math202 : mathématiques pour le numérique
TD 4 : cryptographie

Pierre Hyvernat
Laboratoire de mathématiques de l'université de Savoie
bâtiment Chablais, bureau 17, poste : 94 22
email : Pierre.Hyvernat@univ-savoie.fr
www : http://www.lama.univ-savoie.fr/~hyvernat/

Exercice 1 : mots de passe

Question 1. Combien de mots de passe y a t'il si :

- chaque caractère est une lettre ASCII minuscule et le mot de passe fait au plus 8 caractères,
- chaque caractère est une lettre ASCII et le mot de passe fait exactement 8 caractères,
- chaque caractère est une lettre ASCII ou un chiffre et le mot de passe fait entre 6 et 8 caractères.

Combien de temps faut-il pour tester tous les mots de passe si on peut tester 1 000 mots de passe par secondes (par exemple en essayant des connexions par internet) ou bien 10 000 000 de mots de passe par seconde si on dispose du "hash" du mot de passe en local ?

Question 2. Si on compte tous les mots apparaissant dans un livre en anglais, on trouve environ 1 million de mots différents.

Combien de temps faudrait-il pour tester tous ces mots ?

Combien de temps faudrait-il pour tester les mots de passe générés de la manière suivante : chaque mot de passe est constitué de 4 mots pris au hasard parmi les 2000 mots français les plus courants ?

Exercice 2 : cryptographie symétrique

Question 1. Appliquez le "bloc note à usage unique" (cryptage et décryptage) avec la clé

```
0010 1011 1101 0100 1010 1001 1110 ...
```

et le message

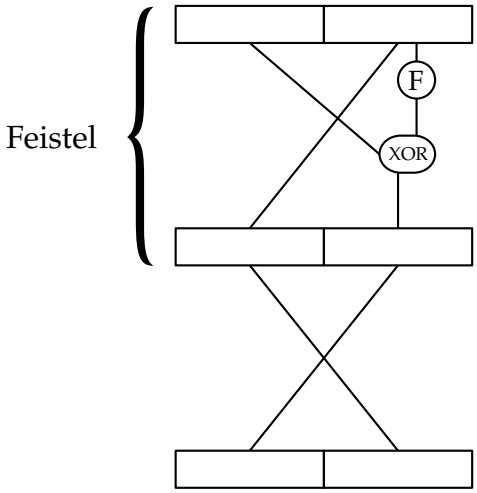
```
0110 1011 0110 0101 0111 1001
```

Expliquez pourquoi le second XOR avec la clé permet effectivement de décrypter le message, c'est à dire d'inverser le premier XOR avec la clé.

Question 2. Les portes de Feistel (figure au verso) sont l'élément clé du système DES. Dans le circuit, F est une fonction quelconque qui ne change pas la taille de son argument. (Notez l'inversion des parties gauches et droites qui suit la porte de Feistel.)

Donnez une formule exprimant les valeurs de parties gauche et droite finales en fonctions des parties gauche et droites initiales.

Vérifiez que si on applique le même circuit sur les parties gauche et droite finales, on retombe sur les parties gauche et droite initiales.



Question 3. On suppose que la partie gauche fait 8 bits et la partie droite 8 bits. On utilise une clé (secrète) $k_0k_1 \dots k_{15}$ de 16 bits et :

(1) on applique la porte de Feistel avec $F_1 : u \mapsto u \oplus k_0k_1k_2 \dots k_7$
(2) on applique la porte de Feistel avec $F_2 : u \mapsto u \oplus k_4k_5k_6 \dots k_{11}$
(3) on applique la porte de Feistel avec $F_3 : u \mapsto u \oplus k_8k_9k_{10} \dots k_{15}$
(4) on échange les parties droite et gauche.

Calculez le message codé si on part de
- `00101110 11110100` comme message
- `11110110 01010111` comme clé.

Question 4. Vérifiez que si on part du message codé et qu'on applique les portes dans l'ordre inverse, on retrouve bien le message original.

Remarque : c'est ainsi que fonctionne le système DES, mais il utilise des blocs de 64 bits (32 à gauche et 32 à droite), une clé de 56 bits et 16 portes de Feistel.

Exercice 3 : Double masque binaire : cryptographie imparfaite

Alice souhaite communiquer un message secret M à Bob (M est une suite de bits). Comme ils ne disposent pas d'une clé secrète partagée, ils utilisent le protocole suivant :
- Alice détermine A, une suite de bits aléatoire de même taille que M,
- Bob détermine B, une suite de bits aléatoire de même taille que M,
- Alice calcule $C_1 = M \oplus A$ et communique C_1 à Bob,
- Bob calcule $C_2 = C_1 \oplus B$ et communique C_2 à Alice,
- Alice calcule $C_3 = C_2 \oplus A$ et communique C_3 a Bob.

Question 1. Quel calcul Bob doit-il effectuer pour obtenir le message M ?

Question 2. Testez ce système avec votre voisin(e) pour un message binaire de taille 8.

Question 3. Si Eve intercepte les communications entre Alice et Bob, comment peut-elle trouver M sans connaitre ni A ni B ?