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

Hálózati kommunikáció védelmére alkalmazott kriptográfiai algoritmusok

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

Adatkapcsolati titkosítások:

* AES: szimetrikus blokk-kódolás

      -támogatja a 128,256 bit hosszú kulcsokat

* RSA: publikus és privát kulccsal rendelkezik (asszimetrikus)

      támogatja a 1024,248,3072 és a 4096 bites kulcsokat

* Üzenet pecsétek:

(sértetlenségért felel)

* MD5: egyirányú

      128 bites

* SHA: bármilyen hosszú karakterláncból adott hosszúságú hash-t állít elő.

több fajtája létezik

     -SHA-256 elterjedt.

IPSEC:

* IPSEC keret
* IPSEC protokol:auth header
* (C)bizalmasság: aes felel
* (I)sértetlenség: md5, sha felel
* (A)hitelesítés: RSA felel
* Diffie-hellman

További protokolcsomagok:

* ISAKMP általános kulcscsere
* IKE: IPSEC hivatalos kulccsere

Titkosítási eljárások között két alapvető esetet különböztetünk meg: szimmetrukus, és asszimetrikus titkosítás.

Szimmetrikus titkosítás:

* lényege, hogy a küldő és a fogadó is ugyan azzal a kulccsal végzi a titkosítást és a visszafejtést
* használata olyan esetben célszerű, mikor a kulcsokat nem szükséges folyton küldözgetni
* leggyakrabban használt algoritmusok: DES, 3DES, AES

Asszimmetrikus titkosítás:

* az algoritmus kulcspárral dolgozik, nyilvános és privát kulcsot használ
* a nyilvános kulcs szabadon továbbítható, a privát kulcsot biztosnágban kell tartani
* a kulcs egyik párjából nem következtethető a másik fele
* Diffie és Hellman módszerén alapszik a működése, RSA módszer során használják

SSL

* Def: célja a kommunikáció titkosítása, mikor az adatot nyílt csatornán továbbítjuk
* használati módja: nem egy hálózatot tesz biztossá, hanem egy pont-pont kapcsolatot
* kliens és szerveroldali támodatás szükséget, hiszen mindkét oldal esetés elvárt a titkosítás
* előnye, hogy az OSI modell szállítási rétege fölött bármely alkalmazáshoz használható
* működése:
  + minden kapcsolat egyedi kulccsal kerül titkosításra
  + gyakra változó, véletlenszerű kulcsot alkalmaz
  + tanúsítvány igazolja a szervert
  + kulccserék történnek szerver és kliens között -> kizárható a man-in-the-middle támadások
  + titkosítás szimmetrikus algoritmus használ: pl.: DES, AES
  + adatintegritást garantál (MD-5, SHA-1), amit kulcsolt MD függvényekkel ér el (MAC)
  + pl.: HTTPS esetén ezt használjuk

Encapsulated Security Payload (ESP) protokoll

* feladata az IP csomag tartalmának rejtése, tartalom integritásának védelme
  + csomag rejtése: IP csomag tartalmának rejtjelezésével
  + integritás végelem: cdomaghoz csatolt MAC kóddal (fejlécre és csomagra is)
* SPI azonosító használata – vevő számára jelzi az alkalmazandó kulcsot
* Hitelesítő MAC kód - opcionális