**“AZƏRBAYCAN HAVA YOLLARI”**

**QAPALI SƏHMDAR CƏMİYYƏTİ**

**MİLLİ AVİASİYA AKADEMİYASİ**

**Sərbəst iş №1**

**Fakültə:** “Aerokosmik”

**İxtisas:** “İnformasiya Texnologiyaları”

**Fənn:** “Veb sistemləri və texnologiyaları”

**Mövzu:** “Məlumatların şifrələnmə metodları”

**Qrup:** 2441a

**Tələbə:** Musa Ələsgərov

**Müəllim:** Heydərzadə Nübar

**BAKI 2024**

**Məlumatların şifrələnmə metodları**

**Giriş**

**Məlumatların Şifrələnməsi Nədir: Növlər, Alqoritmlər, Texnikalar və Metodlar**



Məlumatların şifrələnməsi ümumi və effektiv təhlükəsizlik üsuludur - təşkilatın məlumatlarını qorumaq üçün seçimdir. Bununla belə, bir neçə fərqli şifrələmə metodu mövcuddur.

Kibercinayətlərin artdığı bir dünyada şəbəkə təhlükəsizliyini qorumaq üçün bir çox metodun mövcuddur. Əsl problem internet təhlükəsizliyi üzrə mütəxəssisin öz təşkilatının xüsusi vəziyyətinə ən uyğun olan hansı üsullardan istifadə etməli olduğuna qərar verməsidir.

**Data Şifrələməsi nədir?**

Məlumatların şifrələnməsi,şifrələnmə yolu ilə qorunma üsuludur ki, onun şifrəsi açılsın və ya düzgün şifrələmə açarına malik olan şəxs ona daxil ola bilsin. Şəxs və ya təşkilat şifrələnmiş məlumatlara icazəsiz giriş əldə etdikdə məlumatlar şifrələnir və ya oxunmaz olur.

Məlumatların şifrələnməsi verilənlərin oxuna bilən formdan şifrələnmiş məlumat çevrilməsi prosesidir. Bu, çevrilmə zamanı məxfi məlumatları oxuyan şəxslərin qarşısını almaq üçün edilir. Şifrələmə sənədlərə, fayllara, mesajlara və ya şəbəkə üzərindən hər hansı digər əlaqə formasına tətbiq oluna bilər.

Məlumatların bütövlüyünü qorumaq üçün şifrələmə vacib bir vasitədir və onu şişirtmək olmaz. İnternetdə gördüyümüz demək olar ki, hər şey, istər veb-saytlar, istərsə də tətbiqlər, bir növ şifrələmə qatından keçmişdir.

Bu gün kibercinayətkarlıq riskinin artdığını nəzərə alsaq, internetdən istifadə edən hər bir şəxs və qrup ən azı əsas şifrələmə üsullarını bilməli və istifadə etməlidir.

**Məlumatların Şifrələnməsi Necə İşləyir?**

Şifrələnməsi lazım olan verilənlərə açıq mətn deyilir. Açıq mətni bəzi şifrələmə alqoritmlərindən keçirmək lazımdır ki, bunlar əsasən xam informasiya üzərində aparılacaq riyazi hesablamalardır. Çoxlu şifrələmə alqoritmləri var, hər biri icra və təhlükəsizlik indeksinə görə fərqlənir.

Alqoritmlərlə yanaşı, şifrələmə açarı da lazımdır. Sözügedən açardan və müvafiq şifrələmə alqoritmindən istifadə edərək, açıq mətn şifrəli mətn kimi də

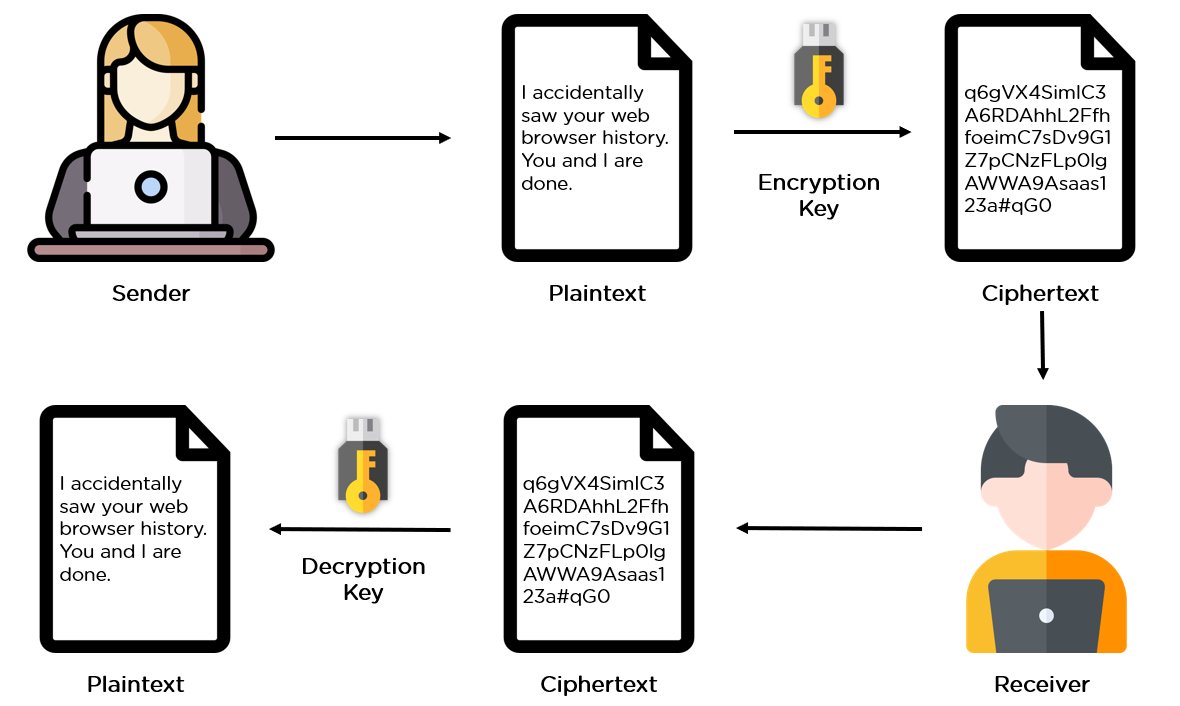
əvvəlcədən bilinən şifrələnmiş məlumatlara çevrilir. Açıq mətni alıcıya göndərmək əvəzinə, şifrələnmiş mətni qorunmayan rabitə kanalları vasitəsilə göndərilir.

Şifrə mətni nəzərdə tutulan alıcıya çatdıqdan sonra o, şifrəli mətni orijinal oxuna bilən formatına, yəni açıq mətnə ​​çevirmək üçün deşifrə açarından istifadə edir. Bu deşifrə açarı həmişə məxfi saxlanmalıdır və mesajı şifrələmək üçün istifadə olunan açara bənzəyir və ya olmaya bilər. Eyni şeyi bir nümunə ilə başa düşək.

Bir nümunənin köməyi ilə iş prosesini başa düşək.

**Misal**

Bir qadın sevgilisinə şəxsi mesaj göndərmək istəyir və o, mesajı xüsusi proqram vasitəsi ilə şifrələyir ki, bu da məlumatları oxumaq mümkün olmayacaq qədər mənasız edir. Sonra o, mesajı göndərir və sevgilisi mesajı tərcümə etmək üçün düzgün şifrəni açmaq üsulundan istifadə edir.



**Məlumat Şifrələmə Texnikalarının 2 Növü?**

Seçmək üçün müxtəlif məlumat şifrələmə yanaşmaları var. Əksər internet təhlükəsizliyi (IS) mütəxəssisləri şifrələməni üç fərqli üsula bölür: simmetrik, asimmetrik və hashing. Bunlar da müxtəlif növlərə bölünür.

**Simmetrik Şifrələmə Metodu nədir?**

Şəxsi açarın şifrələməsi və ya gizli açar alqoritmi də adlanır, bu üsul göndərən və qəbul edənin eyni açara daxil olmasını tələb edir. Buna görə də, mesajın şifrəsini açmaqdan əvvəl alıcının açarı olmalıdır. Bu üsul, üçüncü tərəflər tərəfindən müdaxilə riskinin az olduğu qapalı sistemlərdə ən yaxşı şəkildə işləyir.

Üstünlük simmetrik şifrələmənin asimmetrik şifrələmədən daha sürətli olmasıdır. Lakin mənfi tərəfi odur ki, hər iki tərəf açarın etibarlı şəkildə saxlandığından və yalnız ondan istifadə etməli olan proqram təminatı tərəfindən istifadə olunmalıdır.

**Asimmetrik Şifrələmə Metodu nədir?**

Açıq açar şifrələməsi də adlandırılan bu üsul, şifrələmə prosesi üçün riyazi olaraq bağlı olan iki açardan, açıq və şəxsi açardan istifadə edir. İstifadəçi şifrələmə üçün bir açardan, şifrənin açılması üçün isə digər açardan istifadə edir, baxmayaraq ki, hansını ilk seçdiyinizin fərqi yoxdur.

Adından göründüyü kimi, açıq açar hər kəs üçün sərbəstdir, şəxsi açar isə yalnız mesajların şifrəsini açmaq üçün ona ehtiyacı olan hədəf alıcılarda qalır. Hər iki düymə eyni olmayan, lakin bir-biri ilə qoşalaşmış böyük rəqəmlərdir; Burada "asimmetrik" hissə işə düşür.

**Hashing nədir?**

Hashing məlumat dəsti və ya mesaj üçün sabit uzunluqlu unikal imza yaradır. Hər bir şəxsi mesajın özünəməxsus hashı var və məlumatda kiçik dəyişiklikləri asanlıqla izlənilə bilər. Hashing yolu ilə şifrələnmiş məlumatın şifrəsi açıla və ya orijinal formasına qaytarıla bilməz. Buna görə hashing yalnız məlumatların yoxlanılması üsulu kimi istifadə olunur.

Bir çox internet təhlükəsizliyi üzrə mütəxəssislər faktiki şifrələmə metoduna heşinq etməyi belə düşünmürlər, lakin xətt təsnifatın etibarlı olmasına imkan verəcək qədər bulanıqdır. Nəticə etibarı ilə, bu, heç kimin informasiyaya müdaxilə etmədiyini göstərmək üçün təsirli bir üsuldur.

**Kriptoqrafiyada açar nədir?**

Açar müəyyən qaydada təsadüfi simvollar silsiləsidir. Şifrələmə üsulları məlumatı qarışdırmaq üçün açardan istifadə edir ki, açarı olmayan heç kim məlumatı deşifrə edə bilməyəcək. Müasir şifrələmə mürəkkəb riyazi hesablamalar olan alqoritmlərdən istifadə edir. Müasir açarlar adətən təsadüfi tam ədədlərin əsas ardıcıllığından daha çox təsadüfi olur.

Bu bir neçə səbəbə görə doğrudur:

Kompüterlər insan kriptoqraflarına nisbətən daha az vaxt ərzində daha mürəkkəb hesablamalar apara bilər və bu, daha mürəkkəb şifrələməni həm inandırıcı, həm də zəruri edir.

Kompüterlər məlumatı təkcə hərf və rəqəm səviyyəsində deyil, həm də ikili səviyyədə, verilənləri təşkil edən 1 və 0-larla idarə edə bilirlər.

Əgər kifayət qədər təsadüfi deyilsə, kompüter proqramı şifrələnmiş məlumatı deşifrə edə bilər. Həqiqi təsadüfilik həqiqətən təhlükəsiz şifrələmə üçün vacibdir.

Şifrələmə açarı şifrələmə üsulu ilə birləşdirildikdə mətni insan tanınması üçün çox mürəkkəb edəcək.