



Algoritmuselmélet 6. témakör

Pusztai Pál
pusztai@sze.hu

Tartalom

- A Rivest-Shamir-Adleman (RSA) titkosítás
 - A szükséges matematikai ismeretek
 - Oszthatóság és osztók
 - Prímek és összetett számok
 - Maradékos osztás, kongruenciák, ekvivalenciaosztályok
 - A legnagyobb közös osztó és tulajdonságai
 - Relatív prímek és az Euler-féle Φ függvény
 - Euklidesz algoritmus a legnagyobb közös osztó hatékony kiszámítására
 - Euklidesz algoritmusának kibővítése
 - Lineáris kongruenciák megoldása
 - Moduláris hatványozás
 - A nyilvános kulcsú titkosítás
 - Titkos üzenetküldés és digitális aláírás
 - Nyilvános és titkos kulcsok
 - Kódolás és dekódolás



Az RSA titkosítás

- Korábban
 - Számelméletet a matematika szép, de jobbra haszontalan ágának tartották.
- Napjainkban
 - A számelméleti algoritmusokat széles körben használják.
- A nagy prímszámokon alapuló titkosítás
 - Elméletileg nem feltörhetetlen.
 - A titkosság garanciája
 - Könnyen találhatunk nagy (pl. decimálisan 100 számjegyű) prímszámokat.
 - Nagy prímszámok szorzatát képtelenek vagyunk tényezőkre bontani.
- Az RSA nyilvános kulcsú titkosítás
 - Rivest-Shamir-Adleman (1978)



Az RSA titkosítás

■ Oszthatóság és osztók

Jelölje \mathbf{Z} az egész számok $\{\dots, -2, -1, 0, 1, 2, \dots\}$ halmazát.

A $d \mid a$ jelölés azt jelenti ($a, d \in \mathbf{Z}, d \neq 0$), hogy valamely $k \in \mathbf{Z}$ egész számra $a=kd$ teljesül.

Ha $d \mid a$, akkor a a d **többsese**, d pedig az a **osztója**.

Megjegyzés: A $d \mid a$ akkor és csak akkor teljesül, ha $-d \mid a$, így az általánosság megszorítása nélkül az osztót pozitívnak tekinthetjük.

Pl: a 12 osztói: 1, 2, 3, 4, 6, 12.

Minden a egész szám osztható a **triviális osztóival**, 1-gyel és a -val. Az a nemtriviális osztóit az a **tényezőinek**, **faktorainak** vagy **valódi osztóinak** nevezzük.

Pl: a 12 tényezői: 2, 3, 4, 6.

Az RSA titkosítás

■ Prímszámok és összetett számok

Ha az $a > 1$ egész számnak csak a triviális 1 és az a az osztói, akkor az a számot **prímszámnak** (vagy egyszerűen **prímnak**) nevezzük.

Pl: 2, 3, 5, 7, 11, 13, 17, 19, 23, ...

Ha az $a > 1$ egész szám nem prím, akkor **összetett számnak** (vagy egyszerűen **összetettnek**) nevezzük.

Pl: a 15 összetett, mert $3 \mid 15$.

Az 1 számot **egységnek** nevezzük és ez a szám nem prím és nem is összetett.

Megjegyzés: A 0 és a negatív egész számok nem prímelek, és nem is összetettek.

Az RSA titkosítás

■ Maradékos osztás, kongruenciák

A **maradékos osztás tétele**: Bármely a egész és n pozitív egész számhoz egyértelműen létezik olyan q és r egész szám, hogy $0 \leq r < n$ és $a = qn + r$.

A $q = \lfloor a / n \rfloor$ érték az osztás **hányadosa**, az $r = a \bmod n$ pedig az osztás **maradéka**. Tehát $n \mid a$ akkor és csak akkor teljesül, ha $a \bmod n = 0$.

Ha $a \bmod n = b \bmod n$, akkor azt mondjuk, hogy a és b **kongruens** modulo n .

Jelölés: $a \equiv b \pmod{n}$.

Pl: $61 \equiv 6 \pmod{11}$, $-13 \equiv 22 \pmod{5}$.

Tulajdonság: Ha $a \equiv a' \pmod{n}$ és $b \equiv b' \pmod{n}$, akkor $a + b \equiv a' + b' \pmod{n}$ és $ab \equiv a'b' \pmod{n}$.

Következmény: $ab \equiv a(b \bmod n) \pmod{n}$, hiszen $b \equiv b \bmod n \pmod{n}$.

Az RSA titkosítás

■ Ekvivalenciaosztályok

Egy n pozitív egész számot alapul véve, az egész számokat n db **ekvivalencia-osztályba** sorolhatjuk az n -nel való osztási maradékuk szerint.

Azt az ekvivalencia-osztályt, vagy más néven **maradékosztályt modulo n** , amely az a egész számot tartalmazza a következő módon definiáljuk és jelöljük:

$$[a]_n = \{a + kn : k \in \mathbf{Z}\}.$$

Pl: $[3]_7 = \{\dots, -11, -4, 3, 10, 17, \dots\}$ vagy más jelöléssel $[-4]_7$ vagy $[10]_7$.

Ezzel a jelöléssel $a \in [b]_n$ ugyanazt jelöli, mint $a \equiv b \pmod{n}$.

Az összes ekvivalencia-osztályt tartalmazó halmaz jelölése:

$$\mathbf{Z}_n = \{[a]_n : 0 \leq a \leq n-1\}.$$

Megjegyzés: A $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$ definíció is használatos, ahol a $[0]_n$ helyett 0 áll, $[1]_n$ helyett az 1, és így tovább, azaz minden maradékosztályt a legkisebb nemnegatív eleme reprezentál. Ez az egyszerűsítés nem jelenti azt, hogy megfeledkezünk az alapul szolgáló ekvivalencia-osztályokról, például a -1 egész szám az $[n-1]_n$ maradékosztályt képviseli, hiszen $-1 \equiv n-1 \pmod{n}$.

Az RSA titkosítás

■ Közös osztó és legnagyobb közös osztó

Ha d osztja az a és b egész számokat, akkor a d számot az a és b **közös osztójának** nevezzük.

Pl: a 24 és a 30 közös osztói: 1, 2, 3, 6.

A közös osztó tulajdonságai:

Ha $d \mid a$ és $d \mid b$, akkor $d \mid (a+b)$ és $d \mid (a-b)$, sőt $d \mid (ax+by)$ is igaz tetszőleges x, y egészekre.

Ha $a \mid b$, akkor vagy $|a| \leq |b|$, vagy $b=0$, így ha $a \mid b$ és $b \mid a$, akkor $a = \pm b$.

Ha a és b egész számok közül legalább az egyik 0-tól különböző, akkor a és b közös osztói közül a legnagyobbat az a és b számok **legnagyobb közös osztójának** nevezzük és $\text{lko}(a, b)$ -vel jelöljük.

Pl: $\text{lko}(24, 30)=6$, $\text{lko}(14, 15)=1$, $\text{lko}(5, 7)=1$, $\text{lko}(0, 9)=9$.

Ha a és b egyike sem 0, akkor $1 \leq \text{lko}(a, b) \leq \min(|a|, |b|)$.

Az $\text{lko}(0, 0)$ értékét 0-nak definiáljuk.

Az RSA titkosítás

■ Közös osztó és legnagyobb közös osztó

Az lko függvény elemi tulajdonságai:

$$\text{lko}(a, b) = \text{lko}(b, a),$$

$$\text{lko}(a, b) = \text{lko}(-a, b),$$

$$\text{lko}(a, b) = \text{lko}(|a|, |b|),$$

$$\text{lko}(a, 0) = |a|,$$

$$\text{lko}(a, ka) = |a| \text{ bármely } k \in \mathbf{Z}\text{-re.}$$

Tétel: Ha az a és b egészek legalább egyike 0-tól különböző, akkor $\text{lko}(a, b)$ az a és b összes lineáris kombinációjából álló $\{ax+by: x, y \in \mathbf{Z}\}$ halmaz legkisebb pozitív eleme.

Következmény:

- Ha valamely a és b egészekre $d \mid a$ és $d \mid b$, akkor $d \mid \text{lko}(a, b)$.
- Bármely a, b egész és n nemnegatív egész számokra $\text{lko}(an, bn) = n \text{lko}(a, b)$.
- Ha az n, a és b pozitív egészekre $n \mid ab$ és $\text{lko}(a, n)=1$, akkor $n \mid b$.

Megjegyzés: Az $\text{lko}(a, b) = \text{lko}(|a|, |b|)$ tulajdonság miatt a továbbiakban feltesszük, hogy a és b nemnegatív egészek.



Az RSA titkosítás

■ Relatív prím számok

Az a és b egész számok **relatív príme**k, ha közös osztójuk csak az 1, azaz ha $\text{lko}(a, b)=1$.

Pl: a 8 és a 15 relatív prímek, hiszen a 8 osztói az 1, 2, 4 és 8, míg a 15 osztói 1, 3, 5 és 15.

Állítások:

- Ha az a, b és p egész számokra $\text{lko}(a, p)=1$ és $\text{lko}(b, p)=1$, akkor $\text{lko}(ab, p)=1$.
- Ha p prím, a és b pedig olyan egészek, hogy $p \mid ab$, akkor $p \mid a$ vagy $p \mid b$.

■ Az Euler-féle Φ függvény

Legyen $\mathbf{Z}_n^* = \{[a]_n \in \mathbf{Z}_n : \text{lko}(a, n) = 1\}$, azaz a \mathbf{Z}_n n -hez relatív prím maradékosztályainak halmaza.

Pl: $\mathbf{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Jelölje $\Phi(n)$ a \mathbf{Z}_n^* elemszámát. Ez az Euler-féle Φ függvény. Pl: $\Phi(15) = 8$.

Tulajdonság: $\Phi(n) = n \prod_{p: p \text{ prím és } p \mid n} \left(1 - \frac{1}{p}\right)$. Pl: $\Phi(15) = 15 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 15 \left(\frac{2}{3}\right) \left(\frac{4}{5}\right) = 8$.

Ha p prím, akkor $\mathbf{Z}_p^* = \{1, 2, 3, \dots, p-1\}$, és $\Phi(p) = p-1$.



Feladatok

- Határozzuk meg $\Phi(n)$ értékét az alábbi n értékekre!
 - 9, 30, 42, 100



Az RSA titkosítás

■ Egyértelmű prímfaktorizáció

Tétel: Egy összetett egész szám pontosan egyféleképpen írható fel $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ alakban, ahol a p_i számok prímek, $p_1 < p_2 < \dots < p_r$, az e_i kitevők pedig pozitív egész számok ($i=1, 2, \dots, r$).

Pl: $60 = 2^2 \cdot 3 \cdot 5$.

■ A legnagyobb közös osztó kiszámítása

Elvileg az a és b prímfelbontásából $\text{lko}(a, b)$ meghatározható.

Ha $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ és $b = p_1^{f_1} p_2^{f_2} \dots p_r^{f_r}$, ahol p_1, p_2, \dots, p_r most az a -ban és b -ben előforduló összes prímet jelöli, és a számokat nem osztó prímek 0 kitevővel szerepelnek, akkor

$$\text{lko}(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_r^{\min(e_r, f_r)}.$$

Megjegyzés: A prímtenyezőkre bontás nem oldható meg polinomiális futási időben.

Tétel: Tetszőleges a nemnegatív és b pozitív egész számokra $\text{lko}(a, b) = \text{lko}(b, a \bmod b)$.

Megjegyzés: Ezen tétel alapján könnyű rekurzív algoritmust adni a legnagyobb közös osztó kiszámítására.

Az RSA titkosítás

- A legnagyobb közös osztó hatékony kiszámítása

EUKLIDESZ(a, b)

```

1  if  $b = 0$ 
2      return  $a$ 
3  else
4      return EUKLIDESZ( $b, a \bmod b$ )
    
```

Pl: Az $\text{lko}(30, 21)$ kiszámításakor az alábbi rekurzív hívások adják meg az eredményt:

$$\text{EUKLIDESZ}(30, 21) = \text{EUKLIDESZ}(21, 9) = \text{EUKLIDESZ}(9, 3) = \text{EUKLIDESZ}(3, 0) = 3$$

Tétel (Lamé): Tetszőleges $k \geq 1$ esetén ha $a > b \geq 1$ és $b < F_{k+1}$, akkor az $\text{EUKLIDESZ}(a, b)$ algoritmus k -nál kevesebb rekurzív hívást hajt végre. (F_{k+1} a $k+1$ -edik Fibonacci számot jelöli.)

Hatékonyság: A szomszédos Fibonacci számokra kapjuk a leghosszabb futási időt. Az F_k értéke megközelítőleg $\varphi^k / \sqrt{5}$, ahol $\varphi = (1 + \sqrt{5})/2 = 1.61803\dots$ az aranymetszés aránya, amiből az algoritmus rekurzív hívásainak száma, így a futási idő is $O(\lg b)$.

Megjegyzés: Euklidesz kb. i.e. 300-ban adta meg „ezt” az algoritmust.



Feladatok

- Milyen rekurzív hívásokat eredményez és mit ad eredményül az EUKLIDESZ algoritmus az alábbi bemenő adatok esetén?
 - 50, 35
 - 0, 8
 - 34, 21



Az RSA titkosítás

■ Az EUKLIDESZ algoritmus kibővítése

Feladat: Bővítsük ki az euklideszi algoritmust olyan x, y egészek meghatározása, amelyekre:

$$d = \text{lko}(a, b) = ax + by.$$

Az algoritmus bemenő adata két nemnegatív egész szám, kimenete pedig három olyan egész szám, amely kielégíti az előző egyenletet.

BŐVÍTETT-EUKLIDESZ(a, b)

```

1  if  $b = 0$ 
2      return ( $a, 1, 0$ )
3   $(d', x', y') \leftarrow \text{BŐVÍTETT-EUKLIDESZ}(b, a \bmod b)$ 
4   $(d, x, y) \leftarrow (d', y', x' - \lfloor a/b \rfloor y')$ 
5  return ( $d, x, y$ )
    
```

Megjegyzés: x és y lehet 0 és negatív is.

Hatékonyág: Mivel az EUKLIDESZ és a BŐVÍTETT-EUKLIDESZ algoritmus ugyanannyi rekurziós hívást tartalmaz, így a futási idejük konstans szorzótól eltekintve megegyezik, azaz $a > b > 0$ esetén $O(\lg b)$.



Az RSA titkosítás

a	b	$[a/b]$	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	—	3	1	0

A BŐVÍTETT-EUKLIDESZ algoritmus működése

A BŐVÍTETT-EUKLIDESZ(99, 78) hívás a $(3, -11, 14)$ számhármast szolgáltatja, így

$$\text{Inko}(99, 78) = 3 = 99 \cdot (-11) + 78 \cdot 14.$$

Feladatok

- Milyen (d, x, y) számhármast ad a BŐVÍTETT-EUKLIDESZ algoritmus az alábbi bemenő adatok esetén?
 - 30, 75
 - 899, 493



Az RSA titkosítás

■ Lineáris kongruenciák megoldása

Feladat: Oldjuk meg az $ax \equiv b \pmod{n}$ kongruenciát, ahol b egész, a és n pozitív egész számok!

Megjegyzés: Lehet 0, 1, ill. 1-nél több megoldás is.

Állítások:

- Az $ax \equiv b \pmod{n}$ kongruencia az x ismeretlenben akkor és csak megoldható, ha $\text{lko}(a, n) \mid b$.
- Az $ax \equiv b \pmod{n}$ kongruenciának vagy d különböző megoldása van modulo n , ahol $d = \text{lko}(a, n)$, vagy nincs megoldása.
- Legyen $d = \text{lko}(a, n) = ax' + ny'$ valamely x', y' egészekkel. Ha $d \mid b$, akkor az $ax \equiv b \pmod{n}$ kongruenciának az egyik megoldása $x_0 = x'(b/d) \pmod{n}$.
- Tegyük fel, hogy az $ax \equiv b \pmod{n}$ kongruencia megoldható (azaz $d \mid b$, ahol $d = \text{lko}(a, n)$), és jelölje x_0 az egyik megoldást. Ekkor a kongruenciának pontosan d különböző megoldása van, mégpedig $x_i = x_0 + i(n/d) \pmod{n}$, ahol $i=0, 1, 2, \dots, d-1$.
- Bármely $n > 1$ esetén, ha $\text{lko}(a, n) = 1$, akkor az $ax \equiv b \pmod{n}$ kongruenciának csak egyetlen megoldása van modulo n .

Megjegyzés: A $b=1$ eset azért fontos, mert a keresett x megoldás éppen az a **multiplikatív inverze** modulo n , hiszen $ax \equiv 1 \pmod{n}$. A BŐVÍTETT-EUKLIDESZ algoritmussal kiszámított x érték a multiplikatív inverzét adja, mivel $\text{lko}(a, n) = 1 = ax + ny$, így $ax \equiv 1 \pmod{n}$.

Az RSA titkosítás

LINEÁRIS-KONGRUENCIA-MEGOLDÓ(a, b, n)

```

1  ( $d, x', y'$ )  $\leftarrow$  BŐVÍTETT-EUKLIDESZ( $a, n$ )
2  if  $d \mid b$ 
3       $x_0 \leftarrow x'(b / d) \bmod n$ 
4      for  $i \leftarrow 0, d-1$ 
5          Ki:  $(x_0 + i (n / d)) \bmod n$ 
6  else
7      Ki: „Nincs megoldás”
    
```

Hatékonyság: Az algoritmus $O(\lg n + \ln \text{ko}(a, n))$ futási idejű.

Feladatok

- Határozzuk meg az alábbi kongruenciák összes megoldását!
 - $14x \equiv 30 \pmod{100}$
 - $35x \equiv 10 \pmod{50}$



Az RSA titkosítás

■ Hatványozás

Feladat: Számítsuk ki a^b értékét adott a és b nemnegatív egészek esetén minél kevesebb szorzással!

Megoldás: Egy rekurzív algoritmus, amelyik **ismételt négyzetre emeléssel** csökkenti a szorzások számát.

Pl: $2^{10} = 2^5 \cdot 2^5$, $2^5 = 2 \cdot 2^4$, $2^4 = 2^2 \cdot 2^2$, $2^2 = 2 \cdot 2$.

HATVÁNY(a, b)

```

1  if  $b = 0$ 
2      return 1
3  if  $b \bmod 2 = 0$ 
4       $c \leftarrow \text{HATVÁNY}(a, b / 2)$ 
5      return  $c \cdot c$ 
6  return  $a \cdot \text{HATVÁNY}(a, b-1)$ 
```

Hatékonyság: A rekurzív hívások, és így a szorzások száma $O(\lg b)$.

Az RSA titkosítás

■ Moduláris hatványozás

Egy $a \in \mathbf{Z}_n$ elem $a^0, a^1, a^2, a^3, \dots$ hatványainak sorozata képezhető modulo n , ahol a 0. érték a sorozatban $a^0 \bmod n = 1$, az i . érték pedig $a^i \bmod n$ lesz.

Megjegyzés: Vegyük észre, az $a^i \equiv a(a^{i-1} \bmod n) \pmod{n}$ kongruencia teljesülését (4. dia)!

i	0	1	2	3	4	5	6	7	
$2^i \bmod 5$	1	2	4	3	1	2	4	3	...
$3^i \bmod 5$	1	3	4	2	1	3	4	2	...

i	0	1	2	3	4	5	6	7	8	9	10	11	
$2^i \bmod 7$	1	2	4	1	2	4	1	2	4	1	2	4	...
$3^i \bmod 7$	1	3	2	6	4	5	1	3	2	6	4	5	...

A 2 és 3 hatványai modulo 5 ill. modulo 7

Euler tétele: Bármely 1-nél nagyobb n egész szám esetén $a^{\Phi(n)} \equiv 1 \pmod{n}$ minden $a \in \mathbf{Z}_n^*$ elemre.

Fermat tétele: Ha p prím, akkor $a^{p-1} \equiv 1 \pmod{p}$ minden $a \in \mathbf{Z}_p^*$ elemre.



Az RSA titkosítás

■ Moduláris hatványozás

Feladat: Számítsuk ki az $a^b \bmod n$ értékét, ahol a és b nemnegatív egészek, n pedig pozitív egész.

Megoldás:

- Legyen $\langle b_k, b_{k-1}, \dots, b_0 \rangle$ a b bináris alakja (azaz $k+1$ bit hosszúságú, ahol b_k a legnagyobb helyiértékű jegy, b_0 pedig a legkisebb helyiértékű jegy).

- Felhasználva az

$$a^{2^c} \bmod n = (a^{2^{c-1}})^2 \bmod n$$

$$a^{2^{c+1}} \bmod n = a (a^{2^c})^2 \bmod n$$

azonosságokat és az

$$a^i \equiv a (a^{i-1} \bmod n) \pmod n$$

kongruenciát, kiszámíthatjuk $a^c \bmod n$ értékét egy olyan iterációval, amelyben c értékét duplázásokkal ill. 1-gyel növelgetjük (a b_i jegyeiktől függően) 0-tól b -ig!

Az RSA titkosítás

MODULÁRIS-HATVÁNYOZÓ(a, b, n)

```

1   $c \leftarrow 0$ 
2   $d \leftarrow 1$ 
3  Legyen  $\langle b_k, b_{k-1}, \dots, b_0 \rangle$  a  $b$  bináris alakja
4  for  $i \leftarrow k, 0, -1$ 
5       $c \leftarrow 2c$ 
6       $d \leftarrow (d \cdot d) \bmod n$ 
7      if  $b_i = 1$ 
8           $c \leftarrow c + 1$ 
9           $d \leftarrow (d \cdot a) \bmod n$ 
10 return  $d$ 
    
```

Hatékonyság: A szükséges aritmetikai műveletek száma $O(\lg b)$.

Megjegyzés: A c változó csak magyarázó cézzal szerepel az algoritmusban.

Az RSA titkosítás

i	5	4	3	2	1	0
b_i	1	1	0	0	1	0
c	1	3	6	12	25	50
d	2	3	4	1	2	4

A 2^{50} mod 5 kiszámítása

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298	166	67	1

A 7^{560} mod 561 kiszámítása



Feladatok

- Számoljuk ki az alábbi moduláris hatványok értékét!
 - $2^{15} \bmod 5$
 - $7^{35} \bmod 11$
- Milyen d értékeket állít elő rendre a MODULÁRIS-HATVÁNYOZÓ algoritmus az alábbi bemenő adatok esetén?
 - $a=2, b=15, n=5$
 - $a=7, b=35, n=11$



Az RSA titkosítás

■ A nyilvános kulcsú titkosítás

Felhasználás:

- Titkos üzenetküldés.
- Hamisíthatatlan digitális aláírás.

Tulajdonságok:

Minden résztvevőnek van egy **nyilvános kulcsa** és egy **titkos kulcsa**. Pl. az RSA titkosításnál a kulcsok egész számpárok.

Legyen a titkosításban klasszikusan résztvevő két fél Aliz és Bob és jelölje P_A ill. S_A Aliz nyilvános (public) és titkos (secret) kulcsát, valamint P_B ill. S_B Bob nyilvános és titkos kulcsát.

Legyen \mathcal{D} a megengedett üzenetek halmaza (pl. a véges hosszúságú bitsorozatok halmaza), és $M \in \mathcal{D}$ tetszőleges üzenet.

A nyilvános és titkos kulcs minden résztvevő számára egy „összeillő pár” abban az értelemben, hogy olyan függvényeket határoznak meg, amelyek egymás inverzei, azaz:

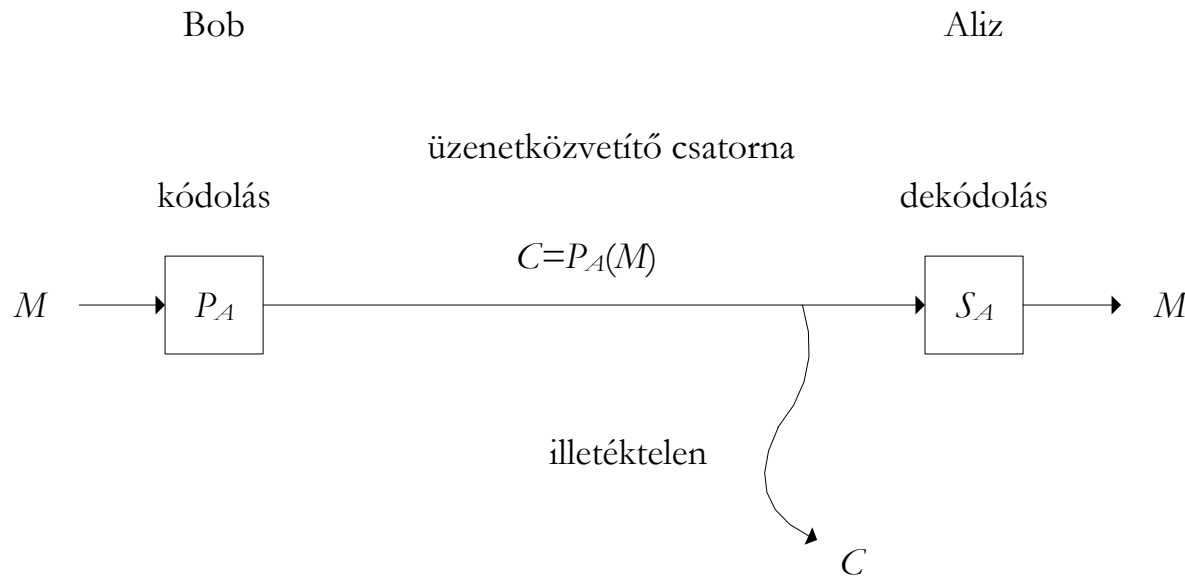
$$M = S_A (P_A (M))$$

$$M = P_A (S_A (M))$$

tetszőleges $M \in \mathcal{D}$ üzenetre.

Az S_A függvény értékeit rövid időn belül csak Aliz képes kiszámolni (csakúgy, mint S_B értékeit Bob), annak ellenére, hogy a P_A kulcsot mindenki ismeri és P_A az S_A inverze gyorsan kiszámítható.

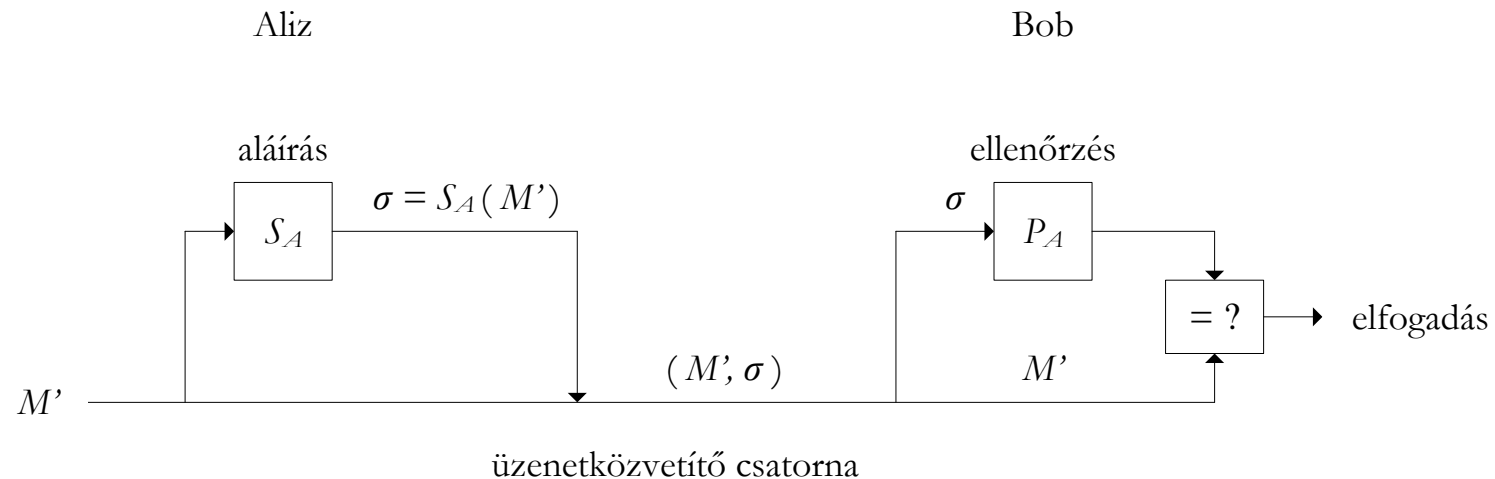
Az RSA titkosítás



Titkos üzenetküldés a nyilvános kulcsú titkosításnál:

- Bob megszerzi Aliz nyilvános kulcsát (pl. egy nyilvános tárból, vagy közvetlenül Aliztól).
- Bob kódolja az elküldendő M üzenetet Aliz P_A nyilvános kulcsával és elküldi a $C = P_A(M)$ **kódolt üzenetet** Aliznak.
- Aliz megkapja a C kódolt szöveget és a titkos kulcsa segítségével dekódolja azt, hogy visszakaphassa az eredeti $M = S_A(C)$ üzenetet.

Az RSA titkosírás



Digitális aláírás a nyilvános kulcsú titkosírásnál:

- Aliz kiszámítja S_A titkos kódja felhasználásával az M' üzenet **digitális aláírását**, $\sigma = S_A(M')$ -t.
- Aliz elküldi az (M', σ) üzenet-aláírás párt Bobnak.
- Bob megkapja az (M', σ) párt, ellenőrizni tudja, hogy Aliztól származik-e, Aliz nyilvános kulcsát felhasználva. Leellenőrzi ugyanis, hogy $M' = P_A(\sigma)$ teljesül-e.

Megjegyzés: A digitális aláírás fontos tulajdonsága, hogy bárki ellenőrizheti, aki hozzá tud férni az aláíró nyilvános kulcsához. Az M' üzenet nem titkosított, „egyenest” érkezik, de titkosítható. (Feltételezhető, hogy a levél tartalmazza Aliz nevét, így Bob tudni fogja, hogy kinek a nyilvános kulcsát kell használnia.)

Az RSA titkosítás

■ A nyilvános és titkos kulcsok meghatározása

Mindenki, aki az **RSA nyilvános kulcsú titkosítás** segítségével szeretne titkosítani, a következő módon készítheti el a nyilvános és titkos kulcsát:

1. Véletlenszerűen ki kell választani két nagy prímszámot, p -t és q -t úgy, hogy $p \neq q$. A p és q prímszámok legyenek pl. 512 bit hosszúak.
2. Ki kell számítani az $n=pq$ értéket.
3. Ki kell választani egy kis páratlan e egész számot, amelyik $\Phi(n)$ -hez relatív prím.
 $\Phi(n) = (p-1)(q-1)$.
4. Ki kell számítani e multiplikatív inverzének értékét modulo $\Phi(n)$, legyen ez az érték d .
5. Nyilvánosságra kell hozni a $P = (e, n)$ párt, az **RSA nyilvános kulcsot**.
6. Titokban kell tartani az $S = (d, n)$ párt, az **RSA titkos kulcsot**.

Megjegyzés:

Könnyű egy nagy számot prímtényezőkre bontani \Rightarrow könnyű az RSA titkosítást megfejteni.

Nehéz egy nagy számot prímtényezőkre bontani ? \Rightarrow ? nehéz az RSA titkosítást megfejteni.



Az RSA titkosítás

- A nyilvános és titkos kulcsok használata

Az RSA nyilvános kulcsú titkosításban $\mathcal{D} = \mathbf{Z}_n = \{[a]_n : 0 \leq a \leq n-1\}$.

Egy M üzenet kódolása a $P(e, n)$ nyilvános kulcs szerint:

$$P(M) = M^e \pmod{n}.$$

A C kódolt üzenet dekódolása az $S(d, n)$ titkos kulcs szerint pedig:

$$S(C) = C^d \pmod{n}.$$

Megjegyzés: Ezek az egyenletek a titkosításra és az aláírásra egyaránt vonatkoznak.

Az RSA titkosítás

■ Egy egyszerű példa

1. Legyen $p = 2$ és $q = 5$.
2. $n = pq = 10$.
3. Legyen $e = 3$, hiszen $\Phi(n) = (p-1)(q-1) = 4$, és $\text{luko}(\Phi(n), e) = \text{luko}(4, 3) = 1$.
4. Az $ed \equiv 1 \pmod{\Phi(n)}$ kongruencia alapján meghatározzuk d -t, e multiplikatív inverzét modulo $\Phi(n)$ (lásd megjegyzés). A $d = 3$ értéket kapjuk.
5. A nyilvános kulcs a $P = (e, n) = (3, 10)$ pár.
6. A titkos kulcs az $S = (d, n) = (3, 10)$ pár.

Megjegyzés: A BŐVÍTETT-EUKLIDESZ algoritmus az $a=e$ és $b=\Phi(n)$ adatokra az $\text{luko}(a, b) = \text{luko}(e, \Phi(n)) = \text{luko}(3, 4) = 1$, $x=-1$, $y=1$ eredményt adja, amelyre $\text{luko}(e, \Phi(n)) = ex + \Phi(n)y$, behelyettesítve $1=3 \cdot (-1) + 4 \cdot 1$, így $ex \equiv 1 \pmod{\Phi(n)}$. Mivel $x=-1$ negatív, ezért $\Phi(n)$ értékkel „eltolva” (hogy d pozitív legyen), a $d=3$ -t kapjuk e multiplikatív inverzére.

Az RSA titkosítás

- A titkosítás egy lehetséges megvalósítása

Legyen a titkosítandó jelsorozat a következő:

Szövegesen	'A'	'l'	'm'	'a'
Binárisan	01000001	01110110	01110111	01100001
Decimálisan	65	118	119	97

A titkosítandó üzenet

Mivel $n = 10$, és $2^3 < 10 < 2^4$, ezért a titkosítás (kódolás) $3 \rightarrow 4$ bites, a visszafejtés (dekódolás) $4 \rightarrow 3$ bites átalakítást jelent.

Binárisan	010	000	010	111	011	001	110	111	011	000	01
Decimálisan	2	0	2	7	3	1	6	7	3	0	1

A titkosítandó üzenet 3 bitenként csoportosítva

Az RSA titkosítás

■ A titkosítás egy lehetséges megvalósítása

A titkosítás a $P(M) = M^e \pmod{n}$ alapján történik, ahol most $e = 3$, $n = 10$.

A MODULÁRIS-HATVÁNYOZÓ segítségével kiszámolható minden $0 \leq M \leq n-1$ értékre a megfelelő $P(M)$ kódérték (igaz 3 biten csak a $0 \leq M \leq 7$ értékek kódjaira lesz szükségünk).

M	0	1	2	3	4	5	6	7
$P(M)$	0	1	8	7	4	5	6	3

A kódolási megfeleltetések decimális alakban

Megjegyzés: Mivel az utolsó szám nem biztos, hogy 3 bit hosszú, ezért az üzenethez hozzátehetjük pl. az utolsó szám bináris hosszát is (2) természetesen kódolva (8), hogy az eredeti üzenet végét (a dekódolás után) majd a megfelelő hosszúságúra tudjuk állítani.

Kódolandó	2	0	2	7	3		0	1	2
Kódolt	8	0	8	3	7	...	0	1	8
Binárisan	1000	0000	1000	0011	0111	...	0000	0001	1000

A titkosított üzenet (4 bites egységekben) hossz kiegészítéssel



Az RSA titkosítás

A titkosítás egy lehetséges megvalósítása

A titkosított üzenet dekódolása az $S(C) = C^d \pmod{n}$ alapján történik, ahol most $d = 3$, $n = 10$.

C	0	1	2	3	4	5	6	7	8	9
$S(C)$	0	1	8	7	4	5	6	3	2	9

A dekódolási megfeleltetések decimális alakban

Megjegyzés: A dekódolt üzenetként, figyelembe véve az utolsóként megkapott $C(8) = 2$ hosszt, amely az utolsó előtti 3 bit hosszát adja, az alábbiakat kapjuk, amely megegyezik az eredeti üzenettel.

Kódolt	8	0	8	3	7	1	6	3	7	0	1
Dekódolt	2	0	2	7	3	1	6	7	3	0	1
Binárisan	010	000	010	111	011	001	110	111	011	000	01

A dekódolt és megfelelő hosszúságúra igazított üzenet

Megjegyzés: Ha p és q prímek decimálisan pl. 100 jegyűek, akkor $n=pq$ decimálisan 200 jegyű, binárisan $200 \lg 10 \approx 665$ jegyű, így az üzenetet tördelhetjük ilyen hosszú, azaz pl. 512 bit = 64 bájt hosszú blokkokra is.



Feladatok

- Tegyük fel, hogy „feltörtük” a $(3, 319)$ RSA nyilvános kulcsot, azaz rájöttünk, hogy $p=11$ és $q=29$.
 - Mi az $M=100$ üzenet kódolt változata?
 - Mi az RSA titkos kulcs?

