ELTE IK Diszkrét modellek alkalmazásai

10. gyakorlat

Koch-Gömöri Richárd

2021. november 24.

Eml: faktorizáció

Adja meg a 42 egész szám prímtényezős felbontását. (faktorizáció)
$42 = 2 \cdot 3 \cdot 7$

$150 = 2 \cdot 3 \cdot 5^2$

ált. prímtényezős alak: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$
a 150 esetében $k = 3, p_1 = 2, a_1 = 1, p_2 = 3, a_2 = 1, p_3 = 5, a_3 = 2$

A számelmélet alaptétele miatt minden természetes számnak létezik prímtényezős felbontása.

Euler-féle φ-függvény

def (Euler-féle φ-függvény): $n \in \mathbb{N}$ esetén $\varphi(n)$ eredménye az n-nél kisebb, n-hez relatív prímek száma.

pl. $\varphi(8)$ kiszámításához:

$1, 2, 3, 4, 5, 6, 7 \implies \varphi(8) = 4$

tétel: Ha $n > 1$ természetes szám, és n prímtényezős felbontása

$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ akkor $\varphi(n) = n \cdot \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$

pl. 8 prímtényezős felbontása: 2^3

$$\varphi(8) = 8 \cdot \left(1 - \frac{1}{2}\right) = 8 \cdot \frac{1}{2} = 4$$

$\implies \varphi(n)$ kiszámolásához n faktorizációja szükséges

Euler-féle φ-függvény

$\varphi(n)$ kiszámításához n faktorizációja (prímtényezős felbontása) szükséges

1 kivétel:

ha n prímszám ugyanis ekkor $\varphi(n) = n - 1$

pl. 53471161 prímszám, $\varphi(53471161) = 53471161 - 1 = 53471160$

tétel: Ha $a, b \in \mathbb{N}$ relatív prímek, akkor $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

$n = p_1 \cdot p_2$ esetben

$\varphi(n) = \varphi(p_1 \cdot p_2) = \varphi(p_1) \cdot \varphi(p_2) = (p_1 - 1) \cdot (p_2 - 1)$

Euler-féle φ-függvény

pl. $\varphi(35) = ?$

$35 = 5 \cdot 7$

$\varphi(35) = \varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = 4 \cdot 6 = 24$

bővített euklideszi algoritmus

Keressük meg $\mathrm{lnko}(2004, 56)$-t

$\mathrm{lnko}(2004, 56) = 4$

Ekkor a 4 felírható 2004 és 56 lineáris kombinációjaként azaz:

Létezik $U, V \in \mathbb{Z}: \quad 4 = 2004 \cdot U + 56 \cdot V$

bővített euklideszi algoritmussal: $U = -5, V = 179$

Diofantikus egyenlet

def (Diofantikus egyenlet): Ismert a, b, c egész számok és x, y egész ismeretlenek esetén az $ax + by = c$ egyenletet diofantikus egyenletnek nevezzük.
RSA-ban csak olyan diofantikus egyenletek megoldására van szükségünk, ahol $c = 1$

Oldjuk meg például a $2x + 5y = 1$ egyenletet.
$\mathrm{lnko}(2, 5) = 1 \mid 1 \implies$ megoldható
bővített euklideszi algoritmussal: $\mathrm{lnko}(2, 5) = 1 = -2 \cdot 2 + 1 \cdot 5$ tehát $U = -2, V = 1$
ekkor a megoldás:
$x = -b \cdot t + U$, $y = a \cdot t + V$, ahol $t \in \mathbb{Z}$ tetszőleges

a feladatban:
$x = -5t - 2$
$y = 2t + 1$
ahol $t \in \mathbb{Z}$ tetszőleges

Diofantikus egyenlet

Oldjuk meg például a $2x + 5y = 1$ egyenletet.

$x = -5t - 2$

$y = 2t + 1$

ahol $t \in \mathbb{Z}$ tetszőleges

pl. $t = 1$ esetén:

$x = -5 \cdot 1 - 2 = -7$

$y = 2 \cdot 1 + 1 = 3$

pl. $t = 2$ esetén:

$x = -5 \cdot 2 - 2 = -12$

$y = 2 \cdot 2 + 1 = 5$

nyilvános/aszimmetrikus kulcsú titkosítás

RSA kulcsgenerálás

elő kell állítani alkalmas n, e, d értékeket

n, e nyilvánosságra hozható, d nem

$\Longrightarrow$ d-t úgy kell generálni, hogy n, e ismeretében d-t nehéz legyen megkeresni

d generálásához újabb one-way function szükséges:

válasszunk p_1, p_2 prímszámokat

legyen $n := p_1 \cdot p_2$

$n = p_1 \cdot p_2$ szorzat kiszámítása könnyű

ha n ismert, p_1, p_2 ismeretlen, akkor $n = p_1 \cdot p_2$ prímtényezőkre bontás (faktorizálás) nehéz

a számelmélet alaptétele miatt a prímtényezős felbontás biztosan létezik, és ez a felbontás egyértelmű

Euler-tétel

Legyen $n \in \mathbb{N}, m \in \mathbb{Z}$, $lnko(n, m) = 1$. Ekkor $m^{\varphi(n)} \equiv 1 \pmod{n}$

pl. $n = 8, m = 5, lnko(8, 5) = 1$
$5^{\varphi(8)} \equiv 1 \pmod 8$
$5^4 \equiv 1 \pmod 8$
$625 \equiv 1 \pmod 8$ igaz

Euler-tétel (mod nélküli írásmóddal): $m^{\varphi(n)} = 1 \ \ (n)$
$1^k = 1 \implies m^{k \cdot \varphi(n)} = 1 \ \ (n)$
$1 \cdot m = m \implies m^{k \cdot \varphi(n)+1} = m \ \ (n)$
korábban láttuk hogy $m = m^{e \cdot d} \ \ (n)$
d-t kifejezve: $d = \dfrac{k \cdot \varphi(n) + 1}{e} \ \ (n)$

RSA publikus kulcs, privát kulcs

$$d = \frac{k \cdot \varphi(n) + 1}{e} \ \ (n)$$

ha n prímtényezős alakja ismert, akkor $\varphi(n)$-t könnyű kiszámolni, így d kiszámítása könnyű

a kulcsgeneráló $n = p_1 \cdot p_2$ felbontásból könnyedén kiszámolja $\varphi(n)$-t, azonban aki nem ismeri p_1, p_2-t annak faktorizálnia kell(ene) n-t

(n, e) publikus kulcs (public key), d privát kulcs (private key)

ez egy aszimmetrikus titkosítás (asymmetric public-private key cryptosystem), röviden nyilvános kulcsú titkosítás

(n, e) ismeretében bárki titkosíthat üzenetet, azt visszafejteni csak d ismeretében lehet

példa

Alice: Legyen $p_1 := 61, p_2 := 53$

Alice: $n = p_1 \cdot p_2 = 61 \cdot 53 = 3233$

Alice: $\varphi(n) = \varphi(3233) = \varphi(61) \cdot \varphi(53) = 60 \cdot 52 = 3120$

Alice: válasszunk kicsi e-t, amire $lnko(e, 3120) = 1$

Alice: pl. $e := 17$ alkalmas

Alice: d-t előállító képlet: $d = \dfrac{k \cdot 3120 + 1}{17}$

Alice: rendezzük: $17 \cdot d - 3120 \cdot k = 1$

Alice: bővített euklideszi algoritmussal: $k = 15, d = 2753$

Alice: publikus kulcs: $(3233, 17)$, privát kulcs: 2753

példa

eml. titkosítás: $c = m^e \mod n$, visszafejtés: $c^d \mod n = m$

Alice: publikus kulcs: $(3233, 17)$, privát kulcs: 2753

Alice nyilvánosságra hozza a publikus kulcsát: $(3233, 17)$

Bob: titkosítsuk az $m = 65$ üzenetet

Bob: titkosítás: $c = 65^{17} \mod 3233 = 2790$

Bob "2790" $\Longrightarrow$ Alice

Alice: visszafejtés: $2790^{2753} \mod 3233 = 65$

RSA biztonság

a kulcsgeneráló $n = p_1 \cdot p_2$ felbontásból könnyedén kiszámolja $\varphi(n)$-t, azonban aki nem ismeri p_1, p_2-t annak faktorizálnia kell(ene) n-t

RSA-2048

2017 őszi adat:

- RSA-2048 faktorizálásához
- a legjobb (ismert) algoritmussal:

$2,5 \cdot 10^{30}$ év szükséges

$1,38 \cdot 10^{10}$ év a világegyetem életkora

$2,5 \cdot 10^{30}$ év $= 2500000000000000000000000000000$ év