Outlines of this talk

le principe des cryptosystème asymétriques est basé sur l'existence d'une fonction dite à sens unique, de telle sorte que le chiffrement du message soit facile mais le déchiffrement soit difficile.
les cryptosystèmes à clé publique permettent aussi d'authentifier l'émetteur du message.
Le cryptosystème RSA qui revient son nom à ses inventeurs Ron Riveste, Adi Shamir et Ronald Rivestn est le cryptosystème à clé publique le plus important.
Il repose sur un résultat d'arithmétique et sur les notions des nombres premiers.

Fonction de chiffrement:

$$E_e : \mathbb{Z}_n \to \mathbb{Z}_n \tag{1}$$

$$x \mapsto E_e(x) = x^e[n] = C \tag{2}$$

Fonction de déchiffrement:

$$D_d : \mathbb{Z}_n \to \mathbb{Z}_n \tag{3}$$

$$C \mapsto D_d(C) = C^d[n] \tag{4}$$

Avec:

(n, e) est la clé publique.

$(d, \varphi(n))$ est la clé secrète.

Exemple:

On veut déchiffrer le cryptogramme $C = 119$ chiffré avec RSA avec clé publique $(253, 3)$.
$235 = 11 \times 23$
$\varphi(11) = 10 \times 22$
Calcul du d:
On a

$$ed = 1[\varphi(n)] \Rightarrow ed \equiv 1[220]$$

Comme $220 = 3 \times 73 + 1$ alors
$220 - 3 \times 73 = 1 \Rightarrow 3 \times (-73) = 1[220] \Rightarrow d = 147[220]$. Dure à calculer $119^{147}[253]$, alors on utilise l'écriture en mode binaire de 147.

Exemple:

$$
\begin{aligned}
(5) \qquad & 147 = 10010011 \\
(6) \qquad & \quad = 1.2^7 + 0.2^6 + 0.2^5 + 1.2^4 + 0.23 + 0.2^2 + 0.21 + 1.2 + 1.2^0
\end{aligned}
$$

Alors on a:

$$
\begin{aligned}
(7) \qquad & 119^{147} = 119^{2^7+2^4+2+1} \\
(8) \qquad & \quad = 119^{2^7} \times 119^{2^4} \times 119^2 \times 119[253]
\end{aligned}
$$

On trouve: $m = 26[253]$.

Outlines of this talk

Déchiffrement du RSA en utilisant le théorème des restes chinois

On a la clé privée est donnée par $(\varphi(n), d)$, si on veut déchiffrer un cryptogramme C, on calcule $m_p \equiv C^{d[p-1]}[p]$

$$m_p = C^{d[p-1]}[p] \tag{9}$$

$$m_q = C^{d[q-1]}[q] \tag{10}$$

$$(p, q) = 1 \Leftrightarrow \exists y_p, y_q \in \mathbb{Z} \ / \ y_p \cdot p + y_q \cdot q = 1$$

Donc:

$$m = (m_p y_q q + m_q y_p p)[n]$$

Déchiffrement du RSA en utilisant le théorème des restes chinois

Exemple:

Déchiffrement du cryptogramme de l'exemple précédent $C = 119$ en utilisant le théorème des reste chinois.
On a: $n = 253 = 11 \times 23$

$$m_{11} = 119^{147[10]}[11] = 9^7[11] = 4[11] \tag{11}$$

$$m_{23} = 119^{147[22]}[23] = 3[23] \tag{12}$$

comme $23 + 11(-2) = 1$, alors

$$m = (4 \times 23 + 3(-2) \times 11)[253]; \tag{13}$$

$$= 26[253] \tag{14}$$