info223 : Science informatique
TD 5 : cryptographie

Pierre Hyvernat
Laboratoire de mathématiques de l'université de Savoie
bâtiment Chablais, bureau 22, 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 ?

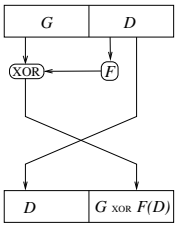
Question 2. Si on compte tous les mots apparaissant dans un livre en anglais, on trouve environ 1 million de mots différents.

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. La porte de Feistel fait l'opération suivante



où F est une fonction qui ne change pas la taille de son argument.

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

$$F \quad : \quad u \ \mapsto \ u \oplus k_0k_1k_2\dots k_7$$

(2) on applique la porte de Feistel avec

$$F \quad : \quad u \ \mapsto \ u \oplus k_4k_5k_6\dots k_{11}$$

(3) on applique la porte de Feistel avec

$$F \quad : \quad u \ \mapsto \ u \oplus k_8k_9k_{10}\dots k_{15}$$

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

Question 2. 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 : Partage de clé : Diffie-Hellman

Question 1. L'échange de clés de Diffie-Hellman fonctionne avec :
- un nombre premier p public, très grand,
- un générateur g de $\mathbf{Z}_p$, en général petit.

Alice choisit un nombre secret a, et Bob choisit un nombre secret b, ensuite :
- Alice envoie $A = g^a \bmod p$ à Bob et Bob envoie $B = g^b \bmod p$ à Alice,
- Alice calcul $B^a \bmod p$ et Bob calcule $A^b \bmod p$: ils arrivent au même résultat.

Effectuez un échange de clés avec votre voisin en utilisant :
- $p = 97$,
- $g = 5$.

Choisissez un nombre secret supérieur à 30.

Question 2. Essayez d'adapter l'échange de clés de Diffie-Hellman au cas où n personnes veulent partager une clé secrète.

Question 3. Faites les calculs suivants :
- $3^{10} \bmod 100$,
- $2^{20} \bmod 111$,
- $7^{15} \bmod 150$,
- $5^{100} \bmod 100$,
- $3^{200} \bmod 20$.