# INFORMATIKAI PROJEKTELLENŐR

DR. BEINSCHRÓTH JÓZSEF

## KRIPTOGRÁFIAI ALKALMAZÁSOK, REJTJELEZÉSEK, DIGITÁLIS ALÁÍRÁS, DIGITÁLIS PÉNZ

# Tartalom

- **Alapvetések**
- **Alapfogalmak**
- **Változatok**
  - Tradicionális módszerek
  - Szimmetrikus kriptográfia
  - Aszimmetrikus kriptográfia
  - Kombinált módszerek
- **Digitális aláírás**
- **Üzenet pecsét**
- **Kulcsgondozás**
- **Digitális pénz**

# A kriptográfia alapvetései

Az Informatikában a bizalmasság biztosításának kérdése kritikus lehet

A biztonság összetevőinek egy része kriptográfián alapul – de a kriptográfia önmagában nem oldja meg a biztonság problémáját.

A titkosítási algoritmusok publikusak! A titkosság kizárólag a kulcsokban rejlik.

Csak publikus, ismert, több éve használt algoritmus elfogadható.

Az üzenetek kell, hogy valamennyi redundanciát tartalmazzanak, de a túl sok redundancia egyszerűsíti a megfejtést. A kriptoanalízis során valamennyi információ szükséges az eredeti üzenetről!

A titkosított üzenetek ismételt elküldésének problémáját a titkosítás nem oldja meg, erre valamilyen külön módszer kell.

Elvárások: tartalom elrejtése, statisztikai jellemzők elfedése, integritás biztosítása, letagadhatatlanság, (szerzői jogok)

# A kriptográfia alapfogalmai

## Kriptográfia (cryptography)

- Titkosítás – rejtjelezés: titkosító eljárások kifejlesztése és alkalmazása

## Kriptoanalízis (cryptoanalysis)

- A titkosítás megfejtése

## Kriptológia (cryptology)

- Kriptográfia + kriptoanalízis

## Kulcs (titkos!?)

- Relatíve rövid karaktersorozat, a hosszúsága kritikus

## Feltörés

- Az üzenet visszafejtése kulcs nélkül
- Számos feltörési módszer ismert (brute force, chipertext only, known plain text, chosen plaintext)

## Kriptográfiai modell

- Alice, Bob
- Kódolás, dekódolás
- Csatorna

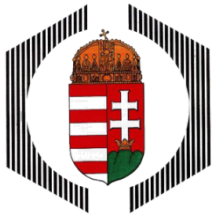
# A kriptográfia változatai

Tradicionális módszerek

Szimmetrikus kriptográfia

Aszimmetrikus kriptográfia

Kombinált módszerek



# A kriptográfia változatai



## Helyettesítő kódolás

- Minden betű vagy betűcsoport egy másik betűvel vagy betűcsoporttal helyettesítődik
- A helyettesítő kódolás általános feltörési módszere: felhasználjuk a természetes nyelvek statisztikai jellemzőit
- Ma: minimális erőforrással feltörhető

## Keverő kódolás

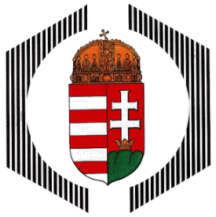
- Nem történik helyettesítés, de a karakterek sorrendje megváltozik
- Ez esetben a statisztikai módszerek nem segítenek, mert az egyes betűk gyakorisága nem változik
- Feltörés: valószínűen előforduló szavakat, kettős betűket stb. keresünk
- Ma: minimális erőforrással feltörhető

## Egyszer használatos bitminta

- A kulcs egy véletlen bitsorozat, legalább olyan hosszú, mint az üzenet
- A kulcsot biztonságos csatornán kell továbbítani, de ezzel az erővel akár magát az üzenetet is továbbíthatjuk a biztonságos csatornán!
- Feltörhetetlen, mivel a titkosított üzenet nem hordoz információt!

# Szimmetrikus kriptográfia: egyetlen kulcs használatára épül

- **Ugyanaz a kulcs használatos a kódoláshoz és a visszafejtéshez.**
- Bonyolult matematika, a kulcs titkos, a kulcs ismeretében mind a kódolás, mind a visszafejtés viszonylag egyszerű, kulcs hiányában a visszafejtés nagyon nehéz (a kódolási algoritmus publikus: bitek felcserélése és bitminták más bitmintákkal való helyettesítése).
- **Probléma: a kulcs, ill. az abszolút biztonságos csatornán történő továbbítása. (A kriptográfiai modellben ez nincs kezelve!)**
- A rejtjelezést megelőzően a feleknek meg kell állapodniuk az alkalmazandó kulcsban.
- Több szereplő esetén bármely két szereplőnek saját kulccsal kell rendelkeznie.
- Abszolút biztonságos csatorna: nem a technológia, hanem szabályok, eljárási utasítások betartása alapján abszolút biztonságos – az emberi
- tényező megjelenik: tévesztések, fegyelem betartása stb.
- **Előny: relatíve gyors.**



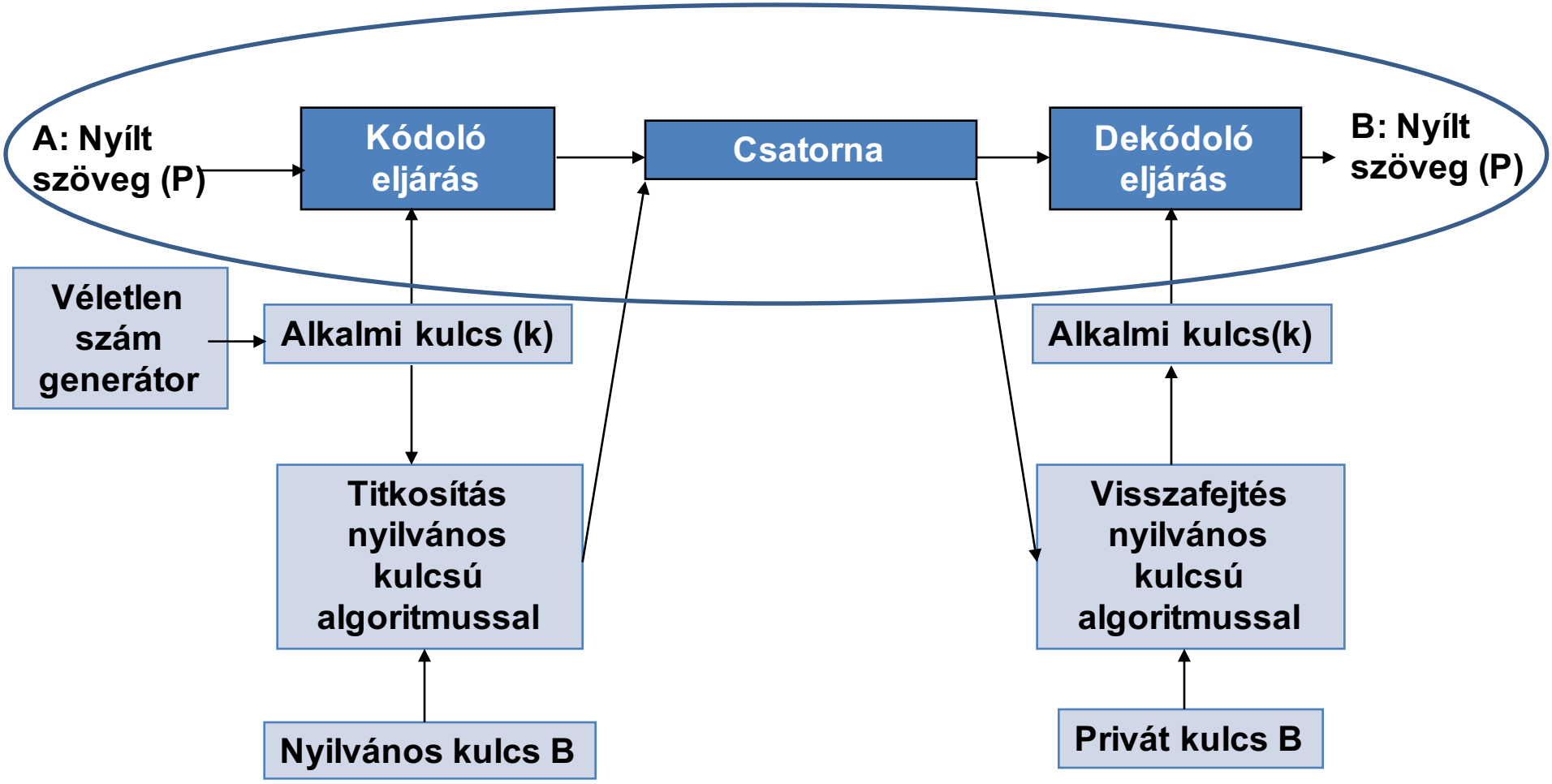
# Aszimmetrikus kriptográfia: két kulcsot használunk



- A kriptográfiai modell némiképpen módosul
- **Valamennyi felhasználónak két kulcsa van: egy titkos és egy nyilvános**
- Az eljárásban a kódoláshoz (E=ecryption) és a dekódoláshoz (D=decryption) tartozó kulcsok különbözőek – $\mathbf{D_l(E_k(P)=P}$ (A kódoláshoz és a dekódoláshoz különböző kulcsot használunk **k és l** különbözik.)
- D-ben és E-ben alkalmazott kulcsok (k és l) között matematikai összefüggés van, de D kulcsának előállítása E kulcsából rendkívül nehéz.
- D kulcsának, ill. P-nek előállítása E kulcsából, ill. E(P)-ből nem lehetséges, azaz a választott nyílt szöveg típusú támadással szemben az eljárás ellenálló. (E(P) halad a nyílt csatornán! Bárki hozzáférhet.)
- Ennek megfelelően **E során használt kulcsot nem kell titokban tartani**! (Publikus kulcs, akár a nyílt csatornán küldhető!)
- A publikus kulccsal kódolt üzenet a privát kulccsal fejthető vissza. A publikus kulcs ismeretében gyakorlatilag sem a privát kulcs, sem a kódolt üzenetből a kódolatlan nem állítható vissza.
- **Hosszú üzenetek továbbítása problematikus** (lassú algoritmusok, akár 1000-szer lassúbbak, mint a szimmetrikus kriptográfia esetén).

# Optimatizálás: mindkét eljárás-ból realizáljuk az előnyöket

# A kombinált módszer alkalmazása



# ACTIVITY – Teszt feladatok

1. **Szimmetrikus kriptográfia esetén**
   a. A kódoláshoz és a dekódoláshoz tartozó kulcsok megegyeznek. _____
   b. A titkosítás erőssége független a kulcsok hosszától. _____
   c. Digitális aláírás nem valósítható meg szimmetrikus kriptográfiával._____
   d. A kulcsok birtokában a titkosított szöveg visszafejthető._____
2. **Aszimmetrikus kriptográfia esetén**
   a. A küldő és a címzett eltérő kulcsot használ. _____
   b. Egy résztvevő privát és nyilvános kulcsa között nincs korreláció. _____
   c. Kiegészítésként szükség van egy abszolút biztonságos csatornára. _____
   d. Van olyan kulcs, amelyet minden résztvevő láthat. _____
3. **A klasszikus titkosítási módszerek esetén**
   a. A helyettesítő kódolás egyszerűen feltörhető._____
   b. Az egyszer használatos bitminta feltörhetetlen kódot eredményez._____
   c. A keverő kódolás feltöréshez nincs ismert módszer._____
   d. Az egyszer használatos bitmintát széles körben használják a gyakorlatban._____

# ACTIVITY – Teszt feladatok

**6. A szimmetrikus kriptográfia**

a. Titkos kulcsokat használ.____

b. Általában lassabban konvergáló algoritmusokat használ, mint az aszimmetrikus kriptográfia.____

c. Túlhaladott megoldás, ma már nem használják._____

d. Titkos matematikai algoritmusokat használ._____

**7. A kombinált titkosítási módszerek esetén**

a. Az alkalmi kulcs titkosításra kerül._____

b. Privát kulcsokat nem használnak.____

c. A szimmetrikus és aszimmetrikus kriptográfia között optimumot jelent.____

d. Túlhaladott megoldások, ma már nem használják őket._____

e. A továbbítandó adatok kódolása az alkalmi kulccsal történik._____

# A digitális aláírás aszimmetrikus kriptográfiára épül

Kiindulás: a titkosítási algoritmus a D(E(P))=P tulajdonság mellett rendelkezzen az E(D(P))=P-vel is!

Az eljárás: Mielőtt a feladó elküldi az üzenetet, saját titkos kulcsával titkosítja. A címzett ezt a lépést majd a küldő publikus kulcsával „semlegesíti”.

A küld levelet B-nek: $E_B(D_A(P))$ kerül továbbításra. A levél előállítása:

- 1. lépés: Saját titkos kulcsával kódol
- 2. lépés: B (a címzett) publikus kulcsával kódol

B kap levelet A-tól: Megkapja $E_B(D_A(P))$-t. Ebből előállítja $D_B(E_B(D_A(P)))=D_A(P)$-t és $E_A(D_A(P))=P$-t.

- 1. lépés: Saját tikos kulcsa segítségével előállítja $D_A(P)$-t
- 2. lépés: $D_A(P)$-t eltárolja, ezzel tudja bizonyítani, hogy a hozzá érkező üzenet $D_A$-val lett titkosítva, azaz A titkosította (írta alá) azt, ha $E_A$-val ebből előállítható P, akkor ez bizonyított
- 3. lépés: A publikus kulcsa segítségével előállítja P-t.

# Üzenet pecsét: hitelesítés titkosítás nélkül

Gyakran nem szükséges az üzenet tartalmát titkosítani, de hitelesítés szükséges (pl. web oldal küldés).

Az üzenet pecsétek központi fogalma a hash.

Hash (kivonat) digitális ujjlenyomat, egy bitsorozat, amelyet ismert algoritmussal az üzenetből készítünk (hash algoritmus).

A hast-t aláírjuk és továbbítjuk.

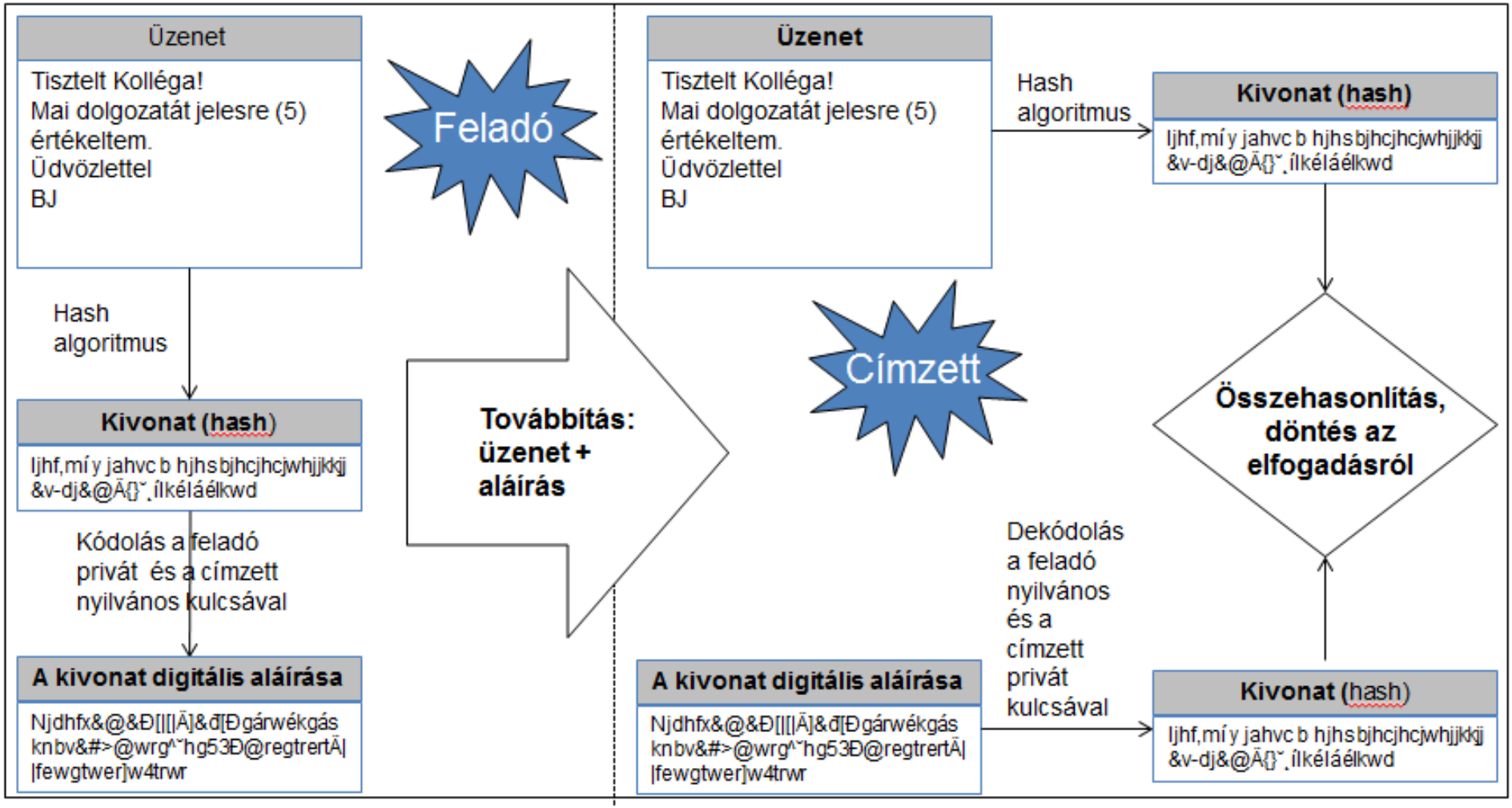
A címzett megkapja a tikosított, aláírt hash-t ugyanakkor maga is elő tudja azt állítani.

A feladó és a címzett ugyanazt a hash algoritmust használja.

A címzett ellenőrzi, hogy a kapott és a helyben előállított hash megegyezik-e.

Az eljárás transzparens – beépülhet az alkalmazásokba.

# A hitelesítés alkalmazásának folyamata



# Az aszimmetrikus kriptográfia központi kérdése a kulcsgondozás

**Probléma**

- Az aszimmetrikus kriptográfia publikus kulcsainak meghamisítása (elfogott kérésre hamis kulcs elküldés, lecserélt weblap stb.)

**Megoldás: a nyilvános kulcsok tanúsított kezelése**

- CA - tanúsító hatóság (a résztvevők megbíznak benne) - tanúsításokat ad ki (**elektronikus közjegyző - Certification Authority**)
  - Nyilvános és magán kulccsal rendelkezik
  - A résztvevők regisztrálnak nála és megkapják a nyilvános kulcsát abszolút biztonságos módon (Megjelennek a CA-nál - nem egy web oldalról töltik le.)
  - Saját kulcsával aláírt tanúsítványokat állít elő. (A tanúsítvány egy fájl, melyben többek között szerepel a **tanúsított résztvevő neve és nyilvános kulcsa** is – a hatóság által lepecsételt személyi igazolvány.)
  - A tanúsítványokat elhelyezi a nyilvános tanúsítványtárban.
  - A CA publikus kulcsát használva lehet megkapnia tanúsított cég nevét (azonosítóját) és a tanúsított cég publikus kulcsát, ill. azt, hogy ezek összetartoznak
  - **A tanúsítvány tartalma: a tanúsítvány sorszáma, a tanúsított neve, a tanúsított email címe, a tanúsított további attribútumai, a tanúsított nyilvános kulcsa, a tanúsítvány érvényessége, a CA neve, a CA aláírása**

# PKI: Hitelesítő, tanúsító rendszer

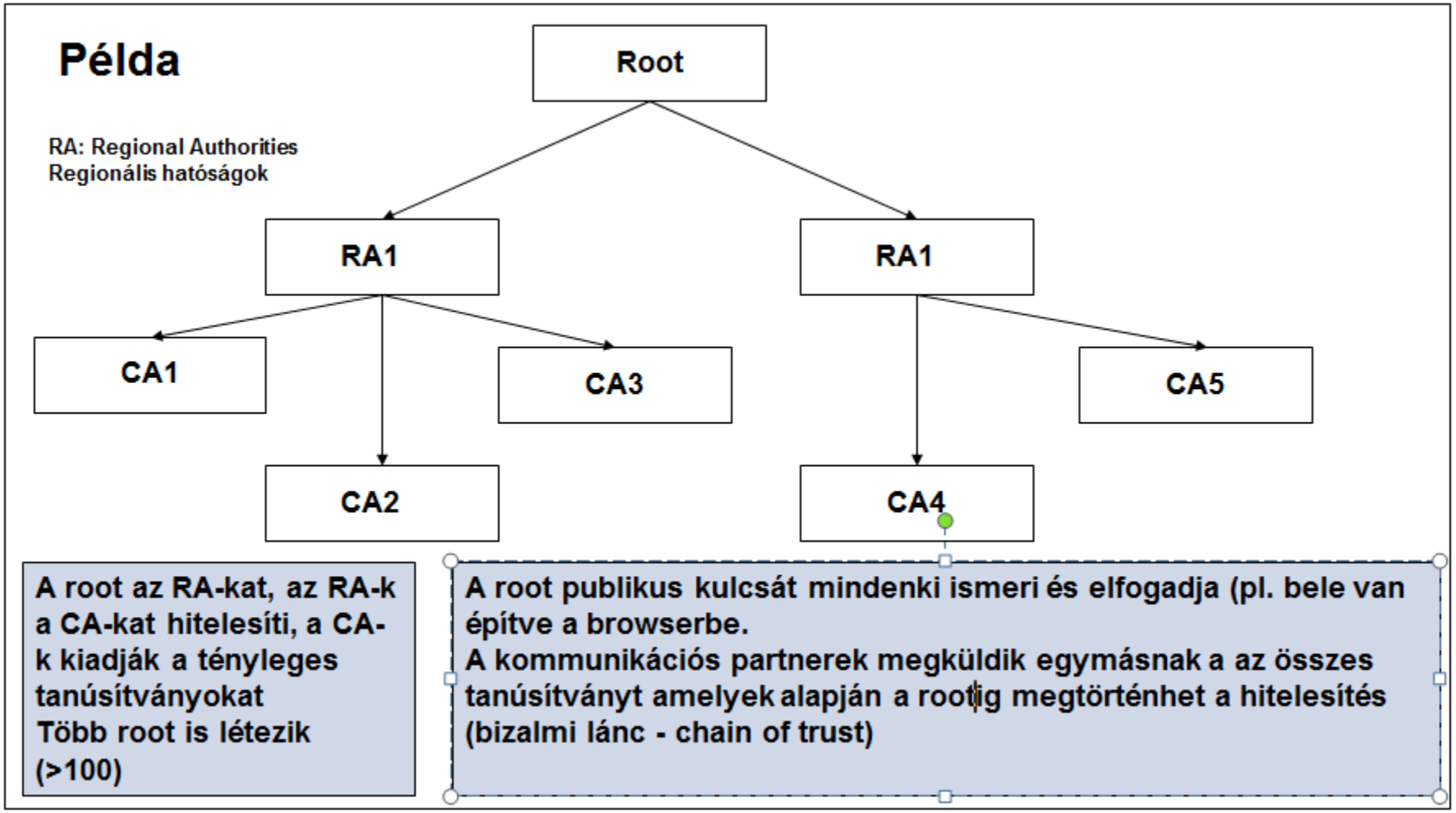
**Probléma**

- Egyetlen CA nem képes ellátni a feladatot: terhelés, bizalom, rendelkezésre állás stb.
- Ha szereplők különböző CA-khoz tartoznak, egymás tanúsítványát nem képesek ellenőrizni.

**PKI (Public Key Infrastructure): a gyakorlatban használt hitelesítő, tanúsító rendszer**

- Megoldás: PKI - Szolgáltatás, az alkalmazásoknak nyújt szolgáltatást.(Ahhoz hasonlóan, ahogy a DNS is az alkalmazásoknak nyújt szolgáltatást.) Összetevői:
  - Felhasználók, CA-k, tanúsítványok, tanúsítvány könyvtárak stb.
  - A PKI szervezetbe rendeli az összetevőket
  - Szabványokat tartalmaz a különféle dokumentumok és protokollok számára

# A kulcsgondozás hierarchikus rendszerben valósul meg



# Digitális pénz (E-pénz)

Készpénz → Számlapénz → E-pénz (digitális pénz)

**Számlapénz hitelesség**

- **Központi kérdés: hitelesség.** Hiteles, amit a kibocsátó bank digitális aláírásával lát el. A digitális aláírás, és a mögötte rejlő algoritmusok biztosítják a pénz eredetiségét, hamisíthatatlanságát.

## E-pénz jellemzők

- Nem feltétlenül kapcsolódik bankhoz.
- Maga az érték egy digitális bitsorozatként tárolódik (fájl, memóriarészlet….)
- Egyszerű, kényelmes, nincs szükség hozzá bankkártyára, böngészőből vagy mobil alkalmazással érhető el.
- Tranzakciós idő: kb. 0., költségek gyakorlatilag nincsenek
- Központi kérdés a bizalom

## Követelmények

- **Anonimitás:** Ki kell zárni a követhetőséget, a vásárlási szokások feltérképezhetőségét.
- **Elfogadottág:** A digitális pénzt úgy kell megalkotni, hogy a felhasználók ne legyenek egyetlen bankhoz se kötve.
- **Off-line működés:** A két fél úgy tud fizetni egymásnak, hogy nem szükséges egy harmadik authentikáló fél.
  **Skálázhatóság:** Újabb felhasználók megjelenésekor nem keletkezik észrevehető lassulás.
- **Hardver függőség**: nagy számolási igény

# Digitális pénz - bitcoin

bitcoin.hu
Magyar Bitcoin Portál

- Erős kriptográfiával védett, nyílt forráskódú fájl egy elosztott P2P-hálózatban (hasonló a fájl megosztó hálózatokhoz). Nincs központi kibocsátó entitás, decentralizált.
- Digitális pénztárcában tartható, számítógépen vagy mobil eszközön.
- Számos váltóhely létezik (valódi pénzért vehető, eladható).
- A biztonságot a bitcoin bányászok biztosítják – ellenőrzés, fejlesztés – bitcoinokat kapnak a munkájukért.
- Közös könyvelés valósul meg az interneten keresztül – minden résztvevő hozzáfér, meg van osztva a hálózat tagjai között (ez a blocklánc, amely a tranzakciók adatait tartalmazza)
- A közös könyvelést a rendszer tagjai (a P2P tagjai) folyamatosan egyeztetik és ellenőrzik – bonyolult matematikai algoritmusok és kriptográfia. Az esetleges hamis tranzakció elutasításra kerül.
- Minden bitcoin egység azonosítható és programozható – számos funkcionalitást jelent, nem egyszerűen pénz (akár szavazati jog is lehet)

# Digitális pénz – NFC mobil

- Az **NFC (Near Field Communication)**
  Kommunikációs szabványgyűjtemény (okostelefonok és hasonló, általában mobil) eszközök között, egymáshoz érintéssel vagy egymáshoz nagyon közel helyezéssel (maximum pár centiméter) létrejövő rádiós kommunikációra.
- Az NFC eszközök kiválóan használhatóak érintésmentes fizetési eszközként, elektronikus jegyként valamint helyettesítik vagy kiegészítik a mobilfizetési megoldásokat. A felhasználó bankkártyájának adatait egy virtuális pénztárcában tárolják és NFC kompatibilis eszközzel használva érintésmentes fizetésre használható.
- Az NFC megoldással rendelkező készülékben egy beépített NFC chip van mely kis hatótávval bír, ezért a készülék akkumulátorába szokták beépíteni a hozzá tartozó antennát.

# Digitális pénz – mobil tárca

- A mobiltárca mint informatikai szolgáltatás **kliens-szerver architektúrában** valósul meg: a kliens a végfelhasználói alkalmazás, ami a mobiltelefonon fut, a szerver az azt kiszolgáló háttérrendszer.
- Két alapvető változat: **közelségi (proximity**) és **távoli (remote)** fizetési megoldások között.
  - a közelségi megoldásokkal a fizikai értékesítési helyen lehet fizetni, így pl. egy boltban a bankkártya-terminálhoz érintve a telefont
  - a távoli megoldások nem igénylik a felhasználó jelenlétét a kereskedőnél, bárhol használhatók, így pl. egy postai csekkre nyomtatott QR-kód beolvasásával
  - léteznek hibrid megoldások is, amik mind közelségi, mind távoli fizetést lehetővé tesznek.
- Az NFC-alapú mobiltárcák a digitalizált fizetőeszköz adatai tárolásához tipikusan az alábbiak valamelyikét használják
  - SIM-kártya - a mobilszolgáltató által biztosított, a SIM-kártyán futó titkosítási algoritmus segítségével
  - biztonságos chip (Secure Element) - a telefonba épített, a rendszer többi részéről leválasztott egységen
  - gazdaalapú kártyaemuláció (Host-based Card Emulation) - a mobiltárca-szolgáltató háttérszerverén, amihez az alkalmazás interneten keresztül kapcsolódik

# ACTIVITY – Teszt feladatok

1. **A digitális aláírás**
   a. Titkosításra alkalmatlan._____
   b. Digitális aláírás esetén minden résztvevő saját titkos hash függvénnyel rendelkezik.____
   c. Az üzenet pecsét az eredeti szöveget nem titkosítja._____
   d. Véd az újraküldés ellen._____
2. **A mobil tárca**
   a. Csak közelségi változatban használható.____
   b. P2P alkalmazás._____
   c. C/S alkalmazás.____

# ACTIVITY – Teszt feladatok

**4. A digitális pénz**

a. Nem biztosít anonimitást._____

b. A digitális pénz infrastruktúrájának központi egysége a központi bank.____

c. A digitális pénz bankkártya használatot feltételez.____

d. Egyik változata a bitcoin.____

**5. A PKI**

a. Hitelesítő és tanúsító szervezet._____

b. Az alkalmazásoknak nyújt szolgáltatást._____

c. Szimmetrikus kriptográfiára épül.____

d. Az egész világra nézve oldja meg a hitelesítés problémáját.____

**6. A CA-k által kiadott tanúsítványok tartalmazzák**

a. A tanúsított szervezet nevét._____

b. A tanúsító digitális aláírását._____

c. A tanúsítvány érvényességét._____

d. A vonali kódolást._____

# Köszönöm a figyelmet!