IP alapú távközlés 2019
IP VPN

Dr. Répás Sándor

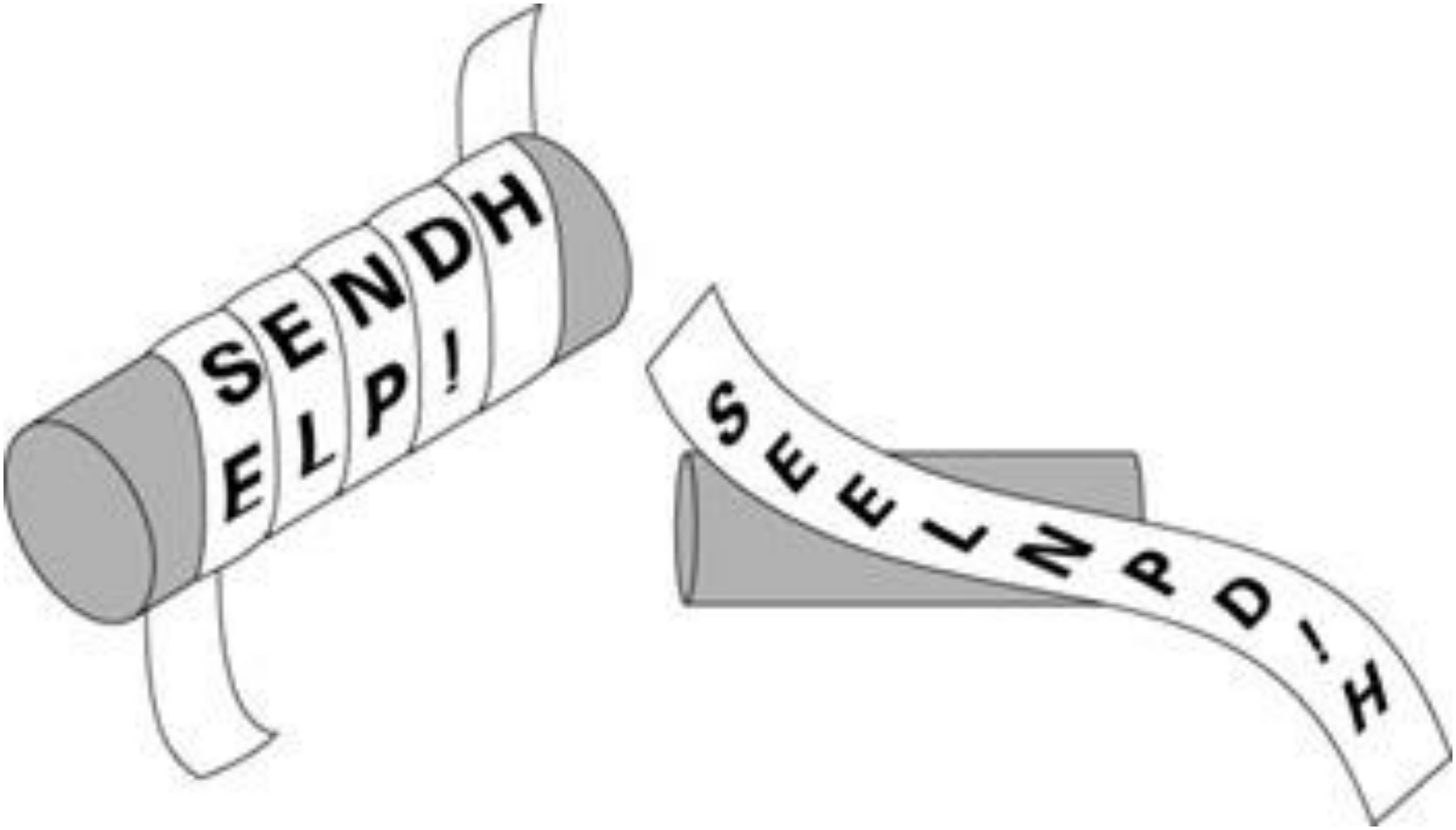
IFMMP

?????

Scytale

- Eredetileg a spártaiak használták katonai célokra
- A kutatások szerint feltalálója Archilochus költő ie. VII. században
- Rúdra tekert szíj belső oldalára írt üzenet
- Szíjat futárral elküldték a címzettnek
- Dekódolásához ugyanolyan vastag bot
- Transzpozíciós kódolás

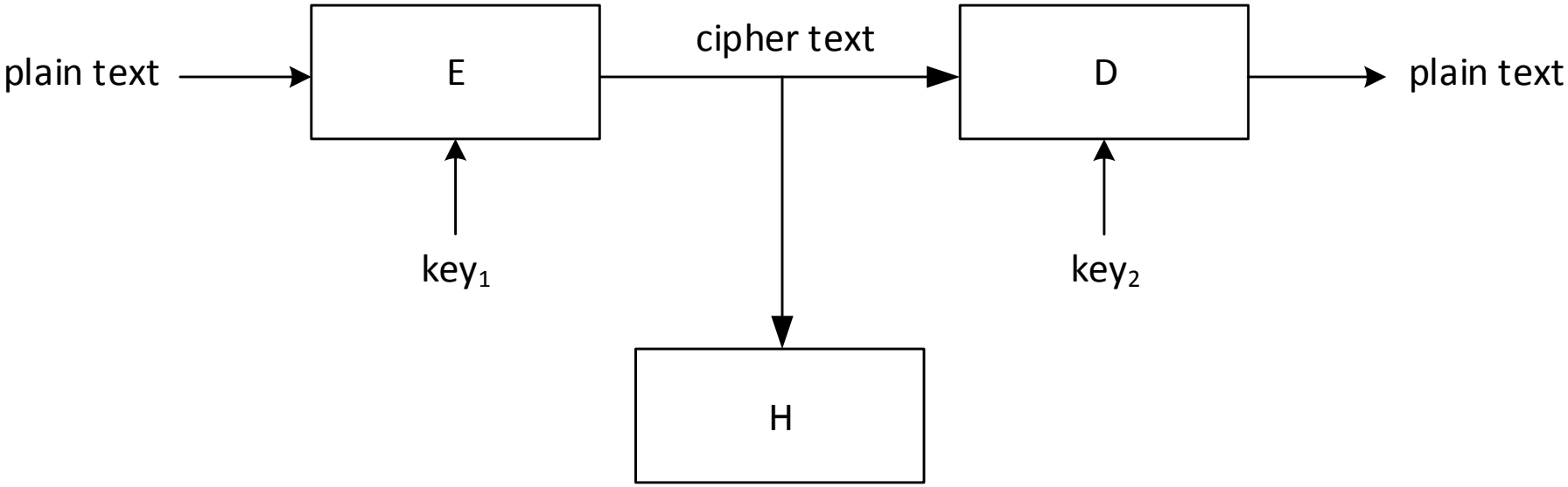
Scytale



Kriptológia

- Titkos kommunikációval foglalkozó tudomány
- Két fő ága:
  - Kriptográfia: titkosítás
  - Kriptoanalízis: titok jogosulatlan megfejtése
- Gyakorlati titkosság: az információ korábban váljon értéktelenné, mint a kor technikai színvonalán, a megfejtése

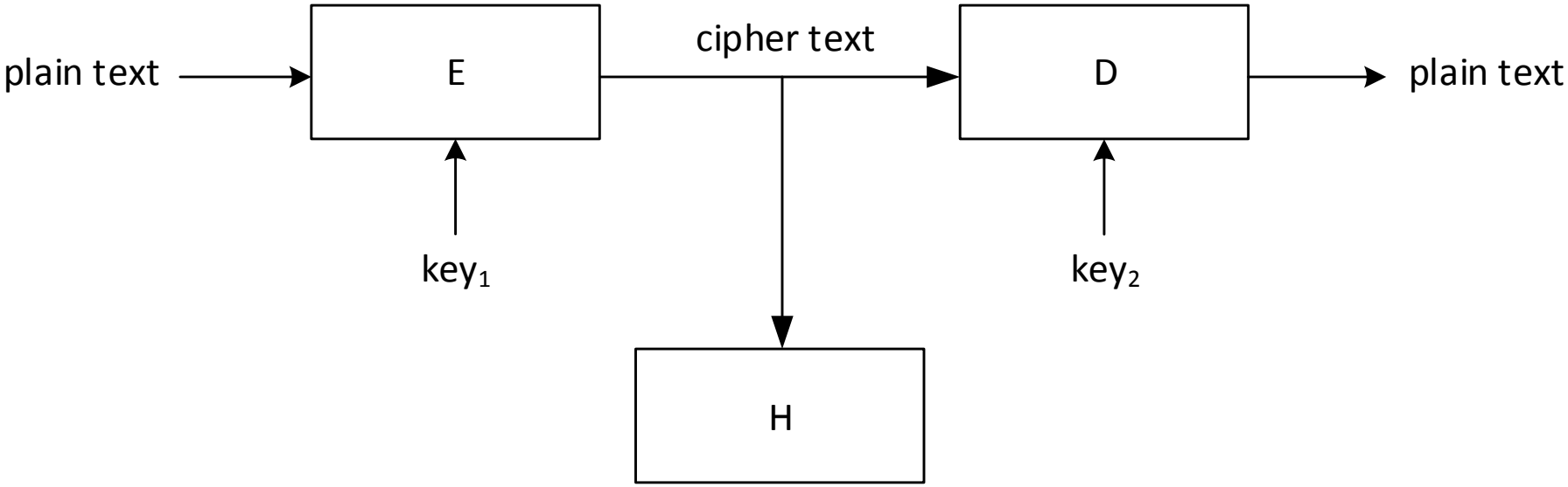
Titkosítás



One time pad (OTP)

- Véletlen átkulcsolásnak/Vernam cipher
- 1917 Gilbert Vernam (1890-1960)
- Kulcs:
  - Hossza megegyezik a kódolandó szöveggel
  - Minden esetben véletlenül generált
  - Feltörhetetlen
  - Gyakorlatban nem alkalmazható:
    - Kulcsgenerálás
    - Kulcs továbbítása

Titkosítás



Titkosítás

- key_1=key_2?
  - Szimmetrikus kulcsú titkosítás
  - Nyilvános kulcsú titkosítás
- Alapvetően
  - Transzpozíció (permutáció)
  - Helyettesítés
- Kulcskezelés
- Kulcscsere

Szimmetrikus kulcsú algoritmusok

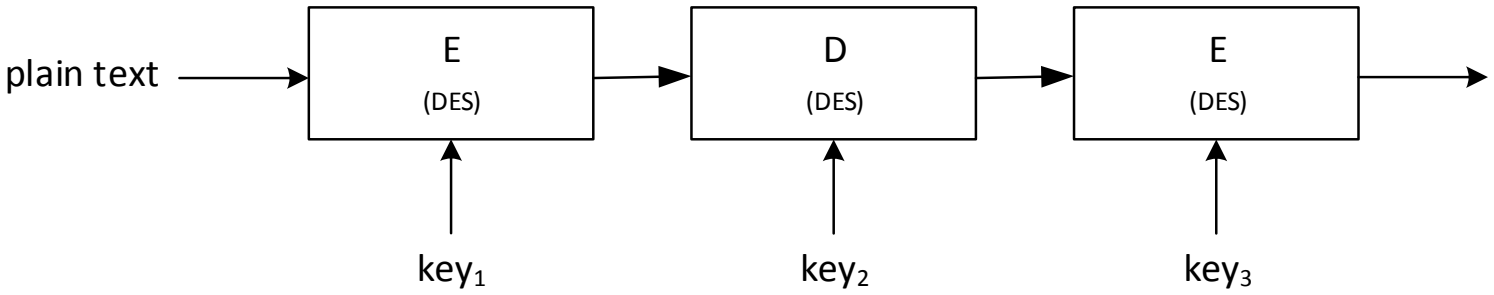
- (Titkos kulcsú blokkrejtjelezők)
- $key_1 = key_2$
- *k* bit hosszú kulcs
- Nyílt üzenetet *n* bit hosszúságú blokkokra
  - Csak n egész számú többszörösével megegyező hosszúságú nyílt üzenet titkosítása
  - Szöveg kiegészítése a megfelelő hosszra (padding)
- Probléma: A titkosító kulcs eljuttatása a címzett(ek)hez
- Ismertebb algoritmusok:
  - DES
  - 3DES
  - AES

DES

- Data Encryption Standard
- IBM 1970-es évek
- Blokkméret 64 bit
- Kulcsméret 56 bit (eredeti terv 128 bit, de NSA)
- Nem törhető fel, de:
  - Rövid kulcsméret
  - Mai technológiával kimerítő kulcskeresés hamar elvégezhető (brute force)

3DES

- Triple Data Encryption Standard
- Cél: Kulcshossz növelése
- Kompatibilitás egyszerű megőrzése a DES-re képes eszközökkel
- E-D-E, vagy D-E-D konfiguráció
- $key_1=key_2=key_3$: Normál DES
- key_1, key_2 és key_3 eltér: 3DES 3*56=168 bites kulcs



AES (Rijndael)

- Advanced Encription Standard
- National Institute for Standards and Technolgy (NIST) 1997-es projektje a DES lecserélésére
- 21 nevezés a pályázatra, 15-öt elfogadtak
- 5-öt választottak:
  - MARS
  - RC6
  - RIJNDAEL
  - SERPENT
  - TWOFISH
- RIJNDAEL győzött

AES (Rijndael)

- Blokk és kulcsméret:
  - 128 bit
  - 192 bit
  - 256 bit
- Hardveres támogatás:
  - Korszerűbb intel mikroprocesszorok AES-NI utasításkészlet
  - AMD esetén AES utasításkészlet
  - SoC-okban: Security System, Security Processor, vagy Crypto Engine

Blokkrejtjelezési módok

- Electronic Codebook (ECB)
  - Bemenet *n* bites blokkokra bontása
  - Blokkok külön-külön rejtjelezve
  - Adott kulcs mellett adott nyílt szöveg blokkhoz egyértelműen tartozik a titkosított párja:
    - Könnyen támadható
    - Blokkok beszúrhatóak, törölhetőek, sorrendjük felcserélhető
- Cipher Block Chaining (CBC)
  - Küldő a rejtjelezett blokkot megőrzi, és rejtjelezés előtt bitenkénti kizáró vagy művelettel hozzáadja a következő rejtjelezendő blokkhoz
  - Első blokkhoz az Inititalization Vectort (IV) adja hozzá
  - Láncolat képződik
  - Sérülés? Dekódolás?

Lenyomatképző algoritmusok

- Hash függvények célja a bemeneti szövegre (vagy egyéb információra) jellemző kimenet létrehozása („újlenyomat”)
- Szempontok:
  - Egyirányú (lenyomatból sosem állítható elő az algoritmus bemenete)
  - Nehéz legyen olyan szöveget előállítani, ami egy előre megadott újlenyomatot (DIGEST) eredményez (születésnap paradoxon)
    - Könnyen lehetne szöveget hamisítani meglévő aláíráshoz
  - Viszonylag rövid legyen a generált lenyomat
- MD5
- SHA1, SHA2, SHA3, SHA5

MD5

- Message Digest 5 (MD5)
- Az MD4 javítása
- 128 bites lenyomat
  - Ez ma már túl rövid a születésnap paradoxonon alapuló támadásoknak
- Használata nem ajánlott, de számos esetben előfordul (Pl sok tanúsítványban is)

SHA

- Secure Hash Algorithm (SHA)
- SHA-1
  - 160 bites lenyomatot képez
  - NSA tervezte
  - 2005 óta nem tartják biztonságosnak
  - 2017-ben publikáltak azonos lenyomattal rendelkező PDF állományt
  - Alkalmazása nem ajánlott. Több rendszer nem fogadja el biztonságosnak.
- SHA-2
  - NSA tervezte
  - Lényegesen eltér az SHA-1-től, de más problémákkal rendelkezik
  - SHA-224
  - SHA-256
  - SHA-384
  - SHA-512(/224-256)

SHA-3

- NIST szabvány, 2015 augusztus 5. (FIPS 202)
- Keccak algoritmus
- NIST SP.800-185 plusz függvények, 2016. december 22.
  - SHA3-224
  - SHA3-256
  - SHA3-384
  - SHA3-512
  - SHAKE128
  - SHAKE256
- Példa a Wikipediáról (1 bit változás a bemenetben, 50%-os valószínűséggel okoz változást a kimenet minden bitje esetében):

```
SHAKE128("The quick brown fox jumps over the lazy dog", 256)
f4202e3c5852f9182a0430fd8144f0a74b95e7417ecae17db0f8cfeed0e3e66e
SHAKE128("The quick brown fox jumps over the lazy dof", 256)
853f4538be0db9621a6cea659a06c1107b1f83f02b13d18297bd39d7411cf10c
```

Üzenethitelesítés

- Címzett biztos lehessen:
  - Üzenet valóban attól származik, akinek tulajdonítja
  - Üzenetet pontosan az, amit a feladója küldött
- CBC-MAC
  - Utolsó blokk a MAC
- HMAC
  - Valamely lenyomatképző függvény
  - HMAC-MD5
  - HMAC-SHA1

Nyilvános kulcsú algoritmusok

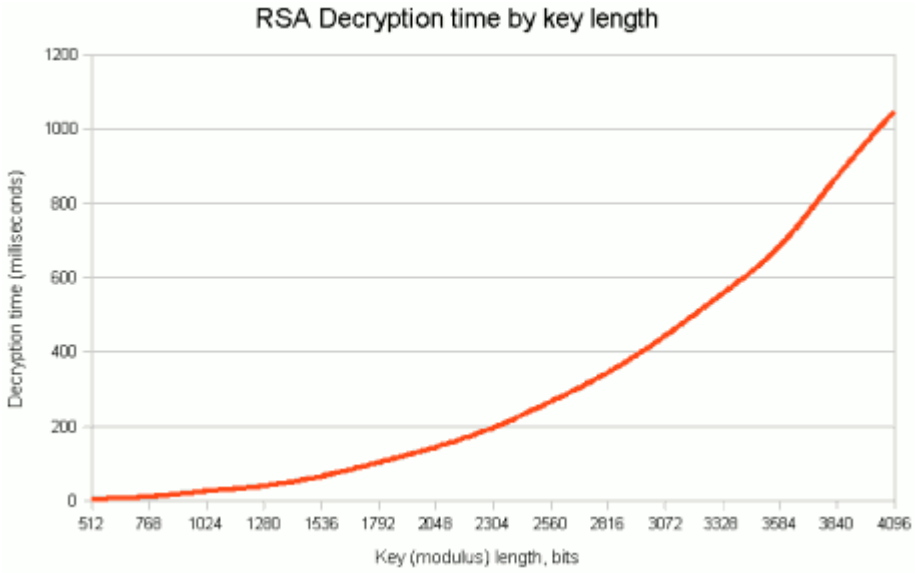
- $key_1 <> key_2$
- Amit az egyik kulccsal elkódolunk, az a másik kulccsal dekódolható
- Az egyik kulcsot titokban tartjuk: privát kulcs
- A másik kulcsot nyilvánosságra hozzuk: nyilvános kulcs
- RSA
- DSA
- EC

RSA

- 1976. Ron **R**ivest, Adi **S**amir, Leonard **A**dleman (RSA)
- 2000. szeptember 20-án lejárt a szabadalmi védelme
- Alapja:
  - Nagy számok faktorizációjának problémája:
    - Egy kellően nagy számról nehéz megállapítani annak prímtényezőit.
    - Jelenleg nem ismerünk az egész számok prímtényezős felbontására hatékony algoritmust
    - Ha egy szám két igen nagy prímszám szorzata, akkor annak prímtényezős felbontása nagyon gyors számítógépekkel is nagyon sokáig tart.
- A legelterjedtebb nyilvános kulcsú algoritmus
- 1994. Peter Shor: egy kvantumszámítógép elvileg végre tudja hajtani a faktorizációt polinom időn belül
- Ajánlott kulcshossz legalább 2048 bit:
  - Rövidebb kulcsok már nem biztonságosak
    - 2013 júliustól Google nem fogadja el biztonságosnak az 1024 bites, vagy rövidebb kulcsokat
  - Hosszabb kulcsoknál viszont problémák léphetnek fel
    - Eszköz kompatibilitás
    - Dekódolási sebesség

RSA dekódolás

- A kulcshossz duplázásával a dekódolási idő 6-7-szeresére nő
- 2GHz Pentium alapú számítógép dekódolási ideje:



Forrás: https://www.javamex.com/tutorials/cryptography/rsa_key_length.shtml

DSA

- Digital Signature Standard (DSS)
  - NIST FIPS 186-(1,2,3,4)
- Digital Signature Algorithm (DSA)
- Célja nem a titkosítás, hanem a digitális aláírás
- Sok helyen az RSA helyett használják (Pl. SSH)

Algoritmikus támadások

1. Rejtett szövegű támadás. Ez a módszer ugyanazon kulccsal titkosított rejtett szövegű üzeneteket használ fel. (ciphertext only attack)
2. Ismert nyílt szövegű támadás. Ismert, összetartozó nyílt szöveg – rejtett szöveg párokat használ fel. (known plain text attack)
3. Választott szövegű támadás. A támadónak lehetősége van megválasztani a nyílt szövegeket, amelyekhez tartozó rejtett szövegeket megkaphatja, vagy a rejtett szövegeket, amelyekhez való nyílt szövegeket megkaphatja. (chosen text attack)

- Az egyre nagyobb sorszámú támadás kategóriák egyre többet követelnek a támadótól

Kulcsmenedzsment

- A használt kulcsokat időnként cserélni kell:
  - Kommunikáció kezdetekor
  - Ne legyen túl sok azonos kulccsal titkosított szöveg
  - Kulcs kompromittálódik:
    - Kitudódás
    - Sérülés
- Kulcs archiválása
- Kulcsgenerálás:
  - Véletlen számok
- Kulcstárolás
- Kulcsok továbbítása

Digitális aláírás

- Letagadhatatlanság
- Sértetlenség
- Bizalmasságot nem biztosít!!!
- Aláírás folyamata:
  - Üzenet lenyomatának elkészítése
  - Lenyomat elkódolása küldő privát kulcsának segítségével
- Aláírás ellenőrzése:
  - Kapott üzenet lenyomatának elkészítése (aláírás nélkül)
  - Üzenettel érkezett aláírás elkódolása a feladó nyilvános kulcsának segítségével
  - Készített és kapott lenyomat összehasonlítása

Titkosított üzenet küldése

- Bizalmasság
- Sértetlenség?
- Titkosítás folyamata:
  - Szimmetrikus titkosításhoz kulcs generálása
  - Üzenet titkosítása szimmetrikus algoritmussal és a generált kulccsal
  - Szimmetrikus kulcs elkódolása címzett nyilvános kulcsával
  - Titkosított üzenet és a hozzá kapcsolódó titkosított szimmetrikus kulcs elküldése
- Üzenet visszafejtése:
  - Kapott üzenetben szereplő szimmetrikus titkosító kulcs dekódolása a címzett privát kulcsával
  - A kapott üzenet visszafejtése a szimmetrikus kulcs segítségével

Tanúsítvány

- Certificate
- Hogyan kezeljük a nyilvános kulcsokat?
- Honnan tudhatjuk, hogy kinek mi a nyilvános kulcsa?
- Honnan tudhatjuk, hogy a nyilvános kulcs tényleg azé, akit gondolunk?
- Mi történjen a kompromittálódott kulcsokkal?
- …

Ötlet

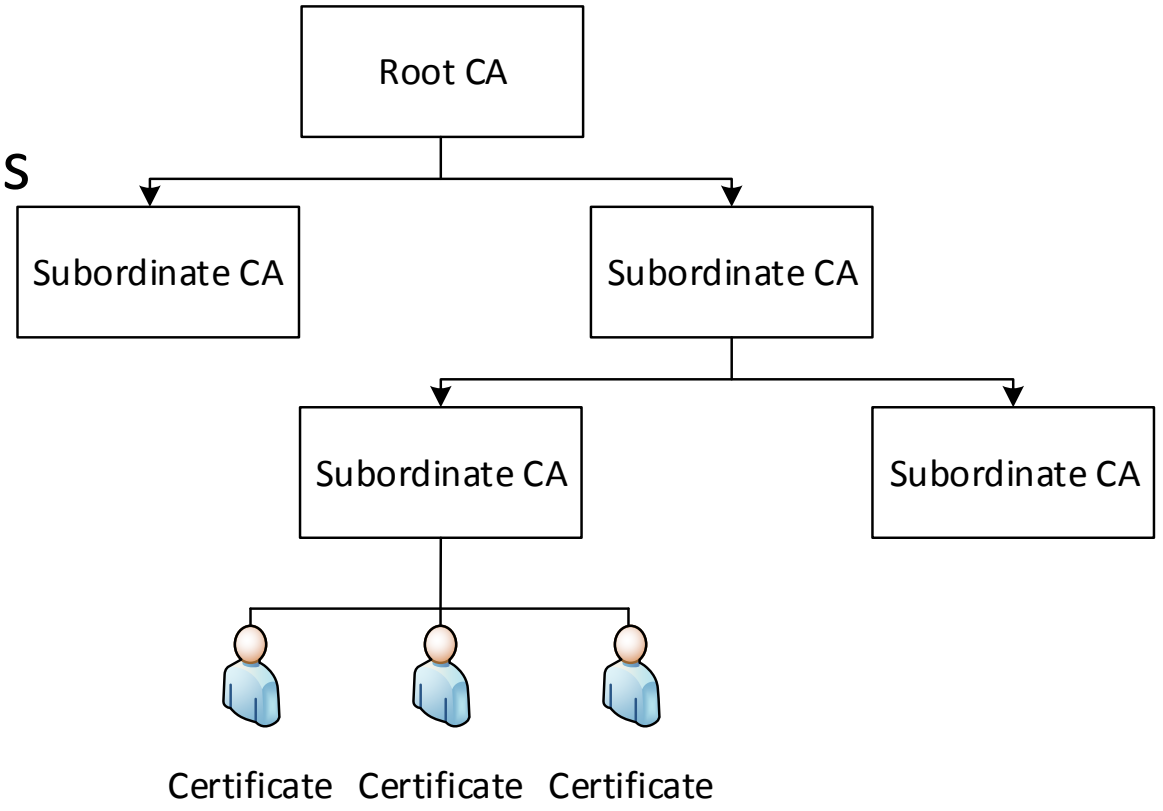
- Valakinek a kulcsában már megbízunk
- Az illető hitelesítse (írja alá) mások kulcsát (és a hozzá tartozó tulajdonságokat)→tanúsítvány
- Két elterjedt megoldás:
  - X.509
  - PGP

X.509

- Trusted root CA
  - Önaláírt tanúsítvány
  - Hosszú érvényesség
  - Az operációs rendszer/böngésző gyártó beépíti, de a felhasználó is telepíthet
- Subordinate CA
  - A felette lévő CA hitelesíti a tanúsítványát
  - Rövidebb, de még mindig hosszú érvényességi idő
  - (Azonos szinten is aláírhatják egymás tanúsítványát)
- Többszintű láncolat is kialakítható
- Az egyes CA-k különböző célokra oszthatnak tanúsítványt

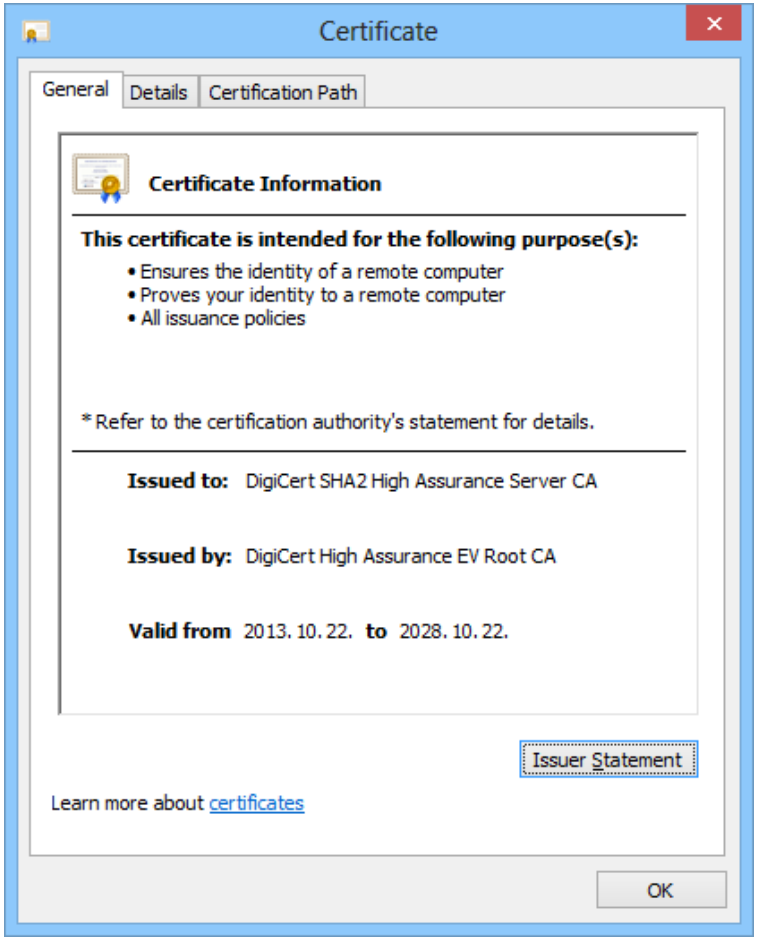
CA láncolat

- Root CA
- Subordinate/Intermediate CA
- Issuing CA
- Clients certificates



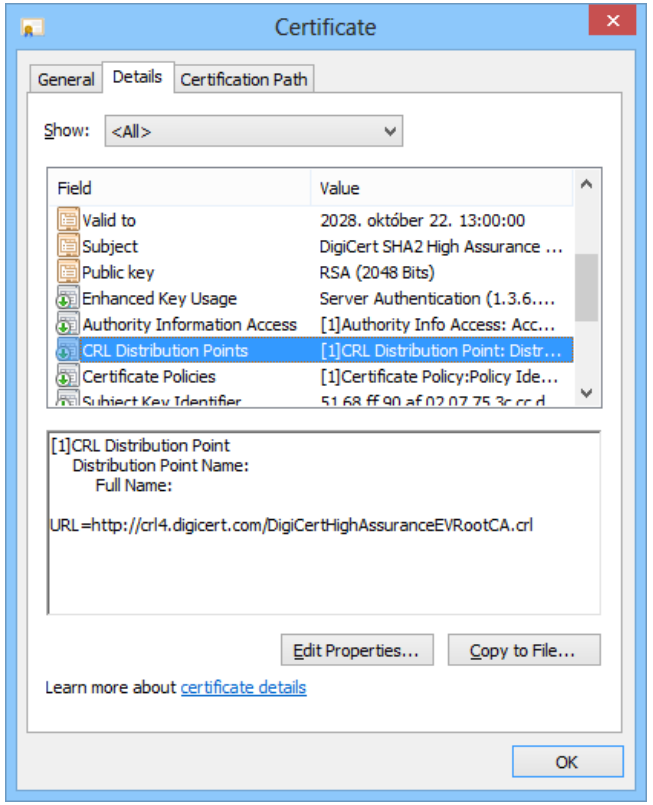
Tanúsítványok néhány tulajdonsága

- Sorozatszám
- Ki kapta
- Ki tanúsította
- Érvényesség kezdete
- Érvényesség vége
- Visszavonási lista elérhetősége
- Mire használható
- Verzió szám
- **A nyilvános kulcs**



CRL

- Certificate Revocation List (CRL)
- A kompromittálódott kulcsú tanúsítványokat vissza kell vonni
- Lista a visszavont tanúsítványokról:
  - Sorozatszámok
  - Általában HTTP URL
  - Természetesen digitálisan aláírva



PKI

- Public Key Infrastructure (PKI)
- Szerepkörök, eljárások, szabályzatok melyek a digitális tanúsítványok:
  - menedzseléséhez,
  - kiosztásához,
  - használatához,
  - tárolásához,
  - visszavonásához szükségesek
- Például:
  - CA szervezete (Pl dolgozók)
  - CA szabályzata
  - Tanúsítványok

PGP

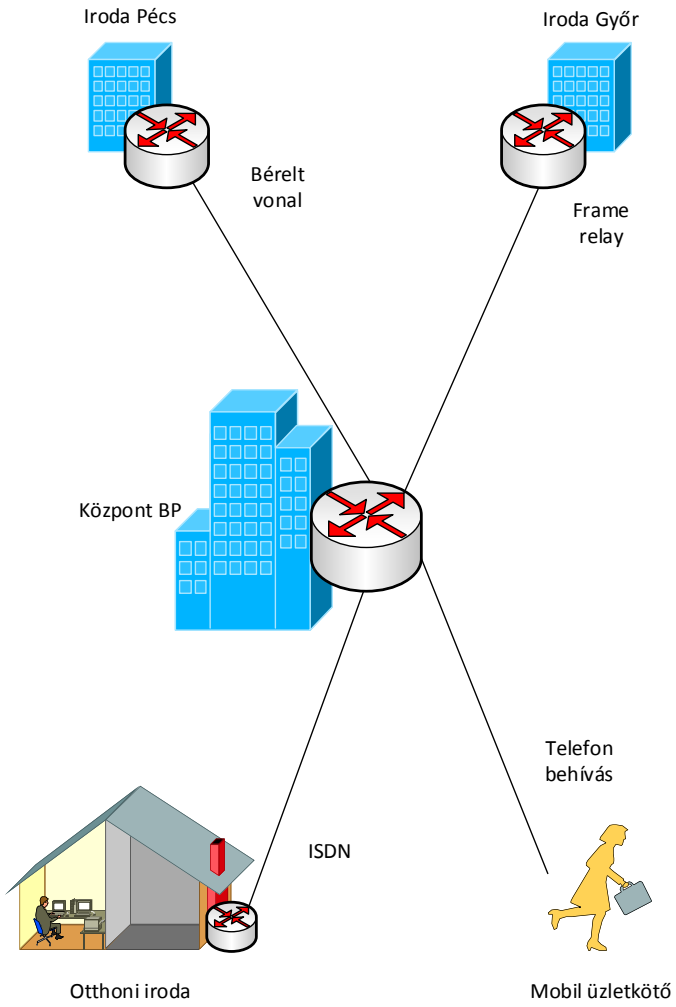
- Pretty Good Privacy (PGP)
- Első verzió: 1991. Philip R. Zimmermann
  - (1993 februárjában meggyanúsították az USA exportszabályainak megsértéséért)
  - 2010-ben a Symantec megvette a PGP-t
  - 1997 júliusban OpenPGP, jelenleg RFC 4880
  - 1997. szeptember 7-én a Free Software Foundation (FSF) kiadta saját OpenPGP kompatibilis programját: GNU Privacy Guard (GnuPG, GPG)
- Web of trust
  - Egymás tanúsítványait írhatják alá, hitelesíthetik

GnuPG

IP VPN

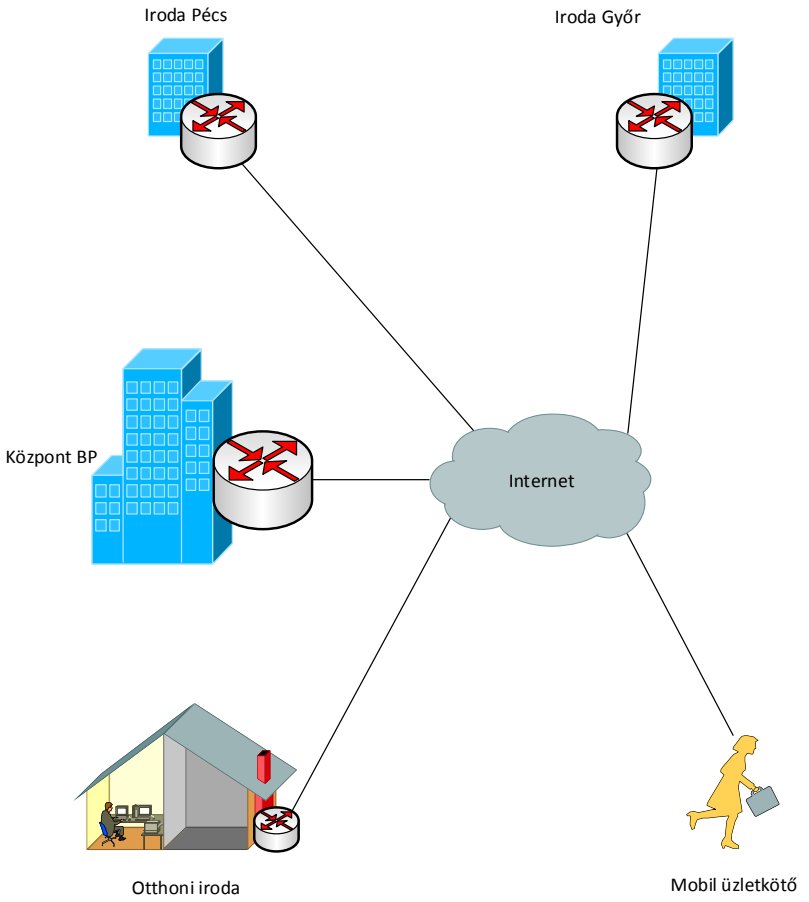
Hagyományos hálózat kialakítása

- Állandó sávszélesség
- Nehézkes kiépítés, bővítés
- Speciális eszközök
- Magas költségek



IP VPN hálózat kialakítása

- Virtual Private Network (VPN)
- Kommunikáció (titkosított) tunnelekben
- Folyamatosan változó sávszélesség
- Egyszerű, gyors kiépítés
- Alacsony költségek
- Egyszerű bővítés
- Site to Site, vagy Remote-Access VPN



Site to Site VPN

- A hagyományos WAN hálózatok továbbfejlődése
- Bérelt vonal, Frame Relay helyett
- A telephelyi LAN-ok közti kapcsolatot biztosító tunnelt egy hálózati eszköz (pl VPN router, tűzfal) építi ki
- A felhasználók számítógépei nem is „tudnak” a VPN igénybevételéről

Remote Access VPN

- A hagyományos betárcsázós, ISDN-es kapcsolatok helyett
- Egy felhasználó részére teszi lehetővé a távoli hálózathoz való csatlakozást
- A VPN kliens általában a felhasználó számítógépére kerül telepítésre és nem külön eszközön
- Általában a felhasználás időtartamára kerül csak kiépítésre a VPN csatorna

IP VPN protokollok

VPN Protokoll	Protokoll, port	Tulajdonság	Szabvány
PPTP	TCP 1723, GRE (IP 47)	Elterjedt, egyszerűen telepíthető, nem biztonságos, elavult.	RFC 2637
L2TP	UDP 1701	Nincs titkosítás	RFC 2661 (3931)
IPsec	UDP 500, 1701, 4500, ESP (IP 50), AH (IP 51)	Framework. „Pilótavizsga” Tanúsítvány és PSK is használható hitelesítésre. Mindkét irányú hitelesítés.	RFC 6071
L2TP/IPsec	UDP 500, 1701, 4500, IP protokoll 50	IPsec segítségével titkosított L2TP. „Egyszerű” konfigurálás, magas biztonság. Mindkét irányú hitelesítés.	RFC 3193
SSTP	TCP 443	SSL/TLS csatorna. Tűzfalakon egyszerűen átjut.	Microsoft
IKEv2	UDP 500	Security Association (SA) létrehozásához: titkosító algoritmus, kulcsok, egyéb paraméterek.	RFC 7296
OpenVPN	UDP 1194, TCP 443	TUN, vagy TAP működés. Tanúsítvány, PSK, felhasználónév/jelszó is használható hitelesítésre. Mindkét irányú hitelesítés. Nem egyszerű beállítás.	OpenVPN Inc.

IPsec

- Nyílt szabványok algoritmus független keretrendszere
- Hitelesítheti és védheti az IP csomagokat
- Biztosít:
  - Bizalmasságot
  - Integritást
  - Hitelesítést
  - Visszajátszás elleni védelmet

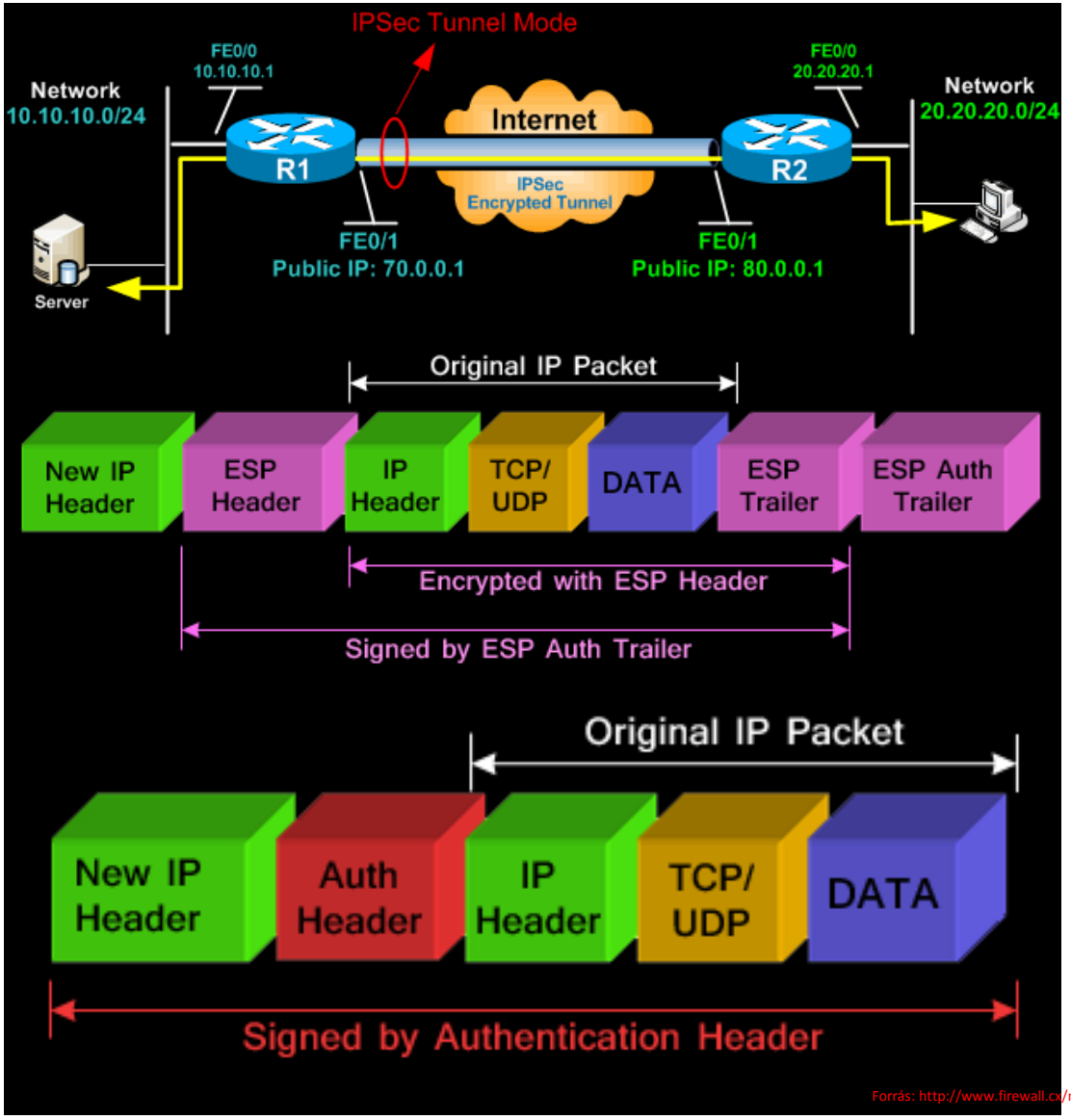
IPsec protokollok

- Authentication Header (AH)
  - Hitelesítés
  - Integritás
- Encapsulation Security Payload (ESP)
  - Titkosítás
  - Hitelesítés
  - Integritás

IPsec módok

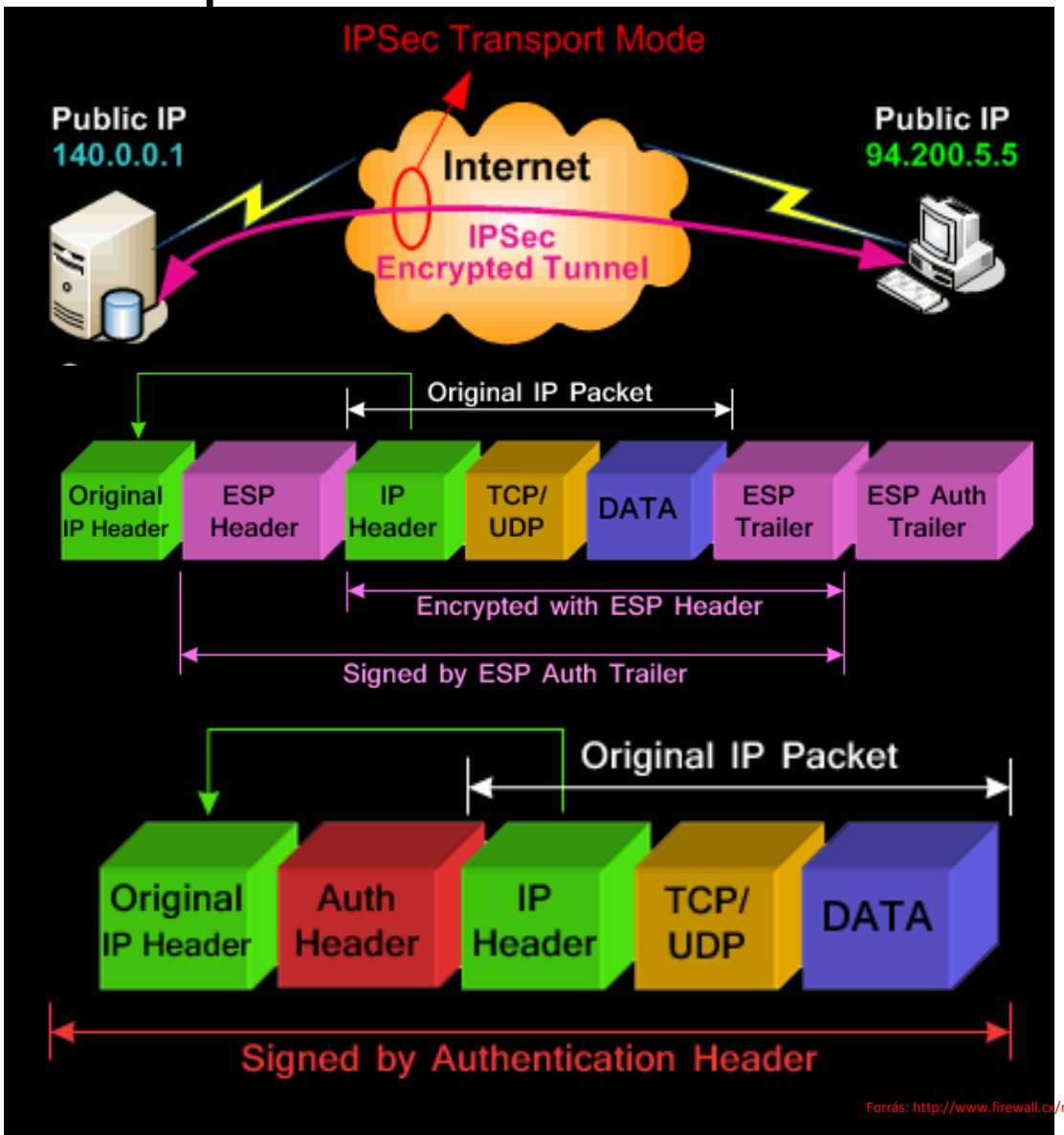
- Tunnel mód
- Transport mód

IPsec tunnel mód



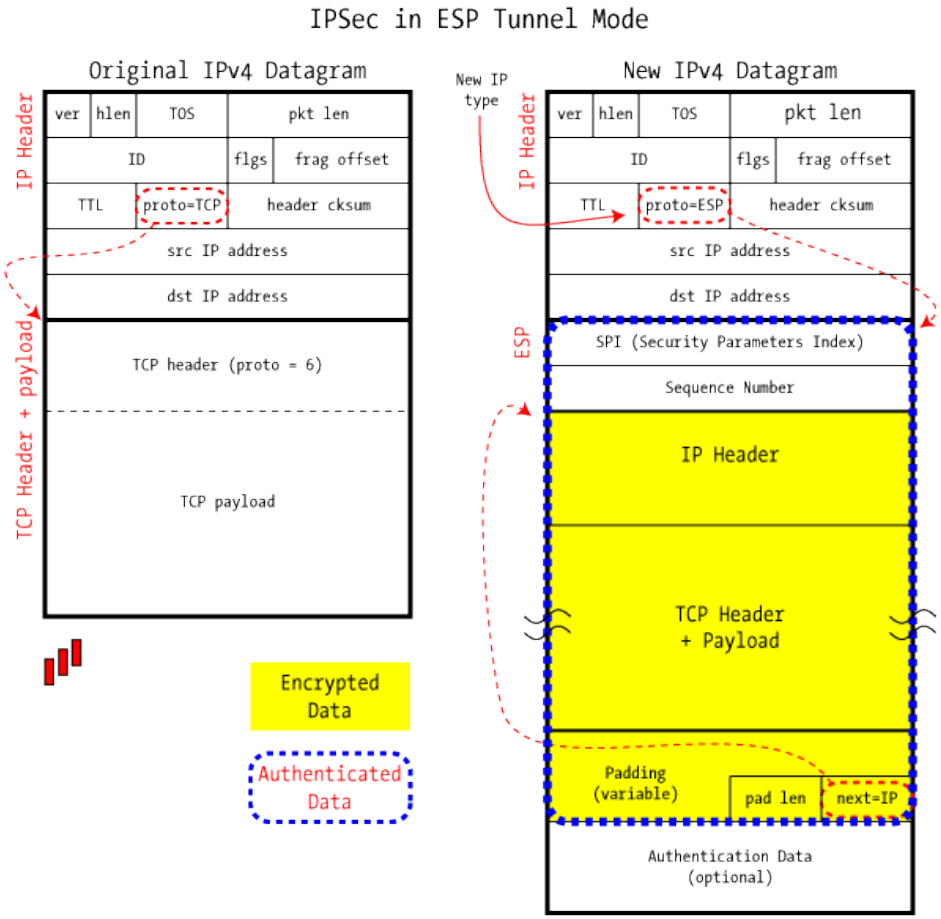
Forrás: http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

IPsec transport mód



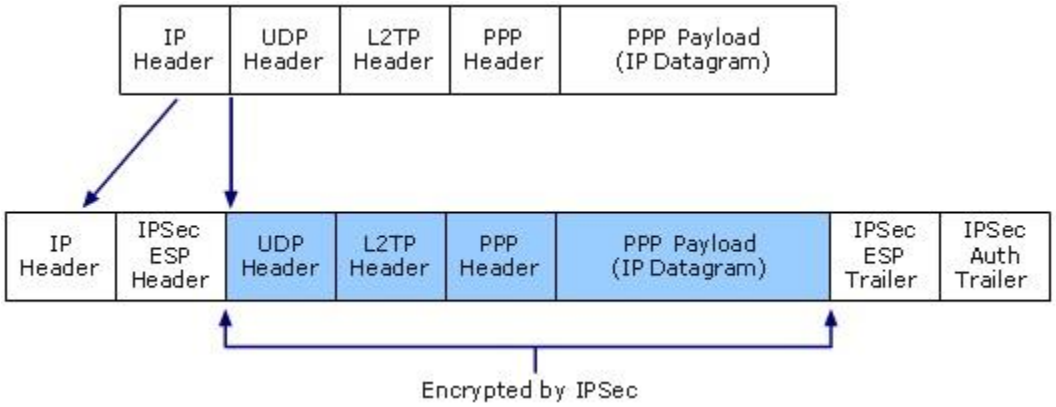
Forrás: http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html

IPsec ESP tunnel mód fejléc



Forrás: http://www.unixwiz.net/techtips/iguide-ipsec.html

L2TP/IPsec fejléc



Hitelesítő eszközök

- Password
  - PAP (Password Authentication Protocol)
  - CHAP (Challange-Handshare Authentication Protocol) (MS-CHAP)
  - Preshared key
- One-Time Password (OTP):
  - HOTP (HMAC-based One-time Password)
  - TOTP (Time-based One-time Password)
  - OCRA (OCRA: OATH Challenge-Response Algorithm, Open Authentication)
  - (Software)
- Certificate:
  - File
  - Smartcard
  - USB Token
- EAP

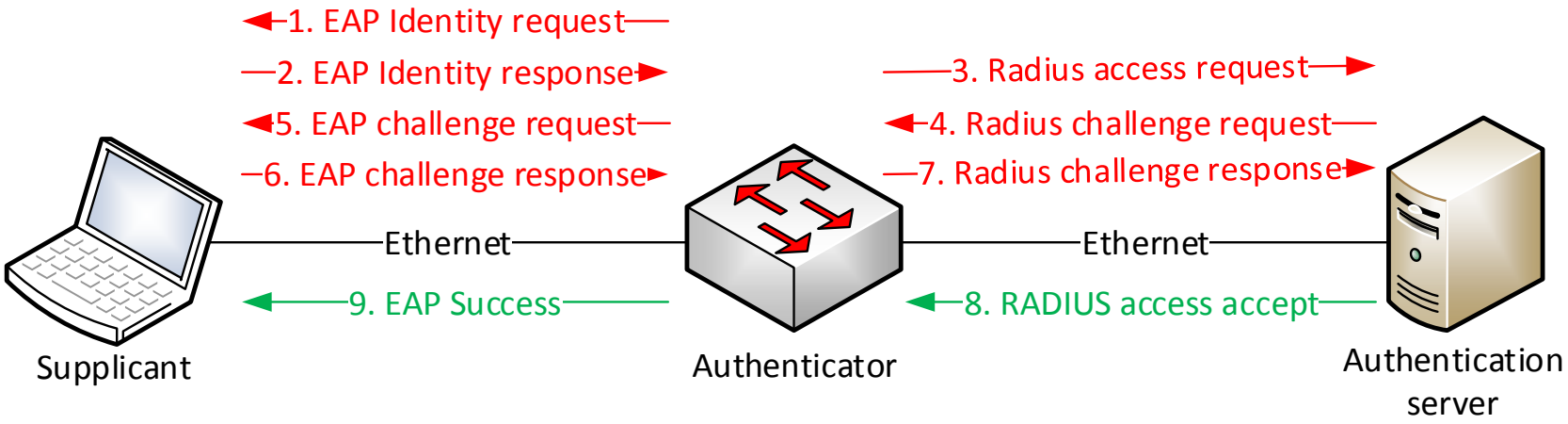
Extensible Authentication Protocol (EAP)

- PEAP (Protected EAP)
  - Szerver oldali tanúsítványokat használ. Védett tunnelben továbbítja az adatokat.
- EAP-MSCHAPv2
  - Szerver oldali tanúsítvány, míg a kliens hitelesítéséhez MSCHAPv2 protokoll.
- EAP-GTC (Generic Token Card)
  - Egyszer használatos jelszavakkal, titkosítatlan hitelesítés.
  - RFC 2284
- EAP-MD5
  - A jelszó MD5 lenyomatát ellenőrzi.
  - RFC 2284
- EAP-TLS (Transport Layer Security)
  - A felhasználók tanúsítvánnyal hitelesítik magukat.
  - RFC 5216
- EAP-TTLS (Tunneled Transport Layer Security)
  - A szerver tanúsítványt, míg a felhasználók jelszavakat alkalmaznak.
  - RFC 5281
- EAP-SIM (Subscriber Identity Module)
  - GSM SIM alapú hitelesítés. Hálózat is hitelesítve.
  - RFC 4186
- És még: EAP-AKA (RFC 4187), EAP-POTP (RFC 4793), EAP-TLV, ZLXEAP, EAP-FAST (RFC 4851), LEAP, …

Forrás: https://www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/802.1x/Overview_of_802_1x_Authe.htm

EAP – Radius

- Enterprise WiFi
  - WPA-Enterprise
  - WPA2-Enterprise
- 802.1X

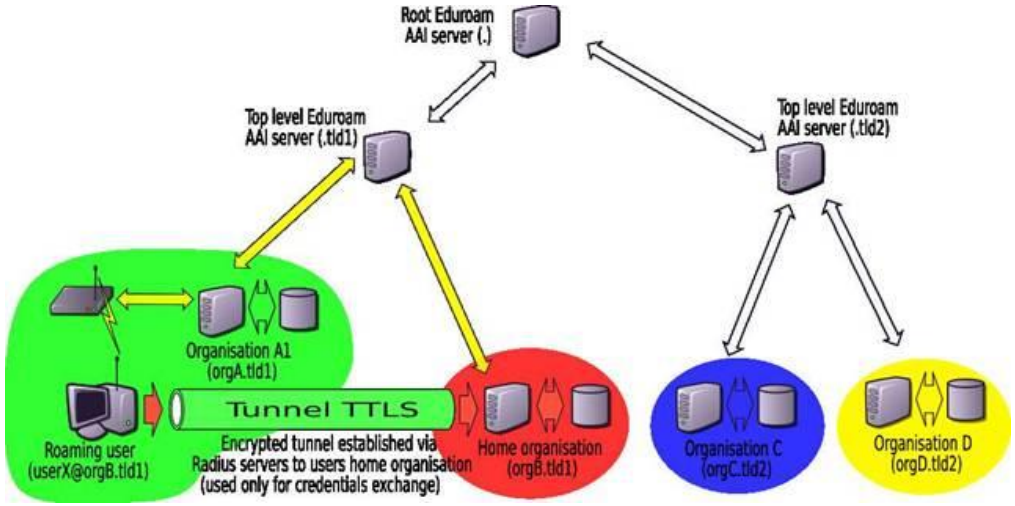


Multifaktoros authentikáció

- Erős hitelesítés
- Two Factor Authentication (2FA)
- Legalább kettő egyidejű alkalmazása a következőkből:
  - Tudok valamit
    - Jelszó
    - PIN kód
  - Rendelkezem valamivel
    - Tanúsítvány
    - Token
    - Mobil telefon
  - Van valamilyen tulajdonságom
    - Retina
    - Véna
    - Arc
    - Újlenyomat

RADIUS

- Remote Authentication Dial-In User Service (RADIUS)
- Livingston Enterprises (1991)
- Széles körben alkalmazott (szabványos)
  - PPPOE
  - VPN
  - WiFi
  - 802.1X
  - SIP
  - …
- RFC 2865 és RFC 2866
- UDP
- Alapesetben nem titkosított
- Skálázható (Proxy)
  - Realm (@ után)
  - Felfűzhetőek
  - Eduroam



Kép forrása: http://eduroam.sourceforge.net/

TACACS+

- Terminal Access Controller Access-Control System (TACACS+)
- RFC 927 TACACS (1980-as évek vége felé kezdte támogatni)
- XTACACS (1990) Cisco nem szabványos bővítése
- RFC 1492 (1993) TACACS+ Nem kompatibilis az előzőekkel
- Titkosított kommunikáció
- TCP, vagy UDP 49 port

Vége