Hálózati biztonság (772-775)

Területei:
- titkosság (secrecy/ confidentality)
- hitelesség (authentication)
- letagadhatatlanság (nonrepudiation)
- sértetlenség (integrity control)

Melyik protokoll réteg jöhet szóba?
- fizikai: vezeték megcsapolása
- adatkapcsolati: adatok kódolása (link encryption)
- hálózati: tűzfalak
- szállítási: végpontok közötti összeköttetés titkosítása
- alkalmazási: felhasználók azonosítása, letagadhatatlanság

Titkosítás alapja (a fizikai szint kivételével): kriptográfia (titkos írás)

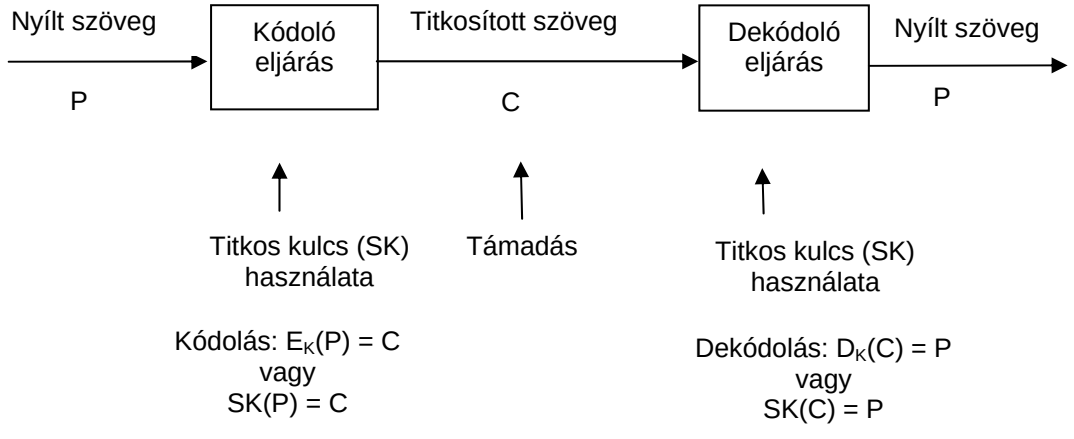
Nem lesz szó:
- operációs rendszer biztonsága
- alkalmazások biztonsága
- vírusok, férgek, trójai falovak, kémprogramok, stb.
- felhasználói azonosítások (biometriai, jelszavas, stb.)

Kriptográfia (775-782)

Rejtjel (cipher):
- karakterről karakterre történő átalakítás
- bitről bitre történő átalakítás

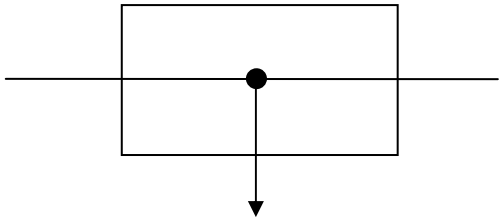
Kód (code):
- egy szó helyettesítése egy másik szóval vagy szimbólummal

Titkosítási modell:

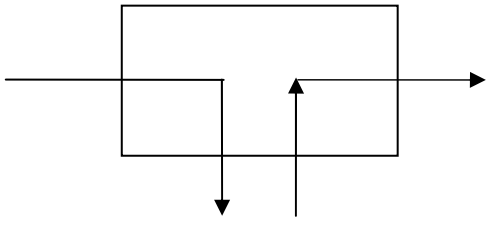


Támadási lehetőségek:

- passzív támadás (üzenet lehallgatása)



- aktív támadás (üzenet megváltoztatása/szabotázs)



Kriptográfia: titkosító eljárások kifejlesztésének tudománya
Kriptoanalízis: a titkosítás megfejtésének tudománya
Kriptológia: mindkettő együtt.

Kerckhoff elve:

- Minden titkosító algoritmusnak nyilvánosnak kell lenni, csak a kulcsok lehetnek titkosak
- ha az algoritmus nyilvános, mindenki ismerheti
- ha a kulcs titkos, védeni kell
- minél hosszabb a kulcs
  - annál nehezebb megfejteni a kódolt szöveget
  - annál nagyobb a munkaigénye a megfejtésnek (munkatényező).

A kódfejtés esetei:

- csak a titkosított szöveg ismert
- a nyílt szöveg és a hozzá tartozó titkosított szöveg ismert, a kulcs nem
- választott nyílt szöveg titkosított párjának saját előállítása.

A titkosítási módszerek csoportosítása:

- helyettesítő típusú rejtjelezés
- keverő típusú rejtjelezés.

Helyettesítő kódok

A nyílt szöveg karaktereinek sorrendje megmarad.

Minden betű vagy betűcsoport egy másikkal helyettesítődik (Ceasar-féle kódolás)

- egybetűs helyettesítés: 26 karakter esetén a kulcs hossza 26! ≈ 4 x 10^{26}
- betűkettősök
- betűhármasok.

Keverő kódok: a nyílt szöveg karaktereinek sorrendje megváltozik

Egyszer használatos bitminta:

Előállítása
***(nyílt szöveg ASCII karakterrel leírva)* XOR *(véletlen bitsorozatú kulcs)* = C**

- Megfejthetetlen!
- Használata nehézkes, nem praktikus.
- Érzékeny a hibákra.

Kriptográfiai alapelvek:

- REDUNDANCIA: az aktív támadások lehetetlenítésére
- FRISSESSÉG: annak ellenőrzésére, hogy az üzenetet nemrég küldték.

Szimmetrikus (titkos) kulcsú algoritmusok (788-797)

A módszer változatlan: keverés és helyettesítés.
Tradicionális kódolás: egyszerű algoritmusok.
Modern kódolás: bonyolult algoritmusok (a kódfejtés hatalmas munka).

Szimmetrikus kulcsú algoritmus: ugyanaz a titkos kulcs (SK) a kódoláshoz és dekódoláshoz

$$D_K(E_K(P)) = P$$

vagy másképpen

$$SK(SK(P)) = P$$

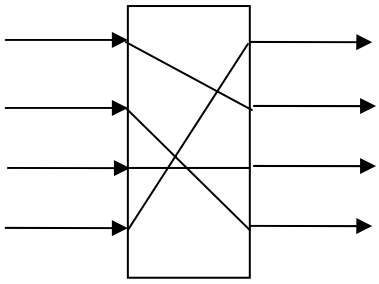
azaz, a nyílt szöveget ugyanazzal a titkos kulccsal (SK) kódolva, majd dekódolva az eredeti nyílt szöveget kapjuk vissza

Blokk kódoló:

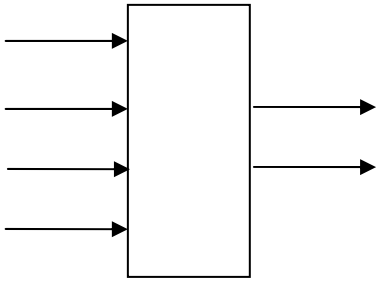
- n bites nyílt szöveg
- m bites kulcs
- n bites titkosított szöveg

Kódoló felépítése:

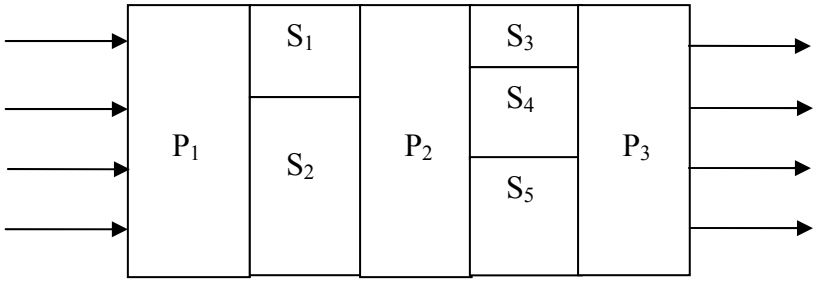
- P- doboz (permutáció): keverő, keverés a kulcs használatával



- S-doboz (substitution): helyettesítő

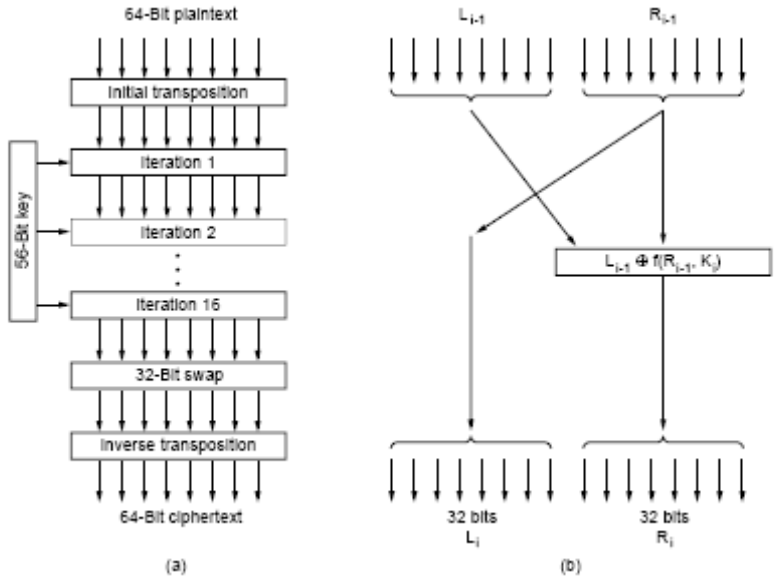


- szorzat típusú titkosító: P - S - P dobozok láncban.



DES (Data Encription Standard): IBM termék szabványosított változata

- 64 bites adatblokk
- 56 bites kulcs (eredetileg IBM termék128 bites volt)
- 64 bites titkosított szövegblokk
- 19 fokozat



A titkosítás lépései:

1. kulcsfüggetlen keverés
2. a/ (első 32 bit) XOR (második 32 bitnek a fokozathoz tartozó kulcsértékkel képzett függvénye)
   b/ (első 32 bit) felcserél (második 32 bit)
3. mint a 2. lépés, csak a kulcsérték más (2. iteráció)
4. …….

17. 16. iteráció
18. 32 bites csere, mint a 2/b pontban
19. inverz kulcsfüggetlen keverés

A kódolás és a dekódolás az IBM szabadalmaztatott kódolójával/ dekódolójával

Háromszoros DES

- két kulcs: SK1 és SK2
- lánc-művelet a titkosított szöveg előállítására:
  kódolás SK1 kulccsal, dekódolás SK2 kulccsal, kódolás SK1 kulccsal
- lánc-művelet a nyílt szöveg visszaállítására:
  dekódolás SK1 kulccsal, kódolás SK2 kulccsal, dekódolás SK1 kulccsal

AES (Advanced Encription Standard) Rijmen és Daemen módszere: Rijndael

A DES-nél és a háromszoros DES-nél hatékonyabb védelem

- helyettesítés + keverés több körben
- blokk és titkos kulcs (SK) bitszáma: 128/128 vagy 128/256
- műveletek egész bájtokra vonatkoztatva
- hardveresen és szoftveresen elvégezhető
- nagyfokú biztonság
- nagy sebesség

Nyilvános kulcsú algoritmusok (804-807)

Diffie és Hellman javaslatai (1976): a kódoláshoz és dekódoláshoz használt kulcsok
- legyenek különbözők,
- egymásból ne lehessen előállítani

Új szabályok:
1. Nem szimmetrikus kulcsok a kódolásnál és dekódolásnál
2. A dekódolót, még ha a kódoló ismert is, rendkívül nehéz legyen előállítani
3. A kódoló feltörhetetlen választott nyílt szöveg támadás esetén, ezért a kulcs nyilvános lehet.

Két kulcs használata szükséges:
- *nyilvános kulcs:* mindenki által elérhető: PK (public key)
- *egyéni kulcs* (saját titkos kulcs): csak egy valaki érheti el: IK (individual key)

Titkosított szöveg küldés ***A***-tól ***B***-hez:
Kódolás: $PK_B(P) = C$ Dekódolás: $IK_B(C) = P$
Titkosított szöveg küldés ***B***-től ***A***-hoz:
Kódolás: $PK_A(P) = C$ Dekódolás: $IK_A(C) = P$

RSA (Rivest, Shamir, Adleman féle titkosítás) 1978

A legfontosabb nyilvános kulcsú titkosító eljárás.
A kulcs hossza: 1024 bit
- nagy biztonság, mert nagy számok prímszámok szorzatára bontását kell elvégezni, ami nagyon nehéz feladat
- lassú eljárás.

Lépések*:* (számelmélet alapján)
1. két nagy prímszám választása (1024 bites): ***p*** és ***q***
2. számítás:
   n = ***p*** x ***q*** pl.: ***p*** = 3 és ***q*** = 11, akkor ***n*** = 33
   z = (***p*** - 1) x (***q*** - 1) pl.: ***z*** = 20
3. ***z***-hez relatív prímszám választása: d (***z***-nek és d-nek ne legyen közös osztója) pl.: ***d*** = 7
4. olyan ***e*** szám keresése, amelyre igaz: ***e*** x ***d*** = 1 mod ***z*** (***z***-vel osztva a maradék 1) pl.: ***e*** = 3

Eljárás:
- nyílt szöveg blokkokra szedése, ahol egy blokk hossza ***k*** bitből áll, ahol ***k***-ra igaz, hogy $2^k < n$ pl.: ***k*** = 5
- kódolás: $C = P^e \pmod n$, ebből ***(e, n)*** pár a nyilvános kulcs (PK) pl.: $C = P^3 \pmod{33}$
- dekódolás: $P = C^d \pmod n$, ebből ***(d, n)*** pár az egyéni kulcs (IK) pl.: $P = C^7 \pmod{33}$

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
Sender's computation				Receiver's computation		

Digitális aláírás (807-813)

Aláírás: titkosított bitsorozat, amely egy küldőt azonosít.
Hitelesség vizsgálathoz aláírás kell
Feltételek:

- a fogadó ellenőrizhesse a feladó valódiságát (hitelesség/authentication)
- a küldő ne tagadhassa le az üzenet tartalmát ((letagadhatatlanság/nonrepudiation)
- a fogadó saját maga ne rakhassa össze az üzenetet (sértetlenség/integrity)

Szimmetrikus kulcsú aláírások (SK alkalmazása)

Központi hitelesség vizsgáló szerv (***KHV***) (mindenki megbízik benne)

- a titkos kulcsok összegyűjtője, kezelője
- az elküldött üzenetek hitelesítője (saját kulcsával is kódolja a kapott titkosított üzenetet)

A küld titkosított üzenetet a közp. hitelesség vizsgálón (***KHV***) keresztül ***B***-nek:

1. ***A*** kódolja és küldi ***KHV***-nek
   $(A, SK_A(B, R_A, t, P)) = C_A$
   A: ***A*** azonosítója
   SK_A: ***A*** titkos kulcsa, amelyet ***A***-n kívül csak ***KHV*** ismer
   B: ***B*** azonosítója
   R_A: ***A*** által választott véletlen szám
   t: időbélyeg
   P: nyílt szöveg
   C_A: ***A*** titkos kulcsával képzett aláírt titkosított üzenet
2. ***KHV*** dekódolja, majd ***B*** titkos kulcsával kódolja:
   $(SK_B(A, R_A, t, P, SK_{KHV}(A, t, P))) = C_B$,
   ahol $SK_{KHV}(A, t, P)$: ***KHV*** aláírása, mellyel tanúsítja, hogy a küldött üzenet ***A***-tól jött
   C_B: ***B***-nek szóló üzenet, amelyet ***B*** saját titkos kulcsával, SK_B-vel dekódolhat.

Nyilvános kulcsú aláírások

Gond a szimmetrikus kulcsú aláírással:

- Kell valaki vagy valamilyen szerv (pl. ***KHV***), amely teljes bizalmat élvez minden résztvevőtől
- Nehéz ilyet találni.

Feltételek:
- $D_K(E_K(P)) = P$
- $E_K(D_K(P)) = P$

Kulcsok (E_K és D_K):
- PK: nyilvános kulcs (public key), kódolásra
- IK: titkos, egyéni kulcs (individual key), dekódolásra

A kódoló által előállított titkosított és aláírt szöveg:

$IK_A(P) = C_A$

$PK_B(C_A) = PK_B(IK_A(P)) = C_{AB}$

B dekódoló által végzett lépések:

$IK_B(C_{AB}) = C_B$

$PK_A(C_B) = PK_A(IK_B(C_{AB})) = PK_A(IK_B(PK_B(IK_A(P)))) = P$

PK_B-vel kódolt üzenetet csak IK_B-vel lehet dekódolni, de ez csak ***B***-nek van
IK_A-val kódolt üzenet PK_A-val dekódolva bizonyítja, hogy az üzenet ***A***-tól jött.

Üzenet pecsétek

Nem mindig kell együtt a titkosítás és a hitelesítés (lassú)
Ha csak a hitelesítés elegendő, akkor pecsétet alkalmaznak

Hitelesítési módszer:
- tetszőleges hosszúságú bitfüzérből (egyirányú hash függvény alapján) fix hosszúságú bitfüzért generálás
- a hash függvény neve : **üzenet pecsét** (MD - message digest)

Az üzenet pecsét tulajdonságai:
- könnyen előállítható egy adott P-hez: MD(P)
- nehéz (lehetetlen) egy adott MD-hez a P-t megtalálni
- ugyanahhoz az MD(P)-hez lehetetlen két P-t generálni (ez csak min. 128 bites kulccsal biztosítható)
- a bemenet 1 bites megváltozása teljesen más kimenetet eredményez (a hash szétszórja a biteket)

Példa: szimmetrikus kulcsú pecsételés (SK alkalmazása)

A által generált pecsételt titkosított üzenet:

$(A, SK_A(B, R_A, t, P) = C_A$

A ***KHV*** által dekódolt, majd pecséttel ellátva ***B***-nek küldött titkosított üzenet:

$(SK_B(A, R_A, t, P, SK_{KHV}(A, t, MD(P)))$

MD5: a legelterjedtebb pecsételő eljárás (Rivest módszere) 128 bites üzenet pecsét, 512 bites blokkok
SH-1 (Secure Hash Algorythm): a másik jelentős eljárás, 160 bites pecsét, 512 bites blokkok.

A nyilvános kulcsok kezelése (817-821)

A nyilvános kulcsokat valahol tárolni kell, hogy mindenki elérhesse.
CA (Certificate Authority): tanúsító hatóság
- tanúsítja az egyes személyekhez tartozó nyilvános kulcsok hitelességét
- tanúsítványt ad
- a tanúsítványt pecséttel látja el
- a tanúsítványt aláírásával látja el.

X.509: tanúsítványokra vonatkozó ITU-T szabvány, de RFC-ben is átvették
- a tanúsítvány leírásának módját adja meg
- definiálja a mezőket a tanúsítványban
- definiálja az egyes mezők funkcióját.

A kommunikáció biztonsága (824-833)

A kriptográfiai eszközök alkalmazása a hálózati forgalom biztonsága érdekében.

IPsec (biztonságos IP)

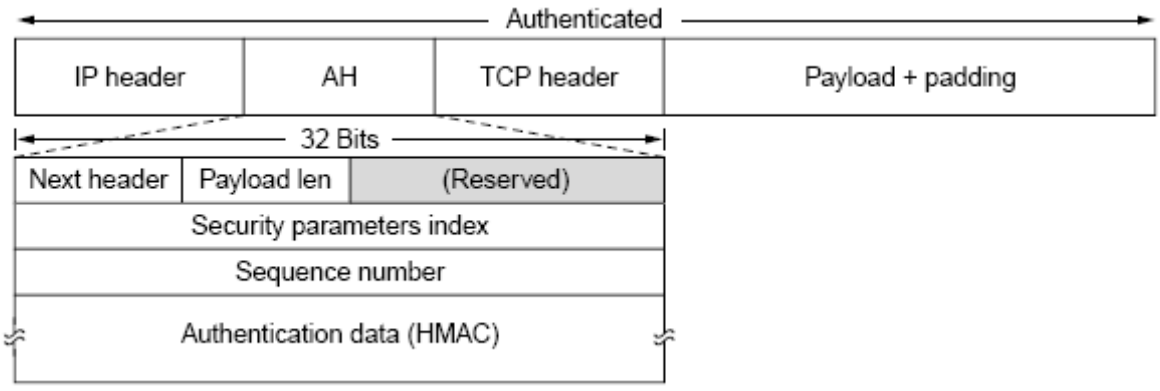
Keretrendszer, amely többféle szolgáltatást tartalmaz választható módon:
- titkosítást
- sértetlenség vizsgálatot
- visszajátszásos támadás elleni védelmet.

Többféle algoritmust tartalmaz, hogy az egyik feltörése esetén legyen másik.

Többféle felbontást tartalmaz, hogy védeni lehessen az alábbi eseteket:
- külön TCP összeköttetés forgalma
- két hoszt közötti összes forgalom
- két biztonságos router közötti összes forgalom.

Összeköttetés alapú: megegyezés kell a kulcsban olyan, mintha összeköttetés lenne
- SA (Security Association - biztonsági kapcsolat) két végpont között
- 2 x SA, ha duplex forgalomban kell a biztonság
- biztonsági azonosító a csomagban.

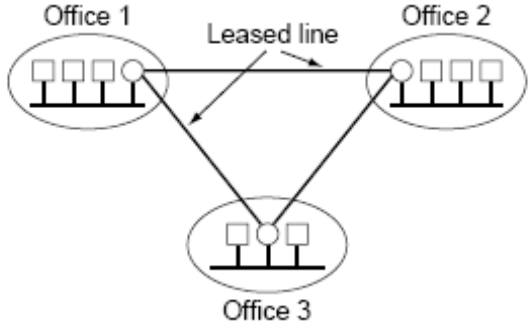
Működési mód:
- szállítási mód:
  - IPSec fejrész az IP fejrész után a törzsbe kerül
  - ez az AH (hitelesítési fejrész)
- alagút mód:
  - az egész IPSEC csomag az IP csomag adatmezejébe kerül
  - be- és kicsomagolás a tűzfalak által



Virtuális magánhálózat: VPN

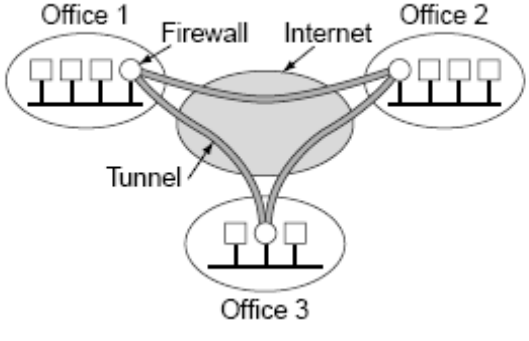
Tényleges magánhálózat:

- vállalati számítógépek + bérelt vonalak



Virtuális magánhálózat:

- vállalati számítógépek LAN-okban + LAN-ok Interneten kialakított alagutakkal összekötve
- belépés/kilépés tűzfalakon keresztül
- SA kapcsolat a két végpont között.



E-levelezés biztonsága (851-857)

Cél: a leveleket csak a címzett olvashassa el

PGP (elég jól biztosított személyiségi jogok, Pritty Good Privacy)

Szoftver csomag az e-levelezés biztonsága érdekében:
- hitelesség vizsgálatot végez
- digitális aláírást ad
- tömörít
- szabadon terjeszthető
- IDEA (International Data Encription Algorythm): olyan, mint a DES és az AES, de a kulcskezelés RSA alapú, a sértetlenség-védelem MD5 alapú

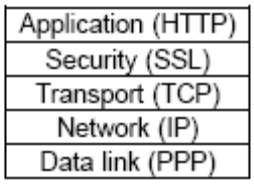
A web biztonsága (866-867)

A dinamikus web-oldalak biztonsága (bankkártya használat, tőzsdézés, stb.) biztonságos összeköttetést igényel.

SSL (Secure Socket Layer, biztonságos csatlakozó réteg)

Netscape terméke, de az Explorer is használja.
Biztonságos összeköttetést hoz létre.
Szolgáltatásai:
- Paraméterek egyeztetése
- Kölcsönös hitelesítés
- Titkos kommunikáció
- Adatok sértetlenségének biztosítása.

Elhelyezkedése a TCP/IP hivatkozási modellben:



Biztonsági szoftver csomag:
- az alkalmazási és a szállítási réteg közé ékelődik
- biztonságos összeköttetés fenntartása a böngésző és a szerver között
- tömörítés kezelése
- titkosítás, hitelesítés, sértetlenség biztosítása
- ha a HTTP-t SSL fölött használják: HTTPS a neve
- portszáma a szervernek 80-ról 443-ra változik
- nemcsak web-böngészővel, mással is használható.

SSL biztonsági elemei banki alkalmazásokhoz:
- Háromszoros DES a titkosításhoz
- SHA-1 a sértetlenség biztosításához

SSL biztonsági elemei kereskedelmi alkalmazásokhoz:

- 128 bites kulcsú RC4 a titkosításhoz
- MD5 a hitelesítéshez

Adatátvitel SSL segítségével:

- 16 KB-os egységekre darabolás
- Tömörítés, ha engedélyezve van
- Üzenethitelesítő kód konkatenálása a tömörített szöveggel
- RC4 titkosítás
- TCP fejrész generálása
- Átvitel TCP összeköttetésen