Fábián Zoltán – Hálózatok elmélet

Kódolások

Titkosítás matematikája – elektronikus aláírás

Tömörítés

Fogalmak 1

- Információ fajtái
  - Analóg – az információ folytonos és felvesz minden értéket a minimális és maximális érték között
  - Digitális – az információ az idő adott pontjaiban létezik. A maximális és minimális érték között csak diszkrét értékeket vesz fel
  - Digitalizálás – Analóg információból digitális információt állítunk elő
- A digitalizálás jellemezői:
  - Mintavételi frekvencia: az analóg jelből milyen gyakran veszünk mintát
  - Bitmélység: Hány biten tároljuk a mintát (Hány bites számnak feleltetjük meg a maximális és a minimális értéket
  - Lineáris vagy nem lineáris a mintavétel (pl. logaritmikus)
  - Pl. hangkártya CD minőség: 44100 Hz a mintavételi frekvencia, 16 bit egy minta mérete, Lineáris mintavételezés
  - Stúdió minőség: 48000 Hz, 32 bit vagy lebegőpontos a minta mérete, lineáris

Fogalmak 2

- Kódolás, dekódolás
  - Az jelsorozatot helyettesítjük más jelekkel =>Ez a kód
  - Pl. ABC betűit pozitív egész számokkal (ASCII kódolás) . Ez nem titkosírás!!!
- Dekódolás
  - Egy kódsorozatot visszaalakítjuk az eredeti értékükre
- A kódolás folyamata
  - Forrás jelsorozat =>Kódoló => jelek átvitele =>dekódoló =>Cél jelsorozat

A kódolás okai

- Az információátvitel vagy tárolás csak így lehetséges
- Kevesebb helyen akarom tárolni az információt
- Titkosítani akarom az információt
- El akarom rejteni az információt
- Végső soron minden információ digitalizálható => elég ha a számsorozatok viselkedését nézzük

Tömörítés – egy fajta kódolás

- Ha a kódolt jelsorozat kevesebb helyet foglal el, mint az eredeti, akkor *Tömörítésnek* hívjuk
  - Ha a tömörítet jelsorozat visszaalakítható az eredetivel egyenértékűvé, akkor *veszteségmentes* a kódolás (tömörítés)
  - A tömörített jelsorozat információveszteséggel alakítható vissza, akkor *veszteséges* a kódolás (tömörítés)
  - A tömöríthetőség feltétele a *redundancia*
    - *R*edundancia: Ismételt információ tárolás vagy olyan információk tárolása, amely más tárolt információkból előállítható

Szteganográfia - Kriptográfia

- Sztganográfia: adatok elrejtése
  - Pl egy kép minden 40. pixelének egyik bitjét módosítom és abban rejtem el az információt
- Kriptográfia: rejtjelezés
- A rejtjelezés kulcsa: az a plusz információ, ami által titkosított lesz a kódolt információ
- A visszafejtéshez használatos kulccsal a visszafejtőnek rendelkezni kell
- Szimmetrikus titkosítás:
  - Ha a titkosításhoz és a visszafejtéshez ugyanazt a kulcsot használhatjuk
- Asszimmetrikus titkosítás: A titkosításhoz és a visszafejtéshez különböző kulcsokat használnak => Kulcspár
- Aszimmetrikus titkosításnál a nyílt átviteli csatornán nem közlekedik a kulcs!

Titkosítás problémái, jósága

- A szimmetrikus titkosításnál a kulcsot el kell juttatnom a visszafejtőnek. Ezt is ellophatják!
- A titkosítás jósága azt jelenti, hogy az adott időpillanatban mekkora erőforrást kell a visszafejtésre fordítani (Számítási teljesítmény, gépidő)
- Ha a visszafejtés annyi ideig tart, hogy már nem felhasználható a titkos információ, akkor a titkosítás jó.
- A kulcs jósága általában függ a lehetséges és megvizsgálandó variációk számától

Jó titkosítás feltételei

- A elküldi B-nek az információ, akkor C nem tudja elolvasni
- C nem tud A nevében információt küldeni B-nek

A titkosírás múltja

- Már az ókori görögök is…
- Római Birodalom – Caesar kódolás – Az ABC betűit eltolták néhány hellyel. Pl: A=>C, B=>D, E=>F, stb…
- Általában a leggyengébb titkosítás a betűk keverése => Monoalfabetikus titkosítás
- A kulcs a megfeleltetési táblázat.
- Feltörése módja
  - Minden nyelvben vannak betűgyakorisági statisztikák. (angolban az e, és az a a leggyakoribb betűk)
  - Ha egy jelnek az értelmét megfejtik, akkor nagyságrenddel csökken a többi jel variációinak száma

A IX században már feltörték a monoalfabetikus titkosításokat!

Az angol nyelv statisztikája

A – 8,2
B – 1,5
C – 2,8
D – 4,3
E – 12,7
F – 2,2
G – 2,0
H – 6,1
I – 7,0
J – 0,2
K – 0,8
L – 4,0
M – 2,4

N- 6,7
O – 7,5
P – 1,9
Q – 0,1
R – 6,0
S - 6,3
T – 9,1
U – 2,8
V – 1,0
W – 2,4
X – 0,2
Y – 2,0
Z – 0,1

A kódolás javítása

- Vigenere kódolás: 26 különböző táblázatot használunk a betűk kódolásához. Minden betűt a következő táblázattal kódolunk. Ha a végére értünk a táblázatoknak, akkor kezdjük elölről a táblázatok használatát
- Polialfabetikus kódolás: Ha mindenbetűhöz más táblát használunk

Ma már ez is megfejthető, ha elég hosszú szöveg áll rendelkezésre és vannak gyors számítógépek

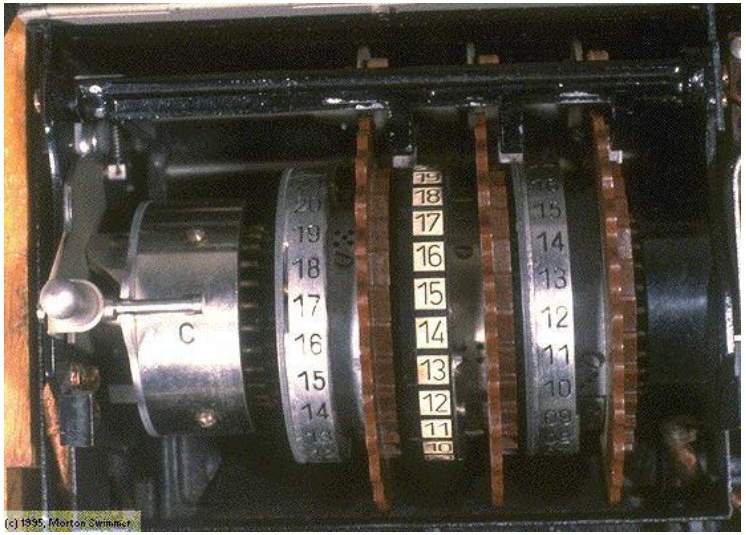
A megfejtés alapja, ha elég hosszú a szöveg és megsejtjük az táblázatok ismétlődését, akkor statisztikát tudunk készíteni

A titkosítás javítása

- Egyszer használatos kulcsok – csak akkor jó, ha a kulcsot biztonságosan el lehet juttatni mindenkinek
- Kódkönyv a küldőnél és a fogadónál – biztonságos, de hogyan jut el a kódkönyv?
- Navaho kódolás – Ismeretlen nyelven küldjük el az üzenetet. A Navaho indiánok közül egyet sem fogtak el a japánok.

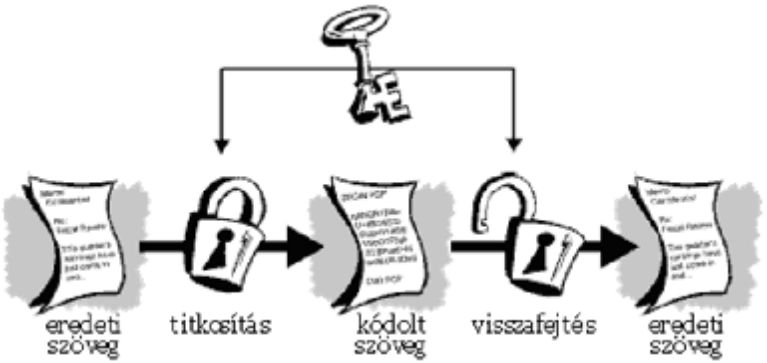
A technikai fejlődés eredményei

- Enigma – Gépesített kódolás – dekódolás
- Hosszú történet – mese



Szimmetrikus titkosítás

- Minden eddigi titkosítási eljáráshoz ugyanazt a kulcsot kellett használni a titkosításhoz és a megfejtéshez.
- Ezt hívják szimmetrikus titkosításnak.
- Matematikai megfogalmazása.
- Ny – Nyílt üzenet, k() – a kulcs, T – titkos üzenet
  - $T = K(NY)$
  - $NY = K^{-1}(T)$, azaz
  - $NY = K^{-1}(K(NY))$



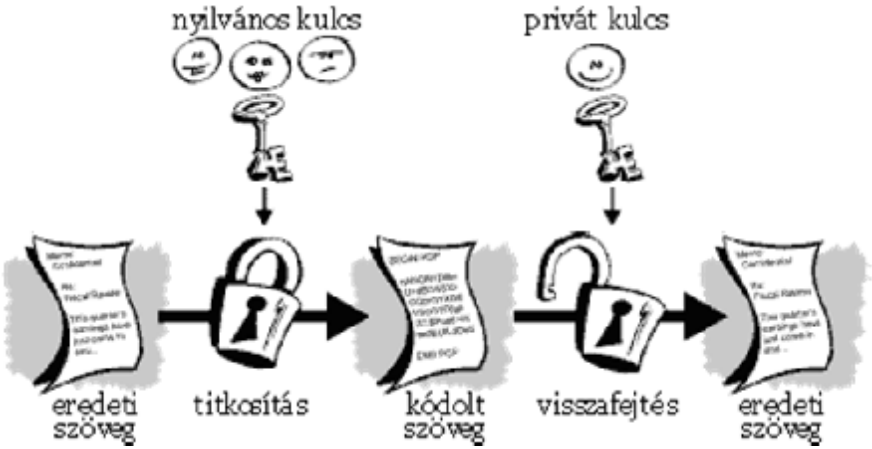
A kulcsmegosztás problémája

- A szimmetrikus titkosításnál a dekódoláshoz szükséges kulcsot el kell juttatni a címzetthez, mielőtt a tikos üzenetet elküldenénk.
- Ha a kulcsot elfogják, akkor lőttek a titkosításnak!
- Titkosítsuk a kulcsot is? A probléma gyökere marad.

Megoldás: Aszimmetrikus titkosítás

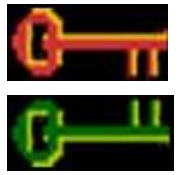
- Tegyük fel, hogy mindenkinek 2 kulcsa van.
- P() titkosítja az üzenetet és Q() a titkos üzenetet visszaállítja.
- Ha NY az üzenet, akkor
  - q(p(NY)) = NY.
- Mivel a titkos üzenet is szövegnek tekinthető (még ha számsorozat akkor is)
  - Q(P(T)) = T

- Mindenkinek két kulcsa van. Az egyik titkos (private key), a másik nyilvános (public key)
- Ha egy üzenetet az egyik kulccsal titkosítunk, majd a másikkal újra titkosítunk, akkor visszakapjuk az eredeti üzenetet!



Anna üzenetét csak Barbara fejtheti meg, mert Mr Smith nem ismeri Barbara titkos kulcsát!

Anna



Agent Mr Smith

Barbara

Kódolás Barbara nyilvános kulcsával

Dekódolás Barbara titkos kulcsával

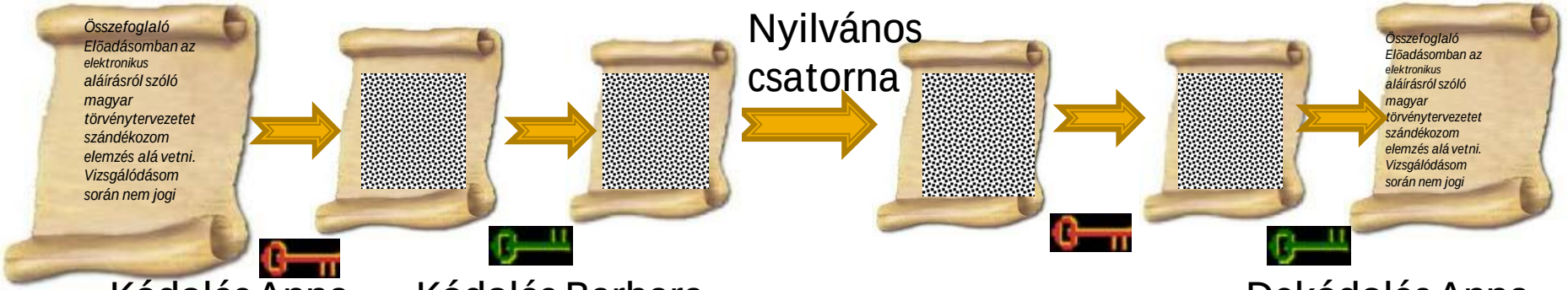
Mr Smith viszont írhat Anna nevében Barbarának, mert ismeri Barbara nyilvános kulcsát!
Az egyszeres kódolás tehát nem elég!

Mr Smith nem tud Anna nevében küldeni levelet, mert nem ismeri anna titkos kulcsát

Anna

Agent Mr Smith

Barbara



Kódolás Anna titkos kulcsával

Kódolás Barbara nyilvános kulcsával

Dekódolás Barbara titkos kulcsával

Dekódolás Anna nyilvános kulcsával

Milyen legyen a kulcs? Egy kis matematika

- Hellman, Diffie két matematikus dolgozta ki a megvalósítást

- Kongruencia

  A ≈ B (mod c), ha A/C maradéka ugyanaz, mint B / C maradéka

- Megjegyzés:
  Matematikában 3 db vízszintes vonal jelzi a kongruenciát

http://hu.wikipedia.org/wiki/Kongruencia

A kongruenciák tulajdonságai

- A maradékok alapján a nulla és a pozitív egész számok maradékosztályokat alkotnak
  - Pl. 2, 7, 12, 17,... mod 5 ugyanannak a maradékosztálynak a tagjai, mert a számokat 5-tel osztva 2-t kapunk mindig maradékul

- A kongruenciák összeadásra, kivonásra, szorzásra, hatványozásra megtartják az eredményüket

(Kommutatív, disztributív)

- Osztásra, gyökvonásra, logaritmusra nem!!!!

Példa

- $A \approx B \pmod c$ — $8 \approx 23 \pmod 5$
- $D \approx E \pmod c$ — $7 \approx 12 \pmod 5$

- $A+D \approx B+E$ — $15 \approx 35 \pmod 5$

- $A-D \approx B-E$ — $1 \approx 11 \pmod 5$
- $A*D \approx B*E$ — $56 \approx 276 \pmod 5$
- $A^2 \approx B^2$ — $64 \approx 49 \pmod 5$

Maradékosztályok száma

- Ha p prímszám => a maradékosztályok száma $\phi(p) = p-1$
- Ha p és q prímszámok, akkor p*q nem prímszám. P*q maradékosztályainak száma (p-1)*(q-1) =>jele: $\phi(p)$
- nem prímszám, akkor a maradékosztályok számának jele $\phi(p)$

kis Fermat tétel

- T tetszőleges pozitív egész szám, p prímszám, akkor:
- $T^{p-1} \approx 1$, (mod p), azaz $T^{p} \approx T$, (mod p)

- Megjegyzés:
  Ez azért jó, mert a megadott hatványra felemelve bármilyen számot, ugyanazt kapjuk vissza egy idő múlva

Nagy Fermat tétel

Ha p,q,r,... stb prímszámok, akkor
P*q*r*,.... = N, összetett szám
T és N relatív prímszámok. Φ(N) esetén

$T^{\phi(N)-1} \approx 1$, (mod p), azaz

$T^{\phi(N)} \approx T$, (mod p)

- Ha választunk két megfelelően nagy prímszámot, akkor a két szám segítségével az eredeti szöveg karaktereit vissza tudom kódolni

RSA kulcsképzés

- A,B,C emberek választanak maguknak két nagy prímszámot. Az egyik szám lesz nyílt kulcs, a másik a titkos kulcs.

Miért tekinthető biztonságosnak, hiszen mindenki ismeri a módszert?

- Jelenlegi matematikai ismereteink alapján a prímszámok megtalálása nagyságrendekkel gyorsabb algoritmus, mint egy meglévő nagy szám prímtényezőkre bontása.
- A számjegyek számával hatványozottan növekszik a felbontáshoz szükséges idő.
- Mai technikával az
  576 bites szám 1-2 év,
  2048 bites szám esetén több millió év a szükséges idő!

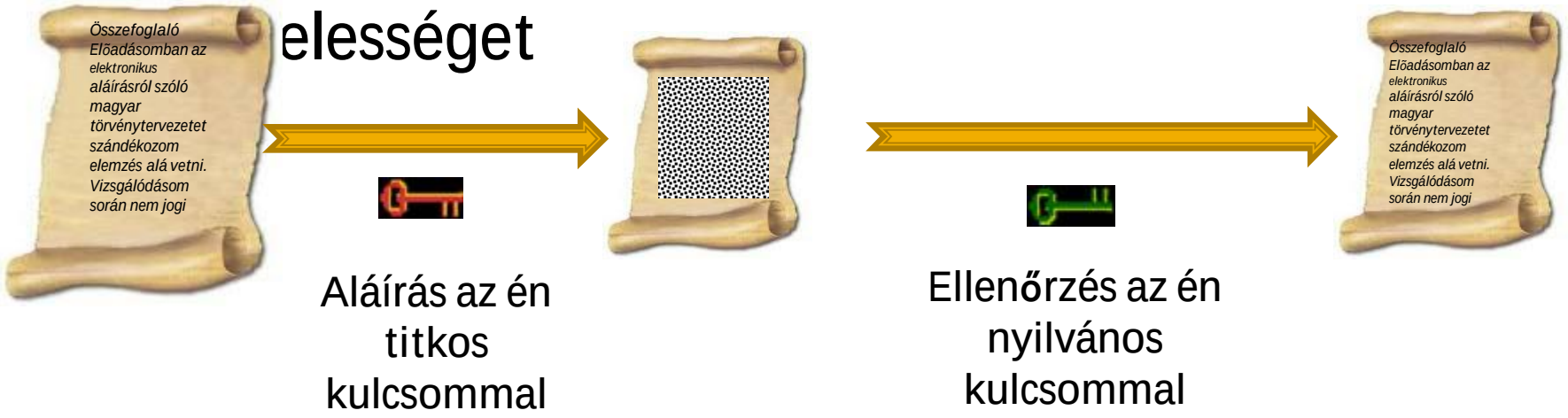
Elég biztonságos!

Gyakori eszközök

- PKI – Public Key Infrastructure – Nyilvános kulcsú infrastruktúra
  - Digitális tartalmak változatlanságát, eredetiségét ellenőrizhetjük vele
- PKE – Public Key Encryption – Nyilvános kulcsú titkosítás
  - A PKI infrastruktúra és a PKE gyakran egy alkalmazásban együtt él.
  - Pl: OpenSSL, vagy a PGP titkosítási – hitelesítési alkalmazások

Elektronikus aláírás

- Olyan eljárás, amivel egy dokumentumról bebizonyíthatjuk, hogy eredeti, nem módosították
  - Az aláíró a saját privát kulcsát használja és a címzett a küldő nyílt kulcsával ellenőrzi a elességet



Aláírás az én titkos kulcsommal

Ellenőrzés az én nyilvános kulcsommal

Tanúsítványok

- Nyilvános titkosítási eljárás során valóban a küldő nyilvános kulcsát használjuk?
  - Ha közvetlenül a küldőtől kapjuk a kulcsot, akkor nem gond
  - Ha nyilvános helyről kapjuk a kulcsot, akkor tanúsítvány kell erről => Certificate

Az elektronikus tanúsítvány tartalma

- A szervezet | személy nyilvános kulcsa
- A szervezet | személy adatai (lakhely, név, stb)
- Egy vagy több olyan digitális aláírás, amely tanúsítja, hogy a személy valódi

A tanúsítvány valóságának igazolása

- Személyek igazolhatják egymásnak
- Tanúsítványszolgáltató szervezet, amelyben mindenki megbízik

- Hitelesítési szolgáltató: (Certification Authority – CA)
  Olyan szervezet, amely elektronikus igazolásokat állít ki
  Megjegyzés: A társadalomban ezt közjegyzőnek hívják

- Az üzleti hitelesítés szolgáltatók maguk hitelesítettek az állam valamely szervezete által.

- Külföldi hitelesítés szolgáltatók
  - VeriSign, Thawte

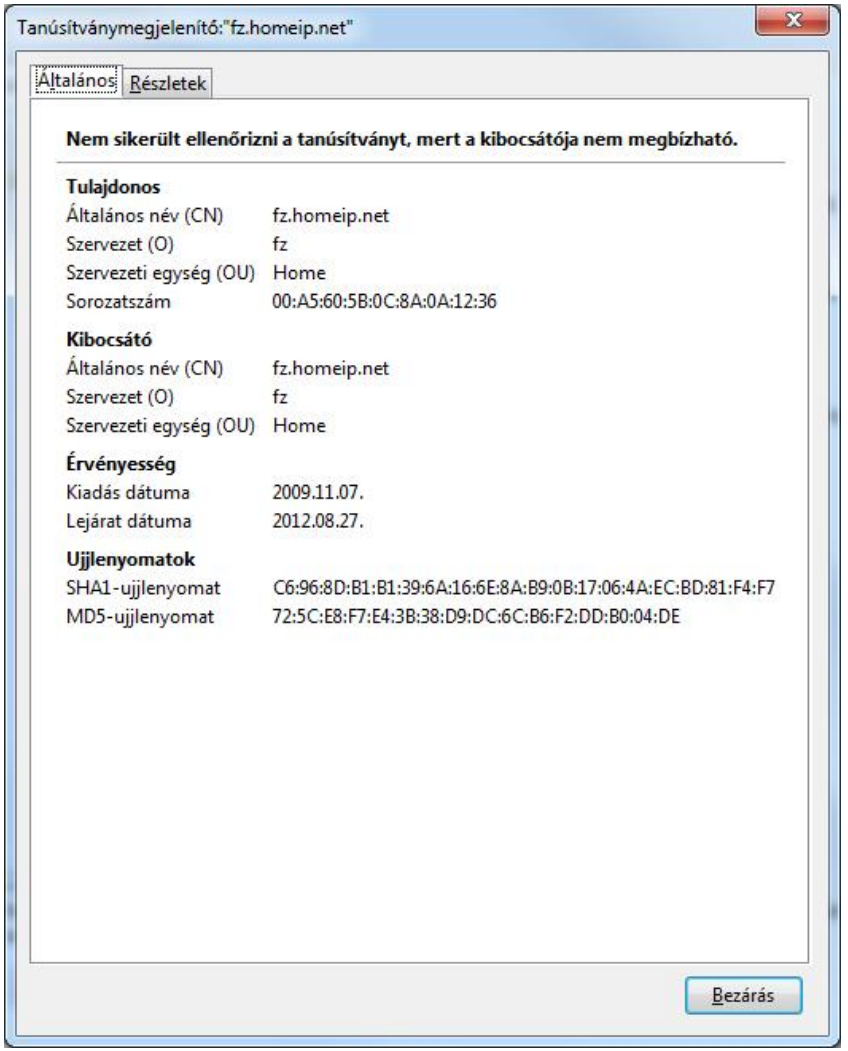
- Üzleti hitelesítésszolgáltatók Magyarországon
  - E-szigno, Netlock, stb...

Hitelesítések módjai

- Személyes hitelesítés
  - Olyan helyen használjuk, ahol usernév / jelszó kell. Lehet külső hitelesítő vagy a saját cégünk is.
- Szoftvertanúsítvány
  - A gépünkre telepítendő program hitelességét igazolja. Tartalmazza a szoftver gyártójának adatait és a hitelesítő adatait is. Ilyenek a Microsoft által aláírt driverek a Windows 7-ben

Helyhitelesítés, szervertanúsítvány

- Igazolja, hogy az adott webhely az, aminek mondja magát.
- A hely hitelesítése lejárati idővel is rendelkezik.
- A böngészők ellenőrzik az aláírás hitelességét és időszerűségét.
- Ha lejárt az ideje vagy nem érvényes, akkor a böngésző figyelmeztet.
- Akkor használják, ha fontos a hitelesítés és a titkosítás, például internet banki szolgáltatások, hivatalos ügyek intézése
- A böngészők ilyenkor SSL protokollal titkosított HTTPS protokollt használnak



Öntanúsítvány

Ha egy cég csak titkosítás céljából használ HTTPS protokollt akkor elegendő lehet az, hogy a saját maga tanúsítja a kulcsot.
Erre figyelmeztetnek a böngészők.