RSA titkosítás kialakulása

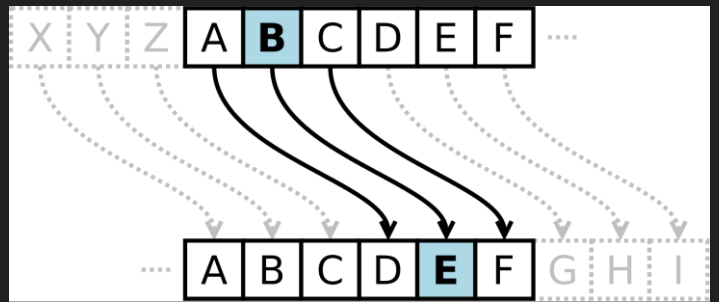
És kriptográfia története…

Kriptográfia története

- a 20. század második feléig a kriptográfiát kizárólag katonai és diplomáciai alkalmazásokban használták
  – kriptgráfia = titkosírás, rejtjelezés
- a 20. század második felétől a kriptográfia megjelent az üzleti életben (elsősorban banki alkalmazásokban)
  – a titkosság mellett fontossá vált az integritásvédelem, a hitelesítés, a letagadhatatlanság, stb.
- a 20. század végétől a kriptográfia a mindennapi élet részévé vált
  – SSL (Secure Socket Layer) – Web tranzakciók biztonsága
  – GSM biztonsági architektúra – mobiltelefon-hálózat biztonsága

Történelmi példák

- „már az ókori görögök is ...” – a spártaiak szkütaléja (i.e. 400)
- „veni, vidi, vici” – Julius Caesar rejtjelezője (~ i.e. 50)
- a „feltörhetetlen” sifre – Vigenère kód
  (1553 - Giovan Battista Bellaso)
  kb. Caesar kód változó eltolásokkal
  Euler felfedezte feltörésésnek lehetőségét
- a rejtjelezés gépesítése – az Enigma (1926)



A one-time pad - valóban feltörhetetlen rejtjelező (1917)

- mod 2 összeadás $\oplus$: $a \oplus b = (a + b) \bmod 2$

$$0 \oplus 0 = 0$$
$$0 \oplus 1 = 1$$
$$1 \oplus 0 = 1$$
$$1 \oplus 1 = 0$$

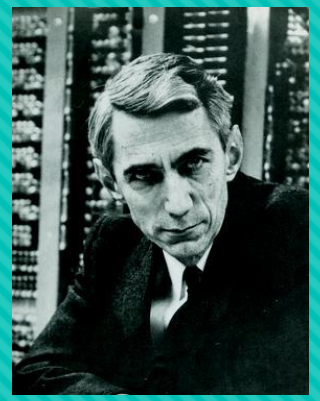
Gilbert Vernam
amerikai
(1890-1960)

- a mod 2 összeadás tulajdonságai:

1. $x \oplus x = 0$
2. 2. $x \oplus 0 = x$

Technikailag teljes egészében megegyezik a Vigenére-féle titkosírással, annyi különbséggel, hogy itt a kulcs hossza megegyezik a kódolandó szövegével, valamint minden esetben automatikusan generálódik (azaz véletlenszerűen állítódnak elő a kulcsot alkotó betűk).

Müködése

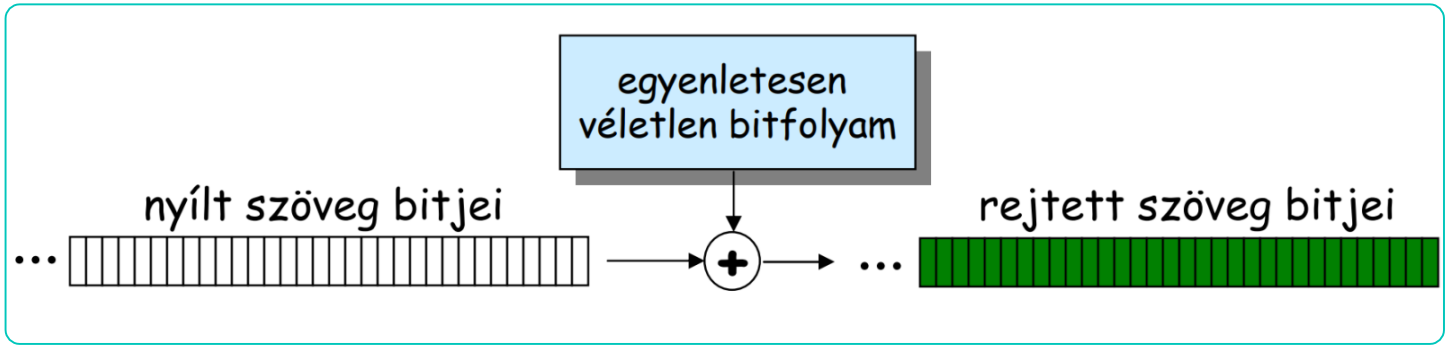


Claude Shannon (amerikai 1916 - 2001) 1949-ben bebizonyította, hogy

$$I(X; Y) = H(X) - H(X \mid Y) = 0$$

Shannon megadta a tökéletesség szükséges feltételét is:

$$H(K) \geq H(X)$$

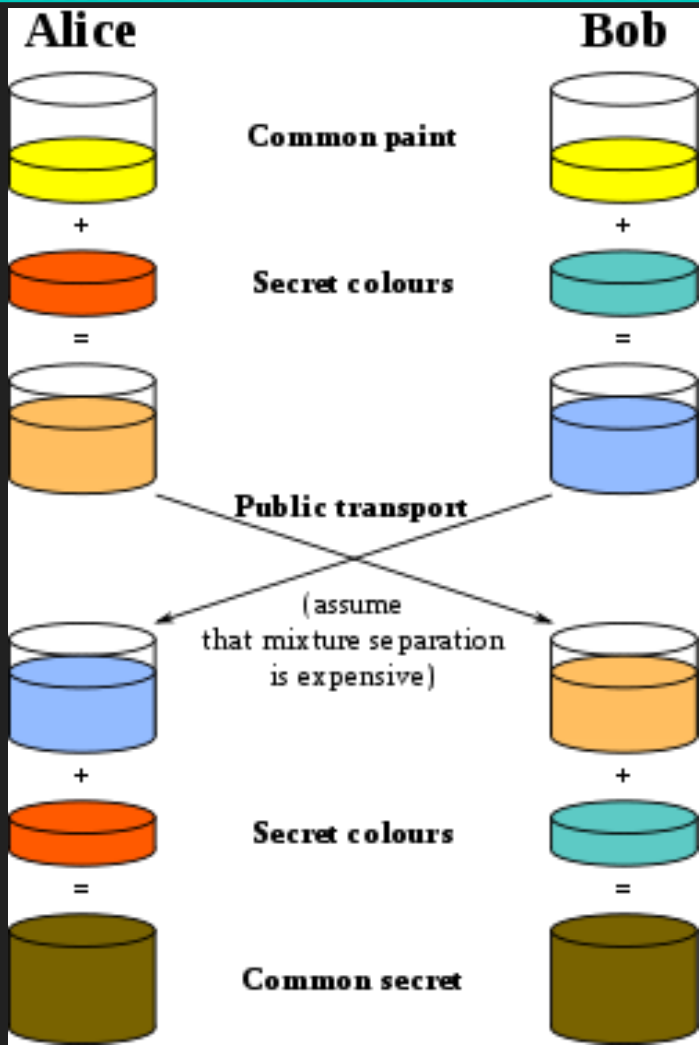


- kódolás
  - $y_i = x_i \oplus k_i$
  - ahol x_i a nyílt szöveg i. bitje, y_i a rejtett szöveg i. bitje
  - k_i az egyenletes eloszlású véletlen kulcsfolyam i. Bitje
- dekódolás
  - $x_i = y_i \oplus k_i = x_i \oplus k_i \oplus k_i = x_i$

Diffie-Hellman-Merkle-féle kulcsmegosztási rendszer (1976)

Olyan függvényt kerestek, ami "egyirányú" függvény = egyik irányba gyorsan tudunk számolni, másik irányba pedig nincs esélyünk, ez a direct hatványozás >>> mod m

amerikaiak
Bailey Whitfield Diffie (1944 -)
Martin Edward Hellman (1945 -)
Ralph Merkle (1952 -)



Számokkal

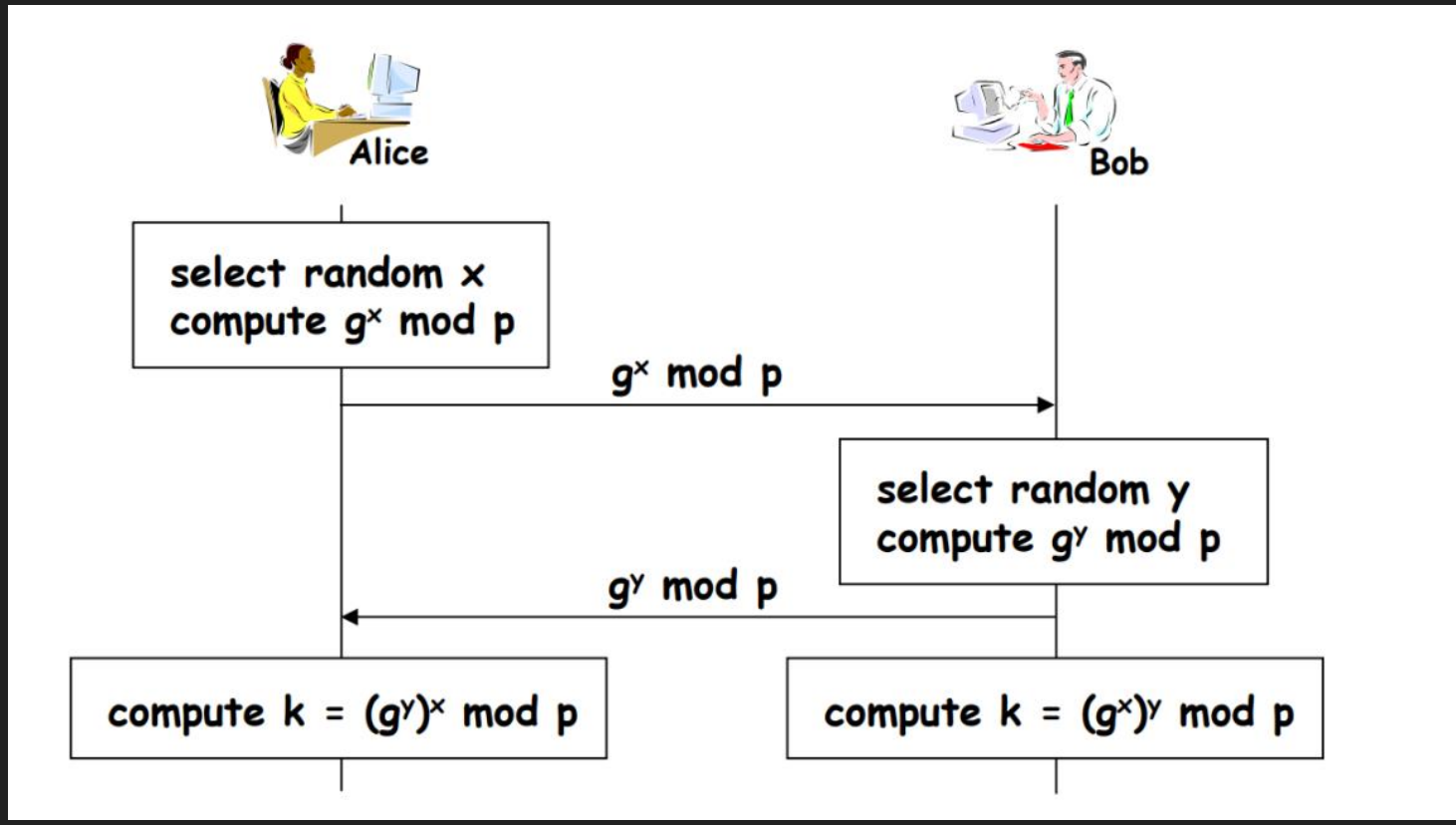
- $[g^Y(\text{mod } n)]^X = [g^X(\text{mod } n)]^Y = g^{XY} (\text{mod } n)$

ahol:

- n prímszám
- g < n (g eleme a modulo n csoportnak)
- X és Y véletlen számok

feltevés: adott egy p prím és a Zp * = {1, 2, …, p-1} egy g generátora

Matematikai összefüggés:



RSA-eljárás

A nyilvános kulcsú kódolás megvalósítása érdekében tovább folytak a kutatások. Az új ötlet a prímek világából származik.

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

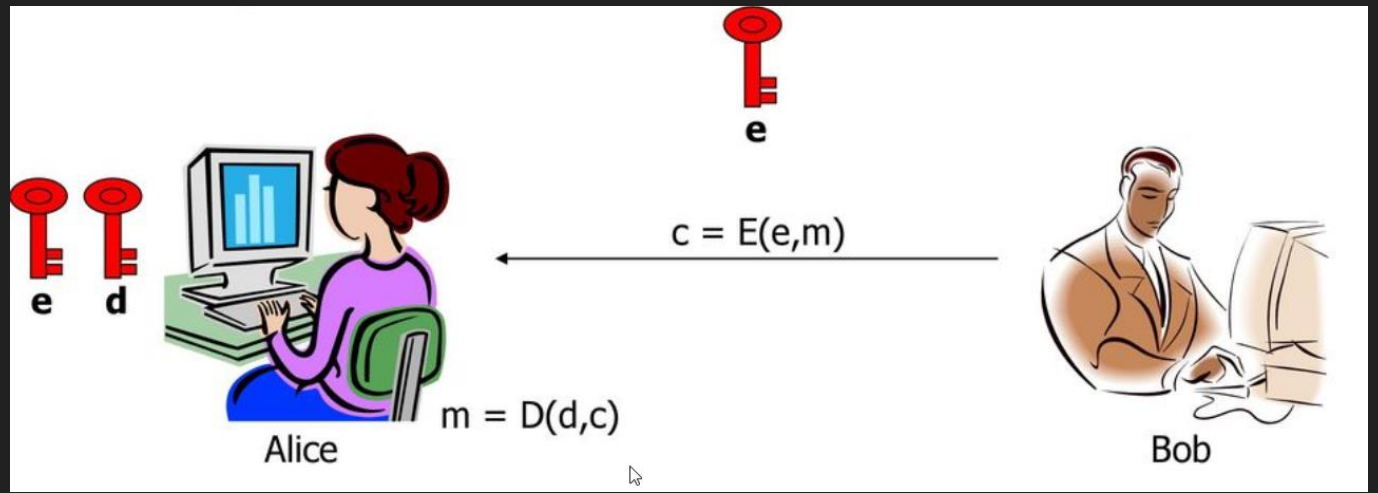
„Tegyük fel, hogy a takarítónő tévedésből kidobta a p és q számokat, de a pq szorzat megmaradt. Hogyan nyerhetjük vissza a tényezőket? Csakis a matematika vereségeként érzékelhetjük, hogy ennek legreményteljesebb módja a szeméttelep átguberálása és memohipnotikus technikák alkalmazása.“

Ifj. Hendrik W. Lenstra

Ron Rivest, Adi Shamir és Leonard Adleman (1977)

MIT számítástechnikai laboratórium

Egy húsvéti jól sikerült ünnepség után, 1977 áprilisában talált rá Rivest a megoldásra, aki munkatársaival együtt jelentette meg a cikket, amely új utakat nyitott a kriptográfiában.



Ron Rivest amerikai (1947 -)
Adi Shamir izraleli (1952 -)
Leonard Adleman amerikai (1945 -)

“Kis” Fermat–tétel (1636)

Pierre de Fermat
francia
(1601 – 1665)

A kis Fermat-tétel szerint bármely ***p*** prímszámra teljesül bármely ***a*** egész szám esetén, hogy

$$a^p \equiv a \ (mod\ p)$$

Azaz ha veszünk tetszés szerint egy ***a*** egész számot, megszorozzuk önmagával ***p***-szer, és levonjuk belőle az ***a***-t, akkor az eredmény ***p***-vel osztható.

$$a^{p-1} \equiv 1 \ (mod\ p)$$

(történelmileg hitelesebb alak)

A tétel Leibniz bizonyította be **1683**-ban

Gottfried Wilhelm Leibniz
német
(1646 – 1716)

A Kínai sejtés és általánosítása

A Kínai sejtés(kb. 2000 évvel korábban):
p akkor és csak akkor prím, ha

$$2^p \equiv 2 \ (mod \ p)$$

Bolyai János
magyar
(1802 - 1860)

Megpróbálta bebizonyítani a "kis" Fermat Tétel fordítottját, ezáltal több álprímet talált. Ezen vizsgálódásai alapján felírható a "Bolyai-prímteszt":
Tetszőleges ***n*** szám esetén keressünk olyan $1 < \boldsymbol{b} < \boldsymbol{n}$, ***n***-hez relatív prím számot, amelyre

$$b^{n-1} \not\equiv 1 \ (mod \ n)$$

- Ha találunk ilyen ***b*** számot, akkor ***n*** nyilván nem prímszám, vagyis összetett.
- Ha pedig minden ilyen ***b*** számra nem teljesül, akkor ***n*** talán prímszám?

Megvalósítás

Legyenek p és q különböző **prímszámok** (általában száz vagy több jegyű decimális számot választunk)

Ekkor, ha n = p*q, akkor a

$$\varphi(n) = (p - 1)(q - 1)$$

Válasszunk egy d > 1 számot úgy, hogy (d, φ(n)) = 1 és határozzuk meg azt az e számot, melyre 1 < e < φ(n) egyenlőtlenség teljesül és amely kielégíti az

$$ed \equiv 1 \pmod{\varphi(n)}$$

kongruenciát.

Ezen értékek megválasztása után a titkosítandó szöveget kódoljuk és az így kapott T értéket titkosítjuk. A titkosított C szöveget a

$$C = T^e \pmod{n}$$

Euler-féle fi-függvény (1763)
(Euler totient (annyiszoros) függvény)

Leonhard Euler
svájci
(1707 – 1783)

Meghatározza egy adott pozitív egész számhoz a nála nem nagyobb relatív prím pozitív egész számok számát.

$$\varphi(n) = |\{ k \in Z \mid 0 < k \leq n \wedge (n,k) = 1\}| \quad (ahol\ n \in N)$$

Ha ***n*** = ***p*** prímszám, akkor

$$\varphi(p) = p - 1$$

(mert éppen akkor prím egy ***p*** egész szám, ha minden nála kisebb pozitív szám relatív prím hozzá, különben lenne önmagánál kisebb prímosztója!)

Példa

1. Alice elküldi Bobnak a k1 = (g^x, (mod n)) értéket,
2. Bob válaszában a k2 = (g^y, (mod n))-t küldi vissza,
3. Alice kiszámolja k3 = (g^y, (mod n))^x (mod n),
4. Bob kiszámolja k4 = (g^x, (mod n))^y (mod n),
5. A közös kulcsuk a (g^{xy}, (mod n)).

Gyakorlati megjegyzések

- 100 jegyű prímeket kell keresnünk, ami a keresés és a prímség eldöntésének problematikáját is jelenti.
- A Prímszám tétel szerint körülbelül $\mathbf{10^{100}/\ln 10^{100} - 10^{99}/\ln 10^{99}}$ darab100 jegyű prím van, ha választunk egy páratlan számot P=0,00868 valószínűséggel prim.
- ***d*** kiválasztása: A kiválasztott ***d*** számot az Euklideszi algoritmussal teszteljük. Amennyiben jól választottunk, d kielégíti a $\mathbf{(d, \varphi(n)) = 1}$ feltételt.
- Euklideszi algoritmus egyenleteiből a szükséges ***e*** szám rögtön leolvasható

Tények

- Az RSA biztonságosan megvalósítja Diffie és Hellman álmát, a kulcscserét is, mivel az algoritmusban e és d szerepe felcserélhető. Az RSA napjaink legismertebb asszimmetrikus kriptográfiai módszere
- Gyakorlati alkalmazásra jelenleg az 1024 – 3072 bites modulusokat tekintjük biztonságosnak.
- Lényeges megjegyezni, hogy az RSA feltörhető, amennyiben az n számot faktoraira tudjuk bontani.
- Az RSA feltöréhez szüksége lenne egy gyors faktorizáló eljárásra. Ez egyelőre nem áll rendelkezésünkre.

A nyilvános kulcsú kriptográfia titkos története

- Ellis, Cocks, és Williamson a brit titkosszolgálat emberei voltak
- 1969-ben Ellis rájött, hogy nyilvános kulcsú kriptográfia lehetséges
- 1973-ban Cocks kitalálta a később RSA néven ismertté vált kódolást
- 1974-ben Williamson (Cocks barátja) felfedezi a később Diffie-Hellman kulcscsere néven ismertté vált eljárást
- **1975**-re Ellis, Cocks, és Williamson a nyilvános kulcsú kriptográfia összes alapvető tételét kidolgozta
  - de hallgatniuk kellett (1997-ig)

Köszönöm a figyelmet!

Created by Czeili Bence