Chapitre 5

Chiffrement à clés publiques

5.1 Le problème

Un système de chiffrement ou cryptosystème comporte un ensemble de clés K, et pour chaque clé une application d'encodage

$$e_K : \mathcal{M} \to \mathcal{E} \ ,$$

et une application de décodage :

$$d_K : \mathcal{E} \to \mathcal{M} \ ,$$

telles que pour tout message en clair, $m \in \mathcal{M}$, on a : $d_K(e_K(m)) = m$.

Si Bob envoie un message à Alice encodé avec une clé secrète K, Alice doit connaître également la clé K pour décoder : dans une système symétrique, c'est à dire avec une seule clé, celle-ci doit être échangée.

Dans un système à clé publique, il y a une clé publique et une clé secrète : $K = (P, S)$.

Alice envoie à Bob sa clé publique. Bob encode le message avec la clé publique d'Alice. Alice reçoit le message de Bob et le décode avec sa clé privée.

5.2 RSA (Rivest, Shamir, Adleman)

Le nombre $n = pq$ est un produit de (grands) nombres premiers. Alice choisit c premier avec $\phi(n) = (p-1)(q-1)$. Sa clé publique est (n, c). Elle calcule sa clé secrète d en inversant c modulo $\phi(n)$.

Bob veut envoyer à Alice un message représenté par $m \in \mathbb{Z}/n$ (ou une suite de tels m). Il calcule et envoit $m' = m^c \bmod n$.

Alice calcule $m'^d \bmod n$.

5.3 El Gamal

p est un grand nombre premier ; g est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Alice choisit sa clé secrète, a et calcule : $A = g^a \mod p$. Sa clé publique est (p, g, A).

Bob choisit b, calcule $B = g^b \mod p$. Il encode le message $m \in \mathbb{Z}/p\mathbb{Z}$ avec la formule $m' = mA^b \mod p$. Il envoit à Alice (B, m').

Alice calcule $m'/B^a = m'B^{p-1-a} \mod p$.