

Debreceni Egyetem

Informatikai Kar

Adatbiztonság munkafüzet

Contents

1	RSA	3
1.1	RSA általánosan	3
1.2	RSA háttér	4
1.2.1	Euklideszi algoritmus	4
1.2.2	Kibővített Euklideszi algoritmus	4
1.2.3	Gyorshatványozás	5
1.2.4	Fermat-teszt	7
1.2.5	Miller-Rabin prímteszt	8
1.2.6	Kínai maradéktétel	9
1.3	RSA feladatok	12
2	Megoldások	13
2.1	RSA megoldásai	13
2.1.1	Euklideszi algoritmus megoldások	13
2.1.2	Gyors hatványozás megoldásai	13
2.1.3	Fermat-teszt megoldásai	13
2.1.4	Miller-Rabin megoldásai	14
2.1.5	Kínai maradéktétel megoldásai	14
2.1.6	RSA megoldásai	14

Chapter 1

RSA

1.1 RSA általánosan

- Vegyünk véletlenszerűen két különböző nagy prímszámot, p -t és q -t.
- Legyen $n = p * q$.
- Vegyünk egy olyan kis páratlan e számot, amely relatív prím $\phi(n)$ -hez.
- Keressünk egy olyan d számot, amelyre $e * d = 1 \pmod{\phi(n)}$.
- Az RSA nyilvános kulcs a $PK = (e, n)$ pár lesz.
- Az RSA titkos kulcs az $SK = (d, n)$ pár lesz.

Nyílt üzenetek halmaza: Z_n . Ebben a sémában az elküldhető (titkosított) üzenetek halmaza $Z_n = \{0, 1, \dots, n - 1\}$.

A titkosítás a $PK = (e, n)$ nyilvános kulccsal:

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

A visszafejtés a titkos kulccsal:

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

1.2 RSA háttér

1.2.1 Euklideszi algoritmus

Maradékos osztás

Tetszőleges a és $b \neq 0$ egész számokhoz léteznek olyan egyértelműen meghatározott q és r számok melyekre igaz, hogy:

$$a = b * q + r \text{ és } 0 \leq r < |b|.$$

Legnagyobb közös osztó

Az a és b számok legnagyobb közös osztója d , ha

- $d|a, d|b$; és
- ha egy c -re $c|a, c|b$ teljesül, akkor $|c| \leq |d|$.

Jelölés: $d = (a, b)$ vagy $d = \text{Inko}(a, b)$ vagy $d = \text{Inko}\{a, b\}$.

Ha $a = b = 0$, akkor definíció szerint a legnagyobb közös osztó 0.

Euklideszi algoritmus

Bármely két egész számnak létezik legnagyobb közös osztója.

Bizonyítás: Euklideszi algoritmus.

Algoritmus:

Az egyik számot maradékosan elosztjuk a másikkal, majd a másik számot a maradékkal stb., mindig az osztót a maradékkal, amíg 0 maradékhoz nem jutunk.

k	0	1	2	3	4
r_k	139	14	13	1	0
q_k	-	9	1	13	

1.2.2 Kibővített Euklideszi algoritmus

Tétel: Az a és b számok legnagyobb közös osztója alkalmas x, y egészekkel kifejezhető $(a, b) = ax + by$ alakban.

$x_0=1, x_1=0, y_0=0, y_1=1$ definíció szerint

$$x_{k+1} = x_k * q_k + x_{k-1} \quad \rightarrow x = (-1)^n * x_n$$

$$y_{k+1} = y_k * q_k + y_{k-1} \quad \rightarrow y = (-1)^{n+1} * y_n$$

k	0	1	2	3 (n)	4
r_k	139	14	13	1	0
q_k	-	9	1	13	
x_k	1	0	1	1	
y_k	0	1	9	10	

$$(a, b) = ax + by$$

$$x = (-1)^3 * 1 = -1 \quad y = (-1)^4 * 10 = 10$$

$$1 = 139 * (-1) + 14 * 10$$

Feladatok

- Keresse meg a 45 és a 211 legnagyobb közös osztóját. Használja a kibővített euklideszi algoritmust, majd ellenőrizze az eredményt.
Inko(211, 45)
- Adott két szám (2340, 113). Határozzuk meg a legnagyobb közös osztóját, x és y -t az alábbi egyenlethől $(a,b) = ax+by$ (ahol Inko = (2340, 113))
- Oldja meg az alábbi egyenletet használva a kibővített euklideszi algoritmust: Inko(1491, 23)=1491*
 $x + 23 * y$

1.2.3 Gyorshatványozás

Sok esetben – többek között a majd ismertetésre kerülő RSA algoritmusban – szükség van egészek hatványa valamely modulus szerinti maradékának meghatározására. Az alábbi módszer alkalmazásával viszonylag kevés művelet elvégzésével megkapjuk a^b modulo m értékét, ahol a egész szám, b 1-nél nagyobb egész, m pozitív egész.

Algoritmus:

1. A kitevőt felírjuk 2 hatványainak összegeként:

$$b = 2^{b_1} + 2^{b_2} + \dots + 2^{b_r}$$

2. Ismételt négyzetre emeléssel számoljuk ki a következő értékeket: $a^{2^0}, a^{2^1}, \dots, a^{2^r}$

$$a^{2^{k+1}} = a^{2^k \cdot 2} = (a^{2^k})^2$$

3. Megkapjuk a keresett hatványt:

$$a^b = a^{2^{b_1}} * a^{2^{b_2}} * \dots * a^{2^{b_r}} \pmod{m}$$

Példa

Számoljuk ki $6^{73} \pmod{100}$ értékét!

A kitevő 2 hatványainak összegeként:

$$73 = 2^6 + 2^3 + 2^0$$

Ismételt négyzetre emelések:

$$6^{2^0} \equiv 6 \pmod{100}$$

$$6^{2^1} \equiv 36 \pmod{100}$$

$$6^{2^2} \equiv 96 \pmod{100}$$

$$6^{2^3} \equiv 16 \pmod{100}$$

$$6^{2^4} \equiv 56 \pmod{100}$$

$$6^{2^5} \equiv 36 \pmod{100}$$

$$6^{2^6} \equiv 96 \pmod{100}$$

A keresett hatványérték:

$$6^{73} = 6^{2^6} * 6^{2^3} * 6^{2^0} = 96 * 16 * 6 \equiv 16 \pmod{100}$$

Feladatok

Gyors hatványozással számolja ki az alábbi értékeket:

- $9^{22} \pmod{79}$,
- $129^{97} \pmod{171}$,
- $23^{209} \pmod{211}$.

1.2.4 Fermat-teszt

Valószínűségi prímteszt, mely a kis Fermat-tételre alapul.

Tétel: Ha p prím és $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$.

Algoritmus:

- Választok egy a -t.
- Kiszámoljuk az $a^{p-1} \pmod{p}$ értéket.
- Ha $a^{p-1} \not\equiv 1 \pmod{p}$ akkor p összetett

Ha p összetett és $(a, p) = 1$ és $a^{p-1} \equiv 1 \pmod{p} \rightarrow p$ álprím az a bázisra nézve.

Ha p összetett és $\forall a$ esetén $(a, p) = 1$ és $a^{p-1} \equiv 1 \pmod{p} \rightarrow p$ Carmichael szám.

Példa

Teszteljük le Fermat prímtesztet alkalmazva a 341 számot (az alapok 2 és 3)! Mit tudunk mondani róla?

Legyen az alap a 2!

$$2^{340} \equiv 1 \pmod{341}$$

Legyen az alap a 3!

- $3^{2^0} \equiv 3 \pmod{341}$
- $3^{2^1} \equiv 9 \pmod{341}$
- $3^{2^2} \equiv 81 \pmod{341}$
- $3^{2^3} \equiv 82 \pmod{341}$
- $3^{2^4} \equiv 245 \pmod{341}$

- $3^{2^5} \equiv 9 \pmod{341}$
- $3^{2^6} \equiv 81 \pmod{341}$
- $3^{2^7} \equiv 82 \pmod{341}$
- $3^{2^8} \equiv 245 \pmod{341}$

Mivel $3^{340} \equiv 3^{2^8} \cdot 3^{2^6} \cdot 3^{2^4} \cdot 3^{2^1} \equiv 56 \pmod{341} \rightarrow$ nem prím

Feladat

- Teszteljük le Fermat prímtesztet alkalmazva a 181 számot, ha az alap a 7-! Mit tudunk mondani róla?
- Teszteljük le Fermat prímtesztet alkalmazva a 127 számot, ha az alap a 5-! Mit tudunk mondani róla?

1.2.5 Miller-Rabin prímteszt

A prímteszt 1-nél nagyobb, páratlan n -ekre működik.

Algoritmus:

Határozzuk meg S és d értékeket:

$$S = \max\{r : 2^r | (n - 1)\} \text{ és } d = (n - 1) / 2^S$$

Tétel: Ha n prím és $(a, n) = 1$, akkor

- $a^d \equiv 1 \pmod{n}$ vagy
- $\exists r \in \{0, \dots, S - 1\}$ hogy $a^{d \cdot 2^r} \equiv -1 \pmod{n}$

Példa

Két körös Miller-Rabin teszt segítségével mutassa meg, hogy a 561 prímszám-e vagy összetett (a bázisok legyenek: 2,13)!

$$S = 4 \quad \leftarrow 560 = 2 * 2 * 2 * 2 * 35$$

$$d = 35$$

$a = 2$ esetén:

- $2^{d*2^0} \equiv 263 \pmod{561}$

- $2^{d*2^1} \equiv 166 \pmod{561}$

- $2^{d*2^2} \equiv 67 \pmod{561}$

- $2^{d*2^3} \equiv 1 \pmod{561}$

A Miller-Rabin teszt alapján az n szám összetett.

$a = 13$ esetén:

- $13^{d*2^0} \equiv 208 \pmod{561}$

- $13^{d*2^1} \equiv 67 \pmod{561}$

- $13^{d*2^2} \equiv 1 \pmod{561}$

- $13^{d*2^3} \equiv 1 \pmod{561}$

A Miller-Rabin teszt alapján az n szám összetett.

Feladat

- Két körös Miller-Rabin teszt segítségével mutassa meg, hogy a 197 prímszám-e vagy összetett (a bázisok legyenek: 7,12)!

- Két körös Miller-Rabin teszt segítségével mutassa meg, hogy a 243 prímszám-e vagy összetett (a bázisok legyenek: 11,15)!

1.2.6 Kínai maradéktétel

Legyenek az m_1, \dots, m_k modulusok páronként relatív prímelek. Ekkor az

$$x \equiv c_1 \pmod{m_1}$$

$$x \equiv c_2 \pmod{m_2}$$

...

$$x \equiv c_k \pmod{m_k}$$

szimultán kongruenciarendszer bármilyen c_1, \dots, c_k egészek esetén megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo $m_1 * m_2 * \dots * m_k$.

Algoritmus:

- $M = m_1 \cdot \dots \cdot m_k$
- $M_i = M/m_i$ ahol $i = 1, 2, \dots, k$
- Legyen y_i egész szám az alábbi kongruencia megoldása
 $y_i * M_i \equiv 1 \pmod{m_i}$ ahol $i = 1, \dots, k$
- $x \equiv \sum c_i * y_i * M_i \pmod{M}$

Példa

- $x \equiv 0 \pmod{5} \rightarrow M_1 = 60/5 = 12$
 $x \equiv 1 \pmod{3} \rightarrow M_2 = 60/3 = 20$
 $x \equiv 2 \pmod{4} \rightarrow M_3 = 60/4 = 15$

- $M = 5 * 4 * 3 = 60$

- $12 * y_1 \equiv 1 \pmod{5}$ $20 * y_2 \equiv 1 \pmod{3}$ $15 * y_3 \equiv 1 \pmod{4}$
 $2 * y_1 \equiv 1 \pmod{5}$ $2 * y_2 \equiv 1 \pmod{3}$ $3 * y_3 \equiv 1 \pmod{4}$
 $2 * y_1 \equiv 6 \pmod{5}$ $2 * y_2 \equiv 4 \pmod{3}$ $3 * y_3 \equiv 9 \pmod{4}$
 $y_1 \equiv 3 \pmod{5}$ $y_2 \equiv 2 \pmod{3}$ $y_3 \equiv 3 \pmod{4}$

- $x \equiv \sum c_i * y_i * M_i \pmod{M}$
 $x \equiv 0 * 3 * 12 + 1 * 2 * 20 + 2 * 3 * 15 \equiv 130 \equiv 10 \pmod{60}$

RSA Példa

Az RSA esetében a titkosított üzenet visszafejtéséhez az alábbi kongruencia rendszerre alkalmazzuk a kínai maradéktételt:

$$m \equiv c_1 \pmod{p}$$

$$m \equiv c_2 \pmod{q}$$

- $c_1 \equiv c^{d \pmod{p-1}} \pmod{p}$
 $c_2 \equiv c^{d \pmod{q-1}} \pmod{q}$
- $M = p \cdot q$

- $M_1 = q, M_2 = p$
- $1 = y_1 \cdot q + y_2 \cdot p$
- $m \equiv c_1 \cdot y_1 \cdot M_1 + c_2 \cdot y_2 \cdot M_2 \pmod{M}$

Adottak a következő adatok:

- $p = 5$ véletlen prím
- $q = 11$ véletlen prím
- $n = 55$ modulus
- $\phi(n) = 40$
- $c = 15$ titkosított üzenet
- $d = 23$ visszafejtő kulcs

$$c_1 = 15^{23} \pmod{4} \equiv 0 \pmod{5}$$

$$c_2 = 15^{23} \pmod{10} \equiv 9 \pmod{11}$$

$$M_1 = q = 11 \quad M_2 = p = 5 \quad M = 55$$

$$y_1 * 5 \equiv 1 \pmod{11}$$

$$y_2 * 11 \equiv 1 \pmod{5} \rightarrow \text{Euklideszi algoritmus}$$

k	0	1	2	
qk	11	5	1	0
rk	-	2	5	
xk	1	0	1	
yk	0	1	2	

$$x = (-1)^2 * 1 = 1$$

$$y = (-1)^3 * 2 = -2$$

$$m \equiv \sum c_i * y_i * M_i \pmod{M}$$

$$0 * 1 * 11 + 9 * -2 * 5 \equiv -90 \equiv 20 \pmod{55}$$

$m = 20$ nyílt üzenetet $e = 7$ nyilvános kulccsal lehet ellenőrizni, hogy $c = 15$ titkosított üzenetet kapjuk-e vissza

Feladatok

- Legyenek a prímek 7 és 13, valamint 17 a titkos exponens. Fejtsük vissza a a 82 titkosított üzenetet a kínaimaradék tétel segítségével!
- Fejtsük vissza a 6 RSA-val titkosított üzenetet a kínai maradék tétel alkalmazásával, ha ismerjük a két prímet:7,13 és a visszafejtő exponens 19!

1.3 RSA feladatok

- Generáljon egy RSA titkosításhoz titkos és nyilvános kulcspárt amennyiben a két választott prímszám a következő: a 463 és az 547, és a titkosító exponens egyike a következő számoknak a feltételeknek megfelelően: 12,47,76,93.
- Fejtsük vissza a 85 RSA-val titkosított üzenetet a kínai maradék tétel alkalmazásával, ha ismerjük a két prímet:7,13 és a visszafejtő exponens 47!
- Bizonyítsa be, hogy ha egy nyílt üzenetet titkosítjuk az (n,e) és (n,f) RSA nyilvános kulccsal, ahol e és f relatív prímek, akkor a nyilvános információk alapján a nyílt üzenet kiszámítható!

Chapter 2

Megoldások

2.1 RSA megoldásai

2.1.1 Euklideszi algoritmus megoldások

$$(a, b) = ax + by$$

- $1 = 211 * 16 + 45 * -75,$
- $1 = 2340 * (-24) + 113 * 497,$
- $1 = 1491 * (-6) + 23 * 389 .$

2.1.2 Gyors hatványozás megoldásai

- $9^{22} \equiv 73 \pmod{79} ,$
- $129^{97} \equiv 108 \pmod{171} ,$
- $23^{209} \equiv 156 \pmod{211} .$

2.1.3 Fermat-teszt megoldásai

- $7^{180} \equiv 1 \pmod{181}$

Fermat-teszt alapján nem lehet egyértelműen kijelenteni, hogy összetett vagy prím-e a szám

- $5^{126} \equiv 1 \pmod{127}$

Fermat teszt alapján nem lehet egyértelműen kijelenteni, hogy összetett vagy prím-e a szám

2.1.4 Miller-Rabin megoldásai

- $a = 7$ esetén: $S = 2, d = 49 \quad 7^{49} \equiv 196 \pmod{197}$

A Miller-Rabin alapján $a=7$ bázisra nézve a szám valószínűleg prím

$a = 12$ esetén:

$$12^{49} \equiv 14 \pmod{197}$$

$$(12^{49})^{2^1} \equiv 196 \pmod{197}$$

A Miller-Rabin alapján a 12 bázisra nézve a szám valószínűleg prím

- $a = 11$ esetén: $S = 1, d = 121$

$$11^{121} \equiv 47 \pmod{243}$$

A Miller-Rabin alapján a 11 bázisra nézve a szám összetett

$a = 15$ esetén:

$$15^{121} \equiv 0 \pmod{197}$$

A Miller-Rabin alapján a 15 bázisra nézve a szám összetett

2.1.5 Kínai maradéktétel megoldásai

- 10
- 20

2.1.6 RSA megoldásai

- $n = 253261, \phi(n) = 252252, e = 47, d = 166379$

$$PK = (253261, 47) \quad SK = (253261, 166379)$$

- $n = 91$

Lineáris kongruencia:

$$m \equiv 85^{47 \pmod{6}} \pmod{7}$$

$$m \equiv 85^{47 \pmod{12}} \pmod{13}$$

$$m \equiv c_1 \cdot y_1 \cdot M_1 + c_2 \cdot y_2 \cdot M_2 = 1 \cdot (-1) \cdot 13 + 2 \cdot 2 \cdot 7 \equiv 15 \pmod{91}$$