

Informatikai biztonság alapjai 3. gyakorlat

Oláh Norbert

2022.

Tartalom

- 1 RSA
 - RSA-séma
- 2 Prímtesztek
 - Prímtesztek
- 3 "A millió kulcsos kérdés" - Az RSA nyilvános kulcsok származásának vizsgálata
- 4 A kulcsforrás észlelése

RSA- kulcsgenerálás

- Választunk két nagy prímet p, q
- RSA modulus kiszámítása $N=p * q$
- Kiszámítjuk $\phi(n) = (p - 1) * (q - 1)$
Választunk 1 véletlen e : $1 < e < \phi(n)$
($e, \phi(n)$)=1 relatív prím legyen (kibővített euklideszi algoritmus)
- Kiszámítjuk d : $1 < d < \phi(n)$ és
 $e * d = 1 \pmod{\phi(n)}$ → d lineáris kongruencia teljesül (d ismeretlen)

RSA-visszafejtés

Kínai maradéktétel

Legyenek az m_1, \dots, m_k modulusok páronként relatív prímek. 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 $m_1 * m_2 * \dots * m_k$.

Kínai maradéktétel

Részletesen:

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

Kínai maradéktétel példa

$$x \equiv 0 \pmod{5}$$

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{4}$$

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

- $M_1 = 60/5 = 12$

$$M_2 = 60/3 = 20$$

$$M_3 = 60/4 = 15$$

Kínai maradéktétel példa

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

Kínai maradéktétel példa

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

$$x \equiv 0 * 3 * 12 + 1 * 2 * 20 + 2 * 3 * 15 \equiv 130 \equiv 10 \pmod{60}$$

Példa

$$p = 5$$

$$q = 11$$

$$n = 55$$

$$\phi(n) = 40$$

$$m = 20$$

$$e = 7$$

$$c = 15$$

$$d = 23$$

Példa

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

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

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

$$M_1 = 11$$

$$M_2 = 5$$

$$M = 55$$

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

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

Példa

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

$$x(y_1) = (-1)^2 * 1 = 1$$

$$y(y_2) = (-1)^3 * 2 = -2$$

Példa

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

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

Prímtesztek

- n összetettségét vizsgáljuk

- Próbaosztás

Tétel: Ha n összetett, pozitív egész, akkor létezik $p < \sqrt{n}$ prímosztója.

$n = a * b$ ahol $a > 1$ és $b > 1$

Állítás: $a \leq \sqrt{n}$ vagy $b \leq \sqrt{n}$

Indirekt állítás: $a \geq \sqrt{n}$ vagy $b \geq \sqrt{n}$

Prímtesztek

- Állítás: $a \leq \sqrt{n}$ vagy $b \leq \sqrt{n}$
Indirekt állítás: $a \geq \sqrt{n}$ vagy $b \geq \sqrt{n}$
Legyen : $a \geq \sqrt{n}$ ekkor $\forall a \in Z \exists p|a$ (p osztója a -nak)
hogy p prím és $p \leq a$
- Eratoszthenész szitája (prím számok keresése)
2, 3, 4, 5, 6, 7, 8, 9, 10, ..., \sqrt{n}
*, *, -, *, -, *, -, -, -...

Fermat-teszt

Valószínűségi prímteszt, mely a kis Fermat-tételre alapul
($a^p \equiv a \pmod{p}$).

- Tétel: $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$
- Algoritmus:
 - Választok egy a -t (prím)
 - $a^{p-1} \equiv 1 \pmod{p}$
 - Ha $a^{p-1} \not\equiv 1 \pmod{p} \rightarrow p$ összetett

Álprímek és Carmichael számok

Definíció:

- 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
(Végtelen sok szám)

Miller- Rabin teszt

- Legyen n páratlan pozitív egész szám
- $S = \max (r : 2^r | n - 1)$ és $d = (n - 1) / 2^S$
- Tétel: hogyha n prím és $(a, n) = 1$ akkor
 - $a^d \equiv 1 \pmod{n}$ vagy
 - $\exists r \in 0, \dots, S - 1$ hogy $a^{d \cdot 2^r} \equiv -1 \pmod{n}$

Miller- Rabin példa

- 8 különböző „a” esetén
- $n=561$
- $S = \max(560/2^r) = 4$ ($560/16=35$)
 $d=560/16$ (2^4)= **35**
- legyen $a=2$ (a, n) = 1 („a”bázis)
 $a^d \equiv 1 \pmod{n}$
 $2^{35} \equiv 1 \pmod{561}$
 $2^{35} \equiv 263 \pmod{561}$

Miller- Rabin példa

- $r \in (0, 1, 2, 3)$ (S-1)
- $2^{(35)^{2^0}} \equiv 263 \pmod{561}$
- $2^{(35)^{2^1}} \equiv 166 \pmod{561}$
- $2^{(35)^{2^2}} \equiv 67 \pmod{561}$
- $2^{(35)^{2^3}} \equiv 1 \pmod{561}$

Tanúk

N összetettségének tanúi

- $a \in (1, 2, 4, 7, 8, 11, 13, 14)$
- $d=14/2=7$;
- $S = \max(14/2^r) = 1$
- $r=0$
- $a^7 \equiv ? \pmod{15}$

A szerzők céljai

Adhat-e bármilyen információt az RSA nyilvános kulcsainak bitjei?

- Svenda P., Nemeč M., Sekan P., Kvasnovskyy R., Formanek D., Komarek D., Matyas V.. 2016. The Million-Key Question – Investigating the Origins of RSA Public Keys. In The 25th USENIX Security Symposium (USENIX Security'16). USENIX, p. 893–910.
- 60 millió kulcs elemzése 22 nyitott és zárt forrású könyvtárból és 16 különböző smart kártyából
- Eltérő implementációkból fakadóan nagy pontossággal meg lehet határozni a könyvtárt vagy az intelligens kártyát

A klaszterezés veszélye, hogy

- csökkenti felhasználók anonimitási halmazát,
- gyorsan azonosítható a sebezhető könyvtár kulcsai

Prímek eloszlása

Az egyes prímek 8 legmagasabb helyértékű bitjét (MSB) ábrázolták egy hőterképen.

Eredmény:

- Lehetőség van megfigyelni a prím generálási intervallumokat.
- Az MSB minták jelentősen különböztek a kártyák és a szoftverek implementációi tekintetében.
- A minták azonosak voltak az ugyanolyan típusú különböző smart kártyáknál és az egy gyártótól származó néhány típusnál is (valószínűleg a közös kódbázis miatt).
- Az 512 bites kulcsok esetében megfigyelt minták feltehetőleg azonosak az 1024 és a 2048 bites erősebb kulcsokkal (közös kódbázis miatt).

Az észlelés gyakorlati hatása- Gyenge kulcsok

- Ha valamelyik könyvtár vagy kártya gyenge kulcsokat állít elő, akkor a támadó meg tudja találni a többi kulcsot ugyanazon sebezhető forrásból.
- A kimutatás lehetősége különösen akkor hasznos, ha egy gyenge kulcs elleni sikeres támadás nagy, de gyakorlatilag elérhető összegű számítási erőforrást igényel.
- A potenciálisan sérülékeny kulcsok kiválasztása elősegíti a támadók számára, hogy forrásokat költsenek az összes nyilvános kulcsra.
- A nyilvános modulokból Infineon JCOP 80K kártyákat (512 bit) sikerült az esetek 4.35% faktorizálni Pollard $p-1$ faktorizációs algoritmusával



Köszönöm a figyelmet!