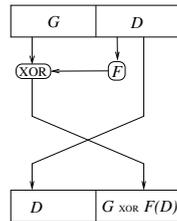


<b>info223 : Science informatique</b> <b>TD 4 : cryptographie</b>
--

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/>

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)  $k_0 k_1 \dots k_{15}$  de 16 bits et :

(1) on applique la porte de Feistel avec

$$F : u \mapsto u \oplus k_0 k_1 k_2 \dots k_7$$

(2) on applique la porte de Feistel avec

$$F : u \mapsto u \oplus k_4 k_5 k_6 \dots k_{11}$$

(3) on applique la porte de Feistel avec

$$F : u \mapsto u \oplus k_8 k_9 k_{10} \dots k_{15}$$

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.

Question 3. 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 4. Essayez d'adapter l'échange de clés de Diffie-Hellman au cas où  $n$  personnes veulent partager une clé secrète.