“ AZƏRBAYCAN HAVA YOLLARI ”

QAPALI SƏHMDAR CƏMİYYƏTİ

MİLLİ AVİASİYA AKADEMİYASİ



**SƏRBƏST İŞ №4**

Fakültə: “Aerokosmik”

İxtisas: “İnformasiya texnologiyalari”

Fənn: “Veb sistemləri və texnologiyaları”

Mövzu : “Məlumatların şifrələnmə metodları”

Qrup: 2441a

Tələbə: Çələbi Gülsüm

Müəllim: Nübar Heydərzadə

BAKI 2024

**Məlumatların Şifrələnməsi**

Şifrələmə şəxsi məlumatların və məxfi təşkilati məlumatların qorunması üçün mühüm vasitədir. Girişə nəzarət, audit və siyasətlər qorunan məlumatların təhlükəsizliyi üçün vacibdir. Bununla belə, bəzi ssenarilərdə əlavə təhlükəsizlik səviyyəsi əlavə etmək üçün şifrələmə tələb olunur. Şifrələmə məlumatların saytlar arasında təhlükəsiz ötürülməsini və ya məlumatın saxlanmasını təmin etməyə kömək edir.

Şifrələmə qərarı asan olsa da, yerləşdirilməsi qeyri-müəyyənliklə dolu ola bilər. Müxtəlif şifrələmə alqoritmləri, şifrələmənin tətbiqi yolları, şifrələmənin tətbiq ediləcəyi səviyyələr və şifrələmə strategiyasını tətbiq etməzdən əvvəl nəzərə alınmalı olan yan təsirlər var.

**Kriptoqrafiya** yunanca Κρυπτός (gizli, sirli) və Γραφος (yazı) sözlərindən yaranıb və hər hansı bir informasiyanın konfidensiallığını təmin etmək üçün istifadə edilir. Kriptoqrafiya məlumatın şifrlənməsini nəzərdə tutur. Şifrələnmiş məlumat yalnız açıq mətni oxuma haqqı olan istifadəçi tərəfindən deşifrə edilə bilər. Şifrləmə məlumatın təhlükəsizliyinə tam zəmanət vermir amma onun icazəsiz istifadəsini dəfələrlə məhdudlaşdırır. Bu mətni deşifrləyib oxumaq üçün açar sözünü və şifrləmə alqoritmini bilmək lazımdır. Şifrlənəcək mətn açıq mətn adlanır, bu mətn şifrləmə açarından istifadə etməklə şifrləmə alqoritmi vasitəsilə şifrlənir.

        İlk kriptoqrafik yazılar bizim eranın əvvəlində meydana çıxır. Qədim Misir əlyazmalarında dini mətnlər və tibbi reseptlər qeyri-standart heroqliflərlə şifrlənirdi. Çinli alim Song Tzu “Döyüş sənəti” kitabında kəşfiyyat və əks-kəşfiyyatın təməl prinsiplərini, həmçinin şifrələnmiş məlumatların işlənməsi və qorunması metodlarını formalaşdırmışdı. Roma imperatoru Yuli Sezar da öz yazışmalarında indi onun adını daşıyan “Sezar şifrəsi”-dən istifadə edirdi. Müasir ingilis əlifbasına tətbiqdə bu şifrə aşağıdakından ibarət idi – adi əlifba yazılırdı, sonra onun altında həmin əlifba, lakin sola üç hərf dövri sürüşmə ilə yazılırdı:

ABCDEFGHIJKLMNOPQRSTUVWXYZ  
DEFGHIJKLMNOPQRSTUVWXYZABC

       Şifrləmə zamanı A hərfi D hərfi ilə, B hərfi E ilə və beləcə əvəz olunurdu. Məsələn: **VENI VIDI VICI** (gəldim, gördüm, qələbə çaldım) sətri şifrləmə zamanı YHQL YLGL YLFL sətrinə keçir. Şifrlənmiş məlumatı alan hərfləri ikinci sətirdə axtarırdı və onların üstündəki hərflərə görə ilkin mətni bərpa edirdi. Sezar şifrində açar əlifbanın ikinci sətrindəki sürüşmənin qiymətidir.

       Birinci Dünya Müharibəsi dövründə kriptoqrafiya artıq qəbul edilmiş bir döyüş insturmentinə çevrildi. Belə ki, Alman səfiri Artur Zimmermanın teleqramının ABŞ xüsusi xidmət orqanları tərəfindən tutulması ABŞ-ın müttəfiqlərin tərəfində müharibәyə girməsinə səbəb olmuşdu. İkinci Dünya Müharibəsində isə kriptoqrafiya kompüter sistemlərinin inkişafı üçün bir növ katalizator oldu. İstifadə olunan şifrələr (almanlarda “Enigma”, ingilislərdə “Turing Bombe”) məlumat nəzarətinin həyati əhəmiyyətini açıq şəkildə göstərdi.

İnternetin inkişafı kriptoqrafiyanı yeni səviyyəyə qaldırdı. Kriptoqrafik metodlar elektron ticarət əməliyyatlarında, telekommunikasiya və digər sahələrdə geniş istifadə olunmağa başlandı. Bunların içərisində ən çox populyarlıq qazanan 2009-cu ildə Satoşi Nakomoto tərəfindən yaradılan kritptovalyuta – [**bitcoin**](https://kriptoinvest.az/2021/01/07/bitcoin-n%c9%99dir/) oldu. İlk rəqəmsal valyuta olan bitcoin tranzaksiyaları üçün bank və ya hər hansı digər maliyyə təşkilatının vasitəçi olmasına ehtiyac qalmır. Kriptovalyuta hər hansı dövlətin siyasətindən, qanunlarından, pul vahidindən aslı deyil və heç bir qurum tərəfindən tənzimlənmir.

         Elektron Gizlilik İnformasiya Mərkəzi (Electronic Privacy Information Center, EPIC) 1998-ci ildə əksər dünya ölkələrində kriptoqrafiya sahəsində milli siyasət və qanunvericiliyin vəziyyəti barəsində hesabat hazırlamışdı. Bu hesabatda ölkələr qəbul etdikləri və həyata keçirdikləri kriptoqrafiyaya nəzarət siyasətinin xarakterindən asılı olaraq yaşıl, sarı və qırmızı rənglə şərti işarələnmiş üç qrupa bölünüb:

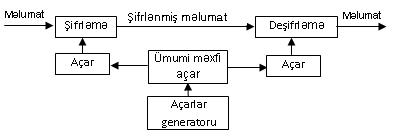
* yaşıl qrup – kriptoqrafiyanın tətbiqini praktiki olaraq məhdudlaşdırmayan ölkələr;
* sarı qrup – ölkə daxilində kriptoqrafiyanın tətbiqi və ikili təyinatlı proqram vasitələrinin ixracına müəyyən nəzarəti həyata keçirmək niyyətində olan ölkələr:
* qırmızı qrup – kriptoqrafiyaya və ölkə daxilində onun tətbiqinə nəzarət edən ölkələr.

      Hesabatın analizi göstərir ki, hazırda dünya ölkələrinin əksəriyyətində kriptoqrafiyanın tətbiqinə nəzarət yoxdur, informasiyanın kriptoqrafik mühafizəsi vasitələri hər hansı məhdudiyyət olmadan istehsal oluna, istifadə edilə və satıla bilər (yaşıl qrup). Kriptoqrafiya vasitələrinin tətbiqinə ciddi nəzarət edilən qırmızı qrupa Belarus, Çin, İsrail, Pakistan, Rusiya və Sinqapur daxildir. Yeni nəzarət tədbirlərinin tətbiqini nəzərdən keçirən ölkələr ABŞ, Hindistan və Cənubi Koreyadır. Bununla yanaşı, hazırda ABŞ müxtəlif ölkələrdə tətbiq edilən kriptoqrafik açarlara beynəlxalq nəzarətin həyata keçirilməsini və bu açarların Braziliya, Sinqapur və Cənubi Afrika Respublikası kimi ölkələrə verilməsini təklif edir. Kriptoqrafiya siyasətinin əsas prinsipləri İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (İƏİT) kriptoqrafik mühafizə vasitələrindən istifadəyə nəzarətin zəifləməsi ilə bağlı beynəlxalq səviyyədə müşahidə edilən tendensiyaya əsaslanaraq, 1997-ci ildə “Kriptoqrafiya sahəsində siyasətin əsas prinsipləri”ni qəbul etdi. Prinsiplər baxılan məsələdə dövlətin və fərdlərin maraqları arasında kompromis tapmağa yönəlmişdi. Hökumətlərə tövsiyə olunurdu ki, şəxsi həyatın toxunulmazlığı hüququna hörmətlə yanaşaraq, milli təhlükəsizlik və hüquq-mühafizə orqanlarının maraqlarını nəzərə alaraq, biznes əməliyyatlarını qorumaq üçün də kriptoqrafiyadan istifadəyə kömək etsinlər. Əsas prinsiplər aşağıdakıları əhatə edir:

1. Kriptoqrafik metodlara etimad. Kriptoqrafik metodlar informasiya və kommunikasiya sistemlərinin istifadəsində etimad yaratmaq üçün etibarlı olmalıdır.
2. Kriptoqrafik metodların seçilməsi. İstifadəçilərin qüvvədə olan qanuna uyğun hər hansı kriptoqrafik metodu seçmək hüququ olmalıdır.
3. Kriptoqrafik metodların istifadəçilərin tələbatı əsasında işlənilməsi. Kriptoqrafik metodlar fərdlərin, biznes sektorunun və dövlətin ehtiyacları, tələbatı və məsuliyyəti əsasında inkişaf etdirilməlidir.
4. Kriptoqrafik metodlar üçün standartlar. Milli və beynəlxalq səviyyədə kriptoqrafik metodlar üçün texniki standartlar, meyarlar və protokollar işlənilməli və qəbul edilməlidir.
5. Şəxsi həyatın toxunulmazlığı və fərdi məlumatların qorunması. Milli kriptoqrafiya siyasətində və kriptoqrafik metodların reallaşdırılması və istifadəsində yazışmaların gizliliyi və fərdi məlumatların qorunması da daxil olmaqla, əsas insan hüquqlarına hörmət edilməlidir.
6. Qanun əsasında giriş. Milli kriptoqrafiya siyasəti qanun əsasında açıq mətnə, kriptoqrafik açarlara və ya şifrlənmiş məlumatlara girişə icazə verə bilər. Belə siyasət bu Prinsiplərdə öz əksini tapan digər prinsiplərə mümkün dərəcədə uyğun olmalıdır.
7. Məsuliyyət. Müqavilə və ya qanunvericiliklə müəyyən edilməsindən asılı olmayaraq, kriptoqrafik xidmətlər təklif edən, kriptoqrafik açarları saxlayan və ya istifadə edən şəxslərin və ya təşkilatların məsuliyyəti aydın şəkildə ifadə edilməlidir.
8. Beynəlxalq əməkdaşlıq. Hökumətlər kriptoqrafiya siyasətlərini koordinasiya etmək üçün əməkdaşlıq etməlidirlər. Bu əməkdaşlığın bir hissəsi kimi, hökumətlər kriptoqrafiya siyasəti adından ticarətə əsassız maneələr yaradılmasının qarşısını almalı və ya maneələri aradan qaldırmalıdırlar.

Kriptoqrafiyada şifrələnmənin 2 əsas üsulu var: simmetrik və asimmetrik.

* Simmetrik şifrləmə üsulunda eyni açar (gizli saxlanılan) həm məlumatı şifrləmək, həm də deşifrləmək üçün istifadə olunur.



* Asimmetrik kriptoqrafiyada iki açardan istifadə olunur. Onlardan biri açıq açar (sahibinin ünvanı ilə birlikdə nəşr oluna bilər) şifrləmə üçün istifadə olunur, digəri gizli açar (yalnız alana məlum) deşifrləmə üçün istifadə olunur. Rəqəmsal imza alqoritmlərində gizli açar şifrləmə, açıq açar isə deşifrləmə üçün istifadə edilir.

