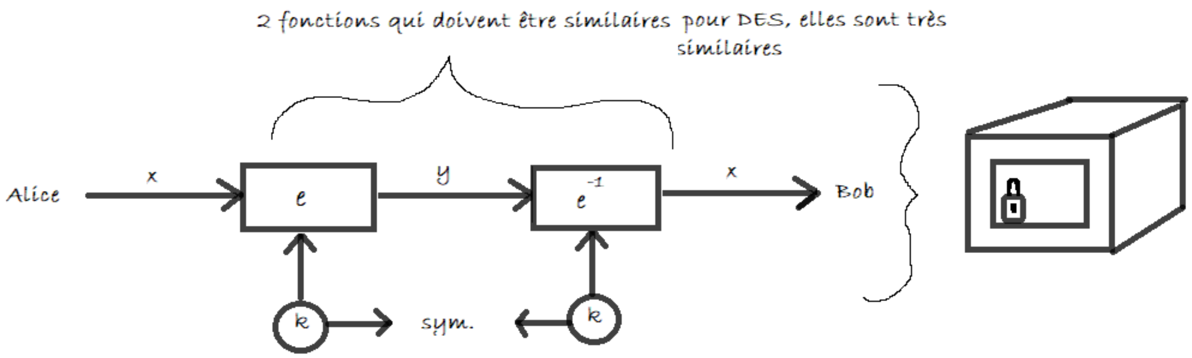
IFT 3275: Cours du 11 février 2021

Professeur: Arnaud L'Heureux

3 mars 2021

Chiffrement symétrique



Inconvénients :

- Partage de clefs
- Nombre de clefs à storer : n personnes $\Rightarrow \binom{n}{2} = \frac{n(n-1)}{2}$ clefs à storer.
- Principe de non-répudiation : Un contrat ne peut pas être remis en cause par Alice ou Bob $\rightarrow$ Signature digitale

Chiffrement asymétrique

$$\begin{array}{rcl} \text{Alice} & \xleftarrow{\quad k_{pub} \quad} & \text{Bob } k = (k_{pr}, k_{pub}) \\ y = ENC_{k_{pub}}(x) & \xrightarrow{\quad y \quad} & x = d_{k_{pr}}(y) \end{array}$$

Ceci permet

- Échange de clef
- Non-répudiation
- Identification
- Encryption

Qui sont tous des mécanismes propres à la cryptographie à clef publique.

Familles d'algorithmes :

- ▷ Factorisation : RSA
- ▷ Logarithme discret : Diffie-Hellman
- ▷ Courbes elliptiques : généralisation

Notions de base sur la théorie des nombres :

Le résultat du $pgcd(r_0, r_1)$ est le plus grand nombre > 0 qui divise r_0 et r_1.

Pour le reste des notes, nous prenons pour acquis que $r_0 > r_1$

EXEMPLE :
$r_0 = 84$ et $r_1 = 30$. Selon le théorème fondamental de l'arithmétique, on peut décomposer r_0, r_1 en produit de nombres premiers, soit $r_0 = 84 = 2 * \underline{2 * 3} * 7$ et $r_1 = 30 = \underline{2 * 3} * 5$. On peut alors trouver leur pgcd() en prenant leur produit de nombres premiers communs, ainsi le pgcd(84, 30) = 2*3 = 6.

Algorithme d'euclide :

$$\boxed{\text{pgcd}(r_0, r_1) = \text{pgcd}(r_0 - r_1, r_1)}$$

PREUVE :

$$\begin{aligned} pgcd(r_0, r_1) = g \Rightarrow g|r_0 \wedge g|r_1 \Rightarrow & r_0 = g * x \\ & r_1 = g * y \end{aligned}$$

Notons que si x et y sont copremiers, $(x - y)$ et y seront aussi copremiers entre eux.
Ainsi, puisque $r_0 = g * x$ et $r_1 = g * y \rightarrow r_0 - r_1 = g(x - y)$
$\Rightarrow pgcd(r_0 - r_1, r_1) = pgcd(g(x - y), gy) = g$

□

EXEMPLE :

Soit $r_0 = 84$ $r_1 = 30$

$$\left.\begin{array}{lll} r_0 - r_1 & = 54 = \underline{2 * 3} * 3 * 3 \\ r_1 & = 30 = \underline{2 * 3} * 5 \end{array}\right\} 6 \Rightarrow pgcd(84, 30) = pgcd(84 - 30, 30), \text{ soit } pgcd(54, 30)$$

ITÉRATIVE :

$$pgcd(r_0, r_1) = pgcd(r_0 - r_1, r_1) = pgcd(r_0 - 2r_1, r_1) = ... = pgcd(r_0 - mr_1, r_1), \text{ pour } m \in \mathbb{Z}$$

$$\text{tant que } (r_0 - mr_1) > 0$$

$$\begin{aligned} pgcd(r_0, r_1) &= pgcd(r_0 \mod r_1, r_1) \\ &= pgcd(r_1, r_0 \mod r_1) \\ pgcd(r_0, r_1) &= ... = pgcd(r_l, 0) = r_l \end{aligned}$$

EXEMPLE :

Calculons le $pgcd(r_0, r_1)$ avec $r_0 = 973$ et $r_1 = 301$

$$\begin{aligned} 973 = 3 * 301 + 70 &\Rightarrow pgcd(973, 301) = pgcd(301, 70) \\ 301 = 4 * 70 + 21 &\Rightarrow pgcd(301, 70) = pgcd(70, 21) \\ 70 = 3 * 21 + 7 &\Rightarrow pgcd(70, 21) = pgcd(21, 7) \\ 21 = 3 * 7 + 0 &\Rightarrow pgcd(21, 7) = pgcd(7, 0) = 7 \end{aligned}$$

Algorithme euclédien étendu (EEA)

$$pgcd(r_0, r_1) = s * r_0 + t * r_1 \text{ pour } s, t \in \mathbb{Z} \rightarrow \text{équation diophantienne}$$

Soit $r_0 = 973$ et $r_1 = 301$

$$\begin{aligned}
973 = 3 * 301 + 70 \rightarrow 70 &= r_0 + (-3)r_1 \\
301 = 4 * 70 + 21 \rightarrow 21 &= 301 + (-4 * 70) \\
&= r_1 + (-4)(r_0 - 3r_1) \\
&= -4r_0 + 13r_1 \\
70 = 3 * 21 + 7 \rightarrow 7 &= (r_0 + (-3)r_1) - 3(-4r_0 + 13r_1) \\
&= 13r_0 - 42r_1 \\
21 = 3 * 7 + 0 \rightarrow pgcd(973, 301) &= 7 = 13r_0 - 42r_1 = 13 * 973 - 42 * 301
\end{aligned}$$

TROUVER L'INVERSE DE $r_1 \mod r_0$, $r_1 < r_0$ et $pgcd(r_1, r_0) = 1$

$$\begin{aligned}
&s * r_0 + t * r_1 = 1 = pgcd(r_1, r_0) \\
&\boxed{t * r_1 \equiv 1 \mod r_0} \rightarrow r_1^{-1} \mod r_0 = t
\end{aligned}$$

EXEMPLE :

$12^{-1} \mod 67\,? \rightarrow r_0 = 67$ et $r_1 = 12 \qquad 12 * t \equiv 1 \mod 67$

$$\begin{aligned}
67 &= 5 * 12 + 7 & 7 &= r_0 - 5r_1 \\
12 &= 1 * 7 + 5 & 5 &= r_1 - (r_0 - 5r_1) = -r_0 + 6r_1 \\
7 &= 1 * 5 + 2 & 2 &= (r_0 - 5r_1) - (-r_0 + 6r_1) = 2r_0 - 11r_1 \\
5 &= 2 * 2 + 1 & 1 &= -r_0 + 6r_1 - 2(2r_0 - 11r_1) = -5r_0 + 28r_1 \\
2 &= 2 * 1 + 0 & 1 &= -5 * 67 + 28 * 12
\end{aligned}$$

Ainsi, l'inverse de 12 mod 67 est 28.

Fonction Phi de Euler

Le nombre d'entiers dans $\mathbb{Z}_m$ relativement premiers à m est $\phi(m)$
EXEMPLE : $\mathbb{Z}_6$ = {0, 1, 2, 3, 4, 5}

$$\begin{aligned}
&pgcd(0, 6) = 6 && pgcd(4, 6) = 2 \\
&pgcd(1, 6) = 1 && pgcd(5, 6) = 1 \\
&pgcd(2, 6) = 2 && \phi(6) = 2 \\
&pgcd(3, 6) = 3 &&
\end{aligned}$$

Ainsi, pour p un nombre premier, $\phi(p) = p - 1 = p^1 - p^0$

Théorème

$$m = p_1^{e_1} * p_2^{e_2} * ... * p_n^{e_n}$$
$$\phi(m) = \Pi_{i=1}^{n}(p_i^{e_i} - p_i^{e_i-1})$$

EXEMPLE : m = 240 = 16*15 = $2^4 * 3^1 * 5^1$ = $p_1^{e_1} * p_2^{e_2} * p_3^{e_3}$

$$\phi(240) = (2^4 - 2^3) * (3^1 - 3^0) * (5^1 - 5^0) = 8 * 2 * 4 = 64$$

Ainsi, il y a 64 nombres copremiers avec 240.

Théorème

Petit théorème de fermat :

$$a^p \equiv a \mod p \qquad a \in \mathbb{Z}, p \text{ premier}$$

Théorème

Théorème d'Euler

$$\text{Si } pgcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \mod m$$

EXEMPLE : m = 12 et a = 5. Le $pgcd(5, 12) = 1$ et $\phi(12) = \phi(2^2 * 3) = (2^2 - 2^1)(3^1 - 3^0) = 2 * 2 = 4$

$$5^4 \equiv 1 \mod 12$$
$$a^{\phi(p)} \equiv \boxed{a^{p-1} \equiv 1 \mod p}$$

RSA

Encryption : (n, e) $\Rightarrow k_{pub}$, où n est le modulo et e l'exposant d'encryption $\quad y = ENC_{k_{pub}}(x) \equiv x^e \mod n$

Décryption : d $\leftarrow$ exposant de décryption $k_{pr} \quad x = DEC_{k_{pr}}(y) \equiv y^d \mod n$

$x, y, n, d \geq 1024$ bits et $x, y \in \mathbb{Z}_n$

—▷ impossible de déterminer d à partir de e et n

—▷ ne peut pas encrypter $> l$ bits où l est la longueur de n en bits

—▷ $x^e \mod n$ et $y^d \mod n \Rightarrow$ facile à calculer

—▷ $n \Rightarrow$ beaucoup de paires (k_{pub}, k_{pr}) sinon $|k|$ trop petit $\Rightarrow$ force brute

Génération de clef

$$k_{pub} = (n, e) \qquad k_{pr} = d \Rightarrow (k_{pub}, k_{pr})$$

1. Choisir 2 gros nombres premiers p et q
2. $n = p * q$
3. $\phi(n) = (p-1)(q-1) = (p^1 - p^0)(q^1 - q^0)$
4. Sélectionner $e \in \{1, 2, 3, ..., \phi(n) - 1\}$ t.q. $pgcd(e, \phi(n)) = 1 \rightarrow$ pour que d existe !
5. Calculer d t.q. $d * e \equiv 1 \mod \phi(n)$

$$pgcd(\phi(n), e) = s * \phi(n) + t * e = 1$$
$$\text{Ainsi } e^{-1} = d = t \mod \phi(n)$$

ALICE	BOB
message $x = 4$	1. $p = 3$ $q = 11$
	2. $n = p * q = 33$
$y = x^e \mod n \xleftarrow{k_{pub}=(n,e)}$	3. $\phi(n) = (p-1)(q-1) = (3-1)(11-1) = 20$
	4. $e = 3$
$y = x^e \equiv 4^3 \equiv 31 \mod 33$	5. $d = e^{-1} \equiv 7 \mod 20$
$\xrightarrow{y=31}$	$y^d = 31^7 \equiv 4 \equiv x \mod 33$

Si on a p et q, on peut déterminer d à partir de la clef publique.

Si j'ai p et $q \rightarrow \phi(n) \rightarrow \phi(n) + e \overset{?}{\rightarrow} d$ t.q. $d = e^{-1} \mod \phi(n)$

Preuve de RSA

$$1\, DEC_{k_{pr}}(y) = DEC_{k_{pr}}(ENC_{k_{pub}}(x)) \equiv (x^e)^d \equiv x^{d*e} \stackrel{?}{\equiv} x \mod n$$

$$d*e \equiv 1 \mod \phi(n) \Rightarrow \boxed{d*e = 1 + t\phi(n)}, t \in \mathbb{Z}$$

$$DEC(y) \equiv x^{de} \equiv x^{1+t\phi(n)} \equiv x^{t\phi(n)}x^1 \equiv \boxed{x\left(x^{t\phi(n)}\right) \mod n \equiv x} \rightarrow \text{ce qu'on veut démontré}$$

$$pgcd(x,n) = 1 \Rightarrow 1 \equiv x^{\phi(n)} \mod n$$

$$1\, pgcd(x,n) = 1 \qquad \boxed{1^t \equiv \left(x^{\phi(n)}\right)^t \mod n}$$

$$DEC_{k_{pr}}(y) = x * 1^t \equiv \boxed{x\left(x^{\phi(n)}\right)^t \mod n \equiv x} \qquad \square$$

$$2\, pgcd(x,n) \neq 1 \Rightarrow pgcd(x,pq) \neq 1$$

$$x = r*p \qquad x = s*q \qquad r,s \in \mathbb{Z}$$

$\rightarrow$ présumer que $x = r*p$ est vrai

$$\Rightarrow pgcd(x,q) = 1$$

$$1 = 1^t \equiv \left(x^{\phi(q)}\right)^t \mod q$$

$$\left(x^{\phi(n)}\right)^t \equiv \left(x^{(q-1)(p-1)}\right)^t \equiv \left(\left(x^{\phi(q)}\right)^t\right)^{p-1} \equiv 1^{(p-1)} \equiv 1 \mod q$$

$$\left(x^{\phi(n)}\right)^t = 1 + u*q,\ u \in \mathbb{Z}$$

$$\boxed{x\left(x^{\phi(n)}\right)^t} = \boxed{x + x*u*q}$$

$$= x + (r*p)*u*q$$

$$= x + r*u*(p*q)$$

$$= x + r*u*n$$

$$= \boxed{x \mod n}$$

$$DEC_{k_{pr}}(y) = \left(x^{\phi(n)}\right)^t x \equiv x \mod n$$