Solutions de l'exercice 1
Semaine 12

Cours Turing

1 Protocole d'El Gamal

a) Pour déchiffrer le message X envoyé par Alice à partir de $M^K \pmod N$ et $X \cdot B_2^K \pmod N$, Bob, qui connaît B_1, calcule d'abord

$$(M^K)^{B_1} \pmod N = (M^{B_1})^K \pmod N = B_2^K \pmod N$$

et effectue ensuite la division

$$\frac{X \cdot B_2^K \pmod N}{B_2^K \pmod N} = X \quad (\text{car } X \text{ est compris entre 2 et } N-1)$$

Une question légitime est ici : comment effectuer concrètement une division en arithmétique modulaire ? Il est bon de savoir que pour tout nombre Z compris entre 1 et $N-1$, on a $Z^{N-1} \pmod N = 1$ (c'est l'énoncé du petit théorème de Fermat). Donc $Z^{N-2} \cdot Z \pmod N = 1$, ce qui se lit encore : Z^{N-2} est l'inverse de Z modulo N. Donc diviser un nombre Y par un nombre Z revient en fait à multiplier Y par Z^{N-2} en arithmétique modulaire !

b) Si Eve vient maintenant à intercepter le message envoyé par Alice, à savoir $M^K \pmod N$ et $X \cdot (M^K)^{B_1} \pmod N$, mais ne connaît pas B_1, elle ne pourra pas répéter la même opération qu'Alice. Et pour apprendre la valeur de B_1 ou K (à partir des valeurs de N, M et B_2), Eve devrait être capable de résoudre le problème du logarithme discret, ce qui est difficile.

Note : On peut montrer également que pour envoyer plusieurs messages $X_1, X_2, X_3, \ldots$ à Bob en utilisant ce chiffrement, Alice doit retirer chaque fois au hasard des nombres $K_1, K_2, K_3, \ldots$ pour assurer la confidentialité de ses messages.