

12.a Ismertesse a hálózati kommunikáció védelmére alkalmazott kriptográfiai algoritmusokat! Magyarázza el működésüket!

Kriptográfia

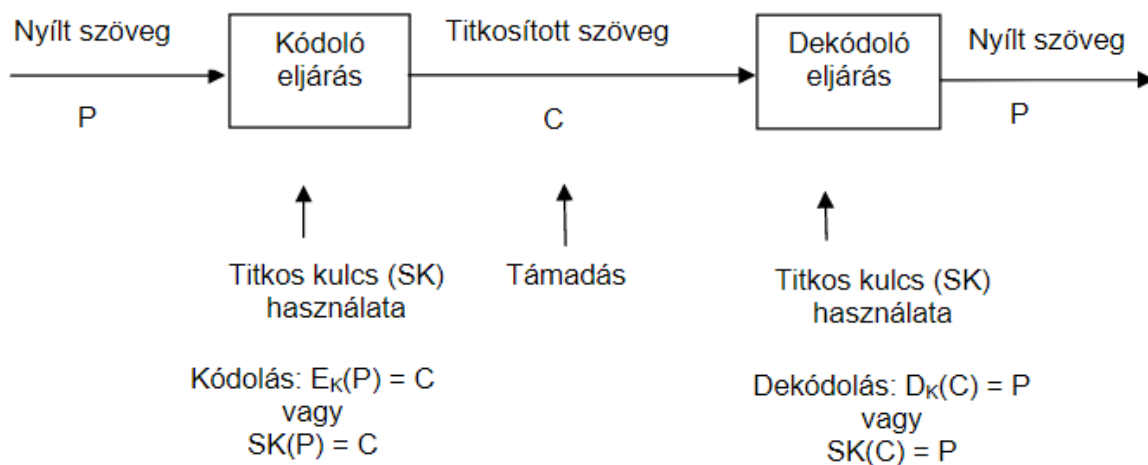
- A kriptográfia lényege, hogy az adatokat biztonságban tárolhassuk az illetéktelen hozzáférések ellen és adatküldésnél a CIA elvek alapján biztonságban áramoljon az információ.
- **Elvárások:** Gyors encryptelés és a megfelelő decrypt kulcs esetén visszafejthetőség vagy egyirányú legyen.

Rejtjel (cipher)

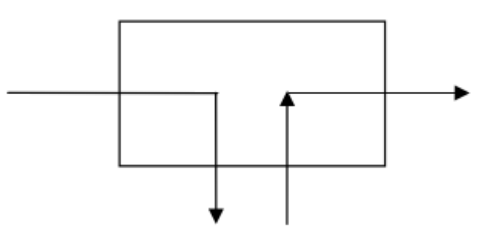
- Karakterről karakterre átalakítás
- Bitről bitre átalakítás

Kód (code)

- Egy szó helyettesítése egy másik szóval vagy szimbólummal.

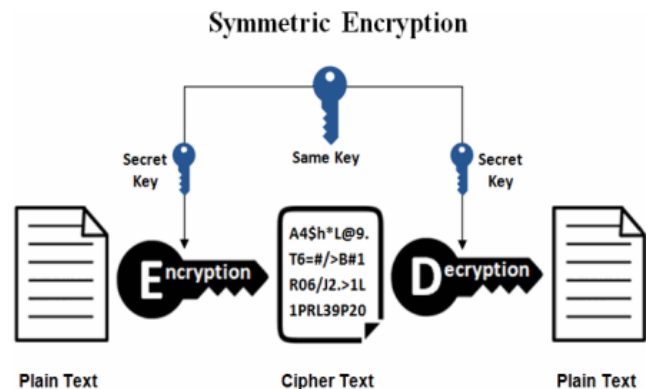


Támadási lehetőségek

Passzív támadás	Aktív támadás
Üzenet lehallgatása	Üzenet megváltoztatása
	

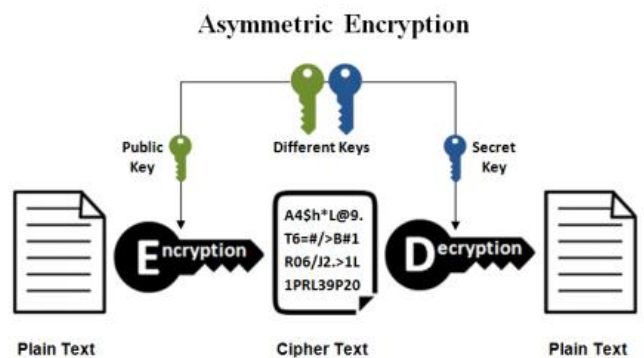
Szimmetrikus titkosítás

- A titkosításhoz és a visszafejtéshez ugyanazt a kulcsot használják.
- Gyorsabb, mint az aszimmetrikus kriptográfia.
- **AES – Advanced Encryption Standard:**
 - o Alacsony memóriaigény, gyors, leváltotta a **DES**-t.
- **DES – Data Encryption Standard**
 - o Blokkrejtjelező,
 - o Eredetileg 56 bites kulcs hossz.
 - o 64 bites input blokkokat fogad és 64 bites rejtjelezett szöveget eredményez.
- **3DES – Tripla DES:**
 - o Kettő vagy három titkosító kulcsot használ



Asszimmetrikus titkosítás

- A titkosításhoz és a visszafejtéshez különböző kulcsokat használnak.
- Lehetővé teszi a hitelesítést és az adatok védelmét közvetlen kulcsmegosztás nélkül.
- **RSA - Manapság leggyakrabban használt**
 - o Titkosításhoz egy nyílt és egy titkos kulcs tartozik.
 - o Nyílt kulcs bárki számára elérhető, és ezzel lehet kódolni a másoknak szánt üzenetet.
 - o Titkos kulccsal lehet megfejteni a nyílt kulccsal kódolt üzenetet.
- **DSA**
 - o Privát kulcsot használjuk az üzenetek digitális aláírásának létrehozásához.
 - o Nyilvános kulcsot használjuk az aláírás ellenőrzéséhez.
- **Diffie-Hellman kulccsere**
 - o Biztonságos kommunikációs csatornát hoz létre, de úgy, hogy közbe nem kell a titkos kulcsot közvetlenül átadniuk.
 - o Két fél a privát kulcsait használja a titkos kulcs létrehozásához, amit csak egymás között használhatnak.

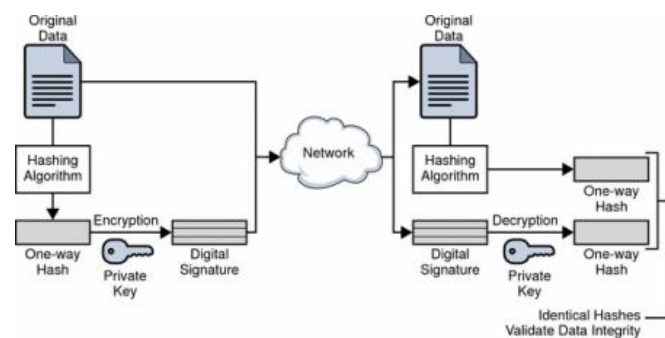


Hash-függvények

- Bemenő adatokból rövid, állandó hosszúságú hash-t állítanak elő.
- A hash függvényeket a hitelesítéshez és az adatok integritásának ellenőrzéséhez használják.

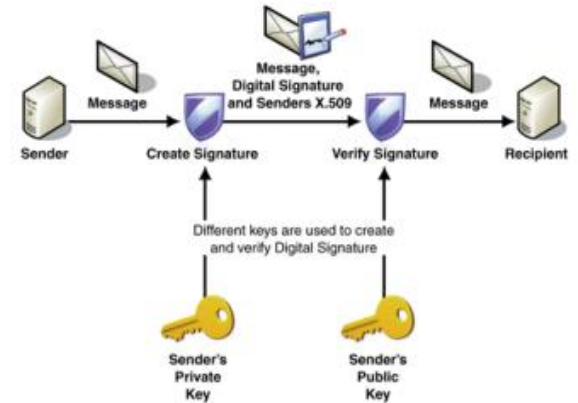
Titkosító protokollok

- Adatkapcsolati rétegbeli titkosítás
- Hálózati rétegbeli titkosítás (IPSec)
- Szállítási rétegbeli titkosítás (SSL, TLS)
- Alkalmazási rétegbeli titkosítás (PGP)



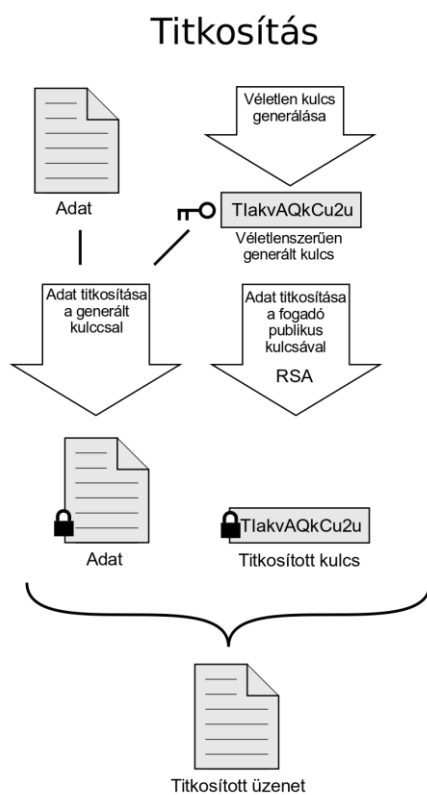
Digitális aláírás

- Olyan elektronikus aláírás, amit digitális tanúsítványt hitelesít.
- Az aláírás tartalmaz egy ellenőrző összeget, amihez szükség van egy hashfüggvényre (SHA-1 vagy MD5).
- **Hozzáfűzzük:**
 - o Aláíró nevét vagy azonosítóját
 - o Aláírás idejét
 - o Hashfüggvény nevét
 - o Egyéb dolgok, amiket fontosnak tartunk



PGP – Pretty Good Privacy

- Ötvözi a szimmetrikus kulcsú titkosítás gyorsaságát az aszimmetrikus kulcsú titkosítás biztonságával, ezért hibrid titkosítási módszernek nevezzük.



Visszafeltetés

