# Egy számelméleti eljárás, amelyen (is) múlhat a bankbetéteink biztonsága.

## A nyilvános kódú titkosírások.

Klukovits Lajos

TTIK Bolyai Intézet

2016. május 5.





## Alapvető fogalmak.

### Definíciók.

- Forrásszöveg: az a szöveg (jelsorozat), amelyet az illetéktelenek elől rejtve akarunk valahová eljuttatni.
- Kódoló függvény, kódoló eljárás: amelynek segítségével a forrásszöveget átalakítjuk.
- Üzenet: Az előbbi átalakítási eljárás eredménye, az „átalakított” forrásszöveg.
- Dekódoló függvény, eljárás: ennek révén rekonstruáljuk az üzenetből az eredeti forrásszöveket.

### Praktikus követelmények.

- A kódoló és a dekódoló függvény lehetőleg legyen bijektív, és nem túl nehezen alkalmazható.
- A dekódoló függvény ne legyen „könnyen megtalálható”.





## Történeti áttekintés.

### Julius Caesar Kr.e. 100-44

- A följegyzések szerint igen egyszerű kódolást alkalmazott: az ábécé betűit sorrendben 3-mal eltolta.
- Így a (bijektív) kódoló függvény

| A | Á | B | C | D | E | É | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C | D | E | É | F | G | H | I | J | K | L | M | N | O |
| M | N | O | Ö | P | R | S | T | U | Ü | V | Y | Z | |
| Ö | P | R | S | T | U | Ü | V | Y | Z | A | Á | B | |

### Egy példa

- Forrásszöveg: Caesar nagy uralkodo
- Üzenet: Écgücu pcjá yuconrér
- A dekódolás is a táblázat szerint végezhető.

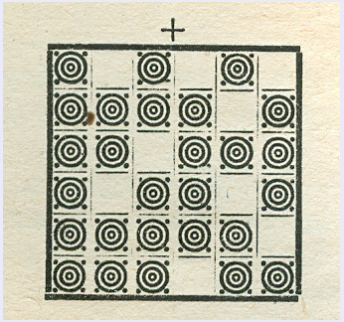




## Egy irodalmi példa.

### Verne, Sándor Mátyás.

- Az előbbinél nehezebben megfejthető kódolási módszer szerepel regényben, az ún. rostély alkalmazásával.



## Digitalizálás.

### Caesar kódolása

Ha a betűkhöz kétjegyű számokat rendelünk, akkor az előbbi 3-mal való eltolás egyszerűen számolható kongruenciával, pontosabban *modulo* 27 kongruenciával.

### A kódtábla.

| A | Á | B | C | D | E | É | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 |
| M | N | O | Ö | P | R | S | T | U | Ü | V | Y | Z | |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | |





## Digitalizálás.

### Egy kódolás.

- A forrásszöveg: Caesar nagy uralkodo
- Digitalizálva:

$$04\ 01\ 06\ 01\ 20\ 15\ 01\ 09\ 26\ 23\ 20\ 01\ 14\ 13\ 17\ 05\ 17$$

- Kódolva. Ha $F, U$ jelöli a digitalizált forrásszöveg ill. az üzenet egy-egy elemét, akkor az

$$U \equiv F + 3 \pmod{27}$$

kongruenciát használva az üzenet:

- 

$$07\ 04\ 09\ 04\ 23\ 18\ 04\ 12\ 02\ 26\ 23\ 04\ 17\ 16\ 20\ 08\ 20$$

- A dekódolás módja: $F \equiv U - 3 \pmod{27}$





## Elemzés.

- Az ilyen típusú — betűeltoláson alapuló — titkosírás igen egyszerű mind az üzenetküldő, mind az azt föltörni akaró számára.
- Így a biztonsági szintje nagyon alacsony, nem használható.

### Mit kívánunk ma egy kriptográfiai rendszertől?

1. Mivel a betűeltolásokon alapuló rendszereknél a kódoló függvény inverze (a dekódoló) egyszerűen megkapható, a bizonsági szint növelése érdekében ezen változtatni kell.
2. A kódolót úgy kell választani, hogy bár könnyen alkalmazható, az inverze nehezen alkotható meg.
3. Nagyon kedvező, ha a kódoló függvényt nem kell titkolni, sőt
4. az üzenetet is nyilvánosan lehet elküldeni, de
5. az üzenetet csak a címzett képes elolvasni, azaz dekódolni, csak ő ismeri a dekódoló függvényt.





## Mit kívánunk ma egy kriptográfiai rendszertől?

### A „vágyak netovábbja".

Egy ún. nyilvános kódú titkosírás, amelyben

1. alkalmazók mindegyike nyilvánosságra hozhatja azt a kódoló függvényt (kódolási eljárást), amellyel a neki szánt üzeneteket titkosítani lehet;
2. az üzenet nyilvánosan elküldhető, azt bárki megismerheti, de
3. kizárólag a címzett képes dekódolni az üzenetet.

### A legegyszerűbb megoldás.

- Ha **A** és **B** akar titkosítva levelezni nyilvános üzenetekkel, akkor
- Meg kell egyezniük egy kódoló-dekódoló függvénypárban.
- Ez egy gyenge pont, mert vissza lehet élni vele.

## Nyilvános kódú rendszer létezhet?

### Diffie és Hellman, 1975

- Leírták egy nyilvános kódú rendszer alapjait, amely digitalizált üzenetekre vonatkozik.
  - A kódoló függvény az $\{1, 2, \ldots, N\}$ halmaz egy permutációja, ahol $N$ egy „elegendően nagy szám".
  - A dekódoló függvény pedig ezen permutáció inverze.
  - A kódolt üzenet nyilvánosan elküldhető.

### Biztonságos lehet ez?

- Egy $\varphi \in S_N$ permutáció inverze látszólag könnyen meghatározható.
- Ez a gond elvethető, ha $N$ elegendően nagy, mondjuk $N \approx 10^{500}$, azaz mintegy 500 jegyű.
- Gondoljunk arra, hogy egyszerű-e egy angol-magyar szótárt magyar-angolként használni.





## A biztonságról még egyszer.

### Két empírikus eredmény.

1. Viszonylag könnyű nagy prímszámot megadni.
2. Jelenleg nem ismeretes olyan eljárás, amely egy amellyel tetszőleges $n$ jegyű szám prímtényezős fölbontását $f(n)$ lépésben meg lehetne határozni, ahol $f \in \mathbb{R}(x)$. Csak olyan eljárások ismertek, amelyeknél a lépések száma $e^n$ nagyságrendű.

### Mi következik ebből?

- Ha két kb. 250 decimális jegyű prímszámok összeszorzunk, akkor csak a szorzat ismeretében gyakorlatilag (az algoritmuselmélet és a technika mai állása szerint) nem tudjuk e számot prímtényezőkre bontani, még akkor sem, ha
- számítógépünk az elvi legnagyobb sebességű, azaz egy lépést $10^{-26}$ másodperc alatt végez el.





## Az elvi működés.

### Előkészületek.

- Tegyük föl, hogy a titkos levelezést folytató társaság tagjai $A, B, \ldots, C$.
- Minden résztvevő elkészít magának egy $\varphi, \psi$ kulcspárt, amelyek egymás inverzei. A $\varphi_A, \varphi_B, \ldots$ „kódoló" kulcsát mindenki nyilvánosságra hozza, és a $\psi_A, \psi_B, \ldots$ „dekódoló" kulcsát titokban tartja.

### Az elvi működés.

- Legyen a két partner $A, B$, és $A$ az $u$ (digitalizált) üzenetet akarja elküldeni $B$-nek.
- $A$ $u$ helyett a $v = (u\psi_A)\varphi_B$ jelsorozatot küldi el (akár nyilvánosan is) $B$-nek.
- $B$ megfejtése: $(v\psi_B)\varphi_A = u$.





## Az elvi működés.

### Igazolás.

- Mivel $v = (u\psi_A)\varphi_B$,
- $$(v\psi_B)\varphi_A = ((u\psi_A)\varphi_B)(\psi_B\varphi_A) = (u\psi_A)\varphi_A = u$$

### Teljesülnek az alapkövetelmények.

1. $A$ üzenetét csak a címzett $B$ érti, mert csak ő ismeri a megfejtéshez elengedhetetlen $\psi_B$ függvényt.
2. Harmadik fél nem tud „hamis" üzenetet küldeni $A$ nevében $B$-nek, mert nem ismeri a kódoláshoz szükséges $\psi_A$-t.
3. Nincs szükség előzetes „kódegyeztetésre", mindenki bármely partnere esetén használhatja ugyanazt a kulcsrendszert.
4. Ez megoldja a hitelesítés, az „elektronikus aláírás" kérdését is.

## Egy gyakorlati megvalósítás.

### 1976

- Az első technikailag is kivitelezhető nyilvános kódú titkosírási rendszert R. Rives, A Shamir és L. Adleman publikálta.
- Rendszerüket röviden RSA rendszernek nevezik.
- Ismertetéséhez néhány elemi számelméleti fogalomra és tételre lesz szükségünk.
- Ezek nem haladják meg egy bevezető számelméleti kurzus kereteit.





## Számelmélet előismeretek.

### A számelméleti kongruencia

- **Definíció.** Legyen $a, b, n \in \mathbb{Z}$ $n > 1$. Ha $n|a - b$, akkor azt mondjuk, hogy *a kongruens b-vel modulo n*. jelölése: $a \equiv b \pmod{n}$.
- Egyszerű észrevétel, hogy ezzel — minden rögzített $n$-re — ekvivalencia-relációt definiálunk az egészek halmazán, és ezen
- relációk megőrzik az összeadást és a szorzást, azaz, ha $a \equiv b \pmod{n}$ és $c \equiv d \pmod{n}$, akkor

$$a + c \equiv b + d \pmod{n}$$
$$ac \equiv bd \pmod{n}$$





## Számelmélet előismeretek.

### A számelmélet alaptétele

*Bármely nemzéró egész szám fölbontható prímszámok szorzatára. Egy adott nemzéró egész két fölbontása csak a tényezők sorrendjében és előjelben különbözhet.*

### Az Euler függvény

- **Definíció.** Az $a, b \in \mathbb{Z}$ egészek *relatív prímek*, ha a $\pm 1$-en kívül nincs más közös osztójuk.
- **Definíció.** Azon $\Phi\colon \mathbb{N} \to \mathbb{N}$ függvényt, amelyre $\Phi(n)$ az $n$-hez relatív prím $n$-nél nem nagyobb természetes számok száma, *Euler-féle* $\Phi$ *függvénynek* nevezzük.
- **Tétel.** *Az Euler-függvány multiplikatív, azaz ha* $m, n \in \mathbb{N}$ *relatív prímek, akkor* $\Phi(mn) = \Phi(m)\Phi(n)$.





## Számelmélet előismeretek.

### Három tétel.

1. *Ha az n természetes szám alaptétel szerinti fölbontása* $n = p_1^{k_1} \dots p_m^{k_m}$, *ahol* $p_1 \dots p_m$ *különböző prímek, akkor*

$$\Phi(n) = \prod_{i=1}^{m} \Phi(p_i^{k_i}) = \prod_{i=1}^{m} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

2. **Kis-Fermat tétel Euler-féle általánosítása.** *Ha* $a, n \in \mathbb{Z}$, $n > 1$ *relatív prímek, akkor* $a^{\Phi(n)} \equiv 1 \pmod{n}$
3. *Ha* $a, b, c \in \mathbb{Z}$, *az* $ax + by = c$ *egyenlet pontosan akkor oldható meg* $\mathbb{Z}$ *fölött, ha* ln. k. o.$(a, b)|c$.

## Az RSA rendszer működése1.

### Digitalizálás 1.

- A magyar ábécé betűihez — a korábban látott módon — rendeljük a 01, 02, ... kétjegyű számokat. Ha a korábbi rendszerünket kiegészítjük az í, ó, ő, ú, ű betűkkel, akkor a $01, 02, \ldots, 33$ számokat használtuk föl.
- Renszerünket kiegészítjük az írásjelek — pont, vessző, kérdőjel, fölkiáltójel — valamint a számjegyek $0, 1, \ldots, 9$, hasonlóan képezett kódjaival, akkor 47-ig jutunk.
- A szóköz kódja pedig legyen a 00.

### Digitalizálás 2.

- Az előbbi eljárással a szöveghez egy sokjegyű számot rendelhetünk.
- A jobb kezelhetőség kedvéért e számot, balról jobbra, osszuk föl $s$ jegyű számokra ($s$ legyen páros). Az utolsó számot zérókkal egészítjük ki $s$ jegyűre.





## Az RSA rendszer működése 2.

### Digitalizálás 3.

| A | Á | B | C | D | E | É | F | G | H | I | Í | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 |
| L | M | N | O | Ó | Ö | Ő | P | Q | R | S | T | U | Ú |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| Ü | Ű | V | Y | Z | . | , | ? | ! | 0 | 1 | 2 | 3 | 4 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
| 5 | 6 | 7 | 8 | 9 | ∅ | | | | | | | | |
| 43 | 44 | 45 | 46 | 47 | 00 | | | | | | | | |





## Az RSA rendszer működése 3.

### Digitalizálás 4.

- Így 1 és $10^s - 1$ közötti számokkal kell dolgoznunk.
- Ez azt is jelenti, hogy az eredeti — Diffie és Hellman féle — eljárásnál $N = 10^s - 1$ jó választás lenne.

### Egy példa.

- Legyen $s = 8$, és tekintsük a A SZÁMELMÉLET SZÉP. kijelentést.
- A digitális változat:
- 01002533|02160615|16071506|26002533|07223400
- Az üzenethez ezen öt 8 jegyű számot kell kódolnunk.





## Az RSA rendszer működése 4.

A „titkos” levelezés résztvevői: $A, B, \ldots, D$.

### A kódoló függvény.

- Minden egyes résztvevő válasz két nagy prímszámot: $(p_A, q_A)$, $(p_B, q_B), \ldots$, és legyen $M_A = p_A q_A$, $M_B = p_B q_B, \ldots$.
- A két prímet mindenki titokban tartja, míg az $M$-eket nyilvánosságra hozza.
- Mindenki választ egy $t_i > 1$ egészet úgy, hogy $\ln. \text{k. o.}(t_i, \Phi(M_i)) = 1$, ahol $i \in \{A, B, \ldots, D\}$
- Az $A$ nyilvánosságra hozandó $\varphi_A$ kódoló függvénye a következő

$$\varphi_A(r) = r^{t_A} \text{ legkisebb nemnegatív maradéka } \mod M_A$$

- ahol $0 < r < M_A$.
- Az így kapott számok (sorozata) a nyilvánosan elküldhető.

## Az RSA rendszer működése 5.

### A dekódoló függvény.

- Legyen $i \in \{A, B, \ldots\}$ A $\psi_i = \varphi_i^{-1}$ függvényeket hasonló alakban állítjuk elő, mint a $\varphi_i$ függvényeket:
- $$\psi_i(u) = u^{m_i} \text{ legkisebb nemnegatív maradéka} \mod M_i$$
- ahol $0 < u < M_i$.
- Hogyan határozzuk meg az $m_i$ kitevőt? E kitevő a biztonság kulcsa.

### A dekódoló kitevő meghatározása 1.

- Tekintsük az $A$ résztvevőt, aki kap egy $v$ kódolt üzenetet.
- Tudjuk, hogy $v = \varphi_A(r) \equiv r^{t_A} \pmod{M_A}$.
- Alkalmazzuk a $\psi_A$ dekódoló függvényt: $\psi_A(r^{t_A}) = r^{t_A m_A}$.
- Ebből kell meghatározni az $r$ eredeti üzenetet.





## Az RSA rendszer működése 6.

### A dekódoló kitevő meghatározása 2.

- Fermat tételéből tudjuk, hogy
$$r^{1+\Phi(M_A)} \equiv r \pmod{M_A}$$
- Ugyanis $\Phi(M_A) = (p_A - 1)(q_A - 1)$ és $\ln.\,k.\,o.(p_A, r) = 1$-re
$$r^{1+\Phi(M_A)} = r(r^{p_A-1})^{k(q_A-1)} \equiv r \cdot 1 = r \pmod{M_A}$$
- Tekintsük a két kongruenciából adódó
$$m_A t_A = 1 + k\Phi(M_A)$$
lineáris egyenletet, amely megoldható $m_A$-ra (és $k$-ra), mert $\ln.\,k.\,o.(t_A, \Phi(M_A)) = 1$.
- Világos, ezen egyenletet csak az tudja megoldani, aki ismeri $\Phi(M_A)$ értékét, azaz $M_A$ prímtényezőit.





## Az RSA rendszer működése 7.

### A $p, q$ prímpárok kiválasztása.

- Sorra választunk 250 ill. 300 jegyű egészeket.
- Prímteszttel ellenőrizzük, hogy az illető szám prím-e.
- Ez nem túl időigényes, hiszen
  - léteznek meglehetősen gyors prímtesztek,

"

  - elég sok" 250 ill 300 jegyű prím van, ugyanis a nagy prímszámtétel szerint közelítőleg minden $\log\left(10^{300}\right)/2 \approx$ 345-ik 300 jegyű szám prím.

### Néhány biztonsági szabály.

1. Az egy párba tartozó $p, q$ prímek ne legyenek „túl közeliek", ellenkező esetben könnyebb az aktuális $M$ faktorizálása. Ezért adtuk meg a korábbi korlátokat.
2. Hasonló okokból a $p, q$ párokat úgy kell választani, hogy $p-1, q-1$-nek legyenek nagy prímosztóik.