Le système RSA

Construction du système par Bob :

- Choix de 2 grands nombres premiers p et q ;
- calcul de $n = pq$ et de $\phi(n) = (p-1)(q-1)$;
- choix d'un b tel que $pgcd(b, \phi(n)) = 1$;
- calcule de $a = b^{-1} \ mod \ \phi(n)$;
- publication de b et n.

Chiffrement de x par Alice :

$e_K(x) = x^b \ mod \ n$

Déchiffrement de $y = e_K(x)$ par Bob :

$d_K(y) = y^a \ mod \ n$

Clé : (n, p, q, a, b)

- clés publiques : n et b,
- clés privées : p, q et a.

Le système RSA

Algo. $square - and - multiply$ pour le calcul de y dans $y = x^c \ mod \ n = sm(x, c, n, |c|, 1)$ avec $|c| = l$ le nombre de bits de la représentation binare de c et $bin(c, i)$ le $i^{ème}$ bit de c.

$$sm(x, c, n, l, z)$$
$$\begin{cases} z \text{ si } l = 0 \\ sm(x, c, n, l-1, (z2 * x \ mod \ n)) \text{ si } bin(c, l) = 1 \\ sm(x, c, n, l-1, z2) \text{ sinon} \end{cases}$$

sachant que $z2 = z^2 \ mod \ n$.

Exemple : $p = 101$, $q = 113$, $x = 9726$.