# Algebrai/aritmetikai algoritmusok a kriptográfiában

Rónyai Lajos

2002. március 5.

Az előadáson bemutatott algoritmusok:

- RSA
- Rabin
- ElGamal
- Elliptikus

## 1 RSA (Rivest-Shamir-Adleman '78)

$p$, $q$ nagy prímek

$n = p \cdot q; e, d$ egészek

$\phi(n) = (p-1)(q-1)$

$e \cdot d \equiv 1 \bmod \phi(n)$

$a \in \mathbf{Z}_n^*$

$a^{\phi(n)} \equiv 1 \bmod n$

$a^{ed} \equiv a \bmod n$

Alice: ír

Bob: olvas

Alice: $n, e$

Bob: $e, d$ (esetleg $p, q$)

$\ddot{U}:= \mathbf{Z}_n^*, T := \mathbf{Z}_n^*$

$a \in \ddot{U}$ üzenet: $E(a) = a^e \bmod n$

$b \in T$ titkos üzenet: $D(b) = b^d \bmod n$

$D(E(a)) = (a^e)^d = a^{ed} \equiv a \bmod n$

Algoritmikus megfontolások:

- $e$-hez $d$-t Euklideszi algoritmus
- $E, D$ számítása gyors hatványozás

Biztonság:

Nehéz $n$-ből $p, q$-t megkapni

# 2 RABIN-kódolás '79

$n = p \cdot q, p = 4k + 3, q = 4l + 3$

$\ddot{U}= T = Z_n^*$ $n$-hez relatív prímek

Alice: $n$

Bob: $p, q$

$E(a) := a^2 \bmod n$

$D(b) := b$ négyzetgyöke mod$n$

Itt általában négy darab négyzetgyök létezik.

Kínai maradéktétel (Szün-Ce)

Pontosan 1 megoldás mod$n \begin{cases} x \equiv a_1 \bmod p \\ x \equiv a_2 \bmod q \end{cases}$

$Z_n \cong Z_p \oplus Z_q$ gyűrű izomorfia

$D(b)$ számításához elég

$x^2 \equiv b \bmod p \qquad$ 2 megoldás $x_1, x_2$

$x^2 \equiv b \bmod q \qquad$ 2 megoldás $y_1, y_2$

Keresett $\pm x_1 \oplus \pm y_1$

mod$p$ a gyökvonás hatékony

Állítás: Legyen $p = 4k + 3$ prím, $b$ négyzetszám mod$p$.

Ekkor $b$ négyzetgyökei mod$p$: $\pm b^{\frac{p+1}{4}}$

Kínai maradéktétel használata

$x \equiv a_1 \bmod p$

$x \equiv a_2 \bmod q$

$p' \equiv 1 \bmod p \qquad q' \equiv 1 \bmod q$

$p' \equiv 0 \bmod q \qquad q' \equiv 0 \bmod p$

$x := a_1 p' + a_2 q' \bmod pq$ a megoldás

Biztonság:

A felbontás nehéz

Gyengéje:

Választott üzenet támadás

# 3 Diszkrét logaritmus feladatok

Adott egy $G$ csoport és annak egy $\alpha$ eleme.

$\alpha \in < G, *, ^{-1}, 1 >$

$*$ asszociatív

1 egységelem: $1 * x = 1x = x * 1 = x$

$y * y^{-1} = 1$

$\beta \in < \alpha > = \{\alpha^i; \quad i \text{ egész}\}$

Ekkor $\beta = \alpha^k$ valamely $k$-ra.

Legkisebb ilyet jelöljük $log_\alpha \beta = k$

Adott $G, \alpha, \beta \in <\alpha>$.

Kell: $log_\alpha \beta$ értéke

Olyan $G$ hasznos, ahol ez nehéz.

Például:

$(\mathbf{Z}_p, +)$ könnyű

$(\mathbf{Z}_p^*, *)$ elég nehéz (alkalmas $p$-re)

$(\mathbf{F}_q^*, *)$ elég nehéz (alkalmas $q$-ra)

$(E, \oplus)$ ez tűnik a legnehezebbnek adott méret mellett, ahol $E$ véges elliptikus görbe

Diffie-Hellmann kulcscsere

A,B közös titok létrehozása

$\alpha, G$-t ismerik mindketten

$A$: véletlen $k$

$B$: véletlen $l$

$A \rightarrow B : \alpha^k$

$A \leftarrow B : \alpha^l$

$A$: $\alpha^{kl}$

$B$: $\alpha^{kl}$

Feltörése számelméleti feltételek mellett egyenértékű a diszkrét logaritmus feltörésével.

ElGamal kódolás

Bob: $\alpha, \beta, a$

$\alpha^a = \beta$

Alice: $\alpha, \beta, G$ - tud benne számolni

$\ddot{U}= G, T = G * G$

Üzenet küldése:

A választ véletlen $k$ egész számot

$x \in \ddot{U}$

$E(x,k) = (y_1, y_2)$

$y_1 = \alpha^k, y_2 = x \cdot \beta^k$

$(y_1, y_2) \in T$ esetén

$D(y_1, y_2) = y_2 \cdot y_1^{-a}$

Ez jó:

$D(E(x,k)) = x \cdot \beta^k \cdot \alpha^{-ak} = x \cdot \beta^k \cdot \beta^{-k} = x$

Üzenet nyújtás:

Titkos üzenet kétszer olyan hosszú, mint az üzenet: $T = G * G$

# 4 Elliptikus görbék/csoportok

Legyen $K$ egy test, char $K \neq 2, 3$.

Az $E: \; y^2 = x^3 + ax + b \quad a, b \in K$ alakú egyenlettel definiált síkbeli görbe elliptikus görbe a $K$ test felett.

$x^3 + ax + b$-nek nincs többszörös gyöke K-ban.

Szimmetrikus az $x$ tengelyre.

E-nek pontja még a $\infty$, aminek az $x$-re vonatkozó tükörképe önmaga.

Pontjain értelmezhető $\oplus$ művelet úgy, hogy $(G, \oplus)$ Abel-csoport.

$(E, \oplus)$ Euler szabálya alapján:

$P \oplus Q$ : a két pontot $(P, Q)$ összekötő egyenes görbével való metszéspontjának az $x$ tengelyre vonatkozó tükörképe.

Ha $P = Q$, akkor az összekötő egyenesükön a görbe $P$-beli érintőjét kell érteni.

$\infty$ játssza a 0 szerepét: a görbe tetszőleges $P, Q, R$ pontjaira $P \oplus Q = Q \oplus P$, $\infty \oplus P = P$, $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

Számunkra érdekes esetek:

$K = \mathbf{Z}_p = \mathbf{F}_p, p$ prím

$K = \mathbf{F}_{2^m}$

Hány pontja lehet $E$-nek?

[E. Artin sejtése vagy H. Hasse tétele] Ha $K = F_p$, $|\#E - (p+1)| \leq 2\sqrt{p}$

Tehát $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ tartományba eshet az elliptikus görbe pontszáma. A megfordítás is igaz, azaz a fenti tartományba eső számok tényleg megkaphatók elliptikus görbék pontszámaként:

[Deuring-Honda-Tate] Legyen $q = p^s$, $p$ prím. $a$ egész, $|a| \leq 2\sqrt{q}$. Ha $a \equiv 0 \bmod p$-ből következik $a^2 \equiv 0 \bmod q$, akkor létezik olyan $\mathbf{F}_q$ felett definiált $E$ elliptikus görbe, melyre $\#E - (q+1) = a$.

Az elliptikus görbék használata az ElGamal módszerben:

A kódolásban szereplő $G$ csoportnak az elliptikus görbe $(x, y)$ pontpárjain értelmezett csoportot választjuk.

$y^2 = x^3 + ax + b$

$\ddot{U} = \mathbf{F}_p$

Az elliptikus görbe pontjának $x$-koordinátájául az üzenetet választjuk.