_2 $= (rw)$ mod q

v $= ((g^{u_1}\cdot y^{u_2})$mod p) mod q

Əgər v = r olarsa, imza doğrudur.

İmzanın yoxlanmasının əsaslandırılması belədir:

$$g^{h(m)s^{-1}} \cdot y^{r\cdot s^{-1}} \ (mod\,p)(mod\,q) = g^{h(m)s^{-1}} \cdot g^{x\cdot r\cdot s^{-1}} \ (mod\,p)(mod\,q) =$$

$$= g^{s^{-1}(h(m)+xr)} \ (mod\,p)(mod\,q) = g^{(k^{-1}(h(m)+x\cdot r))^{-1}(h(m)+x\cdot r)} \ (mod\,p)(mod\,q) =$$

$$= g^{(k^{-1})^{-1}\cdot(h(m)+x\cdot r)^{-1}\cdot(h(m)+x\cdot r)} \ (mod\,p)(mod\,q) = g^{k} \ (mod\,p)(mod\,q) \equiv r$$

Misal. (Süni kiçik parametrlərlə DSA alqoritmi)
Açarın generasiyası. Elə p=124540019 və q=17389 sadə ədədləri seçilir ki, $p-1$ ədədi q ədədinə bölünsün, $(p-1)/q$ = 7162. İxtiyari g=110217528$\in \mathbf{Z}_p^*$ elementi seçilir və $\alpha = g^{7162}$ mod p=10083255 hesablanır. $\alpha \neq 1$ olduğu üçün, α elementi $\mathbf{Z}_p^*$-də tərtibi q olan dövri altqrupun doğuranıdır. Daha sonra $1 \leq a \leq q-1$ şərtini ödəyən ixtiyari x=12496 tam ədədi seçilir və $y=\alpha^x \bmod p=10083255^{12496} \bmod 124540019=119946265$ hesablanır. Açıq açar (p=124540019, q=17389, α=10083255, y=119946265), məxfi açar isə x=12496-dır.
İmzanın generasiyası. M məlumatını imzalamaq üçün, ixtiyari k=9557 tam ədədi seçilir və $r=(10083255^{9557} \bmod p) \bmod q$ =27039929mod$q$=34 hesablanır. Sonra $k^{-1} \bmod q$=7631 hesablanır, $h(M)$ = 5246 (bu misal üçün heş-qiymət ixtiyari götürülmüşdür) və nəhayət, s = 7631 {5246 + 12496· 34}mod q=13049. M üçün imza (r=34, s=13049) cütüdür.
İmzanın yoxlanması. $w = s^{-1} \bmod q$=1799, u_1=5246· 1799 mod q = 12716 və u_2= 34· 1799mod$q$ =8999 hesablanır. Sonra $v=(10083255^{12716} \cdot 119946265^{8999} \bmod p) \bmod q$ =7039929 mod q =34 hesablanır. $v=r$ olduğundan, imza qəbul edilir.

Alqoritmdə H(m) heş-funksiyasından istifadə olunur. DSS standartı SHA-dan istifadəni müəyyən edir. DSA alqoritmindən şifrləmə üçün istifadə etmək mümkün deyil, o yalnız rəqəm imzası üçün nəzərdə tutulub.

ABŞ-da RSA alqoritminin deyil, DSA alqoritminin rəqəm imzası standartı kimi qəbul edilməsi aşağıdakılarla əsaslandırılırdı:

- rəqəm imzasının davamlılığının verilmiş səviyyəsində hesablama aparılan tam ədədlərin yazılışı daha qısadır, buna görə hesablamaların çətinliyi azalır və istifadə olunan yaddaşın həcmi əhəmiyyətli dərəcədə ixtisar olunur;
- parametrlərin seçilməsi zamanı cəmisi üç asan yoxlanılan şərti yoxlamaq kifayətdir;

– bu metodla imzalamə proseduru məxfi açarı bilmədən yeni məlumat üçün rəqəm imzasını hesablamağa imkan vermir (RSA alqoritmində bu mümkündür).

Uzunmüddətli təhlükəsizlik üçün 512 bit uzunluqda *p* kifayət qədər etibarlı deyil, 1024-bit isə tam etibarlı hesab olunur, *q*-nü isə 160 bit uzunluğunda seçmək olar. DSA alqoritmində və RSA-da imzanın yaradılması sürəti demək olar ki, eynidir, lakin imzanın yoxlanılması sürəti DSA alqoritmində 10-40 dəfəyədək yavaşdır.

2.8. QOST R 34.10-94

QOST R 34.10-94 Rusiyanın rəqəm imzası standartıdır [16]. Alqoritm DSA-ya çox oxşardır və aşağıdakı parametrlərdən istifadə edir:

p - sadə ədədi, p-nin uzunluğu ya 509-dan 512 bitə qədər, ya da 1020-dən 1024 bitə qədər diapazonda olur.

q - sadə ədədi, p-1-in bölənidir, uzunluğu 254-dən 256 bitə qədərdir;

a - *p-1* -dən kiçik ixtiyari ədəd, $a^q \bmod p=1$şərtini ödəyir;

x - *q*-dən kiçik ədəd;

$y = a^x \bmod p$;

Bu alqoritmdə həmçinin *H(m)* heş-funksiyasından - QOST 28147-89 simmetrik kriptoalqoritminə əsaslanan QOST R 34.10-94 [17] heş-funksiya standartından istifadə edir.

İlk üç *p, q* və *a* parametrləri açıqdır və kriptoşəbəkənin abonentləri birgə istifadə edə bilərlər. Məxfi açar *x*, açıq açar isə *y*-dir. *M* məlumatını imzalamaq üçün

1. $k<q$ təsadüfi ədədi generasiya olunur;
2. $r=(a^k \bmod p) \bmod q$,
   $s=(xr+k(H(M))) \bmod q$

hesablanır. Əgər $H(M) \bmod q=0$-dırsa, heş-funksiyanın qiyməti 1 qəbul edilir. Əgər $r=0$ -dırsa, başqa *k* generasiya olunur və hesablama yenidən yerinə yetirilir. Məlumatın İmzası iki ədəddən – $r \bmod 2^{256}$ və $s \bmod 2^{256}$ ədədlərindən ibarətdir.

İmzanın yoxlanması üçün aşağıdakılar hesablanır:

$v=H(M)^{(q-2)} \bmod q$

$z_1=(sv) \bmod q$

$z_2=((q-r)\cdot v) \bmod q$

$u=((a^{z_1} y^{z_2}) mod\ p) mod\ q$

Əgər $u=r$ olarsa, imza düzgündür.

DSA-da $s=(k^{-1}(H(M)+xr)) \bmod q$-dür, bu başqa yoxlama tənliyi verir. Qeyd edək ki, q-nün uzunluğu 256 bitə bərabərdir. Qərb kriptoqraflarının əksəriyyəti hesab edir ki, q üçün 160 bit kifayətdir. Standart 1995-ci ilin əvvəlindən qüvvəyə minmişdir.

2.9. ECDSA rəqəm imzası alqoritmi

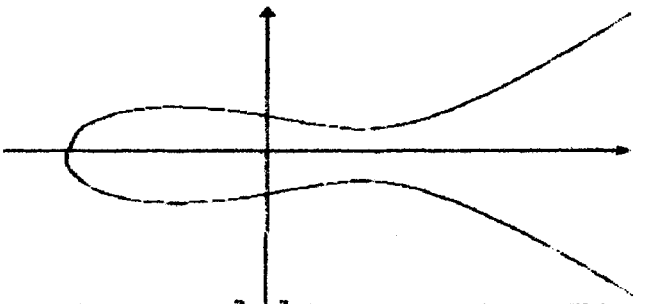
Elektron-hesablama vasitələrinin və kriptoanalizin riyazi üsullarının sürətli inkişafı ona gətirib çıxarmışdır ki, yüksək hesablama və maliyyə resurslarına malik bədniyyətlilər tərəfindən mövcud rəqəm imzası standartlarının real komprometasiyası mümkün olmuşdur. Məsələn, 2001-ci ilin əvvəlində fransız riyaziyyatçıları qrupu (A. Joux və R. Lercier) uzunluğu 397 bit olan sadə ədədin moduluna görə diskret loqarifmləmə problemini dəyəri təqribən 18000 dollar olan hesablama texnikasında həll etmişdir. Elliptik əyrilər əsasında kriptosistemlər tələb olunan təhlükəsizlik səviyyəsini saxlamaqla əhəmiyyətli dərəcədə kiçik ölçülü açarlardan istifadə etməyə imkan verir. Bununla əlaqədar olaraq əvvəllər qəbul edilmiş və kriptodavamlığı diskret loqarifm probleminə əsaslanan rəqəm imzası standartlarının əvəzinə elliptik əyrilərin istifadəsinə əsaslanan yeni standart qəbul edilməyə başlanmışdır. 1998-ci ildə ISO [71], 1999-cu ildə ANSI [46,47], 2000-ci ildə IEEE [68] və NIST [63] yeni ECDSA (Elliptic Curve Digital Signature Algorithm) rəqəm imzası standartını qəbul etmişlər.

Elliptik əyrilərin kriptoqrafiyada istifadəsini bir-birindən asılı olmadan N. Koblits [73] və V. Miller [80] 1985-ci ildə irəli sürmüşlər. Onlar sonlu meydan üzərində elliptik əyrilərdən istifadə edən kriptoqrafik alqoritm ixtira etməmişlər, yalnız mövcud alqoritmləri (Diffi-Helman, Əl-Qamal və s.) elliptik

əyrilərin köməyi ilə realizə etmişlər. Həmçinin hiperelliptik əyrilərin əsasında da kriptosistemlər təklif olunubdur.
Elliptik əyrilərlə bağlı qrupların əsas üstünlükləri bunlardır:

- bu qrupların parametrlərinin nisbətən sadə hesablanması;
- bu qruplarda diskret loqarifmləmə məsələsinin həllinin səmərəli üsulunun yoxluğu və gələcəkdə tapılmasının olduqca az ehtimallı olması. Bu çox böyük davamlılıq zəmanəti ilə kiçik uzunluqlu açarlardan istifadə etməyə imkan verir.
- qeyd olunmuş əsas meydanda elliptik əyrilərin və onlarla bağlı qrupların geniş seçim imkanları. Adi alqoritmlərdə praktik olaraq belə seçim imkanı yoxdur.
- elliptik əyrilər üçün spesifik kriptoanaliz üsullarının tətbiqini istisna edən aydın və sadə şərtlərin varlığı.

Məlum nəzəri nəticələrin məcmusu elliptik əyrilərin etibarlı və səmərəli kriptosistemlər qurmağa unikal imkan verməsini inandırıcı şəkildə sübut edir. Əvvəlcə alqoritmin riyazi əsasları ilə qısaca tanış olaq.



Şəkil 2.1. $y^2=x^3-5x+8$ əyrisinin qrafiki

Real kriptosistemlərdə

$$y^2=x^3+ax+b \qquad (1)$$

tənliyindən istifadə olunur, burada $a,b \in F_p$, $4a^3+27b^2 \neq 0 (\text{mod } p)$, $p>3$- sadə ədəddir.

$E(F_p)$ elliptik əyrisi, (1) tənliyini ödəyən bütün (x, y), $x,y \in F_p$

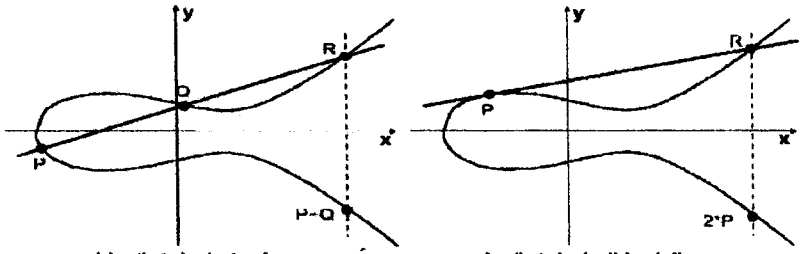
nöqtələrindən və O sonsuz uzaqlaşmış nöqtəsindən ibarətdir. Həqiqi ədədlər meydanı üzərində elliptik əyrinin qrafiki şəkil 2.1-də göstərilib.

Elliptik əyrinin nöqtələri üzərində toplama əməlini təyin etmək üçün aşağıdakıları qəbul edək:

- müstəvidə bütün şaquli düz xətlərin yığıldığı sonsuz uzaqlaşmış $O \in E$ nöqtəsi var;
- əyriyə toxunan düz xətt əyrini daha bir nöqtədə kəsir.

$P, Q \in E$ nöqtələrinin toplama qaydasını belə formulə etmək olar:

- P və Q nöqtələrindən düz xətt keçiririk, bu düz xəttin əyrini kəsdiyi üçüncü R nöqtəsini tapırıq;
- R nöqtəsindən E əyrisini kəsən şaquli düz xətt keçiririk;
- axtarılan cəm bu şaquli düz xəttin əyrini kəsdiyi ikinci $P+Q$ nöqtəsi olacaq (şəkil 2.2);



b) nöqtələrin toplanması a) nöqtələrin iki misli

Şəkil 2.2. Nöqtələr üzərində toplama əməliyyatı

Elliptik əyrinin bu üsulla təyin olunmuş toplama əməlinin aşağıdakı xassələri var:

- İstənilən $P \in E(F_p)$ nöqtəsi üçün $P+O=O+P=P$ xassəsi doğrudur, başqa sözlə, O additiv vahid elementdir.
- İstənilən $P=(x,y) \in E(F_p)$ nöqtəsi üçün $(x,-y) \in E(F_p)$ nöqtəsi P nöqtəsinə nəzərən tərs element adlanır və $-P$ ilə işarə olunur. Əgər $P \in E(F_p)$-dirsə, onda $(x,y)+(x,-y)=O$.
- Elliptik əyrinin istənilən üç P, Q, R nöqtələrinin toplanması üçün $P+(Q+R)=(P+Q)+R$ assosiativlik xassəsi doğrudur.

Bu xassə proyektiv həndəsənin faktlarından istifadə etməklə isbat oluna bilər.

– İstənilən iki $P, Q \in E$ nöqtələri üçün $P+Q=Q+P$ doğrudur.

Beləliklə, elliptik əyrinin nöqtələri toplama əməlinə görə additiv Abel qrupu əmələ gətirir. Həndəsi faktları əks etdirən $E(F_p)$ nöqtələri üzərində təyin olunan toplama əməliyyatı cəbri olaraq aşağıdakı kimi təsvir oluna bilər.

Tutaq ki, $P=(x_1,y_1)$ və $Q=(x_2, y_2)$. Onda $P+Q=(x_3,y_3)$ nöqtəsinin koordinatları belə ifadə olunacaq [9]:

$$x_3=\lambda^2-x_1-x_2$$

$$y_3=\lambda(x_1-x_3)-y_1$$

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, & \text{əgər } P\neq Q\\ \dfrac{3x^2+a}{2y_1}, & \text{əgər } P=Q\end{cases}$$

λ ədədi $P=(x_1,y_1)$ və $Q=(x_2, y_2)$ nöqtələrindən keçirilmiş kəsənin bucaq əmsalıdır. $P=Q$ olduqda kəsən toxunana çevrilir. Buna görə də bucaq əmsalı üçün iki düsturdan istifadə olunur.

Misal. Tutaq ki, $p=23$. $E: y^2=x^3+x+4$ elliptik əyrisinə baxaq. $a=1$ və $b=4$-dür. $4a^3+27b^2=4+432=436\equiv 22 \pmod{23}$. Beləliklə, E həqiqətən elliptik əyridir. $E(F_{23})$ elliptik əyrisi O nöqtəsindən və aşağıdakı nöqtələrdən ibarətdir:

(0, 2)	(0, 21)	(1, 11)	(1, 12)	(4, 7)
(4, 16)	(7, 3)	(7, 20)	(8, 8)	(8, 15)
(9, 11)	(9, 12)	(10, 5)	(10, 18)	(11, 9)
(11, 14)	(13, 11)	(13, 12)	(14, 5)	(14, 18)
(15, 6)	(15, 17)	(17, 19)	(17, 14)	(18, 9)
(18, 14)	(22, 5)	(22, 19)		

Tutaq ki, $P=(4, 16)$ və $Q=(13, 12)$. $P+Q$ və $2P$-ni tapaq. Tutaq ki, $P+Q=(x_3,y_3)$, onda

$$\lambda=\frac{12-16}{13-4}=\frac{-4}{9}=\frac{19}{9}=20$$

$$x_3=20^2-4-13=383=15.$$

$$y_3=20(4-15)-16=224=17.$$

Beləliklə, $P+Q=(15, 17)$.

$2P=P+P=(x_3,y_3)$ belə hesablanır:

$$\lambda = \frac{3\cdot 4^2+1}{2\cdot 16} = \frac{49}{32} = \frac{3}{9} = 8$$

$$x_3=8^2-4-4=56=10.$$

$$y_3=8(4-10)-16=120=17.$$

Beləliklə, $P+Q=(10, 5)$.

ECDSA alqoritminin təsvirinə nəzər salaq. Aşağıdakı parametrlər sistemin bütün istifadəçiləri üçün açıq (ümumi) informasiyadır:

- F_q sonlu meydanı;
- $E(F_q)$ elliptik əyrisi;
- elliptik əyrinin noqtələri sayının böyük sadə böləni n;
- tərtibi n ədədinə bərabər olan P nöqtəsi.

Sistemin hər bir istifadəçisi aşağıdakı qaydada açarlar cütü generasiya edir:

- d tam ədədi təsadüfi seçilir, $1<d<n-1$;
- $Q=dP$ nöqtəsi hesablanır;
- İstifadəçinin məxfi açarı d ədədi, açıq açarı isə Q nöqtəsidir.

İmzanın yaradılması (istifadəçi M məlumatını imzalayır):

- məlumatın heşi $H(M)$ hesablanır;
- n ilə qarşılıqlı sadə olan təsadüfi k, $1<k<n-1$ tam ədədi seçilir,
- $(x_1, y_1)=kP$ nöqtəsi və $r=x_1 \bmod n$ hesablanır. $r=0$ olarsa k-nın seçilməsi təkrarlanır;
- $s=k^{-1}(H(M)+rd) \bmod n$ hesablanır;
- (r, s) cütü məlumatın imzası olur.

İmzanın yoxlanması

- əgər $r=0$ isə, imza düzgün deyil;
- məlumatın heşi $H(M)$ hesablanır;
- $u=s^{-1}H(M) \bmod n$ və $v=s^{-1}r \bmod n$ hesablanır;
- $(x_1, y_1)=uP+vQ$ nöqtəsi hesablanır;
- $r'=x_1 \bmod n$ hesablanır;
- $r'=r$ olarsa, imza düzgün hesab olunur.

İmzanın yoxlanmasının korrektliyi asan isbat edilir. Əgər M məlumatı həqiqətən göndərən tərəfindən imzalanıbsa, onda $s=k^{-1}(H(m)+dr) \bmod n$. Buradan
$k \equiv s^{-1}(H(m)+dr) \equiv s^{-1}H(m)+ s^{-1}rd \equiv u+vd \pmod n$.
Beləliklə, $uP+vQ= uP+vdP=(u+vd)P=kP$. Deməli, $v=r$.

Elliptik əyrilər üzərində kriptosistemlərdən istifadə olunduqda düşmən məlum P və kP nöqtələrinə görə k ədədini tapmalıdır. Bu problem elliptik əyri üzərində diskret loqarifm problemi adlanır. Belə problem diskret loqarifmləmə problemindən daha çətindir. Problemin çətinliyi nöqtələrin toplanması və ikiyə vurulması əməliyyatlarının resurstutumlu olması ilə şərtlənir, bu yuxarıdakı düsturlardan da görünür. Bu daha qısa açarlardan istifadə etməyə imkan verir. Cədvəldə müxtəlif kriptosistemlərdə hesablama cəhətdən açarların ekvivalent ölçüləri bitlərlə göstərilib [43, 79]:

Simmetrik	ECC	RSA/DH/DSA
80	163	1024
112	224	2048
128	283	3072
192	409	7680
256	571	15360

Lakin elliptik əyrilər əsasında sistemlərin geniş yayılmasını məhdudlaşdıran bəzi problemlər də var:

- Belə sistemlərin real təhlükəsizliyi kifayət qədər dərk olunmayıb;
- Yararlı əyrilərin generasiyasının çətinliyi;
- Lisenziyalaşdırma və patentləşdirmə;
- Rəqəm imzasının nisbətən ləng yoxlanması.

2.10. Rəqəm imzasının xüsusi sxemləri

Bir sıra hallarda baxdığımız klassik sxemlərdən fərqli rəqəm imzası sxemləri tələb oluna bilər. Rəqəm imzasının məlum xüsusi sxemlərindən aşağıdakıları göstərmək olar:

- *kölgəli imza sxemi* [54], *A* abonenti sənədi məzmununu bilmədən imzalayır;
- *qrup imzası sxemi* [56], verifikatora (yoxlayıcıya) alınan məlumatın iddiaçıların müəyyən qrupuna aidiyyətinə əmin olmağa imkan verir, ancaq verifikatorun qrup üzvlərindən məhz hansının sənədi imzaladığını müəyyən etmək imkanı yoxdur;
- *ortaq imza sxemi* [41], yalnız müəyyən sayda protokol iştirakçılarının iştirakı ilə formalaşdırılır, başqa sözlə bu sxem imzanın klassik sxemi ilə sirrin bölüşdürülməsi sxemini birləşdirir;
- *konfidensial imza sxemi* [41], imza protokol iştirakçılarından imzanı formalaşdıran olmadan yoxlanıla bilməz;
- *inkarolunmaz imza sxemi*, imzanı yalnız imza sahibi yoxlaya bilər;
- *danılmaz imza sxemi*, imzanın saxtalaşdırılması isbat oluna bilər [53,55]. Bu imza sxemində hər bir açıq açara bir neçə mümkün məxfi açar uyğundur. Bədniyyətli bir məxfi açarı elə keçirə bildiyi üçün, yalnız bir imzanı hesablaya bilər. Məhkəməyə müraciət zamanı qanuni sahib saxtakarlığı aşkar etməkdən ötrü eyni məlumatın iki müxtəlif rəqəm imzasını və açıq açarı (özünün məxfi açarına və bədniyyətlinin tapdığı məxfi açara uyğun) təqdim edir.

2.10.1. Kölgəli imza sxemləri

Kölgəli imza sxemləri ilk dəfə Çaum tərəfindən təklif olunmuşdur [54]. RSA imzalarından istifadə etməklə Çaum bu konsepsiyanın realizəsini belə nümayiş etdirir: Fərz edək ki, *A* istifadəçisinin *B*-yə imzalatmaq istədiyi *M* məlumatı var və o, *B*-nin *M* haqqında bir şey öyrənməsini istəmir. Tutaq ki, *(n, e)* *B*-nin açıq açarı, *(n, d)* isə onun məxfi açarıdır. *A* istifadəçisi *(r, n)=1* şərtini ödəyən təsadüfi *r* ədədi generasiya edir və $x=(r^eM) \bmod n$ ədədini *B*-yə göndərir. *x*-in qiyməti təsadüfi *r* qiyməti ilə "kölgə"ləndiyindən *B* ondan faydalı informasiya əldə edə bilməyəcək.

B imzalanmış $t=x^d \bmod n$ kəmiyyətini A-ya qaytarır.

$$x^d \equiv (r^e M)^d = rM^d \bmod n$$

olduğu üçün A istifadəçisi M-in doğru imzasını $s=r^{-1}t \bmod n$ düsturu ilə hesablaya bilər.

Bu imza sxemi vuruqlara ayırmanın və kök almanın mürəkkəbliyi şərtində təhlükəsizdir. r təsadüfi olduğundan həmin məsələlərin statusundan asılı olmayaraq bu imza sxemi şərtsiz "kölgəlidir". Təsadüfi r ədədi, imzalayanın bu çətin məsələləri həll etməsi halında belə imzalayana məlumat barəsində bir şey öyrənməyə imkan vermir. Kölgəli imzaların vaxt nişanları, anonim girişə nəzarət, rəqəm-nəğd pulları daxil olmaqla çoxsaylı tətbiqləri var.

2.10. 2. Qrup imzası

Qrup imzası anlayışı Çaum və van Heyst tərəfindən [56] təklif olunmuşdur. İmzalayanlar qrupu və bir yoxlayan üçün imza sxemi aşağıdakı şərtlər ödəndikdə qrup imzası sxemi adlanır:

1. Məlumatı yalnız imzalayanlar qrupunun üzvləri imzalaya bilər;
2. Yoxlayan imzanın müəyyən imzalayan tərəfindən generasiya edildiyini yoxlaya bilər, ancaq məhz kimin imzaladığını müəyyən edə bilməz (imzalayanın anonimliyi);
3. Zəruri olduqda imza "açıla" bilər (məsələn, inam mərkəzi tərəfindən), yəni imzanı generasiya edən (imzalayan) müəyyən edilə bilər (imzalayanlar qrupu üzvlərinin köməyi olmadan və ya köməyi ilə).

Həmin işdə qrup imzası üçün dörd sxem təklif olunmuşdur. Nümunə üçün birinci sxemin qısa təsvirini verək. İnam mərkəzi (trusted authority) T hər hansı rəqəm imzası sxemini seçir, hər bir imzalayana məxfi açarlar siyahısı verir (müxtəlif imzalayanlar üçün bu siyahılar kəsişməməlidir), uyğun açıq açarları isə təsadüfi nizamla sertifikasiya olunmuş hər hansı açıq sorğu kitabında nəşr edir. Bundan sonra hər bir imzalayan məlumatların imzalanması üçün T-nin seçdiyi imza sxemində

ona verilmiş məxfi açarlardan birini istifadə edir, hər bir məxfi açar yalnız bir dəfə istifadə oluna bilər, əks halda yoxlayan bir neçə imzanın eyni bir imzalayan tərəfindən imzalandığını müəyyən edə bilər. İmza yalnız və yalnız sertifikasiyalı sorğu kitabındakı hər hansı açıq açara nisbətən yol verilən imza olduqda yoxlayan tərəfdən qəbul edilir. Açıq açarlar sorğu kitabında təsadüfi qaydada nəşr olunduğundan bu və ya digər açıq açarın hansı imzalayana aid olduğunu yoxlayan müəyyən edə bilməz. Yalnız T, açıq açarlarla imzalayanlar arasındakı uyğunluğu bildiyindən verilən imzanı "açа bilər".

Bu sxemin çatışmayan cəhətlərindən biri imzalayanların məxfi açarlarının T-yə məlum olmasıdır, deməli, T özü imzalayanların əvəzinə məlumatları imzalaya bilər. Sxemin müəllifləri bu təhlükənin qarşısını almaq üçün kölgəli açıq açarlardan istifadəni irəli sürürlər. Bu açarların mahiyyəti belədir. Tutaq ki, istifadə olunan rəqəm imzası sxeminde məxfi açarlar Z_{p-1}-dən seçilir, p-sadə ədəddir. Hər bir x məxfi açarına isə $g^x \bmod p$ açıq açarı uyğun gəlir, burada g-Z_p^* qrupunun hər hansı doğuranıdır. Hər bir imzalayan (məsələn, i-ci) $s_i \in Z_{p-1}$ seçir və $g^{s_i} \bmod p$–ni T-yə göndərir. Bundan sonra T $r_i \in Z_{p-1}$ seçir, imzalayana verir və $\left(g^{s_i}\right)^{r_i} \bmod p$–ni açıq açar qismində nəşr edir. Uyğun məxfi açar imzalayan tərəfindən $s_i r_i \bmod (p-1)$ şəklində hesablanır. Bu metodun daha bir üstünlüyü ondan ibarətdir ki, s-in eyni bir qiyməti bir neçə məxfi açarın yaradılması üçün istifadə oluna bilər. Qrup imzası üçün digər sxemlər Çen və Pedersenin [57] işlərində təklif olunub.

2.10.3. İnkarolunmaz imza sxemi

İnkarolunmaz imza da adi rəqəm imzası kimi, imzalanan sənəddən və sənədi imzalayanın məxfi açarından asılıdır. Ancaq adi rəqəm imzasından fərqli olaraq, inkarolunmaz imza imzalayanın icazəsi olmadan yoxlanıla bilməz. İnkarolunmaz imza sxemi aşağıdakı kimidir:

1. *A* rəqəm imzasını *B*-yə təqdim edir;
2. *B* təsadüfi ədəd generasiya edir və *A*-ya göndərir;
3. *A* təsadüfi ədəddən və özünün məxfi açarından istifadə edərək hesablamaları aparır və nəticəni *B*-yə göndərir. Yalnız imza düzgün olduqda *A* bu hesablamaları yerinə yetirə bilər;
4. *B* nəticəni yoxlayır.

Həmçinin *A*-ya sənədi imzalamadığını sübut etməyə imkan verən və imzadan yalandan imtina imkanına yol verməyən əlavə protokollar da təklif olunmuşdur.

2.10.4. İkiqat imzalar

SET protokolu rəqəm imzasının yeni konsepsiyasını- ikiqat imza anlayışını daxil edir. İkiqat imza verilənlərin iki fraqmentini əlaqələndirməyə və emal üçün iki müxtəlif mahiyyətə göndərməyə imkan verir. Məsələn, SET-ə uyğun olaraq kartın sahibi satıcıya emal üçün sifariş haqqında informasiya (OI-order information) göndərməlidir. Eyni zamanda ödənişləri həyata keçirmək üçün şlüzə ödəniş üzrə təlimatlar olan məlumat (PI-payment instructions) tələb olunur.

İkiqat imzanın formalaşdırılması prosesi aşağıdakı mərhələlərdən ibarətdir:

1. Sifariş haqqında informasiya üçün və ödəniş üzrə təlimat üçün məlumat daycestləri generasiya olunur;
2. Verilənlərin yeni blokunu almaq üçün əvvəlki iki məlumat daycesti konkatenasiya olunur (birləşdirilir);
3. Yeni verilənlər bloku son məlumat daycesti almaq üçün yenidən heş-funksiya ilə emal olunur;
4. İmzalayanın məxfi açarından istifadə etməklə son məlumat daycestini şifrləməklə rəqəm imzası formalaşdırılır.

Məlumatı alan onun həqiqiliyini, özünün məlumatı üçün məlumat daycestini hesablayıb onu göndərənin təqdim etdiyi digər məlumatın daycestinə birləşdirərək və nəticə üçün daycesti hesablayaraq yoxlaya bilər. Əgər yenidən hesablanmış heş-qiymət şifrlənmiş ikiqat imza ilə üst-üstə düşürsə, alan tərəf məlumatın həqiqiliyinə inana bilər.

3. Kriptoqrafik heş-funksiyalar

3.1. Heş-funksiyaların növləri

Heş-funksiyaların statistik eksperimentlərin aparılması, məntiqi qurğuların testdən keçirilməsi, sürətli axtarış alqoritmlərinin qurulması, verilənlər bazalarında yazıların tamlığının yoxlanması, saxlama və ötürülmə zamanı parolların mühafizəsi, imzanın formalaşdırılması zamanı məlumatın sıxılmış obrazının alınması və s. zamanı müxtəlif tətbiqləri var. Məsələn, müxtəlif uzunluqlu məlumatların böyük siyahılarında lazımi məlumatın sürətli axtarışını həyata keçirmək üçün bir-biri ilə məlumatları deyil, onların qısa heş-qiymətlərini müqayisə etmək əlverişlidir. Belə heş-funksiyalara əsas tələb, arqumentin qiyməti təsadüfi seçildikdə, onun qiymətlərinin müntəzəm paylanmasıdır.

Elementlərini məlumat adlandıracağımız çoxluğu X ilə işarə edək. Adətən məlumat hər hansı əlifbanın (çox vaxt ikilik əlifbanın) simvolları ardıcıllığından ibarət olur. Tutaq ki, Y qeyd (fiksə) edilmiş uzunluqlu ikilik vektorların çoxluğudur.

İxtiyari $h: X \to Y$ funksiyası asanlıqla hesablanırsa və ixtiyari M məlumatı üçün $h(M)$ qiyməti qeyd olunmuş bit uzunluğuna malikdirsə, heş-funksiya adlanır [3].

Bir qayda olaraq mümkün məlumatların sayı heş-funksiyanın mümkün qiymətlərinin sayından olduqca çox olur. Buna görə də heş-funksiyanın hər bir verilmiş qiymətinə uyğun məlumatlar çox ola bilər. Qeyd edək ki, məlumatların təsadüfi və bərabər ehtimallı seçilməsi halında heş-funksiyanın qiymətlərinin müntəzəm paylanması şərti heş-funksiyanın hər bir qiyməti üçün eyni sayda uyğun məlumatın olmasına ekvivalentdir.

Kriptoqrafiyada heş-funksiyalar aşağıdakı məsələlərin həlli üçün tətbiq edilir:

- verilənlərin ötürülməsi və saxlanması zamanı onların tamlığına nəzarət sisteminin qurulması;
- verilənlərin mənbəyinin autentifikasiyası.

Kriptoqrafiyada istifadə olunan heş-funksiyalar aşağıdakı tələblərə cavab verməlidirlər:

– heş-funksiya biristiqamətli olmalıdır;

– heş-funksiya birqiymətli (collision free) olmalıdır

Güclü və zəif birqiymətlilik fərqləndirilir. Zəif birqiymətlilik halında x-in verilmiş qiymətinə görə, praktik olaraq x-dən fərqli elə y qiyməti tapmaq mümkün deyil ki, $H(x)=H(y)$ olsun. Güclü birqiymətlilik halında isə elə istənilən x və y tapmaq mümkün deyil ki, onlar üçün $H(x)=H(y)$ olsun. Real hesablama sistemlərində söhbət zəif birqiymətlilikdən gedir, çünki ilkin verilənlər üçün variantların sayı adətən heş-funksiyanın mümkün qiymətləri çoxluğundan olduqca böyükdür.

Kriptoqrafik heş-funksiyaların iki mühüm növü – açarlı və açarsız heş-funksiyalar xüsusi olaraq fərqləndirilir [45]. Birincilər simmetrik açarlı sistemlərdə tətbiq olunurlar. Açarlı heş-funksiyaları (Message Authentication Code, MAC) məlumatın autentifikasiyası kodları adlandırırlar. Məlumatın autentifikasiyası kodları əlavə vasitələr cəlb etmədən, istifadəçiləri bir-birinə etibar edən sistemlərdə həm verilənlərin mənbəyinin düzgünlüyünə, həm də verilənlərin tamlığına zəmanət verməyə imkan verirlər.

Açarsız heş-funksiyaları səhvlərin aşkarlanması kodları (Modification Detection Code, və ya Manipulation Detection Code, MDC) adlandırırlar. Onlar əlavə vasitələrlə (məsələn, şifrləmə, mühafizəli kanaldan istifadə və ya rəqəm imzası) verilənlərin tamlığına zəmanət verməyə imkan verir. Bu heş-funksiyalardan həm istifadəçiləri bir-birinə etibar edən sistemlərdə, həm də istifadəçiləri bir-birinə etibar etməyən sistemlərdə istifadə etmək olar.

Bir qayda olaraq heş-funksiyalar birpilləli sıxıcı funksiyaların əsasında qurulurlar [22, 50, 77]; burada, x_i $(i=1,2)$ və y– uzunluqları üyğun olaraq m və n olan ikilik vektorlardır, həm də n heş-funksiyaların uzunluğudur. $H(M)$ qiymətini almaq üçün M məlumatı əvvəlcə uzunluğu m olan bloklara bölünür (əgər məlumatın uzunluğu m-ə bölünmürsə, axırıncı

blok tam olana qədər hər hansı xüsusi şəkildə doldurulur). M_1, M_2, ... ,M_n bloklarına aşağıdakı hesablama proseduru tətbiq olunur:

$H_0=v$

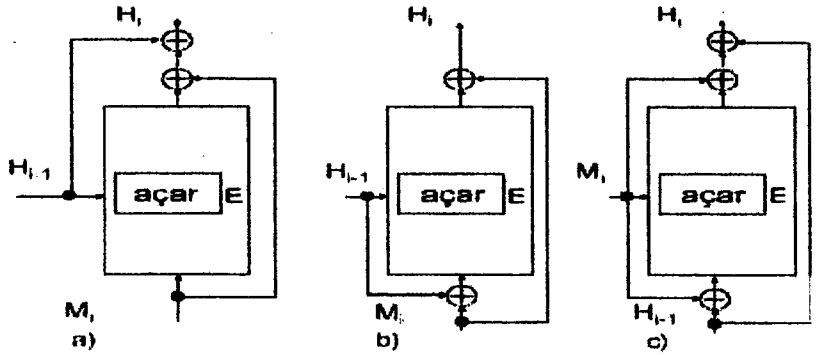
$H_i=f(M_i, H_{i-1}), \ i=1,...,N$

$H(M)=H_n$

burada- H_0 hər hansı qeyd olunmuş başlanğıc vektordur. Əgər f funksiyası açardan asılıdırsa, bu vektoru sıfır vektor götürmək olar. Əgər f funksiyası açardan asılı deyilsə, qısa məlumatların saf-çürük edilməsini istisna etmək üçün (heş-funksiyanın tərsinin tapılması cəhdi zamanı) bu vektoru vaxtı, zamanı, məlumatın nömrəsini göstərən fraqmentlərdən təşkil etmək olar. f funksiyası qismində çox vaxt blok şifrləri istifadə edilir. 128-bitlik blok şifrləri əsasında qurulmuş çox sayda müxtəlif heş funksiyaların davamlılığının analizi göstərmişdir ki, aşağıdakı cədvəldə göstərilən 12 iterativ düsturla verilən funksiyalar davamlıdırlar [77]:

1	$H_i=E_{H_{i-1}}(M_i) \ M_i$
2	$H_i=E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
3	$H_i=E_{H_{i-1}}(M_i) \oplus M_i \oplus H_{i-1}$
4	$H_i=E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i$
5	$H_i=E_{M_{i-1}}(H_{i-1}) \oplus H_{i-1}$
6	$H_i=E_{M_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
7	$H_i=E_{M_{i-1}}(H_{i-1}) \oplus M_i \oplus H_{i-1}$
8	$H_i=E_{M_{i-1}}(M_i \oplus H_{i-1}) \oplus H_{i-1}$
9	$H_i=E_{M_i \oplus H_{i-1}}(M_i) \oplus M_i$
10	$H_i=E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus H_{i-1}$
11	$H_i=E_{M_i \oplus H_{i-1}}(M_i) \oplus H_{i-1}$
12	$H_i=E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus M_i$

Cədvəldəki üçüncü (a), dördüncü (b), altıncı (c) iterativ düsturun strukturunun qrafik təsviri şəkil 3.1-də təqdim olunur.



Şəkil 3.1 Heş-funksiyaların davamlı sxemləri

Adətən 64-bitlik blok şifrləri yaradılır, buna görə də m/2-bitlik şifrlərin əsasında m-bitlik heş-funksiyaların qurulması üçün xüsusi sxemlər təklif olunmuşdur [77]. Belə iterativ heş-funksiyaların strukturu daha mürəkkəbdir və müəyyən spesifik hücumlara baxmaq lazım gəlir.

Bəzi heş-funksiyalar cədvəldə göstərilib. Ən məhşur heş-funksiyalar MD5, SHA, RİPEMD, TİGER-dir.

Heş-funksiya	Heş-qiymətin uzunluğu, bit
Whirlpool	512
SHA-2	256, 384, 512
QOST 34.11-95	256
HAVAL	128, 160, 192, 256
SHA-1	160
RIPEMD	128, 160
MD5	128
MD4	128
UMAC	128, 64
Rijndael CBC–MAC	128
QOST 28147-89 (rejim 4)	64

MD5– heş-funksiyalar alqoritmləri ailəsi MD-nin nümayəndəsi; R. Rivest tərəfindən 1991-ci ildə təklif

olunmuşdur; ixtiyari uzunluqlu informasiya ardıcıllığını 128-bit uzunluqda heş-qiymətə çevirir [84, 85].

RİPEMD– RİPE (Race Integrity Primitives Evaluation) Avropa proyekti çərçivəsində işlənmişdir; MD4 alqoritminin modifikasiyasıdır; ixtiyari uzunluqlu informasiya ardıcıllığını 128 bit (RIPEMD-128) və ya 160 bit (RIPEMD-160) uzunluqda heş-qiymətə çevirir.

TİGER– R. Anderson və E.Biham tərəfindən işlənmişdir. 64-mərtəbəli prosessorlarda realizə üçün nəzərdə tutulub; ixtiyari uzunluqlu məlumatı 192 bit uzunluqda heş-qiymətə çevirir.

"1234567890" sətrinin müxtəlif heş-funksiyalardan alınmış heş-qiymətləri aşağıdakı cədvəldə 16-lıq say sistemində göstərilib.

Alqoritm	**"1234567890" sətrinin heş -qiyməti**
MD2	3853522A2E67FC5EA57BAE1575A3107
MD4	85B196C3E39457D91CAB9C905F9A11C0
MD5	E807F1FCF82D132F9BB018CA6738A19F
SHA1	01B307ACBA4F54F55AAFC33BB06BBBF6CA803E9A
Ripe160	9D752DAA3FB4DF29837088E1E5A1ACF74932E074

3.2. SHA-1 heş-funksiyası

Təhlükəsiz heşləmə funksiyası SHA-1 (Secure Hash Alqorithm) 1992-ci ildə ABŞ-da DSS standartında müəyyən edilən rəqəm imzası alqoritmində istifadə etmək üçün standart kimi qəbul olunmuşdur [62]. *M* məlumatı daxil edildikdə alqoritm 160-bitlik çıxış məlumatı verir. Məlumatın daycesti (Message Digest) adlanan bu verilən rəqəm imzası yaradılarkən istifadə olunur. Alqoritmin işinə ətraflı nəzər salaq.

Əvvəlcə ilkin məlumata elə əlavələr olunur ki, onun uzunluğu 512-yə bölünsün. Məlumatın uzunluğu 512-yə

bölünsə belə, əlavələr yenə də edilir. Əlavə etmə belə baş verir: vahid əlavə olunur, sonra 64-bit qalana qədər sıfır əlavə olunur, daha sonra ilkin məlumatın uzunluğunun 64-bitlik təsviri əlavə olunur.

Beş 32-bitlik dəyişən aşağıdakı 16-lıq sabitlərlə ilkin qiymətlər alır:

A = 67452301
B = EFCDAB89
C = 98BADCFE
D = 10325476
E = C3D2E1F0

Daha sonra bu beş dəyişən uyğun olaraq yeni a, b, c, d, və e dəyişənlərinə köçürülür.

Baş dövr psevdokodda aşağıdakı çox sadə şəkildə təsvir oluna bilər:

```
for(t=0; t<80; t++){
    Temp=(a<<<5) + ft(b,c,d) +e +Wt+Kt;
        e=d; d=c; c=b<<<30; b=a; a=temp;
          }
```

burada, <<<- sola dövri sürüşdürmə operatorudur;

K_t –a aşağıdakı düsturlarla müəyyən edilən 16-lıq sabitlərdir;

$$K_t = \begin{cases} 5A827999, & t = 0..19 \\ 6ED9EBA1, & t = 20..39 \\ 8F1BBCDC, & t = 40..59 \\ CA62C1D6, & t = 60..79 \end{cases}$$

$f_t(x, y, z)$ funksiyaları aşağıdakı düsturlarla verilir:

$$f_t(x, y, z) = \begin{cases} X \wedge Y \vee \neg X \wedge Z, & t = 0..19 \\ X \oplus Y \oplus Z, & t = 20..39, 60..79 \\ X \wedge Y \vee X \wedge Z \vee Y \wedge Z, & t = 40..59 \end{cases}$$

W_t qiymətləri genişləndirilmiş məlumatın 512-bitlik bloklarının 32-bitlik altbloklarından aşağıdakı qaydalarla alınır:

$$f_t(x, y, z) = \begin{cases} M_t, & t = 0..19 \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< 1, & t = 16..79 \end{cases}$$

Baş dövr qurtardıqdan sonra a, b, c, d, və e qiymətləri uyğun olaraq A, B, C, D və E-nin qiymətləri ilə toplanır və genişləndirilmiş məlumatın növbəti 512-bitlk blokuna keçirlər. Heş-funksiyanın çıxış qiyməti A, B, C, D və E qiymətlərinin konkatenasiyasından (ardıcıl birləşdirilməsindən) ibarət olur.

AES layihəsinin işlənməsi gedişində kriptoqrafik alqoritmlərin davamlılığına irəli sürülmüş yeni tələblərə görə üç əsas davamlılıq səviyyəsi nəzərdə tutulur: 2^{128}, 2^{192} və 2^{256} (128, 192, və 256 bit uzunluğunda açarlar). Belə mühafizə səviyyəsini təmin etmək üçün heş-qiymətin minimal uzunluğu 256, 384 və 512 bit olmalıdır. SHA-1 alqoritminə hazırki dövrə qədər heç bir analitik hücum tapılmadığına görə, onu 256, 384 və 512 bit uzunluğunda heş-qiymətin alınması imkanına qədər inkişaf etdirmək qərara alınmışdır. SHA-2 alqoritmi uyğun olaraq üç alqoritmə SHA-256, SHA-384 və SHA-512 alqoritmlərinə bölünür.

3.3. Heş-funksiyalara mümkün hücumlar

Heş-funksiyalara yönəlmiş bütün hücumları iki qrupa bölmək olar:

- alqoritmdən asılı olmayan hücumlar;
- çevirmələr alqoritminin zəifliklərinə əsaslanan (analitik) hücumlar;

Alqoritmdən asılı olmayan hücumlara "kobud güc" hücümu, "ad günü" metodu ilə hücum, açarların tam saf-çürük edilməsi aid edilir. Belə hücumlara qarşı bütün alqoritmlər zəifliyə malikdir, onlardan yeganə qaçış yolu- biristiqamətli və ya kolliziyasız heş-funksiyalarda heş-qiymətin uzunluğunu, MAC-funksiyalarında isə məxfi açarın uzunluğunu artırmaqdır.

Analitik hücumlara "ortada görüş", blokun korreksiyası ilə hücum, qeyd olunmuş nöqtə ilə hücum, baza şifrləməsi alqoritminə hücum, differensial analiz hücumu aid edilir.

Saxta məlumat yaratmaq məqsədi ilə istənilən heş-funksiyaya tətbiq oluna bilən ən sadə hücum aşağıdakılardan ibarətdir. Bədniyyətli müəyyən (r_1) sayda məlumatlar

generasiya edə bilər, onların heş-qiymətlərini hesablayıb alınan qiymətləri əvvəllər ötürülmüş (r_2) sayda məlumatların müəyyən çoxluğundan məlum heş-qiymətləri ilə tutuşdura bilər. Heç olmasa bir üst-üstə düşmə alınsa, hücum uğurlu olacaq. Uğur ehtimalı R-i "ad günü" paradoksunun əsasında qiymətləndirmək olar. Məlumdur ki, bu ehtimal

$$R = 1 - e^{-\frac{r_1 r_2}{2}}$$

düsturu ilə hesablanır, burada n- heş-qiymətin uzunluğu, e natural loqarifmlərin əsasıdır. Ehtimalın qiyməti $r_1=r_2=2^{n/2}$ olduqda ən böyükdür. Bu halda ehtimalın qiyməti təqribən 0,63-ə bərabərdir.

"Ad günü" paradoksu aşağıdakı sualın cavabından ibarətdir. Təsadüfi seçilmiş qrupda neçə nəfər olmalıdır ki, bu qrupda ad günü eyni olan iki nəfərin olması ehtimalı 0,5-ə bərabər olsun. Sualın cavabına görə qrupda cəmisi 23 nəfər olmalıdır. "Ad günü" paradoksuna görə, N elementi olan çoxluqdan həcmi $\sqrt{N}$ ilə müqayisə olunan seçmə varsa, seçmədə iki eyni elementin olması ehtimalı $^1/_2$ ilə müqayisə olunandır. Bu paradoks göstərir ki, açıq mətnin təsadüfi seçilməsi halında heş-qiymətlərin təkrarlanmasını almaq üçün orta hesabla $\sqrt{N}$ sayda açıq mətn götürmək kifayətdir, burada N–nəzəri cəhətdən rast gəlinə bilən heş-qiymətlərin ümumi sayıdır. Beləliklə, uzunluğu 64-bit olan heş-funksiyanın ($N=2^{64}$) kolliziyasını tapmaq üçün $2^{32} \approx 4*10^9$ sayda heş-qiyməti hesablamaq kifayətdir.

Heş-funksiyaların qurulmasının iterativ üsulu onun tərsinin tapılması və ya kolliziyanın qurulması zamanı "ortada görüş" metodundan istifadə etməyə imkan verir [81]. "Ortada görüş" hücumu ad günü metodu ilə hücumun modifikasiyasıdır, əgər dövr (tsikl) funksiyası aralıq X qiyməti və ya məlumat bloku M_i üçün inversiya olunandırsa, dövri strukturlu heş-funksiya üçün istifadə olunur. Bu hücum çətinliyinə görə ad günü hücumu ilə yanaşı qoyula bilər. Bu təhlükədən müdafiə üçün adətən

məlumatın sonuna nəzarət cəmi və məlumatın uzunluğu bloku əlavə olunur.

Əsasında heş-funksiyanın qurulduğu sxemlərin zəifliklərindən istifadə edən hücumlar da mümkündür [51, 52]. Məsələn, blokla şifrlənmə alqoritminə əsaslanan heş funksiyaların kolliziyalarını qurmaq üçün zəif açarların varlığından və ya əlavə etmənin xassəsindən, tərpənməz nöqtələrin varlığından, açarların kolliziyasından və s. istifadə etmək olar.

Məlum olduğu kimi, bir çox hallarda heş-funksiyalar birpilləli sıxıcı funksiyaların əsasında qurulur. Buna görə də heş-funksiyalara hücumlarla uyğun birpilləli sıxıcı funksiyaya hücum arasında sıx əlaqə var.

Blokun korreksiyası ilə hücum, o vaxt istifadə olunur ki, hücum edənə məlumat məlumdur və o, heş-funksiyanın qiymətini dəyişdirmədən onda bir və ya bir neçə bloku dəyişdirmək istəyir. MD5-in bir dövrü bu hücuma davamsızdır. Hücum edən M_i məlumat blokunu götürüb (32 bit olmaqla 16 söz), 11 sözü dəyişməz saxlayır, bir sözü dəyişdirir və qalan 4 sözü hesablayır. Nəticədə M_i ilə eyni heş-qiymətə inikas olunan M_i' bloku alınır. MD5-in tam versiyası (4 dövrlü) bu hücuma davamlıdır.

Diferensial analiz dövr funksiyasının və ya sıxıcı funksiyanın giriş və çıxış qiymətləri arasında asılılığı statistik anomaliyaların müəyyən edilməsi məqsədi ilə tədqiq edir. Diferensial analiz heş-funksiyalar daxil olmaqla müxtəlif kriptosistemlərə tətbiq olunur [51, 52].

Tərpənməz nöqtə hücumu o halda tətbiq oluna bilər ki, dövr funksiyası f-in bir və ya bir neçə tərpənməz nöqtəsi olsun. M_i məlumat bloku $f(X_i, M_i)=X_i$ bərabərliyini ödəyirsə, tərpənməz nöqtə adlanır. Beləliklə, M məlumatına heş-qiyməti dəyişdirmədən M_i blokunu əlavə etmək və ya silmək olar. Belə hücumlardan mühafizə üçün məlumatın uzunluğu hesablanır və məlumatın sonuna əlavə olunur.

4. Rəqəm imzası sxemlərinin təhlükəsizliyi

4.1. İmza sxemlərinin davamlılığı

Kriptosxemin davamlılığı- onun sındırılılmasına yönəlmiş bütün mümkün cəhdlərə qarşı durmaq qabiliyyətidir. Şifrin davamlılığı anlayışı kriptoqrafiyada mərkəzi anlayış olsa da, kriptodavamlılığın miqdari qiymətləndirilməsi indiyədək həll olunmamış problemdir. Kriptosistemlərin davamlılığı çevirmə alqoritmlərinin çətinliyindən, açarın uzunluğundan, daha dəqiq deyilsə, açar fəzasının həcmindən, realizə metodundan (aparat, proqram; proqram realizəsi zamanı əlavə olaraq viruslardan, əlfəcinlərdən və s. mühafizə zəruridir) və s. asılıdır.

Kriptosistemlərin etibarlılığının analizi zamanı həmişə Kirxhof prinsipindən çıxış edərək qəbul etmək lazımdır ki, düşmən tətbiq olunan kriptoalqoritm haqqında bütün informasiyaya malikdir, ona yalnız istifadə olunan real açar məlum deyil. Buna görə kriptosistemin yaradılması və ya onun davamlılığının analizi zamanı düşmənin imkanlarını aşağı qiymətləndirmək lazım deyil, onu yüksək qiymətləndirmək daha yaxşı olardı.

Davamlılığın iki növü var: nəzəri və praktiki. Bu konsepsiyanı K.Şennon elmi kriptoqrafiyanın başlanğıcı hesab olunan klassik işində təklif etmişdir [40]. Praktiki davamlılıq termini tərifin riyazi cəhətdən ciddi olmadığını bildirmir. Praktiki davamlılığın ölçüsü kimi kənar şəxs tərəfindən məxfi informasiyanın müəyyən edilməsi üçün yerinə yetirilməli olan əməliyyatların sayı və yaxud vaxt çətinliyi və ya bu xarakteristikaların bütün açıq mətnlər fəzası üzərində orta qiymətləri götürülür.

Nəzəri davamlılıq kriptosistemin müəyyən formal obyektlə modelləşdirildiyinə və bu model üçün kriptosistemin kənar şəxslər tərəfindən sındırılmasının qeyri-mümkünlüyünün müəyyən şərtlərinin formulə edildiyinə əsaslanır. Kriptoqrafik sxemlərin nəzəri davamlılığının da iki növü var: nəzəri-informasiya və nəzəri-çətinlik. Nəzəri-informasiya davamlılığı o

deməkdir ki, verilmiş hücum nəticəsində düşmənin aldığı informasiya verilmiş təhlükənin həyata keçirilməsi üçün kifayət deyil. Kriptosxemlərin nəzəri-informasiya davamlılığının tədqiqinin əsas məzmunu, məxfi açarların uzunluğunun və ya sxemin onlara analoji elementlərinin aşağı sərhədlərinin isbatından ibarətdir. Bütün hallarda bu sərhədlər kifayət qədər yüksək olur ki, bu da belə sxemlərin praktik tətbiqləri yolunda əsas maneə olur. Bundan başqa aydındır ki, açıq açarlı kriptoqrafik sistemlər prinsipcə belə davamlılığa malik ola bilməzlər.

Əgər verilmiş hücumun əsasında verilmiş təhlükənin həyata keçirilməsi prinsipcə mümkündürsə, ancaq hesablama cəhətdən çətin məsələdirsə, nəzəri-çətinlik davamlılığı haqqında danışırlar. İdeal halda parametrlərin konkret qiymətlərində konkret kriptosxemlərə baxmaq (yaxşı olardı) və bu sxemin açılmasının istənilən alqoritminin verilən saydan az olmayan əməliyyat yerinə yetirməli olduğunu isbat etmək arzu olunandır. Lakin hesablama çətinliyi hesablayıcı modelindən asılıdır və müəyyən sabit dəqiqliyi ilə təyin edilir.

Hazırda nəzəri-çətinlik yanaşması kriptoqrafik sxemlərin davamlılığını yalnız hər hansı isbat olunmamış fərziyyələri cəlb etməklə isbat etməyə imkan verir. Tədqiqatlar nəticəsində müəyyən edilmişdir ki, davamlı kriptoqrafik sxemlərin çoxunun varlığı üçün zəruri və kafi şərt biristiqamətli funksiyaların varlığı haqqında fərziyyədir.

Buna görə hesablamaların çətinliyi nəzəriyyəsi yalnız kütləvi məsələləri, yəni fərdi məsələlərin sonsuz ailəsini nəzərdən keçirir. RSA imza sxemi halında modulun uzunluğu sonsuzluğa can atan sxemlərin sonsuz ardıcıllığına baxmaq və bu zaman imzanı saxtalaşdırmanın istənilən alqoritminin yerinə yetirməli olduğu istənilən əməliyyatların sayının necə artmasını tətqiq etmək olardı. Başqa sözlə, imzanı saxtalaşdırma məsələsinin çətinliyinin aşağı sərhəddini isbat etmək lazımdır. Bu zaman sərhəddin kifayət qədər yüksək olması tələb olunur (məsələn, superpolinomial). Konkret məsələlərin çətinliyinin kifayət qədər yüksək aşağı qiymətlərinin isbatı çətinlik

nəzəriyyəsinin kriptoqrafiyada əsəs məsələsidir. Lakin bu nəzəriyyənin müasir vəziyyəti trivial NP sinfindən konkret məsələlərin çətinliyinin qeyri aşağı qiymətlərini isbat etməyə imkan vermir.

Nəzəri-çətinlik istiqaməti çərçivəsində həmçinin konkret məsələlərin hesablama çətinliyi fərziyyələri əsasında davamlı kriptoqrafik sxemlərin qurulması üsullarına da baxırlar. Bu zaman hər əlahiddə məsələnin spesifik xüsusiyyətlərindən istifadə edildiyinə görə alınmış sxemlər daha ümumi fərziyyələr əsasında qurulmuş sxemlərdən səmərəli olacaq. Bu yanaşma nəzəri-ədədi məsələlərə- diskret loqarifmləmə və faktorizasiya məsələlərinə daha uğurla tətbiq olunur. Diskret loqarifmləmənin sadə modula görə, mürəkkəb modula görə, elliptik əyrilər üzərində olan müxtəlif növlərinə baxılır. Faktorizasiya məsələsinə gəlincə onunla əlaqəsi axıradək aydınlaşdırılmamış iki məsələdən– sadə vuruqları naməlum mürəkkəb modula görə verilmiş dərəcədən köklərin hesablanması məsələsindən və həmin şərt daxilində bu modula görə verilən ədədin kvadratik çıxıq olmasının müəyyənləşdirilməsi məsələsindən biri istifadə olunur.

4.2. Diskret loqarifmləmə məsələsi

Diskret loqarifmləmə məsələsinin çətinliyinə əsaslanan rəqəm imzası sxemlərinin geniş yayılmasını nəzərə alaraq aşağıda qısa xülasə verilir.

F_p sadə meydanında diskret loqarifmləmə məsələsi belə formulə edilir: $a \in F_p$ primitiv elementdir və $b \in F_p^*$, elə yeganə x, $0 \le x \le p-2$ tam ədədi tapmaq lazımdır ki, $a^x \equiv b \pmod p$ olsun.

Kriptoqrafiyada aşağıdakı qruplarda diskret loqarifmləmə məsələsinə baxılır:

- $GF(p)$ sadə tərtibli sonlu meydanın multiplikativ qrupu;
- $GF(2^n)$ sonlu meydanının multiplikativ qrupu;
- sonlu meydan üzərində elliptik əyrilərin nöqtələri qrupu.

Hazırda sadə tərtibli sonlu meydanlarda diskret loqarifmləmə məsələsinin həlli üçün üç üsul: xətti qəfəs, Qauss tam ədədləri sxemi və ədədi meydanın qəfəsi üsulları var. Ədədi meydanın qəfəsi metodu daha sürətlidir və evristik $e^{((1.923+o(1))(\ln n)^{1/3}(\ln\ln n)^{2/3}}$ qiymətləndirilməsinə malikdir [41].

p-1 kiçik sadə vuruqlara ayrıldıqda *GF(p)* meydanında diskret loqarifmin sürətli hesablanması üçün Poliq-Hellman [4] üsulu mövcuddur. Buna görə də *p* elə seçilir ki, *p-1*-in heç olmasa bir böyük sadə böləni olsun.

Alqoritmlərin realizəsi üçün bir sıra üstünlüklərə malik $GF(2^n)$ sonlu meydanlarında diskret loqarifmləri hesablamaq üçün Koppersmit alqoritmi təklif olunmuşdur [4, 13]. Bu alqoritm bir qədər uzunmüddətli öncədən hesablama mərhələsindən istifadə etsə də, diskret loqarifmləri $GF^*(2^k)$, $k<520$ olduqda səmərəli hesablayır. Buna görə də bu meydanlar artıq kriptoqrafik sxemlər üçün yararlı deyil. Diskret loqarifmləmə alqoritmlərinin Koppersmit alqoritminədək hərtərəfli xülasəsi və geniş ədəbiyyat siyahısını [66] -də tapmaq olar.

Diskret loqarifmləmə məsələsinin çətinliyinin qiymətləndirilməsi *p sadə* ədədinin (onun düzgün seçilməsi şərtində) ikilik yazılışının uzunluğundan asılılı olaraq cədvəldə göstərilmişdir:

p-nin uzunluğu (bit)	x açarını hesablama çətinliyi	Alqoritmin istifadə etdiyi yaddaş (bit)	10^9 əməl/san tipli kompüterdə məsələnin həll vaxtı
128	$2*10^{12}$	$7*10^8$	Bir neçə dəqiqə
200	10^{16}	10^8	Bir neçə ay
256	$9*10^{17}$	10^9	Bir neçə on illər
512	$4*10^{24}$	$3*10^{12}$	100 ildən çox arasıkəsilməz iş
1024	10^{34}	10^{17}	
1500	10^{41}	$8*10^{20}$	
2000	$7*10^{47}$	10^{24}	
2200	10^{50}	10^{25}	

Diskret loqarifmləmə məsələsi vuruqlara ayırma ilə sıx əlaqədədir. Diskret loqarifmləmə məsələsi həll olunsa, ədədi

sadə vuruqlarına ayırmaq olar (bunun tərsinin doğruluğu hələlik isbat olunmayıb).

Elliptik əyrilər üçün diskret loqarifmləmə məsələsinin həlli üsullarına gəlincə, kriptoqrafiyada istifadəsi məsləhət görülməyən elliptik əyrilərin məhdud sinfi istisna olmaqla, hələlik hətta subeksponensial üsul belə təklif olunmayıb.

4.3. Rəqəm imzası sxemlərinin təhlükəsizliyi

Rəqəm imzası sxemlərində üç kriptoqrafik alqoritm istifadə olunur: məxfi açarla imzanın formalaşdırılması alqoritmi, açıq açarla imzanın yoxlanması alqoritmi və imzalanan məlumatdan heş-funksiyanın hesablanması alqoritmi. Rəqəm imzasının riyazi əsaslarına həmçinin məxfi və açıq açarların formalaşdırılması alqoritmlərini də aid etmək olar. Buna görə hesab etmək olar ki, rəqəm imzası sxemlərinin təhlükəsizliyi aşağıdakı fərziyyələrə əsaslanır:

- rəqəm imzası sxemində istifadə olunan qrupda diskret loqarifmələmə məsələsi mürəkkəbdir, bu məsələnin həlli açarın açılmasına gətirib çıxarır;
- təsadüfi ədədlər generatorunun entropiyası açarlar generatorunun entropiyasından aşağı deyil, əks halda imzanın davamlılığı hesablanmış qiymətlə müqayisədə aşağı düşəcək;
- açarın fəaliyyət müddəti ərzində iki təsadüfi ədədin təsadüfi emalı nəzərə alınmayacaq dərəcədə kiçikdir, əks halda sxemlərin aşağı çətinliyə malik açılmasına ümid etmək olar;
- heş-funksiya hesablama cəhətdən bərpaolunmazdır, əks halda imzalanmış məlumatı başqası ilə (qəsdən) dəyişdirmək olar;
- heş-funksiyanın kolliziyaları çətin hesablanandır, əks halda kolliziya yaradan məlumatlar cütü hazırlamaq və imzadan sonra imzalanmış məlumatı digəri ilə əvəz etmək olar.

Hesab etmək olar ki, imzanın davamlılığı diskret loqarifmləmənin, istifadə olunan təsadüfi ədədin tapılmasının, heş-funksiyanın kolliziyasının hesablanmasının, heş-

funksiyanın tərsinin tapılmasının çətinliklərinin minimimunu aşmır. Qeyd edək ki, maksimal çətinlik bircinsliyi prinsipinə görə kriptosistemin təhlükəsizliyinin əsasına qoyulmuş və istənilən birinin kriptosistemin təhlükəsizliyini poza bildiyi məsələlərin sayı minimal olmalıdır [36]. Aydındır ki, təhlükəsizliyi yalnız bir məsələyə əsaslanan sistemlər optimaldır.

Rəqəm imzası sxeminin davamlılığı təhlükə-hücum cütünə nəzərən təyin olunur. Verilən təhlükənin həyata keçirilməsi ehtimalı nəzərdən atılacaq qədər kiçik deyilsə, sxem baxılan təhlükə üçün davamsız hesab olunur.

Rəqəm imzası sxemlərinə hücum növlərinin Qoldvasser, Mikali və Rivestin [65] təklif etdiyi təsnifatına baxaq. Hücumlar, hər sonrakı əvvəlkindən güclü olmaqla sadalanırlar.

Məlum açıq açarın əsasında hücum (key-only attack)- bütün mümkün hücumlardan ən zəifidir. Aydındır ki, praktik olaraq düşmən həmişə belə hücumlar edə bilər.

Məlum məlumatlar əsasında hücum (known-message attack)- düşmənin ixtiyarında müəyyən sayda imzalanmış məlumatlar var. Düşmən bu məlumatların seçiminə heç bir təsir edə bilməz.

Məlumatların seçilməsi əsasında sadə hücum (generic chosen-message attack)- Düşmənin müəyyən sayda imzalanmış sənədləri seçmə imkanı var. Fərz olunur ki, açıq açar düşmənə, o seçim edəndən sonra məlum olur.

Məlumatların seçilməsi əsasında istiqamətli hücum (directed chosen-message attack)- İmzalanmış məlumatları seçərkən düşmən açıq açarı bilir.

Məlumatların seçilməsi əsasında adaptiv hücum (adaptive chosen-message attack)- Düşmən açıq açarı və hər addımda ondan əvvəl seçilmiş bütün məlumatların imzasını bilərək imzalanmış məlumatları seçir.

Hər bir hücum müəyyən məqsədin əldə olunmasına yönəlir. Rəqəm imzası sxemi üçün təhlükə sxemin sındırılması və ya imzanın saxtalaşdırılmasıdır. Rəqəm imzası üçün

aşağıdakı təhlükə növlərini ayırmaq olar (güclərinin artması sırası ilə) [22]:

Ekzistensial saxtalaşdırma (existential forgery)- elə keçirilmiş məlumatdan fərqli hər hansı məlumat üçün imzanın yaradılması. Düşmən məlumatın seçiminə təsir edə bilmir. Məlumat təsadüfi və ya mənasız ola bilər.

Selektiv saxtalaşdırma (selective forgery)- əvvəlcədən seçilmiş (hücuma qədər) məlumat üçün imzanın yaradılması.

Universal saxtalaşdırma (universal forgery)- düşmən funksional cəhətdən imzanın yaradılması alqoritminə ekvivalent olan və məxfi açarı bilməyi tələb etməyən alqoritm tapır.

Tam açılma (total break)- məxfi açarın hesablanması. Hesablanmış məxfi açar istənilən məlumat üçün imza yaratma imkanı verir. O, açıq açara cüt olan məxfi açardan fərqli də ola bilər.

Ən güclü hücumların əsasında ən zəif təhlükələrə qarşı yönəlmiş hücumlara, yəni ekzistensial saxtalaşdırmaya yönəlmiş məlumatın seçilməsi ilə adaptiv hücumlara davamlı sxemlər ən etibarlı hesab olunurlar. Belə sxemlərin varlığı biristiqamətli funksiyaların varlığına ekvivalentdir.

4.4. Rəqəm imzası standartları

Rəqəm imzası standartı imzanın yaradılması və yoxlanması alqoritmlərinin kifayət qədər təfsilatla təsvirindən ibarətdir. Standart rəqəm imzası alqoritminin kriptoqrafik davamlılığını təmin edir. Bir sıra vacib detallar (məsələn, açarların paylanması üsulu, təsadüfi ədədlərin generasiyası və s.) standartlarda qeyd olunmaya da bilər. Bu hal ona gətirib çıxara bilər ki, rəqəm imzası funksiyalarını həyata keçirən, hər biri eyni rəqəm imzası standartına uyğun olan müxtəlif rəqəm imzası vasitələri bir araya gələ bilməsin. Rəqəm imzasının faktiki olaraq əsas komponentlərindən biri olduğu tətbiqi sferalar (bank sistemləri, elektron sənəd dövriyyəsi, elektron kommersiya və s.) getdikcə daha qlobal və inteqrə olunmuş

olur. Buna görə də sistemlərin uyuşanlığı məsələləri (o cümlədən, rəqəm imzası vasitələrinin) daha da aktuallaşır. Müasir beynəlxalq standartlar və funksional spesifikasiyalar əsasında rəqəm imzasının milli infrastrukturunun qurulması onların analoji xarici sistemlərlə uyuşmasının (yola getməsinin) şərtlərindən biridir. Standartın kriproqrafik xassələr üzrə parametrləri elə seçilir ki, standarta uyğun gələn kriptoqrafik alqoritmlərin standartlaşdırılması üzrə səylər beynəlxalq və milli səviyyələrdə uzlaşdırılır.

İnformasiya texnologiyaları sahəsində standartların, o cümlədən rəqəm imzası standartlarının işlənməsində bir sıra beynəlxalq və milli təşkilatların– ISO, IEEE, IETF, NIST, ANSI kimi təşkilatların xüsusi rolu var. Rəqəm imzası standartları haqqında aydın təsəvvür yaratmaq məqsədi ilə ISO-nun rəqəm imzası ilə əlaqədar standartları aşağıdakı cədvəldə göstərilib:

ISO 9796	Məlumatı bərpa edən rəqəm imzası sxemləri
ISO 9797	Məlumatın autentifikasiyası kodları
ISO 9979	Kriptoqrafik alqoritmlərin qeydiyyatı
ISO 10118	Heş-funksiyalar
ISO 11770	Açarların idarə olunması
ISO 13888	İnkarolunmazlıq
ISO 14888	Əlavəli rəqəm imzaları
ISO 15946	Elliptik əyrilər əsasında kriptoqrafik üsullar

Mövcud şifrləmə standartları artıq müasir tələblərə cavab vermirlər, buna görə də bütün dünyada onları yeniləri ilə əvəz edirlər. Elektron imzalar, informasiyanın tamlığının təmini və şifrləmə üçün yeni Avropa sxemlərinin (New European Schemes for Signatures, Integrity and Encryption- NESSIE) yaradılması üçün Avropa Komissiyasının nəzarəti altında 2000-ci ilin martında işə başlayan layihə belə layihələrdən biridir. Üç ilə nəzərdə tutulmuş NESSIE layihəsinin məqsədi "informasiya cəmiyyətinin gələcək standart protokolları üçün tikinti blokları" yaratmaqdır [67].

Layihə 10-dan artıq kriptoqrafik primitiv, o cümlədən, blok və axın şifrləmə alqoritmləri, təsadüfi ədədlər generatoru, verilənlər paketinin sürətli autentifikasiyası sxemi, heş-funksiyalar və rəqəm imzası alqoritmləri seçməlidir. Müsabiqəyə təklif olunmuş iddiaçı alqoritmlərin seçiminin əsas kriterilərı kimi təhlükəsizlik, məhsuldarlıq, çeviklik və bazarın tələbləri götürülmüşdür. Hər kateqoriya üzrə ayrıca standart təsdiq etmək nəzərdə tutulur.

4.5. Rəqəm imzası vasitələrinin sertifikasiyası

Mühafizənin səmərəli olması üçün rəqəm imzası vasitələri obyektiv və müstəqil qiymətləndirmə ilə təsdiqlənmiş müəyyən tələblərə cavab verməlidir. İnformasiyanın mühafizəsi üzrə normativ sənədlərin tələblərinə uyğunluğun qiymətləndirilməsinin belə formalarından biri sertifikasiyadır.

Hazırda müxtəlif ölkələrdə qəbul edilmiş və rəqəm imzasının proqram və aparat-proqram realizələrinə tətbiq oluna bilən sertifikasiya prosedurları istehsalçıların realizə etdiyi alqoritmlərin rəqəm imzası standartlarının rəsmi mətnində olan təsvirinə uyğunluğunu yoxlamaqdan ibarətdir.

Sertifikasiya zamanı sertifikasiya olunan vasitənin təkcə standartın tələblərinə deyil, bir sıra digər tələblərə də (etibarlılıq üzrə, əlfəcinlərin olmaması, protokolların keyfiyyəti) cavab verməsini yoxlamaq zəruridir. Aydındır ki, sertifikasiya işi yüksək ixtisas tələb edir, olduqca məsuliyyətli və əməktutumludur, buna görə də uzun müddət tələb edir. Məsələn, ABŞ-da sertifikasiya işi bir ildən artıq çəkir.

ABŞ-da Milli Standartlar və Texnologiyalar İnstitutu (National Institute of Standards and Technology, NIST) tərəfindən akkreditə olunmuş laboratoriyalar, standartın mətnində nəşr olunmuş parametrlərin konkret qiymətləri və sadə ədədlərin generasiyası prosedurunun ilkin parametrləri əsasında DSA alqoritminin parametrlərini müəyyən edən sadə ədədlərin generasiya prosedurunu testdən keçirirlər. Sonra alqoritmin parametrlərinin test qiymətlərində, test elektron

sənədləri üçün imzanın hesablanması və yoxlanması aparılır. Belə testlərin sayı olduqca çox- bir neçə on minlərlə ola bilər. Nəticələrin bütün ardıcıllığı giriş parametrlərinin həmin qiymətlərində etalon proqramın işinin nəticəsi ilə müqayisə etmək üçün laboratoriyaya təqdim olunur. Müqayisənin nəticələri əsasında rəqəm imzasının baxılan realizəsinin standarta uyğunluğu haqqında rəy verilir.

İnformasiyanı mühafizə vasitələrinin informasiya təhlükəsizliyi tələbləri üzrə sertifikasiyası sisteminin təşkilati strukturuna aşağıdakılar aid oluna bilərlər:

- məhsulun sertifikasiyası üzrə dövlət orqanı;
- məhsulun sertifikasiyası üzrə akkreditə olunmuş orqanlar;
- akkreditə olunmuş sınaq mərkəzləri (laboratoriyalar);
- ərizəçilər (məhsulun yaradıcıları, istehsalçıları, satıcıları, sifarişçiləri, istehlakçıları).

İnformasiya təhlükəsizliyi tələbləri üzrə məhsulun sertifikasiyası ilə bağlı bütün növ işlərin aparılması xərcləri məhsulun maya dəyərinə aiddir və ərizəçi tərəfindən ödənilir. Sertifikasiya üzrə orqanlar və sınaq mərkəzləri (laboratoriyalar) məhsulun sınağı zamanı müəllif hüquqlarının qorunması və konfidensiallıq rejiminin təmin olunması üzrə onların üzərinə qoyulmuş funksiyaların yerinə yetirilməsinə görə məsuliyyət daşıyırlar.

5. Açıq Açarlar İnfrastrukturu

5.1. Kriptorafik açarların idarə olunması

İstənilən kriptosistemin təhlükəsizliyi istifadə olunan kriptoqrafik açarlarla müəyyən olunur. Açarların etibarsız idarə olunması halında bədniyyətli açarı əlinə keçirərək, bütün sistemdəki və ya şəbəkədəki informasiyaya giriş əldə edə bilər. Məxfi açarların konfidensiallığı qarantə olunmasa, bütün açıq açarlar arxitekturası dağılar. Beynəlxalq və milli standartlaşdırma praktikasında, açarların idarə olunmasının modelləri, texnololgiyaları və metodları ayrıca normativ sənədlərdə əks olunur ki, bu da bir daha açarların idarə olunmasının bazis rolunu nəzərə çarpdırır.

Beynəlxalq İSO/İEC11770 standartına [70] uyğun olaraq açarların idarə olunması dedikdə avtorizə olunmuş obyektlər arasında açarlarla bağlı qarşılıqlı əlaqənin qurulması və idarə olunması üçün istifadə olunan metod və prosedurların məcmusu başa düşülür. Həmin standart açarların idarə olunması sahəsində aşağıdakı funksiyaları müəyyən edir: generasiya, qeydiyyat, sertifikasiya, paylama, instalyasiya, saxlama, arxivləşdirmə, ləğv etmə, qeydiyyatın ləğvi və məhv etmə.

Simmetrik və asimmetrik sistemlər üçün açarların generasiya olunması fərqlənir. Simmetrik kriptosistemlərdə açarların generasiyası üçün təsadüfi ədədlərin aparat və ya proqram generasiya vasitələri istifadə olunur. Asimmetrik kriptosistemlər üçün açarların generasiyası bir qədər mürəkkəbdir, çünki açarlar bir sıra riyazi xassələrə malik olmalıdırlar.

Saxlama funksiyası açar informasiyasının təhlükəsiz saxlanması, uçotu və silinməsinin təşkilini nəzərdə tutur. Açarların təhlükəsiz saxlanmasının təmini üçün onların digər açarların köməyi ilə şifrlənməsi tətbiq olunur. Belə yanaşma açarların iyerarxiyası konsepsiyasını doğurur. Açarların iyerarxiyasına adətən baş açar (master key), açarları şifrləmə

açarı və verilənləri şifrləmə açarı daxil olur. Qeyd etmək lazımdır ki, baş açarın saxlanması və generasiyası kriptomühafizənin kritik məsələsidir.

Paylama- açarların idarə olunmasında ən məsuliyyətli prosesdir. Bu proses paylanan açarların gizliliyini qarantə etməli, həmçinin operativ və dəqiq olmalıdır. Şəbəkədə istifadəçilər arasında açarların paylanması iki üsulla həyata keçirilə bilər:

- seans açarlarının birbaşa mübadiləsi;
- bir və ya bir neçə açarları paylama mərkəzindən istifadə etməklə.

Açarları periodik olaraq təzələmək lazımdır. Aydındır ki, yeni açıq açarlar generasiya olunduqda, onlar da sertifikatla təsdiq olunmalıdırlar. Bəzi mühafizə sistemləri bu əməliyyatı avtomatlaşdırmağa imkan verir.

Açarların deponə edilməsi, rezervləşdirməyə aidiyyəti olmayan ayrıca məsələdir. Ümumiyyətlə deyilsə, bu halda bir və ya bir neçə müstəqil təşkilat açarın surətini və ya onun müəyyən hissələrinin surətlərinin saxlayıcısı olur. Axırıncı halda açarın tam surətini almaq üçün saxlayıcılar birləşməlidirlər. Deponə etmə adətən hökumət agentliyinin müstəqil tərəf qismində iştirakı kontekstində müzakirə olunur. Qeyd emək lazımdır ki, rəqəm imzası yaradılması üçün istifadə olunan açarların surətini heç vaxt çıxarmaq olmaz.

Qeyd edək ki, açıq açarı bilməklə ona uyğun olan məxfi açarı kriptoqrafik üsullarla almaq praktik olparaq qeyri-mümkündür. Lakin məxfi açarı müxtəlif üsullarla ələ keçirmək mümkündür, buna görə də onu "göz bəbəyi" kimi qorumaq zəruridir. Məxfi açarların sanksiyasız istifadəsinin məsuliyyəti bütünlüklə onun sahibinin üzərinə düşdüyündən, açarların təhlükəsizliy tələblərinin yerinə yetirilməsi olduqca vacibdir.

Məxfi açarlar, yaddaşda onların oxunmasına yol verən açıq şəkildə saxlanmamalıdır. Məxfi açarları portativ personal daşıyıcılarda (disket, intellektual plastik kart, fleş-kart, Toush Memory tabletləri) saxlamaq tövsiyə olunur. Məxfi açar diskin mühafzə olunan sahəsində da saxlanıla bilər. Bir qayda

olaraq, açar əlavə olaraq yalnız qanuni sahibinə məlum olan parol və ya PİN-kod vasitəsilə şifrlənir. Açar, sahibi identifikasiya edən digər metodların köməyi ilə də mühafizə oluna bilər. Kompüterlərin mühafizəsinə də ən ciddi fikir verilməsi zəruridir. Çünki açarın daşıyıcıdan oxunması və onun sonrakı istifadəsi zamanı o, virusların, troya atlarının və digər ziyankar proqram təminatının köməyi ilə oğurlana bilər. Bu nöqteyi-nəzərdən, məxfi açarların prosessor və ya digər miniatür hesablayıcılarla təhciz olunmuş intellektual plastik kartlarda saxlanması daha prespektivli görünür [18]. Onlar kriptoqrafik çevirmələri öz daxilində müstəqil həyata keçirərək açarın kənara çıxmasına yol vermirlər ki, bu da təhlükəsizliyi xeyli artırır.

Açarın saxlama üsulunun seçilməsi riskin dərəcəsindən və tələb olunan təhlükəsizlik səviyyəsindən, həmçinin baxılan mühit üçün hansı üsulun daha yararlı olmasından asılıdır. Avropa təşkilatlarının çoxu hesab edir ki, açarları aparat qurğularında saxlamaq lazımdır, buna görə smart-kart variantını seçirlər. ABŞ-da isə kompaniyaların çoxu açarı şifrlənmiş şəkildə kompüterdə saxlamağı üstün tutur.

5.2. Açıq açarların verifikasiyası

Açıq açarların bilavasitə istifadəsi onların əlavə mühafizəsini və məxfi açarla əlaqəsini müəyyən etmək üçün identifikasiyasını tələb edir. Belə əlavə mühafizə olmasa bədniyyətli özünü həm imzalanmış verilənlərin göndərəni, həm də şifrlənmiş verilənlərin alanı kimi qələmə verə bilər (açıq açarların qiymətini dəyişdirərək və ya onun identifikasiyasını pozaraq). Bütün bunlar açıq açarın verifikasiyası zərurətini doğurur. Açıq açarın göstərilən şəxsə aid olduğunu vaxtında təsdiq etmək və açarın saxlanma və göndərilmə zamanı dəyişdirilməsinin qarşısını almaq üçün rəqəm sertifikatından istifadə olunur. Rəqəm sertifikatı açıq açarı müəyyən istifadəçi və ya tətbiqi proqramla bağlayan rəqəm sənəddir. Rəqəm sertifikatının təsdiqi üçün vəkil olunmuş mərkəzin- sertifikasiya

mərkəzinin (SM) rəqəm imzasından istifadə olunur. SM-in açıq açarından istifadə etməklə hər bir istifadəçi SM tərəfindən buraxılmış rəqəm sertifikatının səhihliyini yoxlaya və onun məzmunundan istifadə edə bilər.

Rəqəm imzasının praktik tətbiqi zamanı qarşıya çıxan ən mühüm məsələ Açıq Açarlar İnfrastrukturunun (AAİ) yaradılmasıdır. Məsələ ondadır ki, rəqəm imzasının yoxlanması üçün əlavə informasiya- açıq açar tələb olunur. Açıq açarların autentikliyi kiçik miqyaslı korporativ şəbəkələrdə Açarların Paylanması Mərkəzləri vasitəsi ilə həyata keçirilə bilər. Ancaq böyük miqyaslı korporativ şəbəkələr və açıq kompüter şəbəkələri üçün bu yanaşma səmərəli deyil və daha məqbul həll AAİ-nin yaradılmasıdır.

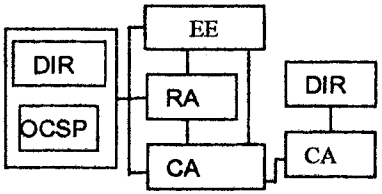
Rəqəm imzası haqqında bir sıra dövlətlərin qəbul olunmuş qanunlarının, beynəlxalq təşkilatların model qanunlarının (layihələrinin) öyrənilməsi göstərir ki, istisnasız olaraq bütün qanunların böyük hissəsi, müxtəlif adlarla adlandırılsa da, AAİ-nin təsvirinə həsr olunur. AAİ-nin tədqiqi, praktik tətbiqi və qanunvericiliklə tənzimlənməsi sahəsində dünyada böyük təcrübə toplanmışdır.

5.3. Açıq Açarlar İnfrastrukturu

Rəqəm imzasının istifadəsi üçün infrastrukturun yaradılması məsələsi mürəkkəb hüquqi, təşkilati və elmi-iexniki məsələlərin kompleksidir. Açıq açarlar infrastrukturunun milli arxitekturasını yaratmaqla yanaşı, həm də subyektlər elektron şəkildə qarşılıqlı əlaqədə olarkən təhlükəsizlik məsələlərini həll etmək lazımdır. Elmi-texniki məsələlər sırasından rəqəm imzasının istifadəsi infrastrukturunun bütün komponentlərinin standartlaşdırılmış alqoritmlər, protokollar və vasitələr tətbiq etməklə qurulması məsələlərini fərqləndirmək olar.

Açıq açarlar infrastrukturu (Public Key Infrastructure- PKI)-şəbəkədə autentifikasiyanı və şifrləməni təmin etməyə imkan

verən texnologiyaların, protokolların, standartların və xidmətlərin kompleksidir [76].



CA– Certification Authority (Sertifikasiya Mərkəzi)
RA– Registration Authority (Reqistrasiya mərkəzi)
DİR– Şəbəkə məlumat kitabı (LDAP, X.511, X.519 və s. protokolları əsasında)
EE– End Entity (Son İstifadəçi)
OCSP– Online Certificate Status Protocol (Sertifikatın statusunu operativ müəyyən etmə protokolu)

Şəkil 5.6. AAİ-nin məntiqi strukturu

AAİ tərkibinə aşağıdakı məntiqi komponentlər daxildir (şəkil 5.6) [25, 28]:

- Sertifikasiya mərkəzi (CA) – Əsas idarəedici komponentdir. Tabeçiliyində olan Reqistrasiya Mərkəzinin (və ya Mərkəzlərinin) və istifadəçilərin rəqəm setrifikatlarını formalaşdırır. Həmçinin sistemin reqlamenti ilə müəyyən olunmuş müddətlərdə geri çağırılmış sertifikatların siyahısını formalaşdırır.
- Reqistrasiya mərkəzi (RA)– İdarəedici komponentdir. İstifadəçilərin identifikasiyası və reqistrasiyasını həyata keçirir. Təkcə funksiyaların bir qismi deyil, AAİ-nin təhlükəsizliyi də istifadəçilərin "düzgün" identifikasiyasına və reqistrasiyasına əsaslanır. Bu işi prinsipcə SM-lər də yerinə yetirilə bilər, lakin çox vaxt bu praktikada tətbiq olunmur. Yalnız reqistrasiya olunmuş istifadəçi Sertifikasiya Mərkəzindən öz açıq açarına sertifikat ala bilər. Bu komponentin funksiyalarına həmçinin sertifikatların və geri çağırılmış sertifikatların siyahısının şəbəkə məlumat kitabında nəşr olunması da aid edilə bilər.
- Son istifadəçilər (EE)– Sertifikatın sahibi və ya AAİ-dən istifadə edən istifadəçilər, proqram və ya sistemlər (məsələn, MS Outlook Express, MS Internet Explorer,

IPSec protokolu və Windows 2000 əməliyyat sisteminə smart-kartla giriş) AAİ-dən istifadə edir. Son istifadəçilər təklif olunan sertifikat və imzaların verifikasiyası zamanı rəqəm identifikasiyası üçün istifadə olunan informasiyanın və ya digər assosiasiya olunan informasiyanın yoxlanması məqsədi ilə SM-dən istifadə edirlər.

– Şəbəkə məlumat kitabı- AAİ-nin opsional komponenti. Sertifikatları və geri çağırılmış sertifikatların siyahısını istifadəçilər arasında LDAP (FTP, HTTP) protokolundan istifadə etməklə yaymaq məqsədinə xidmət edir.

5.4. Açıq Açarlar İnfrastrukturunun xidmətləri

AAİ-nin əsas xidmətləri sertifikatların idarə olunması üzrə xidmətlərdir, bu xidmətlər açıq açarlar infrastrukturunun özəyini təşkil edir. Əsas xidmətlərə aşağıdakılar aiddir:

– istifadəçilər və sertifikat mərkəzləri üçün sertifikatların buraxılması;
– istifadəçilərin məxfi açarlarının kompromətasiyası zamanı və ya sertifikasiya siyasətində müəyyən edilmiş digər hallarda sertifikatların ləğvi;
– sonradan avtomatik bərpa və ləğv etmə ilə sertifikatların fəaliyyətinin dayandırılması;
– maraqlı şəxslərin fəaliyyətdə olan sertifikatların siyahısına girişini təmin etmək məqsədilə sertifikat kataloqları vasitəsilə sertifikatların nəşri (X.500 və ya digər normativ və standartların tələblərinə uyğun olaraq);
– bərpa etmə imkanı ilə sertifikatın saxlanması;
– verilən sertifikatların istifadəsi ilə yerinə yetirilən elektron sənədlərin, bağlaşmaların və digər əməliyyatların yoxlanması imkanını təmin etmək məqsədi ilə istifadədən çıxmış sertifikatların arxivləşdirilməsi.

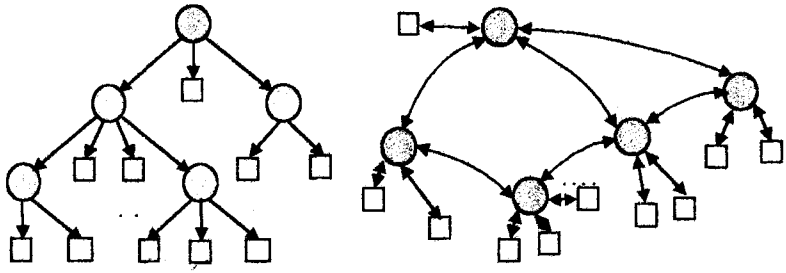
Əsas xidmətlərdən savayı AAİ-də əlavə xidmətlər də dəstəklənə bilər:

- Qeydiyyat. Qeydiyyat xidməti sertifikasiya prosesi obyektlərinin fərdi informasiyalarının qeydiyyatını və nəzarətini təmin edir.
- İnformasiyanın arxivdə saxlanması. Bu xidmət rəqəm sənədləri və digər informasiyaların uzunmüddətli saxlanması və idarə olunması üçün nəzərdə tutulmuşdur.
- Notarial sertifikasiya xidməti. Notarial sertifikasiya xidməti göndərənin autentifikasiyasını, elektron sənədlərin tamlığı və hüquqi qüvvəsinin təsdiqini əhatə edir.
- Açarların ehtiyat surətlərinin yaradılması və bərpası.
- Kataloq xidməti. Xidmətin bu növü istifadəçilər haqqında informasiyanın hərtərəfli idarə olunması və təmini üçündür.
- Açarların tarixinin idarə olunması və korrektə olunması xidməti.

5.5. Açıq açarlar infrastrukturunun modelləri

AAİ qurulması üçün aşağıdakı modellər təklif olunub:

- iyerarxik model- infrastrukturda ən yüksək pillə olan sertifikasiya mərkəzi reqistrasiya mərkəzlərinin işini idarə edir. Reqistrasiya mərkəzləri isə öz növbəsində son istifadəçilərlə qarşılıqlı əlaqəni təmin edir.
- Şəbəkə modeli- müstəqil sertifikasiya mərkəzləri şəbəkə şəklində birləşərək qarşılıqlı (çarpaz) sertifikasiyanı təmin edir.
- qarışıq- özündə əvvəlki iki modelin əlamətlərini əks etdirir.



a)iyerarxik model b)şəbəkə modeli

Şəkil 5.7. AAİ-nin arxitektura modelləri

İyerarxiya prinsipi ilə qurulmuş AAİ-də bütün SM-lər iyerarxik tabeçilik prinsipinə görə birləşirlər (şəkil 5.7.a). Özək (mərkəzi) SM özü üçün və tabe SM-lər üçün sertifikatlar buraxır. Tabe SM-lər isə öz növbəsində iyerarxiyanın sonrakı səviyyəsindəki SM-lər üçün və ya öz istifadəçiləri üçün sertifikatlar buraxırlar. İyerarxik AAİ-də əlaqə saxlayan istənilən iki tərəf özək SM-in açıq açarını bilir. Adətən belə infrastruktur şəbəkənin ölçülərinə və konfiqurasiyasına tam nəzarət imkanı və zərurəti olan korporativ sistemlərdə qurulur.

İyerarxik arxitekturanın aşağıdakı üstünlükləri var:

- adların iyerarxik ağacına asanlıqla inikas olunur;
- qarşılıqlı əlaqədə olan bütün tərəflər üçün sertifikatlar zəncirinin axtarışı, qurulması və verifikasiyası üçün sadə alqoritm verir;
- iki istifadəçinin qarşılıqlı əlaqə prosedurunu sadələşdirir (istifadəçilərdən birinin digərinə öz sertifikat zəncirini təqdim etməsi kifayətdir).

İyerarxik arxitekturanın aşağıdakı nöqsanları var:

- bütün son istifadəçilərin qarşılıqlı əlaqəsini təmin etmək üçün sistemdə yalnız bir özək SM olmalıdır;
- özək SM-in məxfi açarının kompromitasiyası bütün sistemin işini dayandırır və yeni sertifikatın hər bir son istifadəçiyə mühafizəli çatdırılmaçını tələb edir.

Şəbəkə arxitekturasında (şəkil 5.7.b) bütün SM-lər bərabər və ya eyniranqlı olurlar, yəni iyerarxiyanın eyni səviyyələrində yerləşirlər. Şəbəkə modeli 1991-ci ildə F.Zimmerman tərəfindən ümumi istifadə üçün yaradılmış PGP kriptoqrafik paketində realizə olunub və bütün dünyada bu proqramın milyonlarla tərəfdarı tərəfindən istifadə edilir.

Şəbəkə modelinin fərqləndirici xüsusiyyəti - kriptosistemin bütün tərəfdarlarına sertifikatlaşdırma funksiyasının verilməsidir. Eyni zamanda sistemin hər bir iştirakçısının digər iştirakçıya, onun üçüncü şəxslərin açarını cavabdeh sertifikasiya etmə qabiliyyəti nöqteyi-nəzərindən bəslədiyi inamın səviyyəsini müəyyən etmək imkanı var. Hər SM "yaxın" SM-in açıq açarını bilir və bu "yaxın" SM onun üçün

sertifikat buraxır. Sertifikatların yoxlanması verilən SM-dən başlayan sertifikasiya zəncirinin yoxlanmasından ibarətdir. Şəbəkədə bərabər SM-lər arasında inam münasibətləri SM-lərin müstəqil qarşılıqlı çapaz-sertifikasiyası vasitəsilə saxlanır. SM-lər çapaz-sertifikatlar buraxırlar, yəni bir-biri üçün sertifikatlar buraxırlar və bu sertifikatları çapaz-sertifikat cütündə birləşdirirlər. Belə arxitektura açıq şəbəkələrdə tətbiq edilir və İnternet vasitəsilə elektron kommersiya sahəsində xüsusilə geniş yayılmışdır.

Şəbəkə arxitekturasının aşağıdakı üstünlükləri var:

- daha çevikdir və müasir biznesdə mövcud vasitəsiz qarşılıqlı inam münasibətlərinin qurulmasına kömək edir;
- son istifadəçi, yalnız onun sertifikatını buraxan mərkəzə inanmalıdır;
- istifadəçiləri tez-tez öz aralarında qarşılıqlı əlaqədə olan müxtəlif SM-lərin bilavasitə çapaz-sertifikasiyası mümkündür ki, bu da zəncirin verifikasiyasını ixtisar edir.

Şəbəkə arxitekturasının nöqsanları aşağıdakılardır:

- qarşılıqlı əlaqədə olan bütün tərəflər üçün sertifikatlar zəncirinin axtarışı və qurulması çox mürəkkəbdir;
- istifadəçi, onun sertifikatını bütün qalan istifadəçilərin yoxlamasını təmin edən zənciri təqdim edə bilməz.

AAİ-nin qurulması prosesi kifayət qədər əməktutumlu və uzun müddətli prosesdir. AAİ-nin səmərəli həyata keçirilməsi, səhvlərin meydana gəlməsi ehtimalını azaltmaq məqsədi ilə BaltimoreTechnologies kompaniyası tərəfindən xüsusi KeySteps texnologiyası işlənib hazırlanmışdır. Bu metodika AAİ qurulması layihəsinin hər bir mərhələsində məqsədləri, resurs və nəticələri effektiv müəyyən etməyə kömək edir. Metodikanın istifadəsi həyata keçirmə xərclərini, onun müddətini və mümkün layihə risklərini azaltmağa imkan verir. Metodikaya yeddi mərhələ daxildir ki, onların ardıcıl yerinə yetirilməsi informasiya sistemində informasiyanın mühafizəsi tələblərinə cavab verən AAİ-nin uğurlu qurulması və tətbiq olunmasına zəmanət verir.

5.6. Rəqəm sertifikatlarının formatı

Faktiki olaraq rəqəm sertifikatı istifadəçinin şəxsi verilənləri ilə açıq açarını birləşdirir və açıq açarın məhz göstərilən şəxsə aid olduğuna zəmanət verir. Obrazlı deyilsə, rəqəm sertifikatı xüsusi subyektin- Sertifikasiya Mərkəzinin rəqəm imzası ilə təsdiq edilmiş və qlobal şəbəkədə fəaliyyət göstərən şəxsiyyət vəsiqəsidir.

Hal-hazırda rəqəm sertifikatlarının formatına ISO/IEC 9594-8 (ITU Rec.X.509) standartı [72] mövcuddur. Rəqəm sertifikatının formatı Əlavə 2-də göstərilib. İlkin olaraq X.509 standartı 1988-ci ildə X.500 tövsiyələrinin bir hissəsi kimi nəşr olunmuşdur. O vaxtdan bəri bu standarta 1993 və 1995-ci illərdə yenidən baxılmışdır. X.509 standartının tövsiyələri sertifikatın formatını müəyyən edərkən bir çox sərbəstlik dərəcələri nəzərdə tutur. AAİ-nin az və ya çox dərəcədə avtonom istifadəçiləri qrupu (cəmiyyəti) onları konkret- ləşdirərək profil yaradırlar. Məsələn, İnternetdə istifadə üçün profil (RFC 2549) IETF PKI işçi qrupu tərəfindən buraxılır. Avropa parlamentinin direktivlərində təklif edilmiş "kvalifikasiya sertifikatının" profilini təyin edən RFC 3039 standartı da (RFC 2549 əsasında) IETF tərəfindən buraxılmışdır.

Bir sıra ölkələrdə də (ABŞ, Avstriya, İsveç) X.509 profilləri işlənmişdir. Profillərin bütün bu müxtəlifliyi sertifikatların mübadiləsi zamanı əhəmiyyətli çətinliklər yaradır.

X.509 sertifikatına əsas sahələr və əlavə sahələr daxildir. Əsas sahələr PKİ standartlarına uyğun olaraq yaradılmış istənilən proqram təminatı tərəfindən eyni cür interpretə olunmalıdır. Əsas sahələrə aiddir:

- sertifikatın seriya nömrəsi;
- rəqəm imzası alqoritminin identifikatoru;
- sertifikatı buraxanın adı;
- sertifikat sahibinin adı;
- sertifikat sahibinin açıq açarı;

Əlavə sahələr kritiklik əlamətinə malik ola bilərlər. Əgər sertifikatda hər hansı əlavə sahədə kritiklik əlaməti qoyulubsa

və proqram onu interpretə edə bilmirsə, onda proqram belə sertifikatı rədd etməyə borcludur. Əgər kritiklik əlaməti qoyulmayıbsa, sahə sadəcə olaraq nəzərə alınmaya bilər. Standartda bu əlavə sahələr də göstərilə bilər:

- açarın tətbiq sahəsi;
- proqram təminatının tələbi ilə açarın əlavə tətbiq oblastı;
- sertifikatın sahibi və buraxanı haqqında əlavə məlumatlar;
- sertifikat buraxanın geri çağırılmış seritifikatlar siyahısı haqqında informasiya;
- digər başqa məlumatlar.

Əlavə proqramların tətbiqi ilə digər əlavələrin təyini də mümkündür.

Sertifikat onu buraxan SM-in rəqəm imzası ilə imzalanmalıdır. Sertifikatın fəaliyyət müddəti bir qayda olaraq, rəqəm imzasının kriptodavamlılığı ilə əlaqədardır (adətən iki-üç ilə bərabərdir).

Müxtəlif növ sertifikatlar tətbiq olunur. Onlardan bəziləri, məsələn, Pretty Good Privacy (PGP) sertifikatı müəyyən tətbiqi proqramlarla əlaqəlidir. Digər populyar sertifikatlar, məsələn, SET və Imternet Protocol Security (IPSec) sertifikatları kimi, spesifik təyinatlı sertifikatlardır.

ABŞ-da rəqəm sertifikatları üçün hal hazırda dörd sinif nəzərdə tutulub. Sertifikatın sinfi istifadəçinin autentifikasiya səviyyəsini göstərir. Birinci sinif sertifikatı almaq çox asandır – istifadəçinin minimal yoxlanışı nəzərdə tutulub (yalnız tam adı və elektron poçtun ünvanını bildirmək tələb olunur). İkinci sinif sertifikat verilərdə SM şəxsiyyət vəsiqəsini (real, fiziki), sosial sığorta kartının nömrəsini və təvəllüdünü yoxlayır. Üçüncü sinif sertifikatı almaq üçün istifadəçinin kredit qabiliyyəti də yoxlanmalıdır. Dördüncü sinif sertifikatında əlavə olaraq istifadəçinin təşkilatda tutduğu mövqe haqqında informasiya da tələb olunur.

5.7. Sertifikatların geri çağırılması

SM-lərinin funksiyalarından bəlkə də ən vacibi sertifikatların geri çağırılması ilə bağlıdır [25, 31]. Sertifikat verilərdə nəzərdə tutulur ki, o bütün göstərilmiş müddətdə fəaliyyət göstərəcək. Lakin sertifikatın fəaliyyətinin vaxtından əvvəl dayandırılmasını tələb edən şərait yarana bilər. Belə şərait adın dəyişməsi ilə, subyektlə SM arasında assosiasiyanın dəyişməsi ilə (məsələn, əməkdaş təşkilatı tərk edir), uyğun məxfi açarın sındırılması təhlükəsi və ya sındırılması ilə bağlı ola bilər. Bu hallarda SM sertifikatı geri çağırmalıdır.

SM daim etibarsız sertifikatların siyahısını dəstəkləməli və tənzimləməlidir. Bir qayda olaraq bunun üçün geri çağırılmış sertifikatlar siyahısı (Certification Revocation List, CRL) tətbiq olunur. CRL-də sertifikat seriya nömrəsinə görə identifikasiya olunur. Hər dəfə geri çağırılanda sertifikat bu siyahıiya əlavə olunur. Geri çağırılmış sertifikat haqqında yazı sertifikatın rəsmi fəaliyyət müddəti bitəndə CRL-dən çıxarılır. CRL sertifikasiya mərkəzinin rəqəm imzası ilə təsdiqlənməlidir. CRL siyahıları CRDP (Certification Revocation Distribution Point) məntəqələrində sərbəst nəşr olunurlar.

CRL bir sıra nöqsanlara malikdir. Hər şeydən əvvəl siyahının ölçüsünü qeyd etmək lazımdır. SM-in idarə etdiyi sertifikatların sayından asılı olaraq, CRL siyahısı sürətlə böyüyə bilər. Belə böyük faylın ötürülməsi böyük buraxıcılıq qabiliyyəti və hesablama gücü tələb edir.

Başqa və ola bilsin ki, ən ciddi nöqsan bu siyahının təzələmə operativliyidir. Siyahılar CRDP nöqtələrində müəyyən dövrlə (saatda, həftədə, ayda bir dəfə) nəşr olunurlar. Bu müddətlər arasında geri çağırılmış sertifikatlar hələ nəşr olunmadıqlarına görə CRL siyahılarında olmayacaqlar və etibarlı hesab olunacaqlar.

Bu səbəblərə görə sertifikatların geri çağırılması prosesini sadələşdirən metodlar işlənilmişdir. Onardan biri əlavə CRL-dir. Dövri olaraq geri çağırılmış sertifikatların tam baza siyahısı

nəşr olunur. Baza CRL-in nəşrləri arası geri çağırılan sertifikatlar kiçik ölçülü siyahılarda əlavə (delta) CRL-də nəşr olunur. Sertifikatın statusu sorğusunda istifadəçinin səhvən qısa siyahını tam CRL kimi qəbul etməməsi üçün əlavə CRL uyğun surətdə işarə olunur. İstifadəçinin sertifikatında geri çağırılmış siyahının lazımi fraqmentinin saxlandığı sorğu kitabının yerləşdiyi URL olur. Bu sorğu kitabı SM-in istifadə etdiyindən fərqli ola bilər.

5.8. Sertifikatlar zəncirinin yoxlanması

İstifadəçinin istənilən sertifikata inamı sertifikatlar zənciri əsasında müəyyən olunur. Zəncirin başlanğıc elementi, istifadəçinin mühafizə olunan fərdi məlumat kitabında saxlanan SM-nin sertifikatı olur.

Sertifikat zəncirinin verifikasya proseduru sertifikatın sahibinin adı ilə onun açıq açarının bağlılığını yoxlayır. Zəncirin verifikasiyası proseduru bütün "düzgün" zəncirlərin bir inanılmış sertifikasiya mərkəzinin buraxdığı sertifikatlardan başladığını nəzərdə tutur. İnanılmış mərkəz kimi özək SM başa düşülür ki, onun açıq açarı özünün imzaladığı sertifikatda olur. Belə məhdudiyyət verifikasiya prosedurunu sadələşdirir, lakin özü imzalanan sertifikatın varlığı və onun kriptoqrafik yoxlanması təhlükəsizliyi təmin etmir. Belə sertifikatın açıq açarına inamı təmin etmək üçün onun saxlanması və yayılması zamanı xüsusi üsullar tətbiq olunmalıdır, çünki bu açıq açarla bütün digər sertifikatlar yoxlanılır.

Zəncirlərin verifikasiyası alqoritmi bu verilənlərdən istifadə edir:

- sertifikatı buraxanın X.500 adı;
- sertifikat sahibinin X.500 adı;
- sertifikatı buraxanın açıq açarı;
- sertifikatı buraxanın və Sahibin açıq (məxfi) açarının fəaliyyət müddəti;
- zəncirin verifikasiyası zamanı istifadə olunan əlavələr (basicConstraints, nameConstraints);

– hər bir sertifikat buraxan üçün CRL (hətta siyahıda geri çağırılmış sertifikat olmasa belə).

Sertifikatlar zənciri aşağıdakıları ödəyən n sertifikatdan ibarət ardıcıllıqdır:

{1, (n-1)}-dən olan istənilən x üçün, x sertifikatının Sahibi x+1 sertifikatını buraxandır;

x=1 sertifikatı özüimzalanan sertifikatdır;

x=n sertifikatı son istifadəçinin sertifikatıdır.

Sertifikatlar zənciri ilə eyni zamanda qurulan CRL-lər zənciri aşağıdakı şərtləri ödəyir:

{1, n}-dən olan istənilən x üçün, x sertifikatını buraxan x CRL-ni buraxandır;

x=1 CRL-i özüimzalanan sertifikatın Sahibinin buraxdığı CRL-dir;

x=n CRL-i son istifadəçinin sertifikatını buraxan tərəfindən buraxılan CRL-dir.

İki zəncirin qurulmasından (sertifikatlar və CRL-lər) sonra aşağıdakılar yerinə yetirilir:

– zəncirlərdəki sertifikat və CRL-lərin kriptoqrafik yoxlanması;
– sertifikatlar və CRL-lərin fəaliyyət müddətlərinin yoxlanması;
– nameConstraints əlavəsindən istifadə etməklə zəncirin uzunluğunun yoxlanması;
– sertifikatın geri çağırılmasının yoxlanması; əgər aralıq mərkəzin sertifikatı ondan yuxarı mərkəz tərəfindən geri çağırılıbsa, aralıq mərkəzin buraxdığı bütün sertifikatlar etibarsız sayılır;
– sertifikatın qəbul edilən istifadə reqlamentinin və qəbul edilən sahələrinin yoxlanması;
– certificatesPoilicies və extendedKeyUsage əlavələrindən istifadə etməklə açarın istifadəsinin yoxlanması.

Rəqəm sertifikatlarının yoxlanması zamanı, kliyentlərə konkret sertifikatın real vaxt rejimində statusunu yoxlamağa imkan verən protokoldan istifadə etmək ən etibarlı yanaşma olardı. Bu məqsədlə IETF tərəfindən OCSP (Online Certificate Status Protocol) protokolu işlənib hazırlanmışdır. Bu protokol

minlərlə CA və milyonlarla sertifikatlar olan sistemlərlə qarşılıqlı əlaqəyə imkan verir.

RFC 2459 sənədinə uyğun olaraq, geri çağırılmış sertifikatların yayım mexanizmi sertifikatların növünə əsaslanır. Onun istifadəsi üçün əlavə səbəb müxtəlif sertifikatlar üçün geri çağırılma bildirişlərinin müxtəlif sürətlə yayılması ehtiyacıdır. Bir qayda olaraq, SM CRL siyahılarını sertifikatın növündən asılı olmayan, qəbul edilmiş dövrlə (periodla) nəşr edir. Buna baxmayaraq bəzi mühüm sertifikatlar, məsələn, SM-lərin özlərinin sertifkatları daha tez-tez çap olunmalıdır. Misal olaraq, interaktiv bank tranzaksiyalarına baxaq. Həm kliyentə, həm də banka təqdim olunmuş sertifikatların həqiqiliyini yoxlamaq və bir-birini autentifikasiya etmək zəruridir. Əgər CRL siyahıları hər saatdan bir nəşr olunursa, kliyentin (bankın) geri çağırılmış sertifikatı 60 dəqiqə ərzində nəşr olunana qədər etibarlı olacaq. OCSP protokolunu təsvir edən RFC 2560 sənədində belə hallar nəzərə alınıb. SM geri çağırılmış sertifikatlar haqqında məlumatı OCSP protokolunu dəstəkləyən sorğu kitabında nəşr edir. Kliyent sertifikatın statusu haqqında sorğu ilə OCSP serverinə müraciət etdikdə üç cavab ala bilər: "qaydasındadır" ("Good"), "geri çağırılıb" ("Revoked"), "məlum deyil" ("Unknown"). "Qaydasındadır" cavabı sertifikatın geri çağırılmadığını bildirir, ancaq onun etibarlı olmasına zəmanət vermir, sadəcə onun geri çağırılmışların siyahısında olmadığını bildirir. "Geri çağırılıb" cavabı sertifikatın etibarsız olduğunu bildirir. "Məlum deyil" cavabı sertifikatın statusu və onun varlığı haqqında informasiyaya malik olmadığını bildirir.

CRL-dən fərqli olaraq, OCSP protokolu AAİ proqramları tərəfindən verilənlərin avtonom əmalını təmin etmir. Buna görə də OCSP serverinin üzərinə düşən yük olduqca çox ola bilər, üstəlik o, hər bir cavabını da rəqəm imzası ilə təsdiqləməlidir.

5.9. Açıq açarlar infrastrukturu standartları

Standartlar AAİ-nin qurulması və istifadə olunmasında mühüm rol oynayırlar. AAİ sahəsində standartlaşdırma müxtəlif proqramlara vahid AAİ-dən istifadə etməklə öz aralarında qarşılıqlı əlaqədə olmağa imkan verir. Standartlaşdırma xüsusilə aşağıdakı sahələrdə vacibdir:

- reqistrasiya prosedurları;
- sertifikatın formatının təsviri;
- CRL formatının təsviri;
- kriptoqrafik mühafizə olunan verilənlərin formatının təsviri;
- onlayn protokollarının təsviri;
- açarın yaradılması prosedurları.

Uyğun standartları, hər biri AAİ qurulması üçün tələb olunan müəyyən texnoloji seqmentə aid olmaqla dörd qrupa bölmək olar.

Birinci qrup standartlar Beynəlxalq Elektrorabitə İttifaqı (International Telecommunications Union, ITU) tərəfindən hazırlanmış X seriyası standartlarıdır. Beynəlxalq miqyasda tanınmış bu standartlar kataloqların və onda olan informasiyanın kodlaşdırma vasitələrinin təsviri üçün istifadə olunur.

İkinci qrup standartlar IETF təşkilatının kataloqlar və onlara müraciət protokolları PKIX (PKI for X.509 Certificates) kimi tanınan işçi qrupu tərəfindən yaradılmışdır (Əlavə 4). Bu standartlar qrupu İnternet vasitəsilə kataloqdan sertifikat sorğulumağı, geri çağırılmış sertifikatlar siyahısı ilə davranış qaydasını, sertifikatın verilməsi qaydalarını, sertifikasiya praktikası və sertifikatların formatını müəyyən edir. Bu standartlar qrupunda olan X.509 standartı [72] AAİ-də istifadə olunan bütün digər standartların əsasında dayanan fundamental standartdır. Onun əsas vəzifəsi rəqəm sertifikatının və geri çağırılmış sertifikatlar siyahısının formatını müəyyən etməkdir.

Üçüncü qrup standartlar RSA kompaniyasının laboratoriyalarında Apple, Microsoft, DEC, Lotus, Sun və MIT

də daxil olan qeyr-formal konsorsium tərəfindən yaradılan açıq açarlar kriptoqrafiyası (Public Key Cryptography Standards, PKCS) standartlarıdır (Əlavə 5). PKCS standartlarına həm alqoritmdən asılı, həm də alqoritmdən asılı olmayan standartlar daxildir. Yalnız RSA və Diffi-Hellman alqoritmləri təfsilatı ilə təsvir olunubdur. Standartlarda rəqəm imzası, rəqəm zərfləri və genişləndirilmiş sertifikatlar üçün alqoritmdən asılı olmayan sintaksis müəyyən edilir ki, bu da sənaye tətbiqi zamanı istifadə olunan şifrləmə alqoritmlərindən asılı olmadan uyuşanlıq əldə etməyə xidmət edir.

Dördüncü qrup standartlar AAİ üzərində qurulmuş standartlardır. Kriptoqrafiyadan istifadə edən standartların çoxu AAİ-nin istifadəsini nəzərə almaqla hazırlanmışdır. Belə standartlara misal olaraq S/MIME, SSL, TLS, SET, IPSEC standartlarını göstərmək olar.

- S/MİME standartı İETF tərəfindən mühafizəli məlumat mübadiləsi üçün müəyyən olunmuşdur. S/MİME rəqəm imzasının formalaşdırılması və informasiyanın şifrlənməsi üçün AAİ-dən istifadə edir.
- SSL protokolu (Netscape firması) və ona uyğun TLS (İETF) standartı Web-ə mühafizəli müraciətin təmin olunması üçün ən çox istifadə olunan standartlardır. Bununla yanaşı SSL və TLS standartları Web-dən istifadə etməyən kliyent-server proqramları tərəfindən də istifadə edilir. Hər iki protokolun əsasında AAİ durur.
- SET protokolu Visa və MasterCard firmaları tərəfindən yaradılmışdır və plastik kartlardan istifadə etməklə elektron bank hesablaşmaları sistemlərinin təmin olunması üçün nəzərdə tutulmuşdur. Bu protokolda AAİ hesablaşma iştirakçılarının bütün autentifikasiya sisteminin əsaslandığı fundamentdir.
- İPSEC protokolu İETF tərəfindən İP-nin şifrlənməsi protokolu kimi yaradılmışdır və bu protokolda AAİ-dən autentifikasiya və şifrləmə üçün istifadə edilir.

5.10. Sertifikasiya mərkəzlərinə hücumlar

Sertifikasiya mərkəzi AAİ-da aparıcı rol oynadığından onlara yönəlmiş bəzi ən sadə hücumlara nəzər salaq [39].

Fərz edək ki, istifadəçi *B* özünü istifadəçi *A* kimi qələmə vermək istəyir. Bunun üçün *B* açarlar cütü (məxfi və açıq) generasiya edir və açıq açarı (məxfi kanalla) SM-ə *A*-nın adından göndərir. Əgər SM-i aldatmaq və *A*-nın adına sertifikat almaq mümkün olacaqsa, *B* məqsədinə çatacaq. Belə hücumların qarşısını almaq üçün sertifikat almağı sorğulayanın şəxsiyyətini dəqiq identifikasiya etmək zəruridir. Bunun üçün SM, məsələn, şəxsən iştirak etməni və ya şəxsiyyəti təsdiq edən sənədləri təqdim etməyi tələb edə bilər. Hər bir SM özünün autentifikasiya proseduruna malik ola bilər. Aydındır ki, SM xidmətlərinin etibarlı təşkili kriptoşəbəkənin etibarlılığını müəyyən edir.

SM-in məxfi açarını ələ keçirmiş bədniyyətli sertifikatları saxtalaşdıra bilər. Məxfi informasiyanın sızmasının qarşısını almaq məqsədi ilə SM özünün məxfi açarını və onunla imzalanmış sertifikatları xüsusi, çox yüksək etibarlı, zərbəyə davamlı, elektromaqnit şüalanmalardan mühafizə olunan, enerjidən asılı olmayan yaddaşa malik elektron cihazda - sertifikatların imzalanması qurğusunda (SIQ) saxlanmalıdır.

Məlumdur ki, bir sıra standartlara daxil edilən və şifrləmə və autentifikasiyada geniş istifadə olunan RSA kriptosisteminə güc hücumu çoxrəqəmli ədədin (modulun) sadə vuruqlara ayrılması məsələsinə gətirilir. Həm də modul məlumdur və SM-in açıq açarına daxildir. Bu vəziyyət SM-i olduqca uzun (2048 bit və daha çox) açarlardan istifadə etməyə və onları müntəzəm təzələməyə məcbur edir. SM-lərin iyerarxik strukturunda açarların təzələnməsi tezliyi mühüm əhəmiyyət daşıyır. İyerarxiyanın yuxarı səviyyəli SM-lərində açarların tez-tez dəyişdirilməsi qeyri-praktikdir, çünki şəbəkənin çox sayda istifadəçisinin açarının dəyişdirilməsinə səbəb ola bilər.

Başqa hücum modelində *A*-nın tərəfindən istifadəçi *B*-nin ələ alınması imkanı nəzərdən keçirilir. Bu halda *B* SM-in

əməkdaşıdır, elə almanın məqsədi *A* tərəfindən *F*-in adına sertifikatın alınmasıdır. Sertifikat alaraq, *A* *F*-in adından məlumatlar göndərə bilər və verilmiş sertifikat qanuni olduğu üçün bu məlumatlar kriptoşəbəkənin digər istifadəçiləri tərəfindən adekvat qəbul ediləcəkdir. SM-ə belə hücumların mümkünlüyünü nəzərə alaraq sirrin bölüşdürülməsi kimi kriptoqrafik texnikanın əsasında SİQ-ə girişə hədd qoyulmasının xüsusi metodu tətbiq olunur. Məsələn, SİQ-ə giriş üçün SM-in bir neçə əməkdaşının iştirakı tələb oluna bilər. Prosedur xüsusi məxfi açarların təqdim olunmasını (əsas giriş açarının kölgələrini), onların autentikliyinin yoxlanması və təqdim olunan kölgələrin sayının müəyyən sərhəd qiymətindən az olmadığı halda girişə icazə verilməsini nəzərdə tutur. Nəzərdə tutmaq lazımdır ki, sertifikat verilməsi sorğularına bir nəfər tərəfindən nəzarət edilərsə, təsvir olunan hücum uğurlu ola bilər.

Digər hücum köhnə sənədlərin saxtalaşdırılmasından ibarətdir. *A* SM-in açıq açarının tərkibinə daxil olan modula güc hücumunu həyata keçirir. Müəyyən müddət keçdikdən (məsələn, 15 il) sonra nəticədə modulu vuruqlara ayırmağa və SM-in məxfi açarını bərpa etməyə nail olur. Bu məxfi açarın fəaliyyət müddəti artıq qurtarsa da, *A* *B*-nin saxta açıq açarını təsdiqləyən 15-illik sertifikatı saxtalaşdıra bilər. Bunun nəticəsində *A* *B*-nin imzası olan 15-illik istənilən sənədi saxtalaşdıra bilər. Bir sıra hallar var ki, elektron sənədləri uzun müddət saxlamaq (məsələn, uzunmüddətli müqavilələr və s.) lazımdır. Bu zaman onların autentikliyinin və tamlığının yoxlanması imkanı təmin olunmalıdır. Bunun üçün mövcud üsullardan biri adi açarlarla yanaşı, uzunmüddətli açarlardan istifadə olunmasıdır. Uzunmüddətli açarlar istifadə olunduqda CRL siyahılarının qeyri-məhdud artması problemi qarşıya çıxır, çünki uzunmüddətli açarlar da bütün digər açarlar kimi kompromətasiya oluna bilər və bütün fəaliyyət müddətində həmin siyahıda saxlanmalıdırlar. Göstərilən çatışmamazlıqları aradan qaldırmaq üçün uzunmüddətli açarları adi açarlar üçün standart prosedurla, məsələn, iki il müddətinə qeyd etdirmək

məsləhət görülür. İki illik dövr bitdikdən sonra, sertifikat komprometasiya olunmayıbsa, sonrakı iki il üçün yenidən sertifikasiya olunur. İndi komprometasiya olunmuş uzunmüddətli açar iki il müddətində CRL-də saxlanacaq.

Başqa bir hücum növündə bədniyyətli vahid vaxt xidmətinin işini pozaraq yenidən sertifikasiya prosedurunun dövriliyini dəyişdirə bilər. Problem xüsusi vaxt nişanları xidməti (VNX) vasitəsi ilə həll oluna bilər. Bunun üçün bütün uzunmüddətli elektron sənədlər VNX-nin verdiyi xüsusi rəqəm nişanları vasitəsilə qeyd olunmalıdır. Rəqəm nişanları uzunmüddətli sənədlərin imzalandığı açarın (açarların) fəaliyyət müddətinin başa çatmadığına əmin olmağa, həmin açarlar komprometasiya olunduqda belə, uzunmüddətli sənədlərin qanuniliyini müəyyən etməyə imkan verir.

5.11. Milli Açıq Açarlar İnfrastrukturunun arxitekturası

Hal-hazırda idarə, kommersiya və ümummilli informasiya şəbəkələrinin real inteqrasiyasından danışmaq olar. İstifadəçilər öz məsələlərinin həlli üçün müxtəlif mənsubiyyətli şəbəkələrin resurslarından istifadə etmək ehtiyacındadırlar. Şəbəkələrin qarşılıqlı əlaqəsinin tələb olunan təhlükəsizlik səviyyəsini resursların əlyetənliyinin lazımi səviyyəsini saxlamaq şərti ilə AAİ-nin Milli arxitekturasını qurmaq yolu ilə əldə etmək mümkündür. Bunun üçün dövlət səviyyəsində dövlət və kommersiya sertifikasiya mərkəzləri arasında qanunvericilik səviyyəsində hüquqi əlaqələr qurulmalıdır.

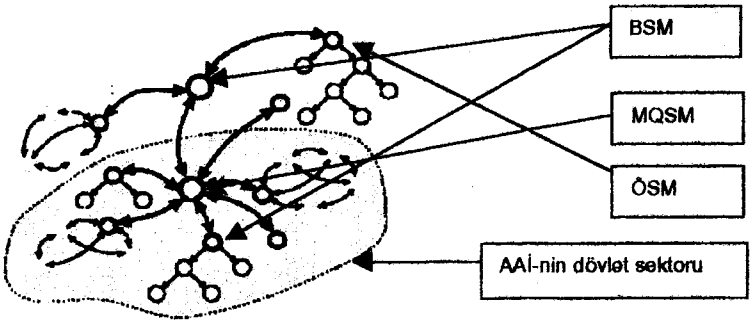
Milli AAİ-nin əsas problemi müxtəlif idarə və təşkilatlar arasında inamın yüksək səviyyəsini təmin edən sertifikasiya zəncirinin qurulmasıdır. Milli AAİ dövlət və qeyri-dövlət sektorlarını birləşdirməlidir.

Bu problemin həllərindən biri sertifikasiya mərkəzləri tərəfindən standartlarda təsbit olunmuş, sınaqdan çıxarılmış mexanizmlərin tətbiqi və çapaz-sertifikatlara verilən tələblərin ödənilməsidir.

Şəkil 5.8–də NİST tərəfindən tövsiyə olunan AAİ Milli arxitekturası göstərilmişdir [76, 44].

Bu arxitekturanın əsas arxitektur komponentləri aşağıdakılardır:

1. Milli sertifikasiya siyasətini idarəetmə orqanı. Bu orqan Milli AAİ-də ümumi siyasəti müəyyən edir, Milli AAİ-də inam domenlərinin qayda və prosedurlarını təsdiq edir.
2. İnam domenləri. Milli miqyasda, inam domeni Milli AAİ-nin tərkib hissəsidir və sertifikasiya siyasətini vahid idarəetmə orqanının idarəsi altında fəaliyyət göstərir. Domendə bir və ya bir neçə SM ola bilər. Hər bir inam domeni bir əsas SM (Principial CA) və domen depozitarisinə malikdir.



Şəkil 5.8. Milli AAİ-nin arxitekturası

3. Domenin sertifikasiya siyasətini idarəetmə orqanı. Bu orqan domenin SM-lərinin praktik fəaliyyətini təsdiq edir və bu fəaliyyətin müşahidəsini (izlənməsini) həyata keçirir. Orqan domen depozitarisinin işini təşkil edir və ya ona nəzarət edir.
4. Sertifikasiya mərkəzləri:
   - Milli qovşaq sertifikasiya mərkəzi (MQSM)- Milli sertifikasiya siyasətini idarəetmə orqanının idarəsi altında fəaliyyət göstərir. MQSM-nin məqsədi milli AAİ-nin müxtəlif inam domenləri arasında, həmçinin idarə (dövlət)

və kommersiya AAİ arasında inam zənciri qurulacaq inam qovşağını təmin etməkdir.

Milli sertifikasiya siyasətini idarəetmə orqanı MQSM ilə çapaz-sertifikat buraxmaq hüququ olan inam domenlərinin baş SM-ni təsdiq edir. Qeyd edək ki, MQSM özək SM deyil, çünki o, sertifikasiya zəncirlərinin başlanğıcı deyil.

- Baş sertifikasiya mərkəzi (BSM)- SM daxilində MQSM ilə çapaz-sertifikat buraxmağa cavabdehdir. İstənilən inam domeninin bir BSM-i ola bilər. İyerarxik arxitekturalı domendə BSM adətən MQSM-in təyin etdiyi istənilən SM-dir.
- Birranqlı sertifikasiya mərkəzi (BRSM)- şəbəkə arxitekturalı inam domenində SM-dir. BRSM-in öz sertifikatı var və bu sertifikat, sertifikat sahibləri arasında paylanır və onlar tərəfindən sertifikasiya zəncirinin inisalizasiyası üçün istifadə olunur. BRSM həmçinin öz inam domeninin digər BRSM-ləri ilə çapaz-sertifikatlar buraxır.
- Özək (mərkəzi) sertifikasiya mərkəzi (ÖSM)- iyerarxik arxitekturalı inam domenində bütün sertifikasiya zəncirlərinin başlanğıcı olan SM-dir. Sertifikat sahibləri və əlaqəyə girən tərəflər ÖSM-in sertifikatını hər hansı etibarlı yolla (məsələn, səlahiyyətli şəxslərin şəxsi görüşündə) alırlar və bütün inam zəncirləri bu nöqtədən başlayır. İyerarxik arxitektura üçün ÖSM eyni zamanda baxılan domenin BSM-idir.
- Tabe sertifikasiya mərkəzi (TSM) – iyerarxik strukturlu domendə inam zəncirlərinin başlanğıc nöqtəsi olmayan SM-dir. TSM sertifikatı iyerarxiyanın yuxarı səviyyəsində yerləşən öz SM-indən alırlar və öz növbəsində tabeçiliklərində olan TSM üçün sertifikat buraxırlar.

5. Depozitari- sertifikatlar bazası və sertifikatların statusu haqqında informasiyanı aktual vəziyyətdə saxlayan onlayn vasitədir. Milli AAİ-də depozitarilər informasiyanı LDAP protokolunun, həmçinin digər vasitələrin köməyi ilə

təqdim edir. Depozitari və SM-in CRL sertifikatlarının saxlanmasına görə milli sertifikasiya siyasətini idarəetmə orqanı cavabdehdir.

6. MQSM-in depozitarisi. Hamı tərəfindən qəbul edilmiş həll MQSM-in depozitarisinə İnternet vasitəsilə açıq müraciət olunmasıdır. Depozitaridə aşağıdakı məlumatlar olur:
   - MQSM-in buraxdığı bütün sertifikatlar;
   - MQSM-in saxladığı bütün sertifikatlar;
   - MQSM-in buraxdığı və saxladığı sertifikatların daxil olduğu bütün çapaz-sertifikat cütləri;
   - MQSM-in buraxdığı bütün sertifikatlar üçün CRL-in cari versiyası;
   - Sertifikasiya zəncirinin axtarışını dəstəkləmək üçün Milli AAİ-nin SM-lərinin buraxdığı bütün və ya əksər sertifikatlar;
   - Milli AAİ-nin SM-ləri arasında çapaz-sertifikat cütlərinin hamısı və ya əksəri;
   - Milli sertifikasiya siyasətini idarəetmə orqanının müəyyən etdiyi digər sertifikat və CRL-lər.

MQSM ümumi metodoloji prinsiplər əsasında idarə SM-lərinin vahid Milli AAİ-da birləşdirilməsi üçün əlaqələndirici elementdir. Qeyd olunduğu kimi MQSM özək SM deyil, ancaq o, mühüm sistem rolu oynayır. MQSM inam domenlərini BSM-in səlahiyyətli şəxslərinin çapaz-sertifikat cütləri vasitəsilə birləşdirən inam qovşağıdır. Qeyd etmək lazımdır ki, açarların paylanması nəzəriyyəsində inam modeli və inamın isbatı çox mühüm və prinsipial məsələlərdir. Hal-hazırda heterogen şəbəkələrdə inamın və inam münasibətlərinin modelləşdirilməsinin nəzəri məsələləri hələlik kifayət qədər öyrənilməmişdir. Milli sertifikasiya siyasətini idarəetmə orqanı MQSM-in fəaliyyətinə nəzarəti həyata keçirir və MQSM ilə çapaz-sertifikasiya proseslərinin həyata keçirilməsi qaydalarını müəyyən edir. MQSM ilə çapaz-sertifikasiyanı həyata keçirən inam domenləri həm dövlət, həm də kommersiya sektorundan ola bilər.

İnam domenlərində fəaliyyət göstərən dövlət və qeyri-dövlət SM-ləri sertifikasiya siyasətini milli idarəetmə orqanının müəyyən etdiyi tələblərə cavab verməyə borcludurlar. Təsərrüfat fəaliyyəti subyektlərinin sertifikatların paylanması sahəsində fəaliyyət göstərmək imkanını müəyyən etmək məqsədi ilə, uyğun fəaliyyətin lisenziyalaşdırılması qaydalarını, fəaliyyətin həyata keçirilməsinin attestasiya və akreditasiya qaydalarını işləmək və qanunvericilikdə təsbit etmək lazımdır. Çarpaz-sertifikasiya proseslərinə yalnız akkreditə olunmuş SM-lər buraxıla bilərlər.

Lakin idarələrin qarşılıqlı əlaqələrində çevikliyin real təmin olunması üçün sertifikasiya siyasətinin müəyyən edilməyə MQSM-nin inhisarından qaçmaq lazımdır. Bunun üçün MQSM-in müəsisə SM fəaliyyətinə qarışması məhdudlaşdırılmalıdır:

- Müəssisələr MQSM-in sertifikasiya siyasətinə tam adaptasiya olunma şərti ilə məhdudlaşdırıla bilməzlər. Hətta belə xidmətlər bazarında elə şərait yaratmaq lazımdır ki, müəssisələr ya özlərinin məxsusi sertifikasiya siyasətindən, ya da idarəetmə orqanının və ya kommersiya sertifikasiya xidmətləri provayderinin müəyyən etdiyi sertifikasiya qaydalarından istifadə edə bilsinlər.
- Müəssisənin digər müəssisə və kommersiya təşkilatları ilə qarşılıqlı əlaqə hüququnu yalnız MQSM vasitəsilə əlaqə ilə məhdudlaşdırmaq olmaz. Alternativ kimi təşkilatların müqavilə əsasında bilavasitə qarşılıqlı əlaqə imkanını vermək zəruridir.

6. Rəqəm imzasının praktik tətbiqi məsələləri

6.1. Mübahisələrin həlli proseduru

Rəqəm imzası sxemlərinin praktik tətbiqi üçün imzanın formalaşdırılması və onun yoxlanması alqoritmləri ilə yanaşı arbitraj proseduru, yəni mübahisələrin həlli də tələb olunur.

Arbitraj aşağıdakı hallarda tələb oluna bilər:

- Sənədin müəllifliyindən boyun qaçırma;
- İmzanın düzgün olmaması haqqında iddia;
- Sənədin lazımi vaxtda alınmaması haqqında iddia;
- Sənəddəki rəqəm imzasının həqiqi olmaması haqqında iddia.

SM-in və işçi yerinin proqram təminatı yoxlama aparmağa və yuxarıda göstərilən səbəblərə görə birmənalı qərar qəbul etməyə imkan verməlidir. İşin məhkəmədə araşdırılması zamanı hakim rəqəm imzasının həqiqiliyi haqqında rəy verən ekspert rolunda çıxış edir [22].

Arbitraj alqoritmi:

1. *B* abonenti hakimə elektron sənədi və imzanı təqdim edir.
2. Hakim *A* abonentindən öz məxfi açarını təqdim etməyi tələb edir. Əgər *A* imtina edərsə, hakim imzanın həqiqi olması barədə qərar qəbul edir.
3. Hakim SM-in sorğu kitabından *A* abonentinin açıq açarını götürərək onun *A* -nın təqdim etdiyi məxfi açarla uyğunluğunu yoxlayır. Əgər açarlar üst-üstə düşürsə, hakim addım 5-ə keçir.
4. Açarların uyğun gəlmədiyi halda hakim SM-ə müraciət edir və *A* abonenti tərəfindən təsdiq olunmuş sənədi təqdim etməyi tələb edir. Əgər sorğu kitabından götürülən açarın sənəddə göstərilmiş açarla üst-üstə düşmədiyi aydınlaşırsa, hakim *B* abonentinin təqdim etdiyi imzanı həqiqi qəbul edir. Bu zaman belə qərarın bütün xərcləri SM-in hesabına kompensasiya olunur. Əgər sorğu kitabındakı və sənəddəki açıq açarlar üst-

üstə düşürsə, yəni *A* abonenti düzgün olmayan məxfi açar təqdim edirsə, hakim rəqəm imzasının həqiqiliyini qəbul edir.

5. Hakim imzanın və sənədin bir-birinə uyğunluğunu yoxlayır. Yoxlamanın nəticəsi müsbət olduqda imza həqiqi hesab olunur, əks halda imza rədd olunur.

Arbitraj və məsələlərin həlli aşağıdakı hallarda mümkün deyil:

- Məxfi açar *A* abonentinin özü tərəfindən yox, açarların xüsüsi generasiya mərkəzi tərəfindən yaradılıb;
- İmzanın yaradılması və yoxlanması alqoritminin yerinə yetirilməsini həyata keçirən aparatura, istifadəçinin nəzarət etmədiyi hər hansı elementlərə malikdir ("qara qutular", yaddaşın mühafizə olunan sahələri və b.).

Nəhayət, hakimin əsaslandırılmış heç bir qərar qəbul edə bilmədiyi çıxılmaz vəziyyətlər də var. Məsələn, *B* abonenti *s*-i təqdim edərək bildirir ki, bu *r* sənədinin altındakı imzadır. *A* abonenti boynuna alır ki, bu onun imzasıdır, lakin o, *r'* sənədini imzalayıb. Eyni vaxtda məlum olur ki, bu sənədlərin heş-qiymətləri üst-üstə düşür, yəni $h(r)=h(r')$. Hakim başa düşür ki, onların ikisindən biri rəqəm imzası sxeminde istifadə olunan heş-funksiya üçün kolliziya tapmışdır və pat vəziyyətinə düşür. Vəziyyətdən çıxış yolu yalnız belə hallarda mübahisələrin həlli qaydası əvvəlcədən razılaşdırıldıqda mümkündür.

6.2. Rəqəm imzası vasitələrinə tələblər

Hazırda isifadəçilərə rəqəm imzası texnologiyasını realizə edən olduqca müxtəlif sistemlər təklif olunur. Belə sistemlərin seçimi zamanı rəqəm imzası funksiyalarını həyata keçirən proqram (aparat) kompleksləri aşağıdakı kriterilərə görə qiymətləndirilə bilərlər:

- kriptodavamlılıq;
- iş süreti;
- imzanın uzunluğu;

– əldə olunan rəqəm imzası sisteminin informasiya emalının qəbul edilmiş texnologiyasına inteqrasiyası;
– rəqəm imzası sisteminə icazəsiz girişdən mühafizə mexanizmləri və tədbirləri;
– təklif olunan həllin hüquqi dəstəyi;
– funksional imkanlar;
– İstifadəçinin rahatlığı.

Rəqəm imzası sisteminin seçimi zamanı diqqət yetirməyin lazım olduğu əsas parametrlərdən biri sürətdir. Verilənlərin çox intensiv mübadiləsi həyata keçirilən və ötürülən informasiyanın saxtalaşdırılmaqdan mühafizəsi vacib olan rabitə sistemlərində bu xüsusilə aktualdır. Bu parametr iki toplanandan- imzanın generasiyası sürətindən və onun yoxlanması sürətindən cəmlənir və heş-funksiyanın yaradılması sürətindən, həmçinin imzanın generasiyası və yoxlamasının həyata keçirildiyi hesablama vasitəsinin növündən çox asılıdır.

İmzanın uzunluğu da vacib parametrlərdən biridir. Məsələn, böyük sayda kiçik uzunluqlu verilənlərin ötürüldüyü dispetçer idarəetmə sistemlərində bütün verilənlər üçün 256 bit uzunluğunda rəqəm imzasından istifadə etmək səmərəli deyil.

Rəqəm imzası sistemlərinin informasiya emalının qəbul edilmiş texnologiyasına inteqrasiyası haqqında qeyd etmək lazımdır ki, rəqəm imzası vasitələri alınarkən bir qayda olaraq sifarişçinin informasiya sistemi formalaşmış olur. Məsələn, elektron poçtun göndərilməsi vasitəsi kimi Microsoft Outlook istifadə edilirsə, rəqəm imzası sisteminin bu poçt proqramına qoşula bilməsi imkanı zəruridir. Rəqəm imzası sistemində müxtəlif əməliyyat sistemləri və platformalarda işləmək imkanını dəstəkləmək üçün qoşulma interfeysləri nəzərdə tutula bilər.

Rəqəm imzası sisteminə icazəsiz girişdən mühafizə mexanizmləri və tədbirləri rəqəm imzası sistemini işə salmaq hüququ olan şəxslərin dairəsini məhdudlaşdırmalıdır. Rəqəm imzası sistemlərini müşaiyət edən sənədlərdə informasiyanın

icazəsiz girişdən mühafizəsi sistemlərinin tətbiqinə dair tövsiyələr olmalıdır. Rəqəm imzası sistemində istifadəçilərdən birinin açarının komprometasiyası halında hərəkətlər nəzərdə tutulmalıdır. Bundan başqa həm rəqəm imzası sisteminin özünün, həm də onun komponentlərinin (məsələn, əməliyyatların qeydiyyatı jurnalının) tamlığına nəzarət etmək imkanı olmalıdır.

Təklif olunan həllin hüquqi dəstəyi cəhətdən qeyd edək ki, Rəqəm imzası sisteminin tətbiqi ilə elektron sənədlərin mübadiləsi aşağıdakı sualların həllini nəzərdə tutulmalıdır:

- mübahisəli halların tənzimlənməsi prosedurlarının olması;
- baş verən mübahisələri araşdıran komissiyanın tərkibinin təsviri;
- tərəflərin məsuliyyəti.

Mübahisəli halların araşdırılması prosedurunun realizəsi üçün rəqəm imzası sistemində istifadə olunan bütün açarların saxlanması imkanı nəzərdə tutulmalıdır.

Funksional imkanlar bir və ya bir neçə imzanın qoyulması və yoxlanmasını, yoxlayana imzanın kimə məxsus olması haqqında müəyyən məlumat təqdim olunmasını təmin edə bilər.

İstifadəçinin rahatlığı mehriban interfeyslə- çoxpəncərəli menyu, strukturlaşdırımış kömək sistemi, rəng palitrasının seçilməsi və s. ilə təmin olunur.

Rəqəm imzası vasitələrinin son seçimi aşağıdakı imkanların olub-olmaması ilə müəyyən oluna bilər:

- bir sənədin altında bir neçə imzanın qoyulması və onların seçilərək yoxlanması;
- rəqəm imzasının təkcə imzalanan sənəddə deyil, ayrıca faylda da saxlanması;
- rəqəm imzası sistemi ilə iş üçün komanda sətrindən istifadə;
- fayllar qrupunun imzalanması və yoxlanması;
- sənədin verilən hissələrinin (sahələrinin) altında imzanın qoyulması və yoxlanması;

– operativ yaddaş sahəsi üçün imzanın qoyulması və onun yoxlanması;
– istifadə olunan açarların arxivləşdirilməsi və s.

6.3. Rəqəm imzası sistemlərinə hücumlar

Bədniyyətlinin hansı yollarla rəqəm imzasına hücumu həyata keçirə bilməsi haqqında biliklər rəqəm imzası sisteminin istifadəçisinə olduqca zəruridir. Rəqəm imzası sistemlərinə aid olan sənədlərdə çox tez-tez bütün mümkün açarların saf-çürük edilməsi üçün tələb olunan əməliyyatların sayı xatırladılır. Bu hücumların mümkün realizasiyası variantlarından yalnız biridir. Yüksək ixtisaslı bədniyyətli heç də həmişə belə "kobud" saf-çürük hücumundan (brute force search) istifadə etmir. Tipik hücumlardan bəzilərinə yaxından nəzər salaq. Rəqəm imzası sistemlərinə mümkün olan hücumları bir neçə qrup üzrə təsnif etmək olar:

– kriptoqrafik alqoritmlərə hücumlar;
– kriptosistemlərə hücumlar;
– realizəyə hücumlar;
– protokolun pozulması ilə bağlı hücumlar;
– rəqəm imzası sistemi mexanizmlərinin tamlığının pozulmasına əsaslanan hücumlar;
– istifadəçilərə hücumlar;

Hücum edən kənar subyekt, imzalayan tərəf (imzadan imtina) və ya imzanı yoxlayan tərəf (imzanın saxtalaşdırılması) ola bilər.

Kriptoqrafik alqoritmlərə hücumlar. Bu tip hücumlar mürəkkəb riyazi məsələlərin, məsələn, böyük sadə ədədin moduluna görə diskret loqarifmləmə məsələsinin həlli ilə əlaqədardır. Hücum edənin uğur şansı olduqca azdır. Hücumun bu növü ikiaçarlı kriptoqrafik alqoritmə və ya heş-funksiyaya qarşı yönələ bilər. Birinci halda imza, ikinci halda sənəd saxtalaşdırılır.

Qeyd etmək lazımdır ki, proqram məhsullarının bir sıra yaradıcıları rəqəm imzası və heş-funksiya standartlarının

mövcudluğuna baxmayaraq özlərinin xüsusi alqoritmlərini yaratmağa cəhd edirlər. Lakin müəlliflərin bu sahədə aşağı kvalifikasiyası ucbatından həmin alqoritmlər riyaziyyatçı-kriptoqraflar tərəfindən yaradılmış keyfiyyətli alqoritmlərə xas olan xüsusiyyətlərə malik olmurlar.

Kriptosistemlərə hücumlar. Kriptosistem dedikdə yalnız istifadə olunan rəqəm imzasının yaradılması və yoxlanması alqoritmi deyil, açarların generasiyası və paylanması mexanizmləri və kriptosistemin etibarlığına təsir edən bir sıra digər vacib elementlər də nəzərdə tutulur. Kriptosistemin etibarlılığı onu təşkil edən ayrı-ayrı elementlərin etibarlığından toplanır. Buna görə bir sıra hallarda alqoritmə hücuma zərurət yoxdur. Kriptosistemin komponentlərindən birinə– məsələn, açarların generasiyası mexanizminə hücuma cəhd etmək kifayətdir. Əgər kriptosistemdə açarların generasiyası üçün realizə olunan təsadüfi ədədlər generatoru etibarlı deyilsə, hətta keyfiyyətli rəqəm imzası alqoritmi istifadə edildikdə belə, kriptosistemin səmərəliliyi böyük şübhə altındadır.

Kriptosistemə hücumlar həmçinin maskalanmış zəifliklər olan rəqəm imzası sistemlərinin və ya icazəsiz girişdən mühafizə vasitələrinin, sənədləşdirilməmiş əlfəcinləri olan digər sistem və tətbiqi proqrarm təminatının yeridilməsinə də əsaslana bilər. Buna yol verməmək üçün kriptoqrafik vasitələr və icazəsiz girişdən mühafizə vasitələri müəyyən təşkilatlar tərəfindən sertifikasiya olunmalıdır.

Realizəyə hücumlar. Bu tip hücumlar bədniyyətlilər tərəfindən daha tez-tez istifadə olunur. Bu onunla əlaqədardır ki, onların həyata keçirilməsi üçün geniş riyazi biliklər tələb olunmur. Hücuma rəvac verə bilən səhv realizələrin geniş çoxluğundan aşağıdakıları nümunə olaraq göstərmək olar:

- rəqəm imzasının məxfi açarı tərpənməz diskdə saxlanılır;
- rəqəm imzası sisteminin işi qurtardıqdan sonra operativ yaddaşda saxlanan açarlar silinmir;
- seans açarlarının təhlükəsizliyi təmin olunsa da, baş açarların mühafizəsinə yetərincə diqqət verilmir;
- ləkələnmiş açarların qara siyahısına giriş açıqdır;

Protokolun pozulması ilə bağlı hücumlar. Belə hücumlara, məsələn, imzalanmış məlumatların təkrarı, məlumatların gecikdirilməsi aiddir. Belə hərəkətlərin qarşısını almaq üçün sənədin rekvizitlərində müəyyən sahələr nəzərdə tutulur. Məlumatın alınmasından imtina faktından mühafizəni təmin edən mexanizmlərin istifadəsi də zəruridir.

Rəqəm imzası sistemi mexanizmlərinin tamlığının pozulmasına əsaslanan hücumlar olduqca müxtəlifdir. Onlara verilənlər bazasından imzalanmış məlumatın pozulması, məxfi açarın proqram və aparat vasitələri ilə ələ keçirilməsi, saxta açıq açarın yeridilməsi, verilənlər bazasında açıq açarın dəyişdirilməsi aiddir. Bu misallar göstərir ki, hücumların geniş spektri rəqəm imzası sistemində dövr edən verilənlərə icazəsiz girişlə [1] əlaqədardır. Qeyd etmək lazımdır ki, rəqəm imzasının yaradılması və yoxlanması proqramının tamlığına nəzarət yoxdursa, bu bədniyyətliyə imzanı və onun yoxlanması nəticələrini saxtalaşdırmağa imkan verər.

İstifadəçilərə hücum. Unutmaq olmaz ki, son istifadəçi də kriptosistemin bir elementidir və bütün digər elementlərlə yanaşı o da hücumlara məruzdur. İstifadəçi özü olmayanda imzalamaq üçün rəqəm imzasının məxfi açarı olan daşıyıcını (disketi) həmkarına verə bilər, daşıyıcını itirə bilər və itgi haqqında daşıyıcı yenidən tələb olunana qədər xəbər verməyə bilər. Sistemlərin çoxunda imzanın yaradılması üçün istifadəçi özünə açarlar generasiya edə bilər. Açarın generasiyası istifadəçinin özünün seçdiyi parollara əsaslana bilər. Buna görə parollara verilən tələblər haqqında istifadəçilər təlimatlandırılmalıdır.

6.4. Rəqəm imzasının intellektual kartlarda realizəsi

İntellektual kartlarda realizə zamanı başlıca problem, əldə olan yaddaşın həcminin kiçik olmasıdır. Bəzi ucuz kartlarda cəmisi 256 bayt RAM (hesablanan verilənlər üçün) və 2000 bayt ROM (alqoritm və sabitlərin saxlanması üçün) ola bilər. İntellektual kartlarda rəqəm imzası sxemlərinin realizəsi

prosesində bir tərəfdən kriptoqrafik alqoritmlərin realizəsinin alqoritmik problemlərini, digər tərəfdən isə onların kriptoqrafik davamlılığını təmin etmək zərurətini nəzərə almaq gərəkdir. Bir-birinə zidd bu tələbləri iki üsulla yerinə yetirməyə çalışırlar: məlum rəqəm imzası sxemlərinin daha səmərəli realizə üsullarını yaratmaqla və təhlükəsizliyin müəyyən qədər aşağı salınması hesabına səmərəli rəqəm imzası sxemləri yaratmaqla.

Belə sxemlərdən biri ESIGN-dir [64]. Sxemin məxfi açarı p və q $(p>q)$ sadə ədədlərindən ibarətdir, açıq açar isə $n=p^2q$ və k tam ədədləridir. İmzalanan m məlumatı və s imzası tam ədədlər hesab olunurlar və $s \in Z_n^*$. Sxemin üstün cəhəti onun kifayət qədər yüksək səmərəliliyidir: alqoritmlərin əməliyyat sürəti RSA sxemində olduğundan təxminən 20 dəfə böyükdür. ESIGN sxeminin intellektual kartlarda realizəsi zamanı k parametri 2-nin qüvvəti kimi, p isə 16, 24 və ya 40 bayt uzunluğunda seçilir. İntellektual kartda aşağıdakı əməliyyatlar realizə olunmalıdır:

1. $x \in Z_{pq}^*$; 2. $F=x^k \bmod n$; 3. $W=\left\lceil \frac{h(m)-f}{pq} \right\rceil$;

4. $g=kx^{k-1} \bmod p$; 5. $Y=w/g \bmod p$; 6. $s=x+ypq$.

İmza sxeminin mikroproqram realizəsi 8-bitlik prosessor üçün işlənilmişdir. 384 bayt operativ yaddaş (RAM), 10 Kbayt daimi yaddaş (ROM) və 8 Kbayt proqramlaşdırılan daimi yaddaş (EEPROM) tələb olunur. Bölmə və reduksiyaya az vaxt sərf olunması üçün sxem, sabitlərin cədvəlini tərtib etmək məqsədi ilə qabaqcadan hesablama mərhələsindən istifadə edir. 1, 2, 4 və $(1/g) \bmod p$ əməliyyatları əvvəlcədən yerinə yetirilə bilər.

İmza alqoritminin səmərəliliyi cəhətindən bu sərfəlidir, çünki əvvəlcədən hesablama mərhələsində diskret qüvvətə yüksəltmə və modulyar inversiya kimi əmək tutumlu əməliyyatlar yerinə yetirilir. Operativ olaraq isə yalnız toplama, vurma və bölmə əmələri yerinə yetirilir.

ESIGN sxemi üçün hazırlanmış intellektual kartda imzanın generasiyası 0,2 san-dən çox çəkmir, proqram və verilənlər üçün yaddaşın ölçüləri 3 kBaytı aşmır.

İntellektual kartlarda realizə etmək üçün bir sıra digər rəqəm imzası sxemləri də təklif olunmuşdur. Məsələn, RSA sxeminin modifikasiyası [74] 512-bitlik operandlarla iş zamanı yüksək sürət əldə etməyə imkan verir: imzanın generasiyası 1,5 san-dən çox çəkmir, imzanı yoxlamaq isə 0,4 san sürür.

Son dövrlərdə smart-kartların tam funksional analoqları-tokenlər geniş yayılmaqdadır. Token USB portu vasitəsilə kompüterə birbaşa qoşulur. Token 64 kBaytadək enerjidən asılı olmayan yaddaşa və aparatda realizə olunmuş 120-bit açarlı DES-X şifrləmə alqoritminə malikdir. İnformasiyanın yaddaşda saxlanma müddəti 10 ildən az deyil, yenidən yazma dövrlərinin sayı isə 100 mindən çoxdur. Tokenin əsas təyinatı mühafizə olunan resurslara müraciət zamanı istifadəçilərin autentifikasiyası və sistemə giriş parollarının, şifrləmə açarlarının, rəqəm sertifikatlarının, istənilən digər məxfi informasiyanın təhlükəsiz saxlanmasıdır.

Token istifadəçinin fərdi açara malik olması və unikal parolu bilməsinə əsaslanan iki faktorlu autentifikasiyanı dəstəkləyir. Buna görə token kompüterin USB portuna taxıldıqdan sonra istifadəçi tokenin unikal parolunu daxil etməlidir. İstifadəçinin müxtəlif parolları və hər bir əlavə proqramın adını yadda saxlamasına ehtiyac yoxdur, onlar tokendə saxlanılır və zəruri olduqda avtomatik istifadə olunurlar.

6.5. Rəqəm imzası və CryptoAPI

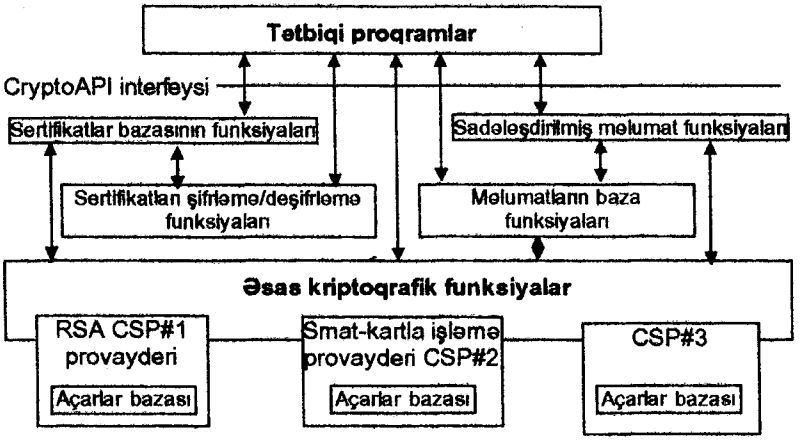
CryptoAPI funksiyaları. Windows 95 OSR2-dən başlayaraq, Windows əməliyyat sistemləri (ƏS) ailəsində açarların generasiyası, şifrləmə, rəqəm imzasının yaradılması və yoxlanması və digər kriptografik məsələlərin realizəsi təmin edilir. Bu funksiyalar əməliyyat sisteminin işi üçün zəruridir, lakin bunlardan istənilən əlavə proqram da istifadə edə bilər.

Bunun üçün yalnız tətbiqi proqramların kriptoqrafik interfeysi CryptoAPİ-nin müəyyən etdiyi qaydada lazımi altproqramlara müraciət etmək kifayətdir.

CryptoAPI müxtəlif sahələrdə istifadə olunur:

- rəqəm imzasının yaradılması və yoxlanması;
- qlobal şəbəkələrdə informasiyanın ötürülməsi vasitələri;
- şəbəkə istifadəçilərinin autentifikasiyası;
- faylları şifrləmə və deşifrləmə vasitələri;
- elektron poçt proqramları;
- kollektiv iş proqramları;
- real vaxtda konfransların keçirilməsi vasitələri;
- bank proqramları, o cümlədən smart-kart texnologiyasından istifadə edən proqramlar.

CryptoAPİ tətbiqi proqramlarla qarşılıqlı əlaqədə olan beş müxtəlif funksional sahədən ibarətdir (şəkil 6.1):



Şəkil 6.1. CryptoAPİ funksiyaları

1. Sertifikatları şifrləmə/deşifrləmə funksiyaları- bu funksiyalar sertifikatları və onları müşaiyət edən verilənləri CCİT X.200-də təsvir olunduğu kimi, OSİ şəbəkəsində idarə edir.
2. Sertifikatlar bazasının funksiyaları – sertifikatların saxlanması və idarə olunması üçün istifadə edilir. Vaxt

keçdikcə istifadəçidə olduqca çox sayda sertifikat toplana bilər. Adətən bu sertifikatlar istifadəçinin özünün və əlaqə saxladığı tərəflərin sertifikatları olur.

3. Əsas kriptoqrafik funksiyalar- tətbiqi proqramda kriptoqrafik imkanlardan daha tam faydalanmaq üçün istifadə olunur.
4. Aşağı səviyyənin məlumatları üçün funksiyalar- PKCS#7 tələblərinə cavab verən məlumatların tez hazırlanması üçün istifadə edilir. Bu funksiyaların təyinatı verilənlərin ötürülmə zamanı şifrlənməsi və qəbul zamanı deşifrlənməsi, həmçinin məlumatların imzalarının yaradılması və yoxlanmasıdır.
5. Məlumatlar üçün sadələşdirilmiş funksiyalar- məlumatlar üçün funksiyaların yuxarı səviyyəsində yerləşirlər və prinsipcə sertifikatlar və aşağı səviyyənin məlumatları üçün funksiyaları birgə realizə edirlər. Onlar tətbiqi proqramlardan funksiyaların çağırışını azaltmaq məqsədi ilə daxil ediliblər.

CryptoAPİ 2.0 hazırda baza əməliyyatları ilə yanaşı sertifikatlarla, RKCS#7 formatında şifrlənmiş məlumatlarla işi də dəstəkləyir. Şifrlənmiş və ya rəqəm imzası ilə təsdiq olunmuş elektron məlumatların formatı, rəqəm sertifikatlarının formatı və bir sıra digər obyektlərin formatı üçün beynəlxalq standartlar Abstract Syntax Notation One (ASN.1) dilindən istifadə etməklə abstrakt formada işlənib hazırlanmışdır. CryptoAPI-də ASN.1 formasında verilənlərlə işləmək üçün, belə verilənlərin Windows üçün "doğma" baytlar ardıcıllığına və tərsinə çevrilməsi üçün funksiyalar da var.

Kriptoprovayderlər. CryptoAPİ funksiyaları tətbiqi proqramlara Windows ƏS-nin kriptoqrafik imkanlarına müraciət etməyi təmin edir. Lakin onlar informasiya emalının mürəkkəb zəncirində "ötürücü halqa"dırlar. Əsas işi proqram (və ya aparat-proqram) modullarının tərkibinə daxil olan funksiyalar yerinə yetirir. Kriptoqrafik altsistemdəki funksiyaların kodu Windowsun bir neçə dinamik yüklənən kitabxanalarında (advapi32.dll, Crypto32.dll) olur. Həqiqətdə bu modullar

kriptoqrafik modulları realizə etmirlər, kriptoqrafik xidmətlər provayderləri- kriptoprovayderlər (Cryptograghic Servise Providers, CSP) adlanan digər modullara müraciət edirlər. Tətbiqi proqram birbaşa kriptoprovaydərə müraciət edə bilməz. Əməliyyat sistemində eyni zamanda bir neçə CSP qoymaq olar.

Üçüncü firmaların yaratdığı CSP-nin Windows ƏS-də işləməsi üçün onu Microsoftun rəqəm imzası ilə təsdiq etdirmək gərəkdir. Rəqəm imzasının periodik olaraq yoxlanması kriptoprovayderin qəsdən əvəzolunmasını (dəyişdirilməsini) istisna edir.

Tətbiqi proqramların hamının qəbul etdiyi standartlara uyğun gəlməsi üçün CryptoAPI xüsusi CSP tipləri daxil edir, məsələn, PROV_RSA_FULL və ya PROV_RSA_SCHANNEL. Verilən tipdən olan kriptoprovayder, uyğun standartla müəyyən edilmiş bütün kriptoalqoritmləri realizə etməlidir. Məsələn, PROV_RSA_SCHANNEL kriptoprovayderi SSL protokolunun realizəsi üçün istifadə olunur və rəqəm imzası və açarların mübadiləsi üçün RSA alqoritmini, heşləmə alqoritmlərindən SHA və MD5-i və CALG_SSL3_SHAMD5 xüsusi funksiyasını dəstəkləməlidir.

Kriptoprovayderləri bir-birindən fərqləndirən cəhətlər aşağıdakılardır:

- funksiyaların tərkibi (bəzi kriptoprovayderlər yalnız rəqəm imzasının yaradılması və yoxlanmasını həyata keçirirlər, verilənlərin şifrlənməsini isə həyata keçirmirlər);
- avadanlığa tələblər (xüsusiləşdirilmiş kriptoprovayderlər istifadəçinin autentifikasiyası üçün smart-kartla işləyən qurğu tələb edə bilər);
- baza əməliyyatlarını həyata keçirən alqoritmlər (açarların yaradılması və s.)

Aydındır ki, Windows ƏS təkmilləşdirildikcə, kriptoqrafik altsistem də genişlənmişdir. Versiyasından asılı olaraq ƏS-də qurulmuş kriptoprovayderlərin tərkibi əhəmiyyətli dərəcədə dəyişə bilər, lakin Windows ƏS olan istənilən kompüterdə PROV_RSA_FULL tipinə məxsus Microsoft Base

Cryptographic Provider olur. PROV_RSA_FULL növünə aid istənilən CSP həm şifrləməni, həm də rəqəm imzasını dəstəkləyir, açarların mübadiləsi və imzanın yaradılması üçün RSA alqoritmindən, heşləmə uçun MD5 və SHA-dan istifadə edir.

Windows ƏS-də qoyulmuş bütün CSP-lərin (kriptoprovay derlərin) siyahısını Windowsun sistem reyestrinin HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider bölməsində görmək olar. Yaxın vaxtlara kimi Base CSP-ni ixrac etmək olardı, tam funksional Enhanced CSP isə yalnız "özününkülərə" verilirdi.

Açarlar. CryptoAPİ-da açarların iki növü var:

– sessiya açarları;

– açıq/məxfi açarlar cütü.

CryptoAPİ-da şifrləmə/deşifrləmə və imzanın yaradılması /yoxlanması açarları fərqləndirilir. Onlar uyğun olaraq "mübadilə üçün cüt" və "imza üçün cüt" adlanırlar. Açarlar tərpənməz diskdə şifrlənmiş şəkildə verilənlər bazasında konteynerlərdə saxlanırlar. Açarların konteyneri unikal ada malik olur və daxilində mühafizəli şəkildə müəyyən bir istifadəçiyə məxsus mübadilə üçün cüt və imza üçün cüt saxlanır. Konteynerlər iki növdə olur– istifadəçi (bu tip defolt istifadə edilir) və maşın İstifadəçi konteynerinə girişə yalnız konteyner sahibinin adından yerinə yetirilən tətbiqi proqramların icazəsi var. Tətbiqi proqramlar belə konteynerdən şəxsi açarları saxlamaq üçün istifadə edə bilər. Yalnız administratorlara maşın konteynerlərinə girişə icazə verilir. Maşın konteynerlərində adətən xidmətlər (servislər) və sistem proqramları tərəfindən istifadə edilən açarlar saxlanır.

Bütün istifadə olunan açarlar üçün CryptoAPI xüsusi idxal və ixrac funksiyaları nəzərdə tutur. Windows 2000 ƏS-də açarları plastik kartlarda saxlamağa imkan verən xüsusi CSP var.

Sessiya açarları simmetrik açarlardır. Sessiya açarlarından RC2, RC4, DES kimi alqoritmlər istifadə edir. Microsoft RSA

Base Provider 40-mərtəbəli sessiya açarları və 512-bitlik açıq açarlarla işləyir. Kriptoprovayder açarların saxlanması və məhv edilməsi üçün cavabdehdir, açıq açarların ixrac (export) əməliyyatı istisna olmaqla, proqramçının açarın ikilik verilənlərinə girişi bağlıdır. Məxfi açarlar ixrac (export) oluna bilməzlər.

Kriptoprovayderlər– həm RSA Base CSP, həm də Enhanced CSP, məxfi açarları istifadəçinin profilində %SystemRoot%\Documents_and_Settings\<User_name>\Appl icationData\Microsoft\Crypto\RSA qovluğunda saxlayır. İstifadəçilərin yerdəyişən profillərində məxfi açar RSA qovluğunda yerləşir və kompütərə yalnız onun işi zamanı yüklənir.

Məxfi açarların mühafizəsi üçün RSA qovluğundakı bütün fayllar avtomatik olaraq təsadüfi simmetrik açarla- istifadəçinin əsas açarı (user's master key) ilə şifrlənir. 64 simvol uzunluğunda olan açar etibarlı təsadüfi ədədlər generatoru ilə yaradılır. Əsas açarların bazasında məxfi açarları şifrləmək üçün istifadə olunan 3DES açarları yaradılır. Əsas açar avtomatik yaradılır və periodik olaraq təzələnir.

Diskdə saxlanan zaman əsas açar istifadəçinin parolu əsasında yaradılan açarı tətbiq etməklə Triple DES alqoritmi ilə mühafizə olunur. Əsas açar RSA qovluğundakı bütün faylların yarandıqca avtomatik şifrlənməsi üçün istifadə olunur.

Rəqəm imzası funksiyaları. CryptoAPİ funksiyalarının adı Crypt prefiksi ilə başlanır. Bir qayda olaraq funksiyaların hər biri BOOL tipli nəticə – uğurla sonuclananda TRUE, səhv baş verdikdə isə FALSE qaytarırlar. CryptoAPİ-nin hər hansı funksiyasından istifadə etmək üçün CryptAcquireContext funksiyası ilə kriptoprovayderi işə salmaq və kriptoprovayderlə işi qurtardıqdan sonra isə CryptReleaseContext funksiyasını çağırmaq lazımdır.

Rəqəm imzası ilə işləmək üçün CryptCreateHash, CryptHashData, CryptSignHash, CryptVerifySignature, CryptDestroyHash funksiyalarından istifadə olunur. Rəqəm

imzasının yaradılması prosesi aşağıdakı mərhələlərdən ibarətdir:

- CryptCreateHash funksiyası ilə heş-obyekt yaradılır;
- CryptHashData funksiyası ilə heş-obyektə verilənlər yüklənir;
- CryptSignHash funksiyası ilə heş imzalanır;
- CryptDestroyHash funksiyası ilə heş-obyekt silinir.

Rəqəm imzasının yoxlanması belə yerinə yetirilir:

- CryptCreateHash funksiyası ilə heş-obyekt yaradılır;
- CryptHashData funksiyası ilə heş-obyektə verilənlər yüklənir;
- CryptVerifyHash funksiyası ilə imza deşifrə olunur və nəticə "öz" heşi ilə müqayisə olunur;
- CryptDestroyHash funksiyası ilə heş-obyekt silinir.

Ədəbiyyat

1. Алгулиев Р.М., Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей.– Москва, 2001.–248 с.
2. Алгулиев Р.М., Алиев Г.М., Модели и бизнес-процессы в электронной коммерции, Баку: Элм, 2003. –84 с.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В., Основы криптографии: Учебное пособие.- М.: Гелиос АРВ, 2001.-480с.
4. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В., Криптография в банковском деле. М.: МИФИ, 1997.
5. Аснис И.Л., Федоренко С.В., Шабунов К.Б., Краткий обзор криптосистем с открытым ключом // Защита информации.-1994.-№2.-с.35-43.
6. Березин Б.В., Дорошкевич П.В., Цифровая подпись на основе традиционной криптографии // Защита информации. – 1992. Вып.2. – с.148-167.
7. Биометрическая аутентификация: Обзор // Защита информации.-1994.- №2.-С. 29-33.
8. Баричев С., Криптография без секретов. М.: ДИАЛОГ-МИФИ, - 1995.
9. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А., Алгоритмические основы эллиптической криптографии, Учебное пособие, М.: Изд-во МЭИ, 2000
10. Брассар Ж., Современная криптология. – М.: Полимед, 1999.
11. Брикелл Э.Ф., Одлижко Э.М., Криптоанализ: Обзор новейших результатов //ТИИЭР.-1988.-Т.76, № 5.-с.75-93.
12. Василенко О. Н., Современные способы проверки простоты чисел. Обзор, Кибернетический сб., вып. 25, 1988, 162-188
13. Введение в криптографию. //Под общей ред. В.В. Ященко-СПб.: Питер, 2001, 288 с.
14. Виноградов И.М., Основы теории чисел.-М.: Наука, 1981.

15. Горбатов В., Полянская О., Доверенные центры как звено обеспечения безопасности корпоративных ресурсов. // JetInfo №11 (78). – 1999. – С. 13-20.
16. ГОСТ Р34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.
17. ГОСТ Р34.11-94. Информационная технология Криптографическая защита информации. Функция хэширования.
18. Груздев С.Л., Раевский А.В., Смарт-карты и персональные компьютеры// Банки и технологии.-1997.-№4.-С.53-59.
19. Диффи У., Первые 10 лет криптографии с открытым ключом // ТИИЭР. 1988. Т.76, №5, с.54-74
20. Диффи У., Хеллман М.Э., Защищенность и имитостойкость: Введение в криптографию//ТИИЭР.-1979.-Т.67, №3-С.71-109.
21. Жельников В., Криптография от папируса до компьютера. – М.: ABF, 1996.
22. Иванов М.А., Криптографические методы защиты информации в компьютерных системах и сетях. М., 2001-368 с.
23. Камерон Стардеван, PKI заступает на дежурство, PC Week/RE, № 6/2001, с.20
24. Карпов А.Г., ЭЦП в "Электронной России" Что будет сделано в 2003 году? //Технологии и средства связи, 2002, № 6, с.72
25. Келли Джексон Хигтинс, PKI: время принимать решение //Сети и системы связи. 2002. № 6
26. Ключевский Б., Специальные криптографические протоколы // Конфидент. –1999.-№ 1-2. – С.71-79.
27. Кнут Д., Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы: пер. с англ. – М., Мир, 1977. – 724 с.
28. Конри-Мюррей Э., Основные компоненты инфраструктуры с открытыми ключами Журнал LAN, №1, 2002 год, http://www.osp.ru/lan/2002/01/040.htm
29. Лидл Р., Нидеррайтер Г., Конечные поля, т. 1, 2, М., Мир, 1988.

30. Лунин А.В., Сальников А.А., Перспективы развития и использования асимметричных криптоалгоритмов в криптографии // Конфидент. –1998.- № 6.- С. 15-23.
31. Майк Фратто, Управление отзывом сертификатов Сети и системы связи. 2000. № 12.
32. Мельников Ю., Электронная цифровая подпись: всегда ли она подлинная? Банковские технологии, №5, 1995.
33. Месси Дж. Л., Введение в современную криптологию // ТИИЭР.-1988.-Т.76, №5.-С.24-42.
34. Отставнов М. Е., От «средств защиты» – к финансовой криптографии // Конфидент. –1999. - № 6. – С. 81-87. г
35. Петров А. А., Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.
36. Ростовцев А. Г., Маховенко Е. Б., Подпись и шифрование на эллиптической кривой: анализ безопасности и безопасная реализация, http://www.ssl.stu.neva.ru/ssl/archieve/protocol.pdf
37. Саломаа А., Криптография с открытым ключом, М., Мир, 1996
38. Симмонс Г. Дж., Обзор методов аутентификации инфор мации // ТИИЭР.-1988.-Т.76, №5.
39. Чмора А. Л., Современная прикладная криптография. 2-е изд., М.: Гелиос АРВ, 2002.
40. Шеннон К. Э., Теория связи в секретных системах // В кн.:Шеннон К. Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963. с.333-402.
41. Шнайер Б., Протоколы, алгоритмы, исходные тексты на языке Си, Триумф, 2002 , 816 с.
42. Adleman L.M., Pomerance C., Rumely R.S., On distiguishig prime numbers from composite numbers, Ann. Of Math. 117(1983), p.173-206.
43. Agnew G. B., Mullin R. C., Onyszchuk I. M., Vanstone S. A., An implementation for a fast public-key cryptosystem, v. 3, N 2, 1991, 63-79
44. Anabelle Lee, Guideline for Implementing Cryptography in the Federal Government. NIST SP 800-21 – 1999.

45. Anderson R., The classification of hash functions. Proc. Of the IMA Conference on Cryptography and Coding, Cirencester, December 1993, Oxford University Press, 1995, p. 83-95.
46. ANSI X9.62, Public key cryptography for the financial services industry – the Elliptic Curve Digital Signature Algorithm (ECDSA), January 1999.
47. ANSI X9.63, Public key cryptography for the financial services industry – Elliptic Curve Key Agreement and Transport Protocols, draft, 1997.
48. Barrett P., Implementing the Rivest, Shamir and Adleman public key encryption algorithm on a standart digital signal processor, Proc. CRYPTO'86, Lect. Notes. In Comp. Sci., v. 263, 1987, 310-323
49. Beauchemin P., Brassard G., Crepeau C., Goutier C., Pomerance C., The generation of random numbers, that are probably prime, J. Cryptology, v. 1, 1988, 53-64
50. Bellare M., Micali S., How to sign given any trapdoor function, Proc. Crypto'88, Lect. Notes. In Comp. Sci., v. 403, 1990, 200-215
51. Biham E., On the Applicability of Differential Cryptoanalysis to Hash Functions. In E.I.S.S Workshop on Cryptographic Hash Functions, p.25-27, March 1992.
52. Biham E., Shamir A., Differential cryptoanalysis of FEAL and N-Hash. //Advances in Cryptology – Eurocrypt'91, p.1-16, 1991.
53. Boyar J., Chaum D., Damgard I., Convertible Undeniable Signature // Advances in Cryptology – Crypto'90 Proceedings. Springer- Verlag, 1991. – p. 189-205.
54. Chaum D., Blind signatures for untraceable payments, //Advances in Cryptology – Crypto'82, Springer-Verlag (1983), p.199-203.
55. Chaum D., van Antwerpen H., Undeniable Signatures //Advances in Cryptology – Crypto'89 Proceedings. Springer- Verlag, 1990. – p.212-216.
56. Chaum D., van Heijst E., Group signatures, Advances in Cryptology – Eurocrypt'91, Springer-Verlag (1991) p.257-265.

57. Chen L., Pederson T.P., New group signature schemes, // Advances in Cryptology – Eurocrypt'94, Springer-Verlag (1994), 171-181.
58. Chokhani S., Ford W., Internet X.509 Public Key Infrastructure Certificate Policy and Certifications Framework.–RFC2527, 1999.
59. Diffie W., Hellman M. E. New Directions in Cryptography // IEEE Transactions on Information Theory. 1976. V. IT-22. P. 644-654.
60. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. On Inform. Theory. – July 1985. – vol. IT –31, No. 4. – P.469-472.
61. Fahn P., Robshaw M.J.B., Results from the RSA Factoring Challenge, Technical Report TR-501, version 1.3, RSA Laboratories, January 1995
62. FIPS PUB 180-1, Secure Hash Standard. – National Institute of Standards and Technology, US Department of Commerce. – 17 Apr 1995.
63. FIPS PUB 186-2, Digital Signature Standard (DSS). – National Institute of Standards and Technology, US Department of Commerce. –2000 January 27.
64. Fujioka A., Okamoto T., Miyaguchi S., ESIGN: An efficient digital signature implementation for smart cards, Proc. Eurocrypt'91. Lect. Notes in Comp. Sci.,v.547,1991,186-194
65. Goldwasser S., Micali S., Rivest R., A secure digital signature scheme, SIAM J. on Computing, v. 17, N 2, 1988, 281-308
66. Gordon D.M., Discrete logarithms in GF(p) using the number field sieve, SIAM Journal of Computing (1) 6 (1993), p.124-138.
67. http://www.cryptonessie.org
68. IEEE P1363, "Standard Specifications for Public-Key Cryptography", February 2000.
69. ISO 7498-2:1989 – Open System Interconnection Reference Model – Security Architecture.
70. ISO/IEC 11770:1996. Information Technology – Security techniques – Key management.

71. ISO/IEC 14888, Digital signature with appendix – Part 3: Certificate-based mechanisms, draft, 1997.
72. ISO/IEC 9549-8:1993 ITU-T Recommendation X.509. Information Technology – OSI – The Directory: Authentication Framework.
73. Koblitz N., Elliptic Curve Cryptosystems, Mathematics of Computation, 48, 1987, pp.203-209.
74. Koç Ç. K., High-Speed RSA Implementation, Technical Report TR-201, version 2.0, RSA Laboratories, November 1994.
75. Kocher P., Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems // Lect. Notes. In Comp. Sci., v.1109- 1996.
76. Kuhn D.R., Hu V.C., Polk W.T., Chang S.J., Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST SP 800-32. – 2000.
77. Lai X. and Massey J.L., Hash Functions Based on Block Ciphers, Advances in Cryptology - EUROCRYPT'92 Proceedings, pp. 55-70, LNCS 658, Springer Verlag, 1993.
78. Lenstra H.W. Jr, Factoring integers with elliptic curves, Annals of Mathematics 126 (1987), 649-673.
79. Menezes A., van Oorschot P., Vanstone S., Handbook of Applied Cryptography. CRC Press, 1997.
80. Miller V. S., Use of Elliptic Curves in Cryptography //Advances in Cryptology – Crypto'85. – Berlin etc.: Springer-Verlag , 1986, Lect. Notes. In Comp. Sci., v.218. – p. 417-426
81. Ohta K., Koyama K., Meet-in-the-Middle Attack on Digital Signature Schemes. In Abstract of Auscrypt'90, p. 110-121, 1990.
82. Pollard J.M., Theorems on factorization and primality testing, Proc. Cambrdge Philos. Soc. 76(1974), p.521-528.
83. Rabin M.O., Digitalized signatures and public-key functions as intractable as factorization, Technical Report MIT/LCS/TR-212, MIT,1979.
84. Rivest R. L., RFC 1320: The MD4 Message-Digest Algorithm. Network Working Group, April 1992.

85. Rivest R. L., RFC 1321: The MD5 Message-Digest Algorithm. Internet Activities Board, April 1992.
86. Rivest R. L., Shamir A., Adleman L., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems //Communications of the ACM. – 1978. – Vol. 21, No. 2- P. 120-126.
87. Robshaw M., Security estimates for 512-bit RSA, Technical Note, RSA Laboratories, 1995
88. Schnorr C.P., Efficient Identification and Signatures for Smart Cards. Advances in Cryptology: Proceedings of Crypto'89, G.Brassard (ed). Lecture Notes in Computer Science, V.435, pp.239-251
89. Solovay R., Strassen V., A fast Monte-Carlo test for primality, SIAM J. Comput. 6(1977), 84-85, 7(1978), 118
90. WAP WTLS, Wireless Application Protocol Wireles Transport Security Specification, Wireless Application Protocol Forum, February 1999.

Əlavələr

Əlavə 1. Şərti ixtisarların siyahısı

AAİ	Açıq Açarlar İnfrastrukturu
ƏBOB	Ən böyük ortaq bölən
ƏS	Əməliyyat sistemi
Rİ	Rəqəm imzası
SM	Sertifikasiya mərkəzi
AES	Advanced Encryption Standard
API	Applied Programming Interface
ASN	Abstract Syntax Notation
CA	Certificate Authority
CAPI	Cryptographic Application Programming Interface
CRDP	Certificate Revocation Distribution Point
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptosystem
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISO	International Standards Organization
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MIC	Message Integrity Code
MIME	Multipurpose Internet Mail Extensions
MIPS	Millions of Instructions Per Second
MD	Message Digest
MDA	Message Digest Algorithm

MDC	Modification (Manipulation) Detection Code
NIST	National Institute of Standards and Technology
NP	Non-deterministic Polynomial
OCSP	Online Certificate Status Protocol
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
RAM	Random Access Memory
RIPE	Race Integrity Primitives Evaluation
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSL	Secure Sockets Layer
SWIFT	Society for World-Wide Interbank Financial Telecommunications
TLS	Transport Level Security
USB	Universal Serial Bus

Əlavə 2. Rəqəm sertifikatının formatı

Version	Sertifikatın versiyası	1, 2, 3
Certificate Serial Number	Sertifikatın seriya nömrəsi	9E09 150E D005 8395 4150 A460 01E7 7BBB
Signature Algorithm Identifier	Rəqəm imzası alqoritminin identifikatoru	sha1RSA
Issuer X.500 Name	Sertifikatı buraxanın adı	OU = EFS File Encryption Certificate L = EFS CN = ITI
Validity Period	Sertifikatın fəaliyyət müddəti	Qüvvədədir -dən: Nov 2 06:59:00 1999 GMT Qüvvədədir -dək: Nov 6 06:59:00 2001 GMT
Subject X.500 Name	Sertifikat sahibinin adı	C=AZ, ST=Baku, O=PKI, CN=Aslanov
Subject Public Key Info	Sahibin açıq açarı	Açarın tipi: RSA açıq açarı Açarın uzunluğu: 1024 Açar: 3081 8902 8181 00B7 ...
Issuer Unique ID version 2	Sertifikatı buraxanın unikal identifikatoru	
Subject Unique ID version 2	Sahibin unikal identifikatoru	
CA Signature	Sertifikat Mərkəzinin imzası	37E7 F141 F186 53BB 5B9E 7CB1 6805 67DB E2C1 B2B7

Əlavə 3. AAİ qurmaq üçün mövcud proqram vasitələri

Proqram vasitəsi, istehsalçı, ölkə	Qiymət
UniCert 3.5 Baltimore Technologies, USA www.baltimore.com	Baza konfiqurasiyası: 36 min dollar Advanced Registration Module 20 min dollar Lisenziya: 1 min istifadəçi 16 min dollar 10 min istifadəçi 100 min dollar
Entrust 5.01 Entrust Technologies USA www.entrust.com	Baza konfiqurasiyası: 25 min dollar Sertifikat (2 il müddətində qüvvədə): 5 min istifadəçi hər bir 0,75 dollar 10 min istifadəçi hər bir 1,5 dollar
Keon 5.5 RSA Security USA www.rsasecurity.com	Tam qurulma qiyməti: (Keon Advanced PKI + Keon Desktop) 1 min istifadəçi 175 min dollar 10 min istifadəçi 990 min dollar
OnSite 4.51 VeriSign USA www.verisign.com	Sistemin istifadəsi üçün: 1 min istifadəçi 70 min dollar 10 min istifadəçi 220 min dollar

Əlavə 4. PKIX qrupunun nəşr etdiyi Internet standartları

- Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 2459)
- Internet X.509 Public Key Infrastructure Certificate Management Protocols (RFC 2510)
- Internet X.509 Certificate Request Message Format (RFC 2511)
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527)
- Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates (RFC 2528)
- Internet X.509 Public Key Infrastructure Operational Protocols – LDAPv2 (RFC 2559)
- Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP (RFC 2585)
- Internet X.509 Public Key Infrastructure LDAPv2 Schema (RFC 2587)
- X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP (RFC 2560)

Əlavə 5. PKCS standartları

- **PKCS #1:** RSA Cryptography Standard
- **PKCS #2:** *Qeydə bax*
- **PKCS #3:** Diffie-Hellman Key Agreement Standard
- **PKCS #4:** *Qeydə bax*
- **PKCS #5:** Password-Based Cryptography Standard
- **PKCS #6:** Extended-Certificate Syntax Standard
- **PKCS #7:** Cryptographic Message Syntax Standard
- **PKCS #8:** Private-Key Information Syntax Standard
- **PKCS #9:** Selected Attribute Types
- **PKCS #10:** Certification Request Syntax Standard
- **PKCS #11:** Cryptographic Token Interface Standard
- **PKCS #12:** Personal Information Exchange Syntax Standard
- **PKCS #13:** Elliptic Curve Cryptography Standard
- **PKCS #15:** Cryptographic Token Information Format Standard

Qeyd: PKCS#2 və PKC #4 standartları PKCS #1-ə birləşdirilmişdir.

Mündəricat

Расим Магамед оглы Алгулиев
Ядигар Насиб оглы Имамвердиев

Технология цифровой подписи

Аннотация

В пособии излагаются основы технологии цифровой подписи и основные понятия инфраструктуры открытых ключей. Исследуются существующие схемы цифровой подписи и их математические основы, вопросы безопасности схем цифровой подписи, основные угрозы и типичные атаки на схемы цифровой подписи.

Рассматриваются научно-теоретические проблемы практического применения технологии цифровой подписи, вопросы реализации на интеллектуальных карточках, а также вопросы применения в конкретной операционной системе и в прикладных приложениях.

Пособие предназначено для студентов и аспирантов, специализирующихся в области информационной безопасности компьютерных сетей. Может быть полезно разработчикам и пользователям компьютерных систем и сетей.

Ключевые слова: атака, аутентификация, ключ, угроза, инфраструктура открытых ключей, целостность, электронная цифровая подпись, цифровой сертификат, хеш-функция, управление ключами.

Rasim Mahammad oglu Aliguliev
Yadigar Nasib oglu Imamverdiyev

Digital Signature Technology

Annotation

The principles of digital signature technology and the main concepts of public key infrastructure have been presented in this manual. The existing digital signature schemes and their mathematical foundations, the issues of security within these schemes, major threats and typical attacks on them have been subjects of research in this manual.

The scientific-theoretical problems of practical application of digital signature technology, the issues of its application on intellectual cards, as well as issues of its implementation in specific operating systems and software applications have been considered.

This manual has been designed for under- and postgraduate students specializing in the field of information security in computer networks. It can also be useful for designers and users of computer systems and networks.

Key words: attack, authentication, key, threat, open keys infrastructure, integrity, digital signature, digital certificate, hash-function, management by keys.

Formatı 60x84 1/16.
Həcmi 8,25 ç.v.
Tirajı 300.
Sifariş №92.
Qiyməti müqavilə ilə.

RNPM-nin mətbəəsində çap olunub.
(İstiqlaliyyət, 8)