Chapitre 7 : Le chiffrement RSA et la factorisation des entiers

SÉcurité et Cryptographie
2013-2014

Sup Galilée INFO3

Introduction aux chiffrements à clef publique

L'objectif des systèmes à clef publique est de rendre la fonction de déchiffrement $D(-, K)$ impossible à retrouver à partir de la fonction de chiffrement $E(-, K)$. Ainsi la la fonction de chiffrement peut être publiée. L'avantage est qu'Alicce (ou tout autre personne) peut envoyer un message à Bob chiffré par $E(-, K)$ sans communication privée au préalable. Bob est la seule personne capable de déchiffrer ce texte en utilisant sa fonction de déchiffrement secrète $D(-, K)$.

Des exemples

La sécurité des systèmes à clef publique repose sur divers problèmes calculatoires.

RSA (Rivest, Shamir, Adleman, 1977) : Il est basé sur la difficulté de la factorisation des grands entiers.

Merkle-Hellman : Problème du sac-à-dos (qui est NP-complet, i.e., aucun algorithme de temps de calcul polynomial n'est connu).

McEliece : Problème du décodage d'u code linéaire (NP-complet).

ElGamal : Problème du calcul du logarithme discret dans un corps fini.

Le chiffrement RSA

Soit $n = pq$ où p, q sont des nombres premiers. Soit $\mathcal{P} = \mathcal{C} = \mathbb{Z}/n\mathbb{Z}$. On définit $\mathcal{K} = \{ (n, p, q, a, b) : ab \equiv 1 \pmod{\phi(n)} \}$.
Pour $K = (n, p, q, a, b)$, on définit $E(x, K) = x^b \bmod n$ et
$D(y, K) = y^a \bmod n$.
Les valeurs n, b sont publiques, et les valeurs p, q, a sont privées.

Exercice

Soit $n = 133$.

1. Calculer $\phi(n)$. ($n = 7 \times 19$ donc $\phi(n) = 6 \times 18 = 108$.)
2. Soient $b = 5$ et $a = 65$. Montrer que $ab \equiv 1 \pmod{\phi(n)}$. (On a $5 \times 65 = 325 = 1 + 3 \times 108$.)
3. Soit p le plus petit facteur premier de n et q le plus grand. Soit $x = 6$. Calculer $E(x, K)$ avec $K = (n, p, q, a, b)$. (On a $p = 7$, $q = 19$, $E(x, K) = 6^5 \bmod 133 = 62$.)