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.

Adatkapcsolati titkosítások

- **AES – Advanced Encryption Standard:**
    - Alacsony memóriaigény, gyors, leváltotta a **DES**-t.
    - Szimmetrikus blokk-kódolás
    - Támogatja a 128, 256 bit hosszú kulcsokat
- **RSA - Manapság leggyakrabban használt**
    - Titkosításhoz egy nyílt és egy titkos kulcs tartozik.
    - Nyílt kulcs bárki számára elérhető, és ezzel lehet kódolni a másoknak szánt üzenetet.
    - Titkos kulccsal lehet megfejteni a nyílt kulccsal kódolt üzenetet.
- **MD5**
    - Egyirányú
    - 128 bites
- **SHA**
    - Bármilyen hosszú karakterláncból adott hosszúságú hash-t állít elő.
    - Több fajtája létezik
    - SHA-256 elterjedt

Szimmetrikus titkosítás

- Lényege, hogy a küldő és a fogadó is ugyanazzal a kulccsal végzi a titkosítást és a visszafejtést.
- Használata olyankor célszerű, amikor a kulcsokat nem kell 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 biztonságban kell tartani.
- A kulcs egyik párjából nem következtethető a másik fele.
- Diffie-Hellman módszerén alapszik a működése, RSA módszer során használják.

IPSec

AH – Authentication Header

- Sértetlenséget, hitelesítést és visszajátszás elleni védelmet biztosít.
- Beszúr egy AH fejlécet, ami egy MAC-et tartalmaz.
- A visszajátszás detektálásának érdekében, az IP csomagokat sorszámozza.
- Az AH fejlécben található MAC érték a sorszámot is védi.

ESP – Encapsulated Security Payload

- Feladata az IP csomag tartalmának rejtése és opcionálisan a tartalom integritásának védelme.
- IP csomag tartalmának rejtését rejtjelezéssel oldja meg.
- **Tartalom integritásának védelme:** ESP fejlécre és a csomag tartalmára számít MAC kódot és azt a csomaghoz csatolja.
- ESP MAC nem védi az IP fejléc mezőit.

ISAKMP – Internet Security Association and Key Management Protocol

- Általános célú keretprotokoll, ami bármilyen konkrét kulcscsere protokoll üzeneteit képes szállítani.

IKE – Internet Key Exchange

- IPSec hivatalos kulcscsere protokollja.
- A host-ok ebben a fázisban hitelesítik egymást shared secret vagy RSA kulcs segítségével.
- Felépítenek egy kétirányú ISAKMP SA-t.
- Az ISAKMP SA-t alkalmazva megvitatják az egyirányú IPSec SA-kat.

SSL célja

- Titkosított kommunikációt biztosító protokoll, ami nyílt hálózatokban, kapcsolatorientált kommunikációban nyújt védelmet.
- Csak egy-egy kommunikációs csatornát biztosít.
- Gyakran használják a weboldalak biztonságos titkosítására is.

SSL szerkezeti felépítése

- Minden egyes kapcsolat egyedi kulccsal titkosít.
- Tanúsítvány igazolja a szervert.
- Biztosítja az adatintegritást. (MD5, SHA-1)

SSL működése

1. Kliens csatlakozik a kiszolgálóhoz.
2. Kiszolgáló elküldi a hitelesítési tanúsítványt a kliensnek.
3. Kliens ellenőrzi a tanúsítvány hitelességét, majd létrehozza a titkosított kapcsolatot a kiszolgálóval.
4. Kliens és kiszolgáló között így már biztonságosan lehet adatokat cserélni.
5. Ha az SSL kapcsolat megszakad, akkor a kliens és a kiszolgáló kapcsolata is megszakad.

SSL alprotokolljai

Rekord protokoll

- Feladata a kliens és a szerver és a felsőbb SSL protokoll entitások védelme:
    - Titkosítás, integritásvédelem, üzenet-visszajátszás elleni védelem

Handshake protokoll

- Rekord protokollban használt kriptográfiai algoritmusok és paramétereik egyeztetése.
- Kulcscsere és hitelesítés

Change-Cipher-Spec protokoll

- Egyetlen üzenetből áll, ami a Handshake protokoll kulcscsere részének végét jelzi.
- Ezt az üzenetet elküldi, utána az adott fél az új algoritmusokat és kulcsokat kezdi használni a küldése.
    - A vétel még mindig a Handshake előtti állapot szerint történik.

Alert protokoll

- Figyelmeztető és hibaüzenetek továbbítása.