Exercices
Semaine 12

Cours Turing

1 Fonctions de hachage et détection d'erreurs

a) Ecrire un programme qui prend en entrée une chaîne de caractères, composée uniquement de lettres majuscules, et dont la sortie est un caractère (aussi une lettre majuscule) qui satisfait la condition : si deux chaînes en entrée diffèrent en une position seulement, alors les deux caractères en sortie doivent être différents.

b) Alice écrit maintenant un message (une chaîne de caractères) et lui ajoute un caractère selon votre schéma ci-dessus. Elle envoie le tout à Bob, mais pendant la transmission, il se peut qu'une erreur se produise et qu'un des caractères de la chaîne envoyée par Alice soit remplacé par un autre tiré au hasard. Ecrire un programme qui prend en entrée la chaîne de caractères reçue par Bob et sorte la réponse oui ou non suivant qu'une erreur a été introduite ou non dans la chaîne.

2 Fonctions de hachage et correction d'erreurs

a) Ecrire un programme qui prend en entrée une chaîne composée de 4 bits $X_1X_2X_3X_4$, et dont la sortie est une chaîne de 3 bits $X_5X_6X_7$ qui satisfait les conditions suivantes :

- si deux chaînes en entrée diffèrent en 1 position seulement, alors au moins 2 bits des deux chaînes en sortie doivent être différents ;

- si les deux chaînes en entrée diffèrent en 2 positions, alors au moins 1 bit des deux chaînes en sortie doit être différent.

b) Alice écrit maintenant un message encodé par 4 bits et lui ajoute 3 bits selon votre schéma ci-dessus. Elle envoie le tout à Bob, mais pendant la transmission, il se peut qu'une erreur se produise et qu'un des bits de la chaîne envoyée par Alice soit inversé (un 0 devient un 1, ou réciproquement). Ecrire un programme qui prend en entrée la chaîne de 7 bits reçue par Bob et :

- sorte la réponse oui ou non suivant qu'une erreur a été introduite ou non dans la chaîne ;

- indique à quelle position l'erreur a eu lieu.

3 Protocole d'El Gamal

Ce protocole diffère légèrement du protocole de RSA, mais permet également à Alice d'envoyer directement un message à Bobt.

- Bob choisit tout d'abord un grand nombre premier N, ainsi que deux nombres entiers M et B_1 compris entre 2 et $N-1$; il calcule ensuite $B_2 = M^{B_1} \pmod N$, et publie N, M et B_2.

- Pour communiquer un message X (compris entre 2 et $N-1$) à Bob, Alice tire au hasard un nombre K entre 1 et $N-1$ et envoie à Bob le message crypté suivant, composé de deux parties :

$$(M^K \pmod N,\ X \cdot B_2^K \pmod N)$$

a) Pour déchiffrer le message envoyé par Alice, que fait Bob ? A vous de jouer !

b) Et si Eve intercepte le message d'Alice, peut-elle le déchiffrer ?