Kódoláselmélet 2020 szeptember 16

1

RSA titkosítás

p, q különböző páratlan prímek, $n = pq$

$ed \equiv 1 \mod \varphi(n) = (p-1)(q-1)$

$E: \mathbb{Z}_n \to \mathbb{Z}_n$ $\quad\quad$ $D: \mathbb{Z}_n \to \mathbb{Z}_n$

$m \mapsto m^e$ $\quad\quad$ $m \mapsto m^d$

$$D(E(m)) = E(D(m)) = m^{ed} \equiv m \pmod n$$

<u>publikus kulcs</u>: e, n $\quad$ <u>titkos</u>: $d, p, q, \varphi(n)$

Feltörési lehetőségek

(1) ha tudjuk $E(m) = m^e$-t és e-t, akkor találgatással nem lehet megkeresni m-et, mert n nagy szám.

(2) Ha tudja faktorizálni az n számot pq-ra, akkor megvan $(p-1)(q-1)$ is és akkor e-ből megkaphatja d-t az

$$ex + (p-1)(q-1)y = 1$$

$\boxed{\text{lnko}(e,(p-1)(q-1))=1 \text{ maradék lehet negatív de abszolút értékben kicsi}}$

ez gyors, mert euklo számolás gyors

$\to$ diofantoszi egyenlet megoldásaként $(x = d)$ mint ahogy a kulcsot is generáltuk. De ismereteink szerint a prímfaktorizáció nehéz.

(3) $(p-1)(q-1)$-nek titkosnak kell lennie, mert segítségével d meghatározható, sőt

$n - (p-1)(q-1) = p + q - 1$ azaz a két prím összege is megvan, és n-ből ezt meg lehet oldani p és q-ra is.

Szerencsétlen paraméterek az RSA-hoz

Fixpontok: Ha $m = \pm 1$, akkor $E(m) = m^e = m$ mert e (és d) szükségképpen páratlan

$$ed \equiv 1 \mod \underbrace{(p-1)(q-1)}_{4\text{-el osztható}}$$

Mindig van még két másik fixpont

$$\left.\begin{array}{l} m \equiv 1 \mod p \\ \text{és } m \equiv -1 \mod q \end{array}\right\} \text{ vagy fordítva}$$

mert $m^e \equiv 1 \mod p$ és $m^e \equiv -1 \mod q$ minden fennáll.

Ha rosszul van megválasztva e, akkor túl sok fixpont jöhet be (nem jó titkosítás)

Példa: $e = \dfrac{(p-1)(q-1)}{2} + 1$

ekkor $e \equiv 1 \mod p-1$ és $\mod q-1$ is!

azaz $m^e \equiv m \mod p$ és q is $\Rightarrow m^e \equiv m \mod pq$

azaz minden m fixpont!

Az is leellenőrizhető, hogy $\text{lnko}(e, (p-1)(q-1)) = 1$ azaz a kód készítésénél ez előfordulhat.

Ha p és q közel egyenlők:

$$\left(\frac{p+q}{2}\right)^2 - pq = \left(\frac{p-q}{2}\right)^2$$

Tehát elég olyan $\sqrt{n}$-hez közeli $x > \sqrt{n}$ számot keresni, hogy $x^2 - n$ négyzetszám, mondjuk y^2. Ekkor

$$p = \frac{x+y}{2} \quad \text{és} \quad q = \frac{x-y}{2}.$$

Ha $p \pm 1$ vagy $q \pm 1$ bármelyikének csak kis prímosztói vannak

Példa: Ha $p-1 = 2^a \cdot 3^b \cdot 5^c$ alakú, akkor kevés (a,b,c) számhármas van úgy hogy $p < n$ teljesüljön. Ezek mindegyikét ki lehet próbálni és így faktorizáltuk n-et.
Ezért nem jók a $2^p - 1$ alakú Mersenne-prímek és a $2^{2^n}+1$ Fermat prímek.

Rossz, ha d túl kicsi:

Elég kipróbálni az összes lehetséges kicsi d-t, hogy $m^{ed} \equiv m \pmod n$

Wiener's attack
ha $d < \sqrt[4]{n}$ — 4

Rossz, ha e nagyon kicsi:

Példa: két független $n_1 = p_1 q_1$ és $n_2 = p_2 q_2$ titkosítás, de azonos $e=2$ kitevő.
Ha véletlenül 1 és 2 ugyanazt az m üzenetet akarja elküldeni, akkor tudjuk $\boxed{m^2 \bmod n_1}$ és $\boxed{m^2 \bmod n_2}$ értékeket. Szinte biztos, hogy $\text{lnko}(n_1, n_2) = 1$. Ekkor a kínai maradéktétel segítségével meg tudjuk oldani az $y \equiv m^2 \pmod{n_1 n_2}$ kongruenciát. De $m^2 < n_1 n_2$ és $y < n_1 n_2$, azaz $y = m^2$, és gyökvonással megvan m.
Megj: $e=3$ is feltörhető, $e = 2^{16}+1$ jónak tűnik.

p és q-nak globálisan egyedinek kell lennie

Ha tudjuk $n=pq$-t, akkor azt az interneten elérhető összes prímmel eloszthatjuk (próbálgatás)
Ha van két RSA titkosítás, amelyben ugyan az valamelyik prím, akkor $\text{lnko}(\underset{n_1}{p_1 q}, \underset{n_2}{p_2 q}) = q$ és mindkettő feltörhető (feltéve hogy $p_1 \neq p_2$)

Láttuk, hogy ha $n=pq$-t tudjuk faktorizálni; akkor megkaphatjuk d-t amivel feltörhetjük az RSA-t.
Fordítva is igaz:

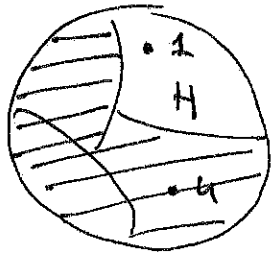
<u>Tétel</u>: Legyen adott egy RSA titkosítás az (n,e) nyilvános kulccsal. Ha ezt <u>úgy</u> fel tudjuk törni, hogy találunk d-t amelyre
$\forall m$-re $[\, \text{lnko}(m,n)=1 \Rightarrow m^{ed} \equiv m \pmod n \,]$
akkor az n-et tudjuk faktorizálni.

<u>Lemma</u> (<u>Legalább a fele lemma</u>) Legyen $n, k \in \mathbb{N}$ és tegyük fel, hogy valamely $u \in \mathbb{Z}_n^*$ elemre $u^k \neq 1$. Ekkor a $\mathbb{Z}_n$ elemek legalább felére (sőt $\mathbb{Z}_n^*$ elemeinek legalább felére) is teljesül hogy ~~x~~. $x^k \neq 1$

$\mathbb{Z}_{10}^* = \{1,3,7,9\} \cong (\mathbb{Z}_4;+)$
$3 \cdot 7 = 1, \; 9 \cdot 9 = 1$

Biz: $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \text{lnko}(x,n) = 1\}$ csoport a szorzásra nézve. $H = \{y \in \mathbb{Z}_n^* \mid y^k = 1\}$ részcsoportja $\mathbb{Z}_n^*$-nak és $u \notin H$ ezért valódi részcsoport.

A H mellékosztályai ugyan olyan méretűek és diszjunktak, ezért $|\mathbb{Z}^* \setminus H| \geq |H|$ és H-n kívüli bármely elemre $x^k \neq 1$. ∎



$nx + my = 1$
$\Downarrow$
$my \equiv 1 \pmod n$

A tétel bizonyítása

Ha $\text{lnko}(m,n) = 1$ és $m^{ed} \equiv m \pmod n$
akkor $m^{ed-1} \equiv 1 \pmod n$ [mert m-nek van inverze mod n]

Tehát van olyan $k = ed-1$ egészünk, hogy minden m-re ha $\text{lnko}(m,n) = 1$, akkor $m^k \equiv 1 \pmod n$.

$m = -1$-re gondolva kapjuk, hogy $2 \mid k$. Kezdjük el felezgetni ezt a kitevőt addig, míg tudja ezt a tulajdonságot. $\boxed{m^{k/2} \equiv 1 \mod n}$ Az előző lemma szerint véletlenül választva 100 db m-et ez a tulajdonság $1 - 2^{-100}$ valószínűséggel tesztelhető (mégpedig gyorsan).

Tehát találhatunk olyan k-t, amelyre ez a tulajdonság teljesül, de $k/2$-re már nem.

A kis Fermat-tétel miatt az nem lehet, hogy

$p-1 \mid k/2$ és $q-1 \mid k/2 \Rightarrow m^{k/2} \equiv 1 \bmod p$ és q is

(6)

(A) Tegyük fel hogy csak az egyik teljesül, mondjuk

$p-1 \mid k/2$ de $q-1 \nmid k/2$.

Ekkor minden $\text{lnko}(m,n)=1$ elemre $m^{k/2} \equiv 1 \pmod p$ de $m^{k/2} \not\equiv 1 \pmod q$ csak az ilyen elemek felére teljesül. Ha találunk olyan m-et, amelyre $m^{k/2} \not\equiv 1 \pmod q$ amit hamar találunk próbálgatással, akkor

$p \mid m^{k/2}-1$ és $q \nmid m^{k/2}-1$ azaz

$\text{lnko}(m^{k/2}-1, n) = p$ és megvan a faktorizáció.

(B) A második eset az, amikor $p-1 \nmid k/2$ és $q-1 \nmid k/2$.

Ekkor minden m-re ha $\text{lnko}(m,n)=1$ akkor

$(m^{k/2})^2 = m^k$

$m^{k/2} \equiv \pm 1 \bmod p$ és $\pm 1 \bmod q$ is, mert

$m^k \equiv 1 \bmod p$ és $\bmod q$ is. Tehát az esetek

$1/4$ részében $m^{k/2} \equiv 1 \bmod p$ és q, ~~legalább~~ $1/4$ részében $\boxed{m^{k/2} \equiv -1 \bmod p \text{ és } q}$ és a maradék felében az egyik $+1$ a másik -1. Tehát ugyanazt csinálhatjuk mint az első esetben és próbálgatással találunk m-et, hogy

$\text{lnko}(m^{k/2}-1, n) = p$ vagy q.

~~$m^{k/2} \equiv -1 \bmod n$~~

Prímtesztelés

Példa: Fermat prím $\underbrace{2^{2^n}+1}_{p_n}$ alakú ~~...~~ prímszámok

$$p_0 = 3 \qquad p_1 = 5 \qquad p_2 = 17$$

p_3, p_4 ezek prímek, de $p_5 = 2^{32}+1 = 641 \cdot 6700417$

Euler észrevette $\quad 3^{p_5-1} \not\equiv 1 \mod p_5 \implies p_5$ nem lehet prím.

Ha p prím, akkor $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$ csoport ciklikus, azaz van $\mathbb{Z}_p^* = \{1, g, g^2, \dots, g^{p-2}\}$ a g generátor elemmel.

Példa: $p = 7 \qquad g = 2$

$1, 2, 4$ nem jó, mert $g^3 \equiv 1 \mod p$

$$g = 3: \quad \begin{array}{cccccc} 1, & 3, & 2, & \overset{-1}{\overset{\equiv}{6}}, & 4, & 5 \\ \| & \| & \| & \| & \| & \| \\ g^0 & g^1 & g^2 & g^3 & g^4 & g^5 \\ \| & & & & & \\ g^6 & & & & & \end{array}$$

$$g^{p-1} \equiv 1 \pmod p$$

$$(g^k)^{p-1} = (g^{p-1})^k \equiv 1^k \equiv 1 \pmod p$$

Tehát a prímtesztelés más feladat (könnyebb) mint a prímfaktorizáció.

<u>Miller-Rabin teszt</u> Adott egy páratlan prímjelölt p

$p-1 = 2^r \cdot m$, egy adott $a \neq 0$ elemre $(0 < a < p)$

számoljuk ki $a^m, \; a^{2\cdot m}, \; a^{2^2\cdot m}, \; \ldots, \; a^{2^r\cdot m}$

$$a^{2\cdot m} = (a^m)^2, \quad a^{2^2\cdot m} = (a^m)^4$$

Ha p prím, akkor $a^{2^r\cdot m} \equiv 1 \mod p$

$$x^2 \equiv 1 \text{ de } x \not\equiv 1 \pmod p$$

ha p prím, akkor $x \equiv -1 \pmod p$.

<u>Def</u>: a <u>átmegy a Miller-Rabin teszten</u>, ha az $a^m, (a^m)^2, (a^m)^4, \ldots, (a^m)^{2^r} \mod p$ sorozatban megjelenik az egyes, és előtte -1 van (kivéve, ha $a^m \equiv 1$).
Különben azt mondjuk, hogy <u>nem ment át</u> / megbukik a teszten.

<u>Tétel</u>: Ha p prím, akkor az $1, \ldots, p-1$ számok mindegyike átmegy a teszten.
Ha p nem prím, akkor ezen számok legalább $3/4$-e megbukik a teszten.

Akár 100 tesztet elvégezve, nagyon nagy valószínűséggel prím, ha minden teszt átmegy és nem prím, ha valamelyik megbukik.