Adatstruktúrák és Algoritmusok

5. gyakorlat

Az RSA algoritmus

A gyakorlat felépítése

- A MODHAT (moduláris hatványozás algoritmus ismertetése);
- Az RSA algoritmus ismertetése;
- Az RSA algoritmus matematikai alapjai (kihagyható);
- Primtesztek, Carmichael számok;

A moduláris algoritmus

A MODHAT algoritmus az $\mathrm{mod}(a^b, m)$ értékét számolja ki.
INPUT: $a \in \mathbb{Z}_+$, $b \in \mathbb{Z}_+$, $n \in \mathbb{Z}_+$. A b szám a 2-es számrendszerben

$$b = b_k b_{k-1}, \ldots, b_0 \qquad \text{azaz} \qquad b = \sum_{i=0}^{k} b_i 2^i.$$

OUTPUT: $c = \mathrm{mod}(a^b, m)$.

	MODHAT(a,b,m $\parallel$ c)
1.	$c \longleftarrow 1$
2.	FOR $i \longleftarrow k$ DOWNTO 0 DO
3.	$\quad c \longleftarrow \mathrm{mod}(c^2, m)$
4.	$\quad$ IF $b_i = 1$ THEN
5.	$\quad\quad c \longleftarrow \mathrm{mod}(ca, m)$
6.	RETURN(c)

Feladat

Számoljuk ki a $\mathrm{mod}(63^{90}, 17)$ *értékét.*
Először átírjuk a 90-et 2-es számrendszerbe. $90 = 1011010_{②}$.
Ezt követően alkalmazzuk a MODHAT algoritmust.

b_i	$\mathrm{mod}(c^2, 17)$	$\mathrm{mod}(63c, 17)$
1	$\mathrm{mod}(1^2, 17) = 1$	$\mathrm{mod}(63 \cdot 1, 17) = 12$
0	$\mathrm{mod}(12^2, 17) = 8$	—
1	$\mathrm{mod}(8^2, 17) = 13$	$\mathrm{mod}(63 \cdot 13, 17) = 3$
1	$\mathrm{mod}(3^2, 17) = 9$	$\mathrm{mod}(63 \cdot 9, 17) = 6$
0	$\mathrm{mod}(6^2, 17) = 2$	—
1	$\mathrm{mod}(2^2, 17) = 4$	$\mathrm{mod}(63 \cdot 4, 17) = 14$
0	$\mathrm{mod}(14^2, 17) = 9$	—

Tehát $\mathrm{mod}(63^{90}, 17) = 9$.

Feladat

Számoljuk ki a $\mathrm{mod}(2^{40}, 41)$ *értékét.*
Először átírjuk a 40-et 2-es számrendszerbe. $40 = 1010000_{②}$.
Ezt követően alkalmazzuk a MODHAT algoritmust.

b_i	$\mathrm{mod}(c^2, 41)$	$\mathrm{mod}(2c, 41)$
1	$\mathrm{mod}(1^2, 41) = 1$	$\mathrm{mod}(2 \cdot 1, 41) = 2$
0	$\mathrm{mod}(2^2, 41) = 4$	—
1	$\mathrm{mod}(4^2, 41) = 16$	$\mathrm{mod}(2 \cdot 16, 41) = 32$
0	$\mathrm{mod}(32^2, 41) = 40$	—
0	$\mathrm{mod}(40^2, 41) = 1$	—
0	$\mathrm{mod}(1^2, 41) = 1$	—

Tehát $\mathrm{mod}(2^{40}, 17) = 1$, *de ez számolgatás nélkül is látható a kis Fermat tétel alapján.*

Az RSA algoritmus

- RSA algoritmust Ron Rivest, Adi Shamir és Leonard Adleman által kidolgozott titkosítási eljárás. Az eljárás matematikai alapja az, hogy a prímfaktorizáció, azaz egy nagy egész szám prímszámok szorzataként való felbontása a jelenleg rendelkezésre álló számítógépekkel és algoritmusokkal nem megoldható.
- A szükséges matematikai előismeret annak a ténynek az ismerete, hogy ha p, q prímszámok, a egy olyan egész szám, amelyre $\mathrm{lnko}(a, pq) = 1$, akkor

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

Ettől a képlettől működik az RSA algoritmus.

Alice üzenetet ír Bobnak.

- M az üzenet;
- C a titkosított üzenet;

ugyanis Alice azt szeretné, ha az üzenetét csak Bob tudná dekódolni. Titkosítani a P, dekódolni az S függvénnyel fogunk. Azaz

$$P(M) = C, \qquad P = P(n, e) \qquad S = S(n, d) \qquad S(C) = M.$$

A P és az S függvények egymás inverzei, ugyanis

$$M = S(C) = S(P(M)) = (S \circ P)(M).$$

- A szöveges üzenetből először egy bitsorozatot készítünk, ami a kettes számrendszerben egy pozitív egész szám. Ez a szám az M.
- Titkosítani az n és e pozitív egészekkel fogunk. Ezek nyilvánosak, mindenki számára láthatóak, **tehát az n és e számok segítségével mindenki tud titkosítani**.
- Fontos még, hogy $\mathrm{lnko}(M, n) = 1$ teljesüljön, azonban ez könnyen elérhető, (az n két nagy prímszám szorzata, ha ezeknél a prímeknél kisebb az M szám, akkor biztosan teljesül, hogy $\mathrm{lnko}(M, n) = 1$. Ebből arra következtethetünk, hogy hosszú üzenet titkosítására nincs lehetőségünk, de ez nincs így, a hosszú üzenetet részekre bontjuk, a részek már titkosíthatók.)

Titkosítás

A titkosítás a következő módon történik:

$$\boxed{C = P(M) = \mathrm{mod}(M^e, n)}$$

(szavakba öntve: az M et az e-edik hatványra emeljük és vesszük a kapott szám n modulus szerinti maradékát.) Ez a MODHAT algoritmussal könnyen elvégezhető, mivel a MODHAT algoritmus gondoskodik arról, hogy a hatvány "ne szálljon el", azaz végig kezelhető méretű maradjon.

- Bob megkapja a titkosított üzenetet, azaz azt, hogy C. Ahhoz, hogy **dekódolni** tudja az üzenetet, **szüksége van az** n **és** d számokra.
- A d az n és az e számokból számolható.
- Az n két prím szorzata, $n = pq$. A p és q prímeket csak Alice és Bob ismerik. Az $\mathrm{lnko}(M, n = pq) = 1$ feltétel teljesüléséhez elegendő, ha az M szám számjegyeinek a száma a p és a q számjegyeinek a számánál is kisebb.
- A dekódoláshoz először ki kell számolni az f értékét:

$$f = (p - 1)(q - 1),$$

  majd az d értékét.
- A d szám az e szám f modulusra vonatkozó multiplikatív inverze. Ehhez persze teljesülnie kell az $\mathrm{lnko}(e, f) = 1$ feltételnek, ennek megfelelően az e számot eleve így kell megválasztanunk.

A dekódolás a következő módon történik:

$$\boxed{S(C) = \mathrm{mod}(M^d, n).}$$

A működés tényleg nagyon egyszerű, csak két dolgot kell megjegyezni hozzá:

- a d az e szám f-re vonatkozó multiplikatív inverze, azaz létezik olyan k egész szám, amellyel $de = 1 + kf$;
- $f = (p-1)(q-1)$, így alkalmazható a kis Fermat tételt követő következmény.

Azt is idézzük fel, hogy

$$S(C) = C^d = (M^e)^d = M^{ed} = M^{1+kf} = M(M^{(p-1)(q-1)})^k,$$

amiből kapjuk, hogy

$$\mathrm{mod}(C^d, n) = \mathrm{mod}(M(M^{(p-1)(q-1)})^k, n) = M.$$

Feladat

Legyen $M = 65$ az üzenet, amit Alice küld a Bobnak, $n = 899$ és $e = 11$. Ezek nyilvánosak. Az n prímfaktorizációja szigorúan titkos, ezt csak Alice és Bob ismerik.
$n = 899 = 29 \cdot 31$, azaz $p = 29$, $q = 31$.
$f = (p-1)(q-1) = 28 \cdot 30 = 840$.
Ekkor $\mathrm{lnko}(M, n) = \mathrm{lnko}(65, 899) = 1$ és
$\mathrm{lnko}(e, f) = \mathrm{lnko}(11, 840) = 1$, tehát teljesülnek a titkosítás és a dekódolás feltételei.
Először titkosítsunk: $C = P(M) = \mathrm{mod}(M^e, n)$, ami a moduláris hatványozás algoritmussal számolható.

b_i	$\mathrm{mod}(c^2, 899)$	$\mathrm{mod}(65c, 899)$
1	$\mathrm{mod}(1^2, 899) = 1$	$\mathrm{mod}(65 \cdot 1, 899) = 65$
0	$\mathrm{mod}(65^2, 899) = 629$	—
1	$\mathrm{mod}(629^2, 899) = 81$	$\mathrm{mod}(65 \cdot 81, 899) = 770$
1	$\mathrm{mod}(770^2, 899) = 459$	$\mathrm{mod}(65 \cdot 459, 899) = 168$

Tehát a tikosított üzenet: $C = 168$.

Most nézzük meg, hogy Bob tudja-e dekódolni az üzenetet. Ehhez először számoljuk ki d-t, ami az e-nek az $f$re vonatkozó multiplikatív inverze. Ez kibővített euklideszi algoritmussal számolható.

e_k	f_k	q_k	r_k	d^*	x^*	y^*
11	840	0	11	1	-229	$3 - 0 \cdot (-229) = 3$
840	11	76	4	1	3	$-1 - 76 \cdot 3 = -229$
11	4	2	3	1	-1	$1 - 2 \cdot (-1) = 3$
4	3	1	1	1	1	$0 - 1 \cdot 1 = -1$
3	1	3	0	1	0	$1 - 3 \cdot 0 = 1$
1	0	–	–	1	1	0

Ellenőrzés: $11 \cdot (-229) + 840 \cdot 3 = 1$. Tehát $d = -229 + 840 = 611$.

A dekódoláshoz az $S(C) = \mathrm{mod}(C^d, n)$, ami a moduláris hatványozás algoritmussal számolható.

b_i	$\mathrm{mod}(c^2, 899)$	$\mathrm{mod}(168c, 899)$
1	$\mathrm{mod}(1^2, 899) = 1$	$\mathrm{mod}(168 \cdot 1, 899) = 168$
0	$\mathrm{mod}(168^2, 899) = 355$	—
0	$\mathrm{mod}(355^2, 899) = 165$	—
1	$\mathrm{mod}(165^2, 899) = 255$	$\mathrm{mod}(168 \cdot 255, 899) = 587$
1	$\mathrm{mod}(587^2, 899) = 252$	$\mathrm{mod}(168 \cdot 252, 899) = 83$
0	$\mathrm{mod}(83^2, 899) = 596$	—
0	$\mathrm{mod}(596^2, 899) = 111$	—
0	$\mathrm{mod}(111^2, 899) = 634$	—
1	$\mathrm{mod}(634^2, 899) = 103$	$\mathrm{mod}(168 \cdot 103, 899) = 223$
1	$\mathrm{mod}(223^2, 899) = 284$	$\mathrm{mod}(168 \cdot 284, 899) = 65$

Tehát az eredeti üzenet "$M = 65$" volt.

Matematikai alapok az RSA algoritmus működéséhez

Mint ahogy azt a korábbi részben említettük, az RSA algoritmus működése az

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

képlet ismerete, ahol p, q (különböző) prímszámok, a egy olyan egész szám, amelyre $\mathrm{lnko}(a, pq) = 1$. Most megnézzük hogyan jön ki ez a tétel. (Ez az a bizonyos kihagyható rész.)

Ez az összefüggés valahogy kiszenvedhető az úgynevezett kis Fermat tételből, azonban az elegáns út a bizonyításhoz az Euler-Fermat tételen keresztül vezet.

Kis Fermat tétel

Theorem

Ha p prím, $a \in \mathbb{Z}$ úgy, hogy $\mathrm{lnko}(a, p) = 1$ (azaz a p prím nem osztója az a számnak), akkor

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

A kis Fermat tétel könnyen kijön az alábbi egyszerűbb állításból:

Állítás *Ha p prím, $a \in \mathbb{Z}_+$, akkor $a^p \equiv a$ modulo (p).*

Az Euler-Fermat tétel

Ha $a \in \mathbb{Z}$, $n \in \mathbb{Z}_+$, $n > 1$, $\mathrm{lnko}(a, n) = 1$, *akkor*

$$a^{\varphi(n)} \equiv 1 \qquad \mod (n)$$

A φ egy számelméleti függvény, amely tetszőleges n nemnegatív egész számhoz a $0, 1, \ldots, n-1$ sorozatban n-hez relatív prímek számát rendeli.

- Könnyű látni, hogyha $n = pq$, azaz az n két prímszám szorzata, akkor $\varphi(n) = (p-1)(q-1)$.
- Tehát az f az RSA algoritmusban nemcsak azért f, mert a d, e után az jön az ábécé-ben, hanem azért is, mert az f az n-nek a φ-je.

A

Most tekintsük az Euler Fermat tétel bizonyítását.
Legyenek a és n olyanok, mint az Euler-Fermat tételben. Tekintsük a $\mathbb{Z}_n$ maradékosztály gyűrűt. Ez a szorzásra nézve egy félcsoportot alkot. Az invertálható elemek ennek a félcsoportnak egy részcsoportját alkotják.
Tehát Z_n-ben azok a maradékosztályok, amelyek n-hez relatív prímek, csoportot alkotnak, amelyet redukált maradékosztály csoportnak nevezünk. Ennek a csoportnak a rendje (elemeinek a száma) éppen $\varphi(n)$.
Lagrange tétele szerint elem rendje osztója a csoport rendjének.
Ehhez megint kell két definíció, csoport rendje, elem rendje.

Egy $G = G(\cdot)$ csoport rendjének a G halmaz számosságát nevezzük.
Ha $g \in G$ és G véges halmaz, azaz G véges rendű csoport, akkor létezik olyan $n \in \mathbb{Z}_+$, amelyre $g^n = 1$, ahol 1 jelöli a multiplikatív egységet.
A fentiek alapján tudjuk értelmezi az $g \in G$ elem rendjét, amit $|g|$ módon jelölünk és

$$|g| := \min\{z \in \mathbb{Z}_+ | g^z = 1\}$$

módon értelmezünk.
Így kapjuk, hogyha a és n relatív prímek, akkor Lagrange tétel alapján (elem rendje osztója a csoport rendjének)

$$a^{\varphi(n)} \equiv 1 \mod (n),$$

tehát a tételt bebizonyítottuk.

A kis Fermat tételen alapuló prímteszt

- A kis Fermat tétel azt mondja ki, hogyha p prím és $\text{lnko}(a, p) = 1$, akkor $a^{p-1} \equiv 1 \mod (p)$. Ebből kontrapozícióval kapjuk, hogyha $\text{lnko}(a, p) = 1$ de $a^{p-1} \not\equiv 1 \mod (p)$, akkor p nem prím.
- Tehát, ha egy pozitív egész szám megbukik egy ilyen prímteszten, akkor az biztosan összetett szám, tehát nem prím. Ha azonban átmegy egy ilyen prímteszten, akkor még nem biztos, hogy prím.
- Azok a számok, amelyek az összes kis Fermat tételen alapuló prímteszten átmennek, mégsem prímek, az úgynevezett Carmichael számok. Ezek száma végtelen. Ilyen szám például az 561, amelyet maga Carmichael talált meg 1910-ben.

Álprímek

A $p \in \mathbb{Z}_+$, $p > 1$ *számot* ***álprím****nek nevezzük, ha létezik* $a \in \mathbb{Z}_+$ *úgy, hogy* $\mathrm{lnko}(a, p) = 1$ *és*

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

de p *nem prím.*

Charmichael számok

A $p \in \mathbb{Z}$, $p > 1$ számot Carmichael számnak nevezzük, ha

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

minden olyan $a \in \mathbb{Z}_+$ esetén, amelyre $\mathrm{lnko}(a, p) = 1$, de p nem prím, azaz a ***Charmichael számok*** *azok az 1-nél nagyobb pozitív egész számok, amelyek minden olyan prímteszten átmennek, amelyek a kis Fermat tételen alapulnak, mégsem prímek.*

Charmichael számok: 561, 1105, 1729, 2465, 2821, 6601, 8911, ... végtelen sok van belőlük.

KÖSZÖNÖM A FIGYELMET!