Algoritmul RSA

p, q nr. prime mari

$n = p \cdot q$ modul de cifrare

e exponent de cifrare aleator a.î. e și $(p-1)(q-1)$ relativ prime

d exponent de descifrare a.î. $e \cdot d \equiv 1 \bmod (p-1)(q-1)$

$d \equiv e^{-1} \bmod (p-1)(q-1)$

d și n relativ prime

$\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$

$\begin{cases} (e, n) - \text{cheie publică} \\ d - \text{cheie privată} \end{cases}$

Fermat:

$x^{k \cdot \varphi(n)} \bmod n = 1$ dacă

x și n sunt prime între ele

cifrare: $c \equiv m^e \bmod n$

descifrare: $m \equiv c^d \bmod n$

semnare: $s \equiv m^d \bmod n$

verificare: $m \equiv s^e \bmod n$

Metode de spargere ale algoritmului RSA

① Text cifrat ales

a) Se interceptează mesajul c. Se dorește aflarea mesajului original m ($m \equiv c^d \bmod n$).

Se alege aleator un număr $r < n$.

Se calculează:

$x \equiv r^e \bmod n$

$y \equiv xc \bmod n$

$t \equiv r^{-1} \bmod n$

Atacatorul va cere semnarea lui y fără hash.

$u \equiv y^d \bmod n$

Atacatorul va calcula $u \cdot t$:

$t \cdot u \bmod n \equiv r^{-1} y^d \bmod n \equiv r^{-1} r^{ed} c^d \bmod n$

$\equiv r^{-1} r^{k(p-1)(q-1)} c^d \bmod n \equiv c^d \bmod n$

$= m.$

b) Se dorește semnarea mesajului m fără hash. Se alege un x aleator:

$y \equiv x^e \bmod n$

$m \equiv y \cdot m' \bmod n$

Se trimite m către semnare:

$s = m^d \bmod n$

Se calculează:

$$\begin{aligned} s \cdot x^{-1} \bmod n &\equiv m^d x^{-1} \bmod n \\ &\equiv y^d m'^d x^{-1} \bmod n \\ &\equiv x^{ed} m'^d x^{-1} \bmod n \\ &\equiv x^{\varphi(n)} \cancel{x \cdot x^{-1}} \cdot m'^d \bmod n \\ &\equiv (m')^d \bmod n \quad \text{mesajul } m' \text{ semnat} \end{aligned}$$

c) Se dorește semnarea mesajului m_3. Acesta se va sparge în două mesaje m_1 și m_2.

$m_3 \equiv m_1 m_2 \bmod n$

Se trimit m_1 și m_2 către semnare.

$m_3^d \equiv (m_1^d \bmod n)(m_2^d \bmod n)$

! Soluții: Nu semnați mesaje necunoscute. Aplicați mereu un hash înainte.

② Modulii comuni

Două seturi de chei au același n, dar d și e diferiți. Același mesaj m este criptat ~~de către~~ cu cele două chei:

$c_1 \equiv m^{e_1} \bmod n$

$c_2 \equiv m^{e_2} \bmod n$

Atacatorul interceptează mesajele criptate și dorește aflarea lui m. El va găsi folosind algoritmul lui Euclid extins două numere r și s a.î. $r \cdot e_1 + s \cdot e_2 = 1$.

Atacatorul va calcula $(c_1^{-1})^2 \cdot c_2^1 \equiv m \bmod n$

! Soluție: Nu folosește același n pentru două chei.

③ Exponență de cifrare mică

Se dorește aflarea lui m cifrat cu un e mic. Atacatorul interceptează ~~acela~~ criptări ale mesajului cu d și n diferite, dar același e.

$e = 3$

$c_1 \equiv m^3 \bmod n_1$

$c_2 \equiv m^3 \bmod n_2$

$c_3 \equiv m^3 \bmod n_3$

Atacatorul găsește folosind Lema Chineză a Resturilor un c a.î.:

$c \equiv m^3 \bmod n_1 \cdot n_2 \cdot n_3$

$m < n_1, n_2, n_3 \Rightarrow m^3 < n_1 \cdot n_2 \cdot n_3 \Rightarrow c = m^3 \Rightarrow m = c^{\frac{1}{3}}$

Sunt suficiente e mesaje identice cifrate cu chei publice diferite dar cu același e pentru a-l afla pe m.

! Soluție: Faceți padding cu valori aleatoare înainte de criptare.

④ Exponență de descifrare mică

d poate fi aflat dacă are lungimea peste 1/4 din lungimea lui n și dacă e are lungimea mai mică ca modulul n.

! Soluție: d trebuie ales mare

⑤ Numere prime apropiate

Se dorește aflarea numerelor p și q.

$\left(\frac{p+q}{2}\right)^2 - n = \left(\frac{p-q}{2}\right)^2$ dacă p și q au dimensiuni suficient de apropiate. Se testează toate numerele $x > \sqrt{n}$ a.î. $x^2 - n = y^2$ și se rezolvă sistemul $\begin{cases} p = x + y \\ q = x - y \end{cases}$

! Soluție: p și q trebuie să fie de ordine de mărime diferite

⑥ Eroare hardware

Se dorește aflarea numerelor p și q.

Un mesaj m semnat cu d se poate descompune astfel:

$$E \equiv m^d \bmod n$$

$$\equiv a \cdot E_1 + b \cdot E_2 \bmod n$$

$$\begin{cases} a \equiv 1 \bmod p \\ a \equiv 0 \bmod q \end{cases} \qquad \begin{cases} b \equiv 0 \bmod p \\ b \equiv 1 \bmod q \end{cases}$$

$\hat{E}$ este un mesaj semnat greșit datorită unei erori hardware. $\hat{E}_1$ a fost calculat greșit. Atacatorul află E și $\hat{E}$. ~~și dorește~~

$$E - \hat{E} = a(E_1 - \hat{E}_1)$$

Atacatorul calculează $\text{cmmdc}(E_1 - \hat{E}_1, n) = \text{cmmdc}(a(E_1 - \hat{E}_1), n) = q$

❗ Soluție: Faceți padding cu valori aleatoare înainte de criptare.

⑦ Atac asupra ofrării și semnării

În mod normal întâi se semnează și apoi se ofrează.

A trimite un mesaj lui B dar întâi ofrează cu cheia lui B și apoi semnează cu cheia sa:

$$c \equiv (m^{e_B} \bmod n_B)^{d_A} \bmod n_A$$

B găsește x a.î. $m' x \equiv m \bmod n_B$.

B își înlocuiește cheia publică cu $x \cdot e_B$ și astfel pretinde că a primit mesajul m' de la A.

❗ Soluție: Ori folosește un e fixat, ori face întâi semnarea și apoi ofrarea