Informatikai biztonság alapjai 3. gyakorlat

Oláh Norbert

2022.

Tartalom

RSA

Ron Rivest; Adi Shamir; Len Adleman

- Nyílt kulcsú
- Aszimmetrikus

RSA

Ron Rivest; Adi Shamir; Len Adleman

- Az eljárás a nagy számok faktorizációjának problémáján alapul, vagyis hogy egy kellően nagy számról nehéz megállapítani annak prímtényezőit.
  Ha egy szám két igen nagy prímszám szorzata, akkor ennek prímtényezős felbontása még nagyon gyors számítógépekkel is nagyon sokáig tart.
- Számításelméleti okok miatt nem fejthető vissza olyan gyorsan, hogy érdemes legyen megpróbálni.
  Matematikailag nem bizonyított, hogy a titkosított adat visszafejtésére nem létezik kellő gyorsaságú algoritmus, ezért a jövőben ilyen algoritmus felfedezése lehetséges.

RSA

Nyílt üzenetek halmaza: Z_n
ahol $n = p \cdot q$ (p és q nagy prím)
Titkosított üzenetek halmaza: Z_n

RSA- függvények

- Kulcsgenerálás
  Nyilvános információk: n,e
  Titkos információk: p,q,$\phi(n)$,d
  PK: (n,e)
  SK: (n,d)
- Titkosítás
  Input: (M,PK)
  Output:CT
- Visszafejtés
  Input: (CT,SK)
  Output: M

RSA- kulcsgenerálás

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

RSA-visszafejtés

Kínai maradéktétel
Legyenek az $m_1, ..., m_k$ 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 $c_1, ..., c_k$ egészek esetén megoldható, és a megoldások egyetlen maradékosztályt alkotnak modulo $m_1 \cdot m_2 \cdot ... \cdot m_k$.

Kínai maradéktétel

Algoritmus:

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

Kínai maradéktétel példa

$x \equiv 0 \pmod 5$
$x \equiv 1 \pmod 3$
$x \equiv 2 \pmod 4$

- $M = 5 \cdot 4 \cdot 3 = 60$
- $M_1 = 60/5 = 12$
  $M_2 = 60/3 = 20$
  $M_3 = 60/4 = 15$

Kínai maradéktétel példa

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

Kínai maradéktétel példa

- $x \equiv \sum c_i \cdot y_i \cdot M_i \pmod{M}$
  $x \equiv 0 \cdot 3 \cdot 12 + 1 \cdot 2 \cdot 20 + 2 \cdot 3 \cdot 15 \equiv 130 \equiv 10 \pmod{60}$

Feladat

Kínai maradéktétel segítségével fejtse vissza a 15 titkosított üzenetet:

$p = 5$

$q = 11$

$n = 55$

$\phi(n) = 40$

$c = 15$

$d = 23$

Példa

$x \equiv c_1 \pmod{m_1}$
$x \equiv c_2 \pmod{m_2}$
$c_1 = 15^{23(mod\ 4)}\ mod\ 5 = 0$
$c_2 = 15^{23(mod\ 10)}\ mod\ 11 = 9$
$M_1 = 11$
$M_2 = 5$
$M = 55$
$y_1 \cdot 11 \equiv 1 \pmod{5}$
$y_2 \cdot 5 \equiv 1 \pmod{11} \rightarrow$ kibővített euklideszi algoritmus

Példa

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

$$y_1 = x = (-1)^2 * 1 = 1$$
$$y_2 = y = (-1)^3 * 2 = -2$$

Példa

$$x \equiv \sum c_i \cdot y_i \cdot M_i \pmod{M}$$
$$0 \cdot 1 \cdot 11 + 9 \cdot -2 \cdot 5 (mod\ 55) = -90 (mod\ 55) = 20$$

Prímtesztek

- n összetettségét vizsgáljuk
- Próbaosztás
  Tétel: Ha n összetett, pozitív egész, akkor létezik $p \leq \sqrt{n}$ prímosztója.
  $n = a \cdot b$, ahol $a > 1$ és $b > 1$
  Állítás: $a \leq \sqrt{n}$ vagy $b \leq \sqrt{n}$
  Indirekt állítás: $a > \sqrt{n}$ és $b > \sqrt{n}$

Prímtesztek

- Állítás: $a \leq \sqrt{n}$ vagy $b \leq \sqrt{n}$
  Indirekt állítás: $a > \sqrt{n}$ és $b > \sqrt{n} \rightarrow a \cdot b > n$
  Legyen $a \leq \sqrt{n}$ ekkor $\forall a \in Z$ esetén $\exists\, p|a$ (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-tételen alapul ($a^p \equiv$ a mod p).

- Tétel: Ha p prím és $(a, p) = 1$, akkor $a^{p-1} \equiv 1 \pmod{p}$
- Algoritmus:
  - Választok egy a-t (prím)
  - $a^{p-1} \equiv 1 \pmod{p}$ ellenőrzése
  - 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 Carmichael sok szám van)

Miller- Rabin teszt

- Legyen n páratlan pozitív egész szám
- Írjuk fel $n-1$-et a következő alakban $n-1 = 2^S \cdot d$, ahol d páratlan.
- $d = (n-1)/2^S$
- Tétel: hogyha n prím és (a, n)=1 akkor
  - $a^d \equiv 1 \pmod{n}$ vagy
  - $\exists r \in \{0, ..., S-1\}$ hogy $a^{d*2^r} \equiv -1 \pmod{n}$

Miller- Rabin példa

- 8 különböző „a" esetén
- n=561
- $n-1 = 2^S \cdot d \rightarrow S$= **4** (560/16=35)
  $d = 560/2^4 =$ **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-ig megy)
- $2^{(35)^{2^0}} \equiv 263 \pmod{561}$
- $2^{(35)^{2^1}} \equiv 166 \pmod{561}$
- $2^{(35)^{2^2}} \equiv 67 \pmod{561}$
- $2^{(35)^{2^3}} \equiv 1 \pmod{561}$

Tanúk

N összetettségének tanúi

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

A szerzők céljai

Adhat-e bármilyen információt az RSA nyilvános kulcsainak bitjei?

- Svenda P., Nemec 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

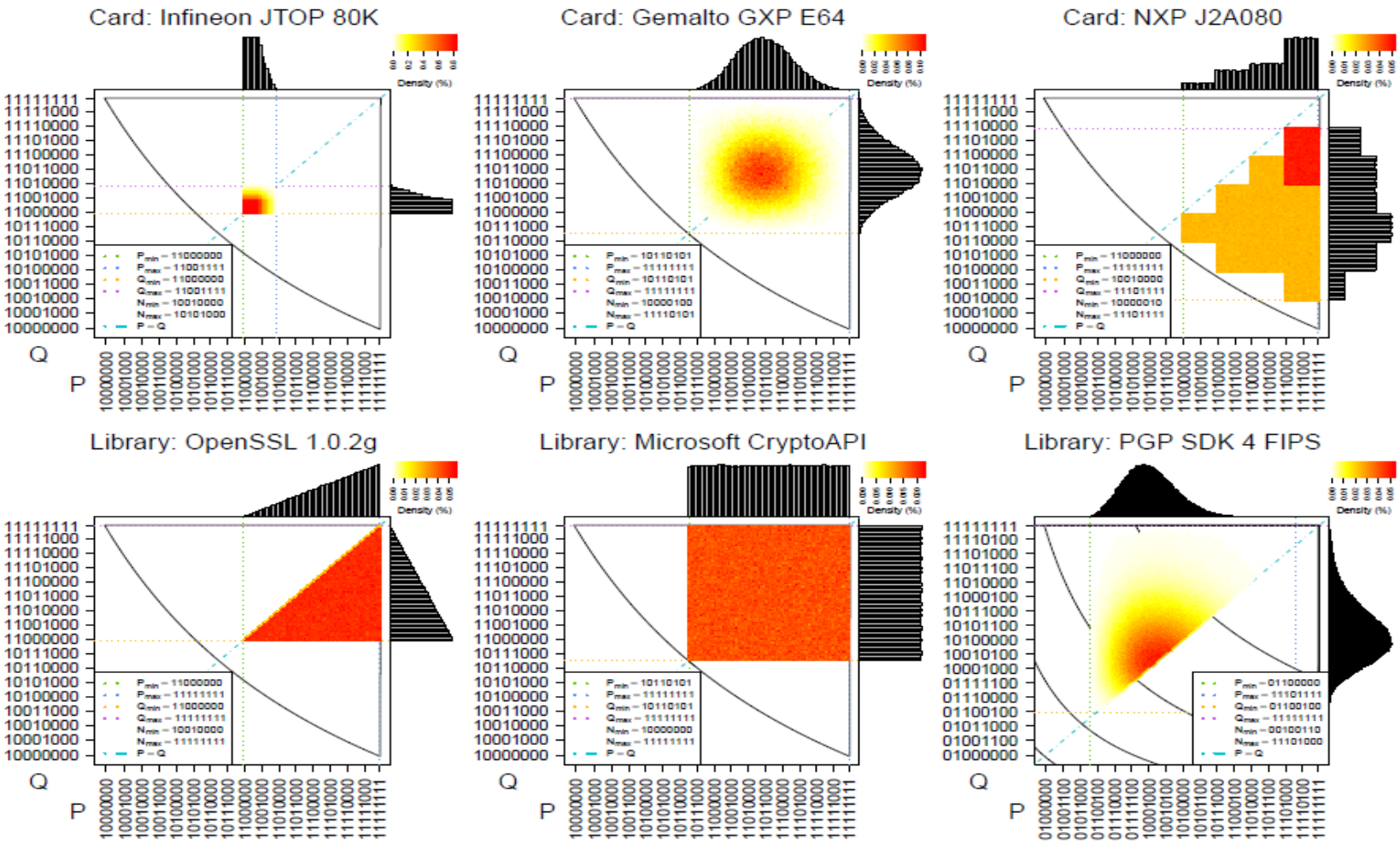
- csökkenti felhasználók anonimitási halmazát,
- gyorsan azonosítható a sebezhető könyvtár kulcsai

Prímek eloszlása

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

Hőtérkép



Fehér (nem valószínű) Narancs (sokkal valószínűbb)

A kulcsforrás észlelése

Intuitív módon az osztályozás a következőképpen működik:

- Azokat modulus biteket, amelyekről tudják, hogy hordozzák a torzítást azonosítják a modulusból származó további bitekkel (egy maszk, 6 + 3 bit a módszerükben) .
- A tanulási halmazon adott forráshoz az összes lehetséges maszk kombináció (2^9) gyakoriságának kiszámítása.
- Az ismeretlen nyilvános kulcsok osztályozásához a maszk által kiválasztott biteket külön értékként "v" -ként vonják ki
- A legvalószínűbb forrást a v érték legmagasabb kiszámított gyakorisággal rendelkező forrás (2. lépés) azonosítja. Ha ugyanazon forrásból több kulcs található (v_i több érték), magasabb osztályozási pontosság érhető el az egyes kulcsok valószínűségének elemenkénti szorzásával.

Side channel attacks

- Mellékcsatornás támadások / Kerülő utas támadások
- ezek nem az algoritmust, hanem annak implementációját támadják
- kivitelezésükhöz a titkosító rendszer nagyon pontos megfigyelésére van szükség
- komoly gyakorlati fenyegetést jelentenek
- cache timing attack: Meltdown és Spectre
- IoT és a kriptovaluta alkalmazások tömegesen használnak RSA kulcspárt

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!