Infbizt 2

Kriptográfiai alapfogalmak

-egyabécés titkosító: betűk tetszőleges összekeverése, minden nyílt betűt egy titkossal helyettesítünk

Alapfogalmak

-nyílt szöveg (plaintext): üzenet amit védeni szeretnénk

-titkosított szöveg: titkosítással átalakított üzenet

-kulcs: titkosításhoz/megfejtéshez használt kritikus információ

-titkosítás: nyílt szöveg „olvashatatlanná tétele” a kulcs segítségével

-titkosító algoritmus: titkosított szöveg vissza alakítása „olvasható” szöveggé a kulcs segítségével

-feltörés: titkosított szövegből nyílt szöveg (kulcs nélkül)

Kerchoffs elv

A rendszer egy részének kitudódása ne okozza a a rendszer egészének kitudódását.

Kriptográfiai algoritmus biztonsága függ:

-algoritmus erősségétől

-kulcs hosszától

Hamis biztonság: egy erősnek látszó de gyenge biztonság

Vernam titkosító:

-feltörhetetlen

-ha a kulcsot véletlenszerűen választottuk nincs rá mód hogy kitaláljuk melyik kulcs az igazi

Szimmetrikus (titkos kulcsú kriptográfia):

-a kulcsot csak a feladó és a címzett ismeri

-előzetes kommunikáció

Aszimmetrikus(nyilvános kulcsú kriptográfia):

-egy nyilvános kulcs

-egy magán kulcs

-nyilvános kulccsal titkosítunk és a magán kulccsal megfejtjük

Hash függvények

Hash matematikai függvények, amelyek konkrét adathalmaz alapján egy rövidített kódot generálnak.

-determisztikus: ugyanaz a bemeneti adat mindig ugyanazt a hash értéket eredményezi

-gyors számítás: hatákonyan kell számítani a hash-értéket, meg nagyobb adatmennyiségen is

-ellentmondások elkerülése: két különböző bemenetnek nem szabad ugyanazt a hash-értéket eredményeznie

Hash algoritmusok:

-MD5

-SHA-1

-SHA-2

-SHA-3

Adatbázisban csak hash-t tárolunk

Sózás: a jelszó mellett kell egy másik érték is, dátum vagy random string és ez az érték pár kerül be az adatbázisba (jelszó+só)