IP alapú távközlés

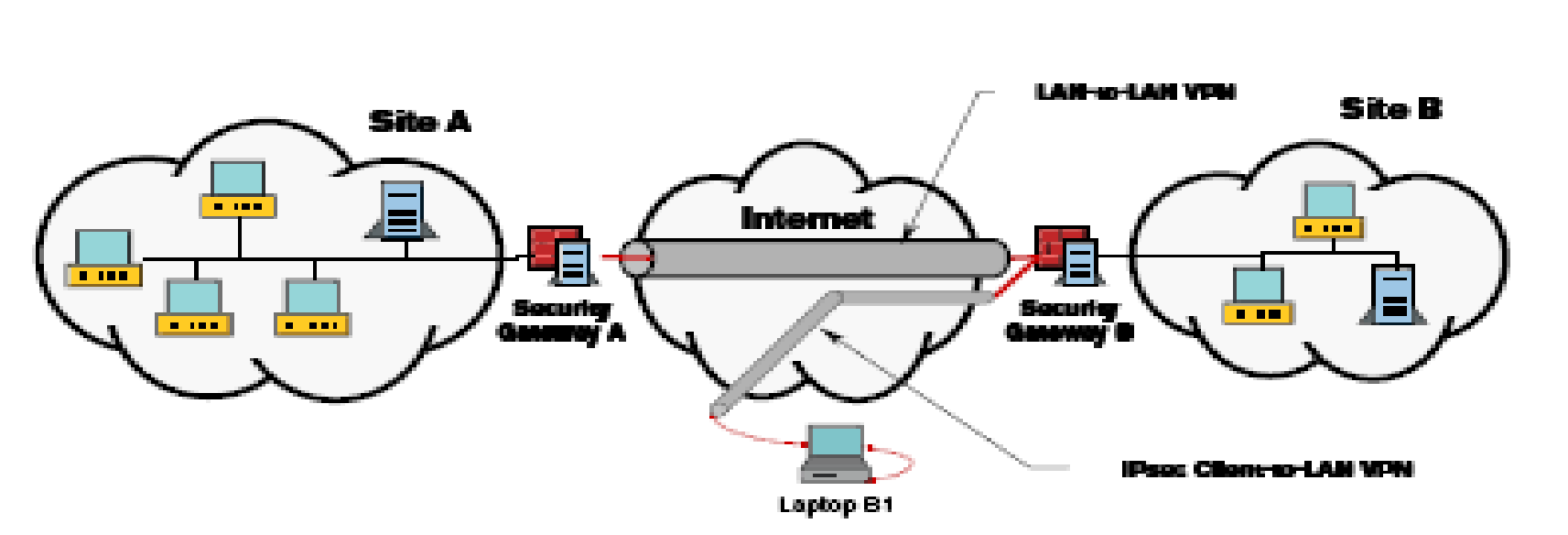
Virtuális magánhálózatok
(VPN)

Jellemzők

- Virtual Private Network – VPN
  - Publikus hálózatokon is használható
    - Több telephelyes cégek hálózatai biztonságosan összeköthetők
    - Olcsóbb megoldás, mint bérelt vonalat használni közvetlenül a telephelyek között
  - Titkosított adatforgalom a lehallgatás ellen
    - Biztonságos adatátvitel a mobil felhasználók és a cég hálózata között
  - Független a kommunikáló partnerek hálózati csatlakozási típusától

Jellemzők

- VPN elemei
  - Kommunikáló partnerek ⇒ security gateway
    - Tűzfal, router
    - Más speciális, VPN kompatibilis eszköz
  - Kommunikáció nyelve ⇒ IPsec protokoll

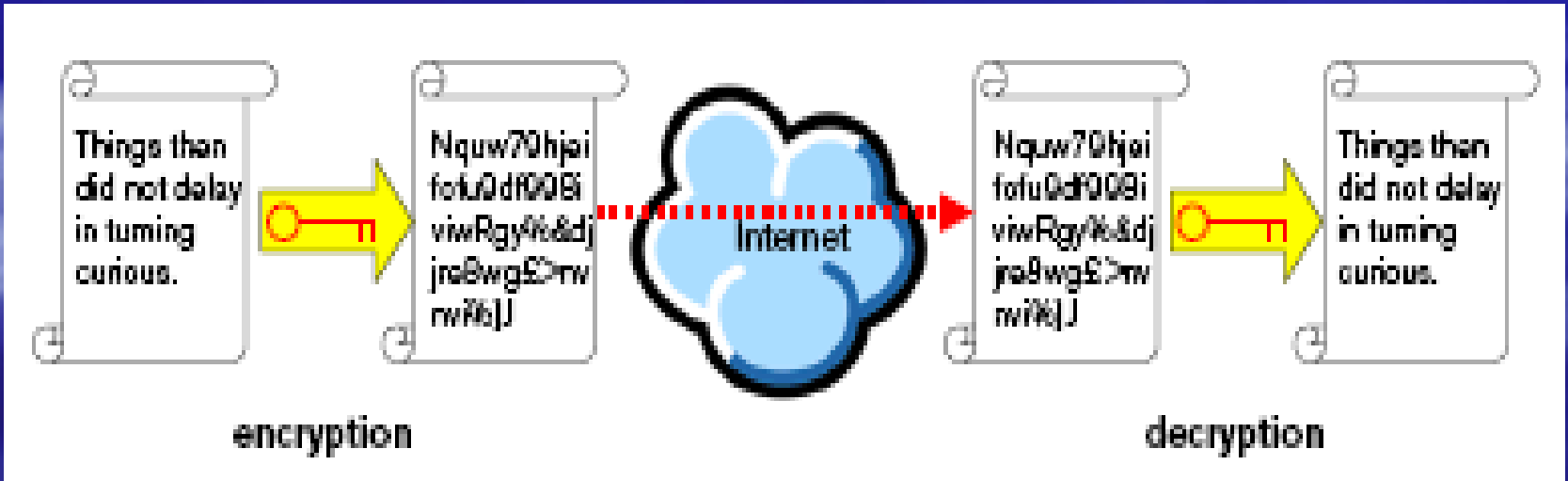


Jellemzők

- Titkosítás
  - Elemei
    - Titkosítandó szöveg
    - Titkosítási algoritmus + kulcs
  - Felhasználási területei
    - Digitális pénzügyi tranzakciók $\Rightarrow$ banki műveletek
    - Mobiltelefonok
    - Digitális aláírás
    - Virtuális magánhálózatok

Titkosítás

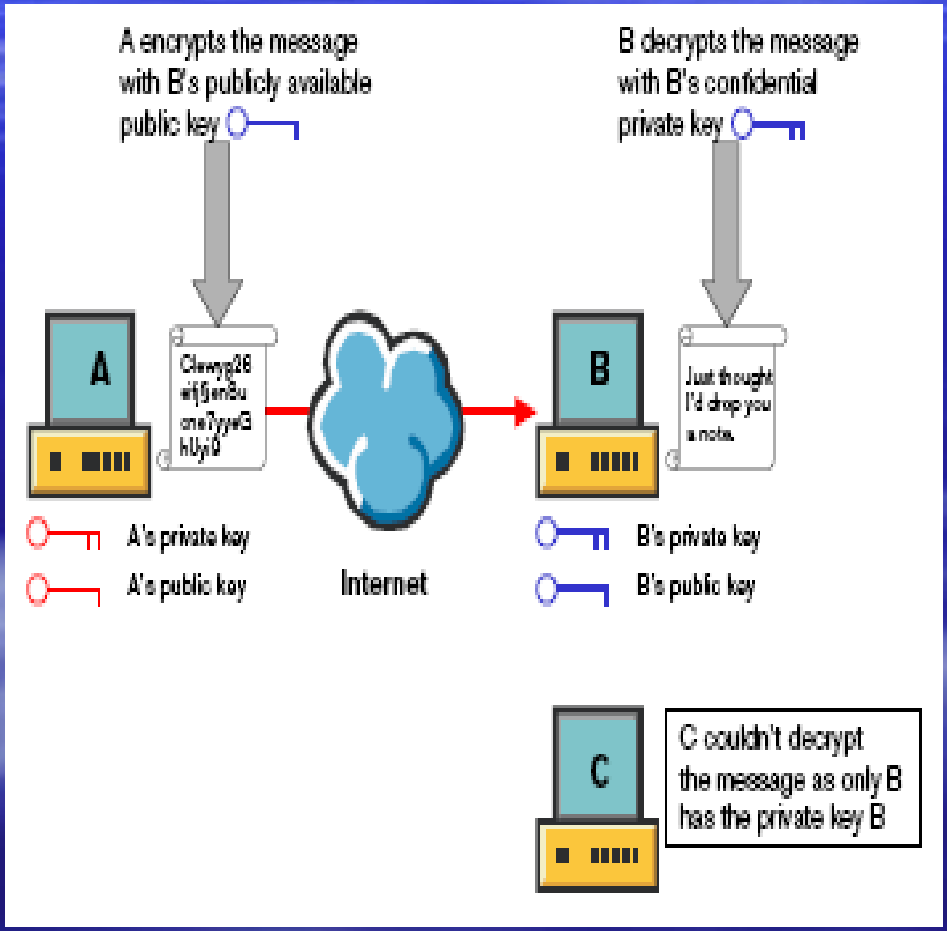
- Szimmetrikus titkosítás
  - Rejtett (titkos) kulcsú titkosítás
    - Kritikus pont a kulcs erőssége
      - ajánlott a „jó” véletlenszám-generátorok használata
    - Szabványos algoritmusok: 3DES, IDEA, Blowfish



Titkosítás

- Szimmetrikus titkosítás
  - Nagy mennyiségű adat titkosítására előnyös
  - Probléma: titkos kulcs továbbítása a másik félnek
    - Csak egy kapcsolatra (session) érvényes kulcs
    - Kulcscsere algoritmus
      - Diffie-Hellman módszer
- Aszimmetrikus titkosítás
  - Nyilvános kulcsú titkosítás
  - '70-es évektől kezd terjedni a használata

Titkosítás



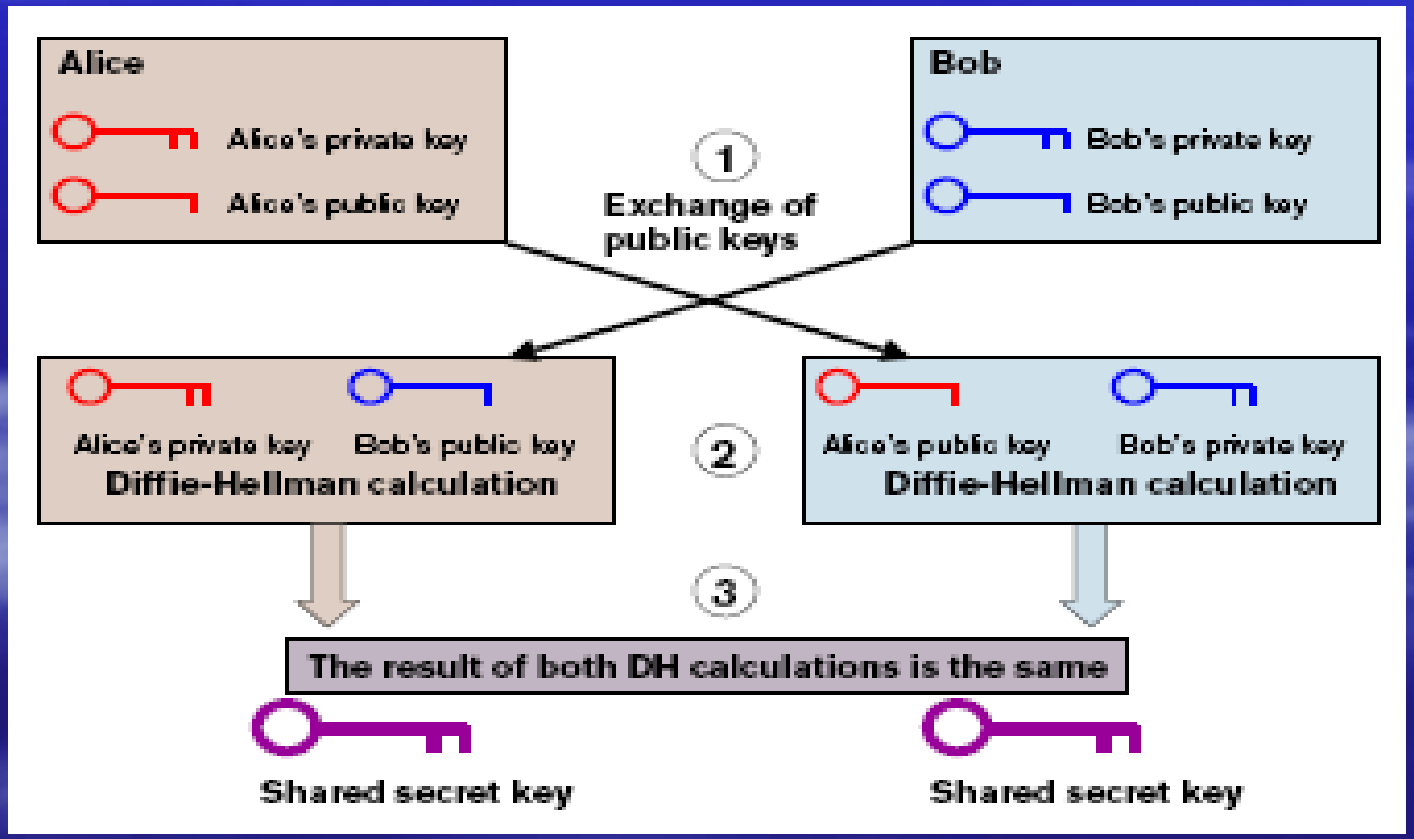
- Aszimmetrikus titkosítás
  - Két kulcs: nyilvános és titkos kulcs
    - Meghatározott módon generálják
    - Csak matematikailag kapcsolódnak egymással
    - Egyik sem található ki a másikból

Titkosítás

- Aszimmetrikus titkosítás
  - Erőforrás igénye magasabb a szimmetrikusénál
    - Titkos kulcs hitelesítése és titkosítása
    - Digitális aláírás generálása
    - Diffie-Hellman kulcscsere módszer
  - Diffie-Hellman kulcscsere módszer
    - Azonos rejtett kulcsok használata továbbításuk nélkül
      - kulcspár generálása
      - nyilvános kulcsok kicserélése
      - az algoritmus segítségével azonos rejtett kulcsok előállítása a szimmetrikus titkosításhoz

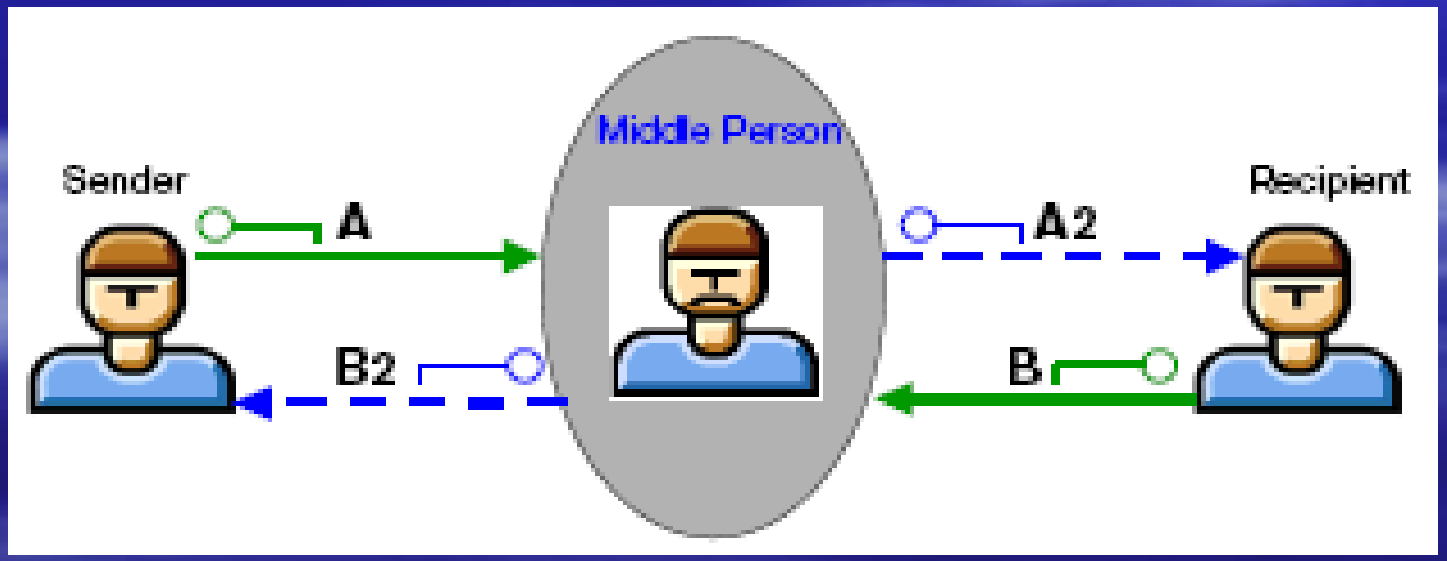
Titkosítás

- Aszimmetrikus titkosítás
  - Diffie-Hellman kulcscsere módszer



Titkosítás

- Aszimmetrikus titkosítás
  - Diffie-Hellman kulcscsere módszer
    - *„Man-in-the-middle attack” (láhatatlan harmadik fél)*
      - Észrevétlenül lehallgathatja és megváltoztathatja a kommunikációban résztvevők adatcsomagjait

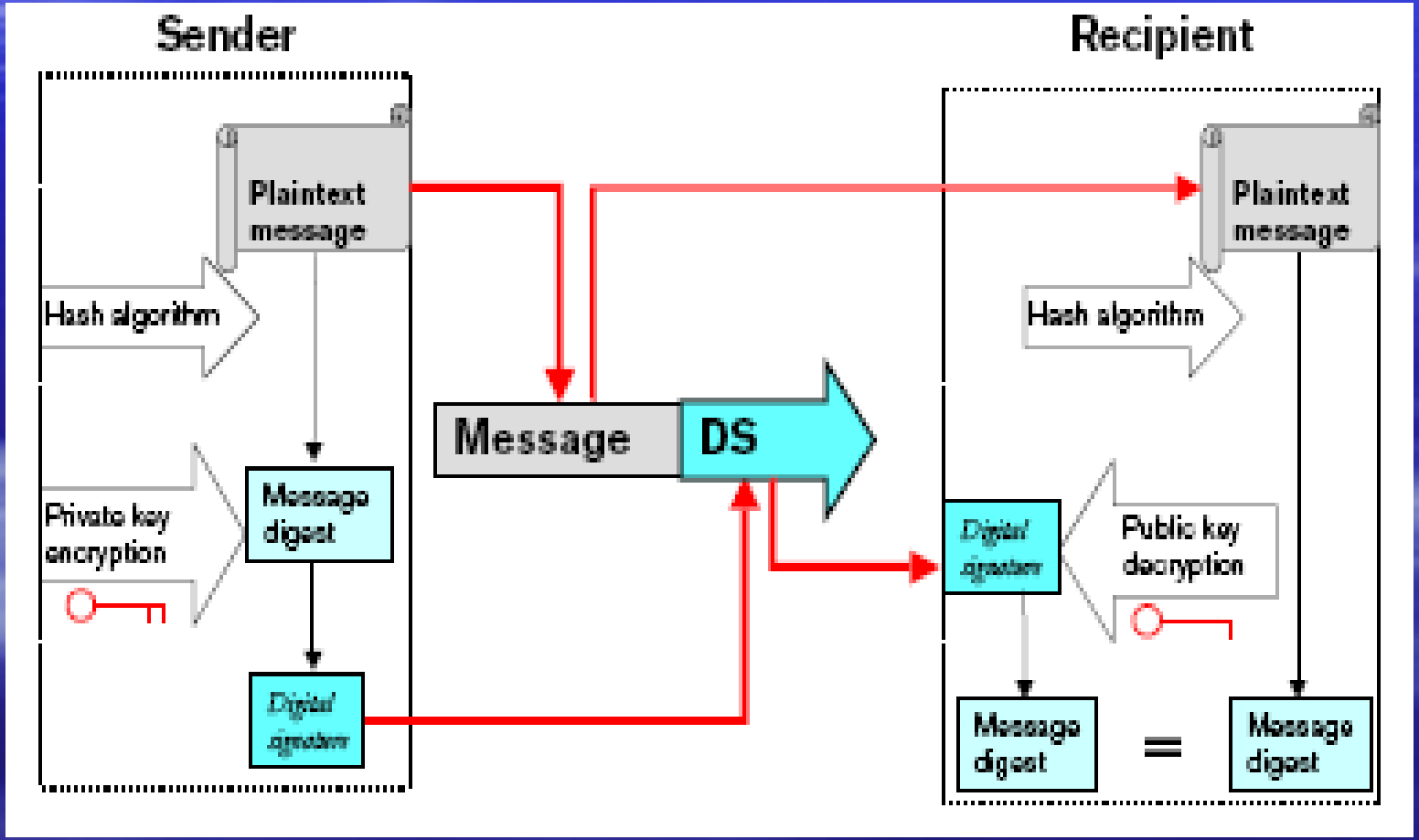


Hitelesítés és integritás

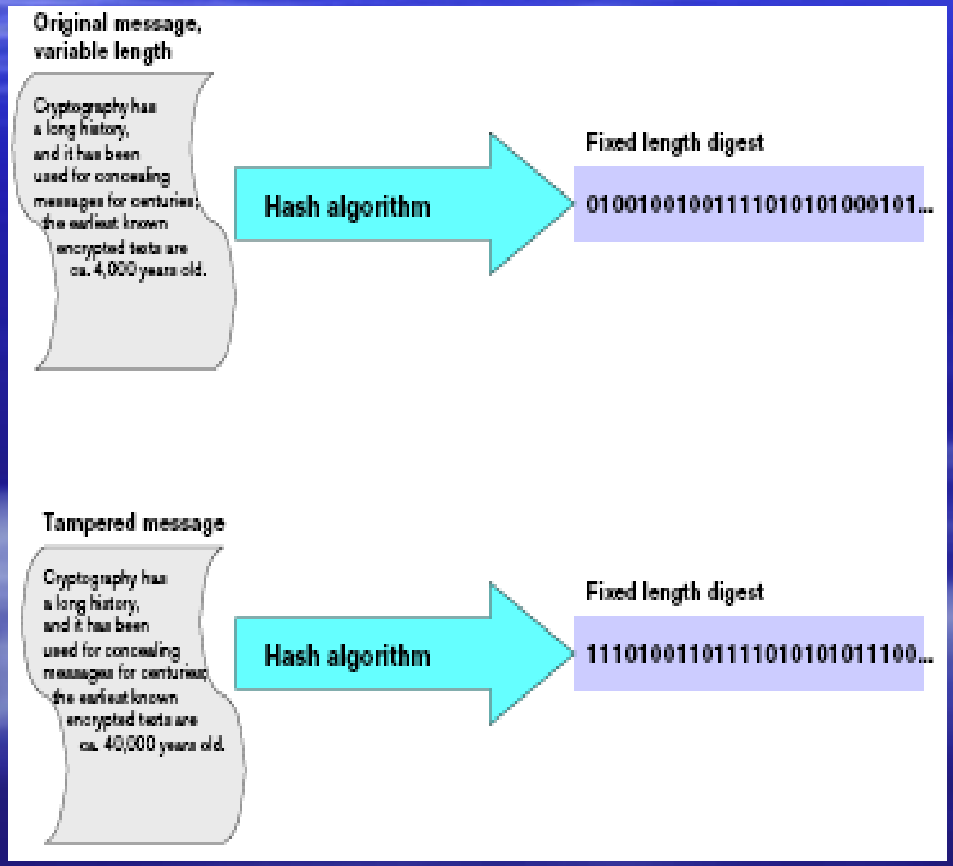
- Hitelesítés és integritás
  - Kommunikációban résztvevők hitelességének és az adatok változatlanságának biztosítása
    - digitális aláírás és tanúsítvány alkalmazása
    - Nyilvános kilcsú titkosítással és kulcsmenedzsmenttel kiegészítve: „***Public Key Infrastructure (PKI)”***
- Digitális aláírás
  - Biztosítja a küldő hitelességét és az adatok integritását
  - Nyilvános kulcsú titkosításon alapul

Hitelesítés és integritás

- Digitális aláírás



Hitelesítés és integritás



- Digitális aláírás
  - Ujjlenyomat (message digest)
    - irreverzibilis algoritmussal képezik
    - nehéz hamisítani
    - minden egyes üzenetből nagy valószínűséggel egyedi ujjlenyomat képezhető

Hitelesítés és integritás

- Digitális tanúsítványok
  - „Tanúsítvány hatóságok” (Certificate Authorities, CA) állítják ki
    - a nyilvános kulcsot és a személyes információkat tartalmazó tanúsítványt a privát kulccsal aláírják
    - Tartalma:
      - Tanúsítvány tulajdonosának neve és azonosítója
      - CA neve, nyilvános kulcs, tanúsítvány „fokozata”, érvényesség ideje
  - A kommunikáló felek „bemutatják” a saját tanúsítványukat egy megbízható CA aláírásával ellátva

Hitelesítés és integritás

- Digitális tanúsítványok
  - CA nyilvános kulcsáról másolattal kell rendelkeznie a kommunikáló feleknek
    - CA megbízhatóságának ellenőrzése
    - CA által aláírt tanúsítványok aláírásának érvényesítése
  - Certificate Revocation List (CRL)
    - CA-k kötelessége kezelni
    - Visszavont, érvénytelen tanúsítványok listája
      - elveszett vagy ellopott privát kulcs
      - megváltozott személyes adatok

IPsec protokoll

- Jellemzők
  - RFC 2401 szabványban rögzítették
  - Hitelesítési és/vagy titkosítási szolgáltatásokkal egészíti ki az IP hálózatokat
  - Két fő prokollból épül fel:
    - Authentication Header (AH)
    - Encapsulating Security Payload (ESP)
  - Security Associations (SA)
    - kommunikáló felek közötti két egyirányú csatorna
    - AH és ESP protokollok segítségével jönnek létre

IPsec protokoll

- Jellemzők
  - SA data
    - IPsec kapcsolatokhoz szükséges információk: kulcsok, algoritmusok, üzemmódok, élettartam, stb.
    - Internet Key Exchange (IKE) fázis során rögzítődik a tartalmuk
  - Security Association Database (SAD)
    - SA-kat tárolja, Security Parameter Index (SPI) segítségével azonosítva
    - Az SPI-t az AH és ESP protokollok fejrésze is tartalmazza

IPsec protokoll

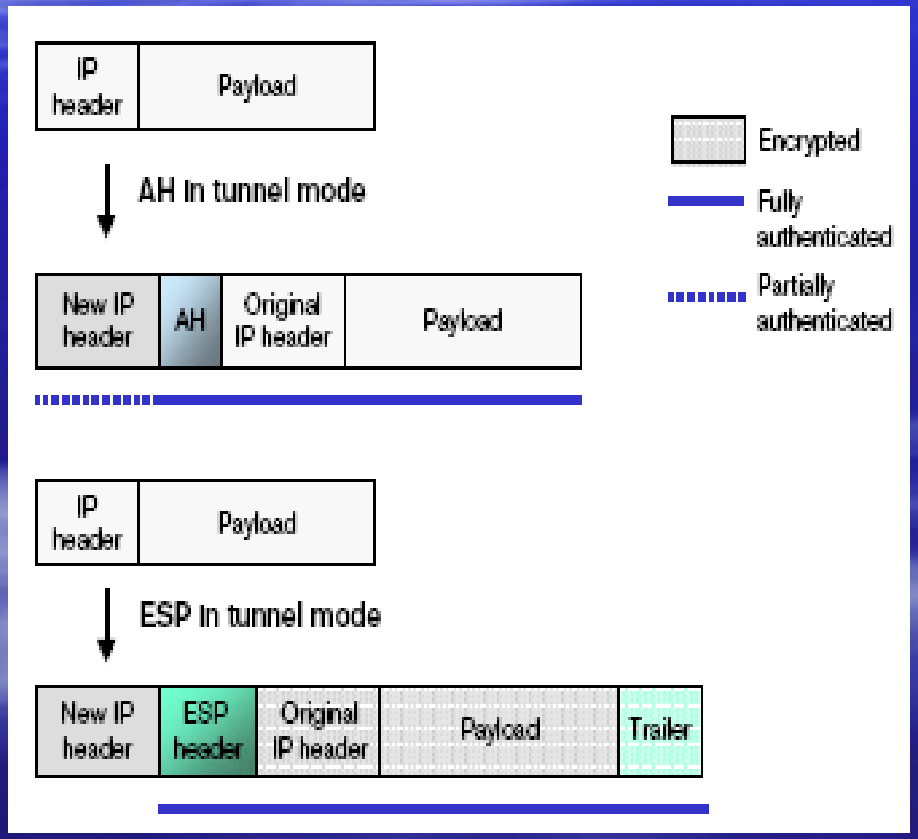
- Authentication Header (AH)
  - alapvetően a küldő fél hitelesítését és az adatok integritásának megőrzését segíti
    - véd a „replay attack” típusú támadásokkal szemben
    - titkosítási szolgáltatásokkal nem rendelkezik
    - Az eredeti IP csomagba szúrják be, IP header módosul
  - AH mezői tartalmazzák
    - szállítási protokoll típusát, az SPI értékét,
    - sorszámot a „replay attack” támadások kivédésére
    - csomag hitelesítéséhez digitális aláírást
    - az integritás ellenőrzéséhez rejtett kulccsal titkosított aláírást (adatrész, AH mezők és néhány IP fejrész mező)

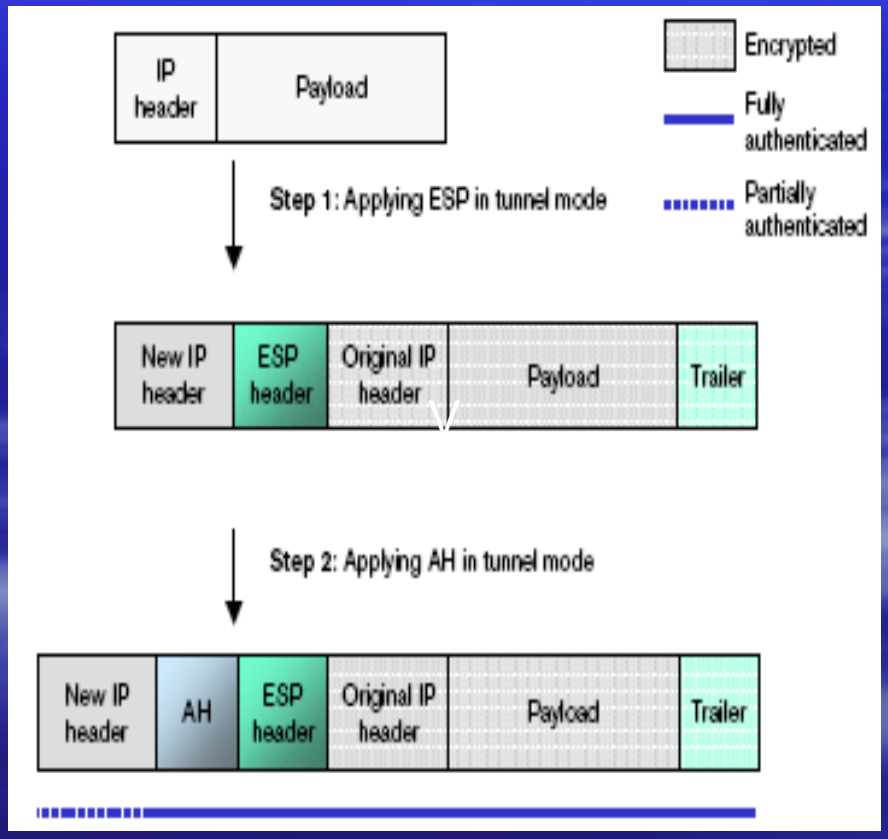
IPsec protokoll

- Encapsulating Security Payload (ESP)
  - alapvetően titkosítási és adatintegritási valamint hitelesítési szolgáltatásokat nyújt
  - véd a „replay attack” támadások ellen is
  - Az IP csomagba ESP fejrészt szúrnak be, mely két mezőből áll:
    - SPI és sorszám mező
  - Az eredeti IP csomagot titkosítja
    - Kitöltő adatok a csomag adatrészét követően
  - Titkosítatlan ESP hitelesítő információ a kitöltő adatrészt követően
    - IP adatmezőből és az eredeti IP és ESP fejrészből áll

IPsec protokoll

- Tunnel és Transport üzemmód



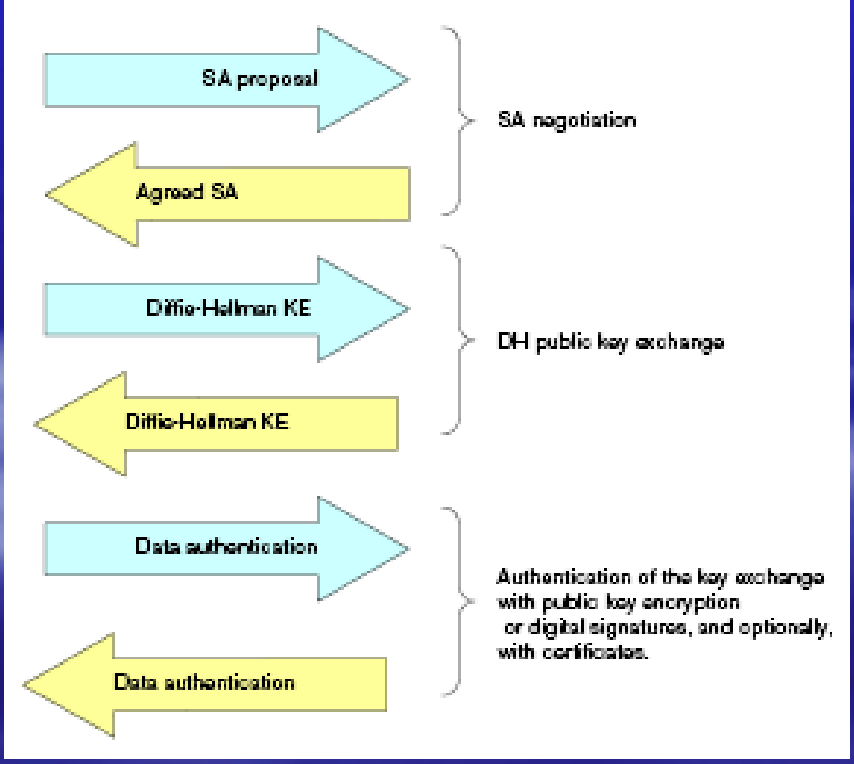


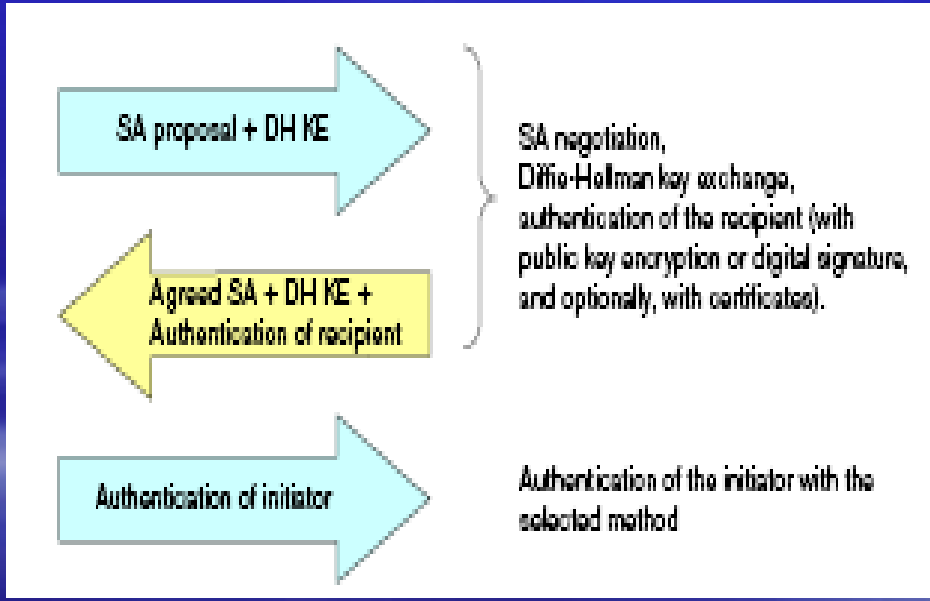
IPsec protokoll

- Internet Key Exchange (IKE)
  - ***„IPsec”***-hez szükséges paraméterek, kulcscsere és módszerek rögzítése az ***„IKE”*** fázis során ***„SA”***-kban
  - IKE 1. fázis
    - IKE SA létrehozása a „security gateway”-ek közötti további kommunikációhoz mindkét oldalon
      - Kommunikáló felek authentikálják magukat
      - Diffie-Hellman kulcscsere
      - Authentikáció ellenőrzése

IPsec protokoll

- Internet Key Exchange (IKE)
  - IKE 1. fázis





IPsec protokoll

- Internet Key Exchange (IKE)
  - IKE 2. fázis
    - IPsec SA létrehozása az IKE SA-k segítségével
      - Titkosítás és dekódoló eljárások rögzítettek
      - Az IPsec indítványhoz szükséges titkos kulcs szintén az IKE 1. fázisban rögzítették
      - Az IPsec élettartam rögzítése
    - Különböző szintű IPsec SA-k
      - Hálózatok ill alhálózatok
      - Hosztok és protokollok
      - Portok
    - IKE SA-k ritkábban generálódnak újra, mint az IPsec SA-k

IPsec protokoll

- Manuális IPsec üzemmód
  - Titkosításhoz és dekódoláshoz szükséges kulcsok manuális megadása
    - Nincs IKE
    - Nincs kulcscsere szabályos időközönként
    - Nincs védelem a ***„replay attack”*** típusú támadások ellen