**MÖVZU 12.**

**ELEKTRON KOMMERSIYADA İNFORMASİYA**

**TƏHLÜKƏSİZLİYİ. ELEKTRON İMZA**

1. Ekranlaşdırıcı sistemlər
2. Web-əlavələrin qorunması
3. İnformasiyanın şifrlənməsi
4. Steqanoqrafiya

**1**. Məlumatların təhlükəsizliyinin təmin olunması Internetdə mövcud olan əsas problemlərdən biridir. Internetdə informasiya mübadiləsi öz təyinatına görə azad və nəzarətsizdir. Əgər əlavə təhlükəsizlik tədbirləri qəbul olunmazsa, o zaman Internetdə tranzaksiyaların konfidensiallığını və məlumatların bütövlüllüyünü təmin etmək ptaktiki olaraq mümkün deyildir. İnformasiya sahəsində təhlükəsizlik dilemması aşağıdakı qaydada formalaşdırılır: sistemin qorunması ilə onun açıq olması arasında seçim etmək lazım gəlir.

**Ekranlaşdırıcı sistemlər**

Öz kompüterlərinə icazəsiz daxilolmaların qarşısını almaq üçün kompüter texnologiyasından istifadə edən bütün korporativ və idarə şəbəkələri daxili şəbəkə ilə Internet arasında *ekranlar* *{firewall)* qoyurlar ki, onun da vəzifəsi xarici istifadəçilər tərəfindən daxilolmalara nəzarət edilməsindən ibarətdir. Daha çox təhlükəsizliyi *TCP/IP* protoikolundangeri çəkilmə və Internetə daxil olma üçün şlüzlərdən istifadə olunması yolu ilə təmin etmək olar.

Ekran *{firewall)* — müştərilərin bir sistem çoxluğundan digər çoxluqdakı serverdə saxlanılan informasiyaya çıxışının bir-birindən ayrılması vasitəsidir.

Ekran bu iki informasiya sistemləri çoxluğu arasındakı bütün informasiya axınlarına nəzarət edərək özünəməxsus «informasiya membranı» rolunu oynayır. Вu mənada ekran - filtrlər dəsti kimi başa düşülə bilər ki, bunlar da onlardan keçən informasiyanı təhlil edərək və onların əsasında olan alqoritmlər əsasında qərar qəbul edir: bu informasiyanı buraxsın və yaxud onun ötürülməsinə rədd etsin. Bundan başqa, belə bir sistem girişlərin bir-birindən ayrılması prosesi ilə bağlı olan hadisələri, o cümlədən informasiyaya bütün «qeyri-qanuni» girişləri qeydiyyatdan keçirə bilər, dərhal münasibət göstərilməsi tələb olunan vəziyyətlər haqqında xəbərdarlıq edə bilər.

Adətən ekranlaşdırıcı sistemləri qeyri-simmetrik edirlər. Ekralnar üçün «daxili» və «xarici» anlayışlar müəyyən olunurlar və ekranın vəzifəsi daxili şəbəkənin «potensial düşmən» ətrafdan müdafiə olunmasından ibarətdir.

Ekranlaşdırıcı sistemlər qarşısında aşağıdakı tələblər qoyulur:

• daxili (müdafiə olunan) şəbəkənin təhlükəsizliyinin qorunması və bütün xarici birləşmələr üzərində tam nəzarətin həyata keçirilməsi;

• təşkilatın təhlükəsizliyinin sadə və tam qaydada təmin olunması üçün ekranlaşdırıcı sistem güclü və çevik idarəetmə vasitələrinə malik olmalıdır;

• ekranlaşdırıcı sistem lokal şəbəkənin istifadəçiləri üçün hiss edilməz olmalı və onların öz qanuni fəaliyyətini həyata keçirməsini çətinləşdirməməlidir;

• ekranlaşdırıcı sistem əhəmiyyətli dərəcədə effektiv işləməli və «pik» rejimində (qızğın rejimdə) bütün daxil olan və çıxan trafiki işləyib başa çatdırmalıdır. Bu onun üçün lazımdır ki, *firewall* çoxlu sayda çağırışlarla «basılmasın» və bu da onun işini poza bilməsin;

• təhlükəsizliyin təmin olunması sistemi istənilən bütün icazə olunmayan daxilolmalardan qorunmalıdır;

• ekranların idarə edilməsi sistemi təşkilatın bütün bölmələri və filialları üçün mərkəzləşdirilmiş qaydada vahid təhlükəsizlik siyasətinin keçirilməsini təmin etməlidir;

• *firewall* sistemi avtorizasiya vasitələrinə malik olmalıdır.

*Firewall-1* sistemi üçün mərkəzi modul – bütün kompleksin idarə edilməsi moduludur. Bu modulla şəbəkənin təhlükəsizliyi administratoru işləyir. O, girişin məhdudlaşdırılması siyasətini müəyyən edir, bunun haqqında informasiya filtrdən keçirilmə moduluna verilir. Filtrdən keçirilmə modulu şəbəkə interfeyslərinə daxil olan bütün paketləri nəzərdən keçirir və qəbul olunmuş qaydalardan asılı olaraq bu paketləri buraxır və yaxud onları kənara atır, qeydiyyat jurnalında müvafiq yazı edir.

Privat (xüsusi) sənədlərə çıxış zamanı istifadəçilərə ad və parol (məxfi ad) verilir, özü də parol açıq halda heç bir yerdə saxlanılmır. Bu tələb onun üçün lazımdır ki, potensial haker özgənin parolunu oxuya bilməsin. Sistem leqal istifadəçiləri identifikasiya etmək üçün kompüterin yaddaşında xüsusi alqoritmlə hesablanmış parolların nümunələri saxlanılır.

**2.**  *Web-*əlavələrin qorunması

*Web-əlavələr* iki protokolla qorunurlar: *Secure HTTР (S-HTTF)* və *Secure Sockets Layer (SSL);* onlarserverlər və brauzerlər üçün autentifikasiyanı, həmçinin məxfiliyi və serverlə və brauzerlərlə birləşmə üçün məlumatların bütövlüyünü təmin edirlər. Hipermətnlərin ötürülməsi protokolunun *(HTTP)* himayə olunması üçün istifadə olunan *S-HTTP* sənədlərin avtorizasiyasını və müdafiə olunmasını təmin edir. *SSL* də oxşar müdafiə metodlarını təklif edir, lakin o, kommunikasiya kanalı üçün nəzərdə tutulub.

*SSL* əsasında açıq açardan istifadə etməklə assimmetrik şifrələnmə sxemi durur. Texniki və lisenziya xüsusiyyətlərindən asılı olaraq bu protokol o qədər də etibarlı sayılmır, buna görə də tədricən müdafiə olunmuş elektron tranzaksiyaların standartı - *SEL (Secure Electronic Transaction)* tətbiq olunur ki, o da gələcəkdə Internetdə kredit kardları ilə alışlar üzrə hesablaşmalarla bağlı olan tranzaksiyaların işlənilməsi üçün *SSL* standartı ilə əvəz olunacaqdır. Yeni standartın müsbət cəhətləri arasında tranzaksiyanın bütün iştirakçılarının autentifikasiyası imkanlarını da daxil etməklə təhlükəsizliyin güclənməsini göstərmək olar.

**3. İnformasiyanın şifrlənməsi**

Informasiyanın qorunması fəndlərindən biri məlumatların *şifrlənməsidir (kriptoqrafiya)*. Adi yanaşma ondan ibarətdir ki, sənədə hər hansı bir şifrlənmə metodu (onu *açar* adlandıraq) tətbiq olunur, bundan sonra sənədi adi vasitələrlə oxumaq mümkün olmur. Onu ancaq həmin açarı bilən oxuya bilər. Şifrlənmə və cavab məlumatı da oxşar qaydada baş verir. Əgər informasiya ilə mübadilə prosesində şifrlənmə və oxunma üçün eyni açardan istifadə olunursa, belə kriptoqrafik proses *simmetrik* olur.

Simmetrik prosesin əsas qüsuru ondan ibarətdir ki, informasiya ilə mübadiləyə başlamazdan əvvəl açarın ötürülməsini yerinı yetirmək lazımdır, bunun üçün yenə də qorunan əlaqə lazımdır, yəni problem təkrar olunur, ancaq digər səviyyədə. Əgər müştəri tərəfindən malın və yaxud xidmətin kredit kardının köməyi ilə ödənişinə nəzər salsaq, belə çıxır ki, ticarət firması özünün hər bir müştərisi üşün bir açar yaratmalı və hansı bir yolla isə onlara bu açarları verməlidir. Bu isə həddindən artıq narahatdır.

Buna görə də hazırda Internetdə qeyri-simmetrik kriptoqrafik sistemlərdən istifadə olunur ki, bunlar da bir deyil, iki iki açardan istifadə olunmasına əsaslanır. Bu aşağıdakı qaydada baş verir. Şirkət müştərilərlə iş üçün iki açar yaradır: biri — açıq *(public —* açıq), digəri isə — bağlı *(private —* şəxsi) açar. Həqiqətdə isə bu, vahid bir açarın bir-biri ilə bağlı olan iki «yarısıdır».

Açarlar elə qurulublar ki, bir yarım tərəfindən şifrələnmiş məlumatin şifri ancaq açarın ikinci yarısı tərəfindən açıla bilər. Çüt açar yaradaraq, ticarət şirkəti açıq açarı (açıq yarısın) yayımlayır, və bağlı açarı (öz yarımını) etibarlı saxlayır.

Həm açıq, həm də bağlı açar hər hansı bir kod ardıcıllığını nəzərdə tutur. Şirkətin açıq açarı onun serverində yerləşdirilir, oradan isə hər bir şəxs onu əldə edə bilər. Əgər müştəri firmaya sifariş etmək istəyirsə, o, açıq açarı götürüb özünün sifarişini və kredit kardı barədə məlumatı kodlaşdıra bilər. Kodlaşdırmadan sonra bu məlumatı ancaq bağlı açarın sahibi oxuya bilər. Heç bir iştirakçı, hətta sifariş verənin özü də özünün məlumatını oxuya bilmir.

Əgər firma sifarişin icraya qəbul olunması barədə qəbz göndərmək lazım gələrsə, onu özünün bağlı açarı ilə kodlaşdıra bilər. Müştəri həmin şifri firmanın açıq açarı ilə aça bilər. O, tam əmindir ki, qəbzi məhz həmin firma göndərmşdir, çünki firmanın bağlı açarına heç kimin girişi yoxdur.

Digər tərəfdən SMS məlumatlara da çıxmaq məqsədəuyğundur ki, bu da edilən hər bir tranzaksiya haqqında dərhal məlumat almağa imkan verər.

**4.** **Steqanoqrafiya.** *Steqanoqrafiya* – informasiyanın gizli ötürülməsi və yaxud gizli saxlanılması texnikasını nəzərdə tutur. Steqanoqrafiya öz qarşısında məlumatın ötürülməsi faktının gizlədilməsi məqsədini qoyur.

Steqanoqrafik proqram təminatı informasiyanı səsi və təsviri generasiya edən sistemin işi zamanı baş verən adi maniə və yaxud qüsurlar şəklində gizlədir. Gizlədilmiş məlumatın aşkar olunmaması üçün o, təbii maneələrin malik olduğu statistik göstəricilərə malik olmalıdır. Multimediyada bu məlumat videokadrlar arasında gizlədilə bilər.

Kriptoqrafiyanın steqanoqrafiyadan fərqi ondan ibarətdir ki, onda məlumatın verilməsi faktı deyil, ancaq onun mənası və məzmunu gizlədilir. Vacib məlumatların göndərilməsi zamanı steqanoqrafiyadan istifadə olunması çox risklidir. Steqanoqrafiya – informasiyanın qorunmasının çox da etibarlı olmayan vasitəsidir. Ona görə də steqanoqrafiyanın etibarlılığını artırmaq üçün əvvəlcədən kriptoqrafik dəyişmələrdən də istifadə etmək lazımdır.

**Elektron-rəqəmli imzaların yaradılması və elektron poçt vasitəsilə verilən məlumatların qorunması üçün kriptosistemlərin tətbiq olunması**

**Əsas anlayışlar, terminlər və onların təyinatı.** Elektron poçt vasitəsilə göndərilən məlumatların qorunması məqsədilə Amerikalı proqramçı Filip Simmerman (Philip R.Zimmermann) 80-ci illərin axırında 90-cı illərin əvvəlində xüsusi istehlakçılar üçün açıq şifrlənmə proqram sistemi - Pretty Good Privacy (PGP) işlənib hazırlanmış və pulsuz istifadə üçün təklif olunmuşdur. PGP hazırda dünyada ən tanınmış şifrlənmiş proqram əlavəsi olmaqla həm kommersiya əsasında, həm də pulsuz olaraq (Freeware) yayılır.

Hər hansı bir xüsusi tədbirsiz oxuna bilən, dərk olunan və başa düşülən məlumat **açıq mətn (plaintext, cleartext)** adlanır.

Açıq mətnin başa düşülmək üçün əlçatmaz olması məqsədilə onun təhrif edilməsi prosesı **şifrlənmə (encryption** və yaxud **enciphering)** adlanır.

Açıq mətnin şifrlənməsinin nəticəsi **şifr-mətn (ciphertext)** olur.

Əks proses, yəni şifrmətnin ilkin şəklə gətirilməsi **şifrin açılışı (decryption** və yaxud **deciphering)** adlanır.

🗐 🡺🔒 🗐 🡺 🔓 🗐 **açıq mətn şifrlənmə şifr-mətn şifrin açılması açıq mətn**

Şək. Şifr-mətnin yaranma prosesi

Kriptoqrafiya – məlumatların qorunması haqqında elmdir, kriptoanaliz – kriptoqrafik yaranmaların təhlili və onların açılışı haqqında elmdir. Kriptoqrafiya və kriptoanalizi – kriptologiya birləşdirir.

Kriptologiyada ən vacibi - **«açar»** və  **«şifr»** anlayışlarıdır.

**Şifr**, və yaxud kriptoqrafik alqoritm– məlumatın şifrlənməsi və şifrin açılması proseslərini təsvir edən riyazi düsturdur.

**Açar** - müəyyən, bir qayda olaraq, məxfi söz, rəqəm və yaxud frazadır (ibarədir).

Açıq mətni şifrləmək üçün şifr açarla birgə istifadə olunur. Bir şifrlə, lakin müxtəlif açarlarla eyni bir məlumat müxtəlif şifrmətnlərə çevrilə bilər.

Kriptoqrafiya **davamlı**, və yaxud **zəif** ola bilər.

Kriptoqrafiyanın davamlılığı onunla ölçülür ki, şifr-mətndən ilkin açıq mətnin bərpa edilməsinə nə qədər vaxt və resurs lazım gələcəkdir. Davamlı kriptoqrafiyanın nəticəsi kimi şifrin açılması üçün lazımi alətlər olmadan çətinliklə açıla bilən şifr-mətni göstərmək olar. Beləliklə, şifr-mətnin qorunulma dərəcəsi bütövlükdə iki şeydən asılı olur: açarın məxfiliyindən və kriptoalqoritmin davamlılığından. Bununla yanaşı, həm açarın məxfiliyi, həm də kriptoalqoritmin davamlılığı hazırda kompüterlərin hesablama imkanları ilə nizamlanır.

Kriptoalqoritm, açarlar və onları calaşdıran və hesablama maşınları üçün proqramda reallaşdırılan protokollar – **kriptosistemi** təşkil edir.

Əgər kriptosistemdə göndərən və alan məlumatın şifrlənməsi nə şifrin açılması üçün eyni açarın surətindən istifadə edirlərsə, bu cür sistem **simmetrik sistem**, tətbiq olunan açar isə - **gizli** və yaxud **simmetrik açar** adlanır.

Aydındır ki, simmetrik kriptosistemin köməyi ilə məlumatlarla mübadilə olunması üçün alan və göndərən qabaqcadan razılaşdırılmış açarların surətlərini bir-birləri ilə dəyişməlidirlər. Əgər onlar coğrafi cəhətdən uzaq yerdədirlərsə, bu zaman inanılmış kuryerin xidmətindən istifadə etməlidirlər ki, daşınma zamanı bu açar digərlərin əlinə keçə bilməsin. Simmetrik kriptosxemlərin qlobal problemi açar idarəolunması kimi adlandırılan **(key management)** proseduranın yerinə yetirilməsinin çətinliyi ilə bağlıdır.

Qərbdə bank və kommersiya sferalarında 70-ci illərdən geniş tətbiq olunan simmetrik alqoritmin misalı kimi – **Data Encryption Standart (DES)** göstərmək olar. Hazırda onu **Advanced Encryption Standart (AES)** əvəz edir.

Simmetrik açarın tətbiqi prosesi şək. –də göstərildiyi kimidir.

🗝

🗐 🡺🔒 🗐 🡺 🔓 🗐

**açıq mətn şifrlənmə şifr-mətn şifrin açılması açıq mətn**

Şək. Simmetrik açarın tətbiq olunması prosesi

Açarların idarəolunması problemi **açıq,** və yaxud  **assimetrik açarlı** (bunun konsepsiyası 1975-ci ildə Uitfild Diffi və Martin Hellman tərəfindən təklif olunub) kriptoqrafiyanın kəşfi ilə həll olundu.

Açıq açarlı kriptoqrafiya – assimmetrik sxem olmaqla burada **cüt açarlar (keypair): açıq açar (publickey)** –onunla məlumat şifrlənir -və **bağlı açar (privatekey)** – onunla şifr-mətnin şifri açılır - təttbiq olunurlar.

Açıq açar bütün dünyaya yayılır, bağlı açar isə məxfi saxlanılır.Acıq açarın surətinə malik olan istənilən şəxs, məlumatı şifrəliyib göndərə bilər ki, bunu da ancaq bağlı açarla oxumaq mümkündür.

Assimmetrik açarın tətbiqi prosesi şək. –də göstərildiyi kimidir.

*açıq açar bağlı açar*

☺😐☹ ☺

🗝 🗝

🗐 🡺🔒 🗐 🡺 🔓 🗐

**açıq mətn şifrlənmə şifr-mətn şifrin açılması açıq mətn**

Şək. Assimmetrik açarın tətbiq olunması prosesi

Assimetrik kriptoqrafik alqoritmlərin misalı kimi aşağıdakı göstərmək olar:

* Elgamal (müəllifinin, Tahir Elqamalın şərəfinə adlandırılıb)
* RSA (onun ixtiraçıları – Ron Rivesta, Adi Şamir və Leonard AdAmanın şərəfinə adlandırılıb)
* DH / DS (konsepsiyanı təklif etmiş müəlliflərin adlarına görə: Diffie-Hellman və Devi Kravits tərəfindən ixtira olunmuş rəqəmli imzanın alqoritmi kimi qəbul olunan alqoritmin – Digital Siqnature Algorithm – adına görə adlandırılıb). Son vaxtlar bu kriptosistem DH / DSS kimi identifikasiya olunur.

Assimetrik sxemlərin meydana gəlməsi texnoloji inqilab oldu ki, bu sistem geniş istifadəçi dairəsinə davamlı kriptoqrafiya təklif edə bildi.

Açıq açarlı kriptosistemlərdən istifadənin əlavə üstünlüyü ondan ibarətdir ki, onlar elektron rəqəmli imzaların (ERİ) olduğu elektron sənəd şəklindəki məlumatlarla mübadilə etmək imkanı yaradır.

ERİ möhürün və kağızda özünün imzası kimi eyni məqsədə xidmət edir. Lakin özünün rəqəmli təbiətinə görə ERİ əl imzasını və möhürü üstünləyir. ERİ nəinki müəllifliyi təsdiq edir (yəni o, **avtorizə** vasitəsidir), o, həm də imzalanmış elektron sənədin məzmununun ötürülmə prosesi zamanı dəyişilib-dəyişilməməsini müəyyən etməyə imkan verir (yəni **bütövlülüyə nəzarəti** təmin edir).

Müəllifliyin təsdiq edilməsinin sadə üsulu şək. göstərildiyi kimidir.

*bağlı açar açıq açar*

☺ ☺😐☹

🗝 🗝

🗐 🡺🔒✍ 🗐 🡺 🔓 🗐 **açıq mətn imzalanma imzalanmış tutuşdurma tutuşdurulmuş**

**mətn mətn**

Şək. Müəllifliyin təsdiq edilməsinin sadə üsulu

Məlumatın alanın açıq açarı ilə şifrlənməsi əvəzinə göndərən onu özünün şəxsi imzası ilə «imzalayır». Əgər alınan imzalanmış şifr-mətnin tutuşdurulması zamanı alan şəxs məlumatı göndərənin açıq açarı ilə aça bilirsə, məlumatın mənbəyi identifikasiya olunmuş hesab edilir.

Lakin bu sadə üsul ciddi qüsurlarına görə tətbiq olunmur. Aydın olmuşdur ki, məlumatın açıq açarla şifrlənməsi zamanı məlumatın həcmi ciddi olaraq artır – demək olar ki, iki dəfə.

Üsulun yaxşılaşdırılması dəyişilmə prosesinə yeni tərkibli ilkin məlumatın – birtərəfli davamlı heş-funksiyanın daxil edilməsi hesabına təmin olunur.

**Birtərəfli davamlı heş-funksiya** – riyazi alqoritm olmaqla sərbəst ölçüdə olan məlumatı **heş-əhəmiyyətə** (sabit uzunluğa malik olan sətirə) çevirir.

Bu cür heş-funksiya dəyişilmə məqsədlərinə tətbiqən iki xüsusiyyətə malikdir:

* bu funksiyanən heş-əhəmiyyətindən iklin məlumatı və yaxud hər hansı bir hissəsini hesablayıb çıxarmaq mümkün deyildir;
* iki sərbəst məlumatlar üçün heş-əhəmiyyətin təkrarlanması ehtimalı həddindən artıq azdır.

Başqa sözlə, elə bir süni yaradılmış saxta məlumat yoxdur ki, o, dəyişildikdən sonra ilkin məlumatın heş-əhəmiyyətini təkrarlaya bilsin.

Birtərəfli davamlı heş-funksiyasının dəyişilməsi prosesindən istifadə edən kriptosistemlərdə ilikn məlumatdan məhdud uzunluqda sətir törənir (qenerasiya olunur) ki, bu da **məlumatın daycesti (message digest)** adlanır.

Sonradan isə məlumatın alınmış daycesti (messajı) göndərənin bağlı açarı ilə «imzalanır» (yəni şifrələnir). Yaradılmış «imza» ilkin materiala calaşdırılır və alınmış material elektron poçt vasitəsilə alan şəxsə göndərilir. Alan şəxs bu məlumatı elə o zaman oxumaq imkanına malik olur, çunki o, açıq mətni görür. Göndərənin müəllifliyinə və alınmış məlumatın bütövlüyünə əmin olmaq üçün alan şəxs öz kompüter ində qurulmuş kriptosistemin köməyi ilə göndərənin açıq açarı vasitəsilə imzanın şifrini açır. Əgər ünvan sahibi (adresat) tərəfindən hesablanmış və məlumatla birlikdə alınmış daycestlər üst-üstə düşürlərsə, onda məlumat imzalanqdan sonra dəişməmişdir.

Şək. bu proses haqqında təsəvvür yaradır.

🗐 🡺 💳 **heş-funksiya**

**açıq mətn**

**bağlı açarla imza-lanmış daycest**

**🡻**

🖂 🡺 🖆 🡺 🗐

**məlumatın daycesti**

🡹 **açıq mətn**

**+**

🗝

**göndərənin bağlı açarı**

**imza**

Şək. Birtərəfli davamlı heş-funksiyalı kriptosistemlərin sxemi