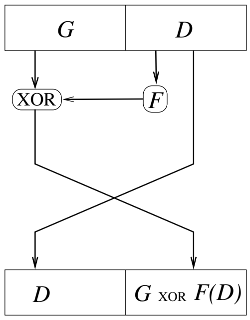
info223 : Science informatique
TD 3 : cryptographie

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/`

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

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

(2) on applique la porte de Feistel avec

$$F \quad : \quad u \mapsto u \oplus k_4 k_1 k_2 \dots k_{11}$$

(3) on applique la porte de Feistel avec

$$F \quad : \quad u \mapsto u \oplus k_8 k_1 k_2 \dots k_{15}$$

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

Question 4. 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 5. Essayez d'adapter l'échange de clés de Diffie-Hellman au cas où n personnes veulent partager une clé secrète.

Partie 1 : RSA

- Bob choisit deux nombres premiers p et q et un nombre d premier avec $(p-1)(q-1)$. Il publie les nombres $n = pq$ et $e = d^{-1} \bmod (p-1)(q-1)$ (clé publique)
- pour lui envoyer M, Alice calcule $C = M^e \bmod n$. Elle envoie C à Bob.
- pour décrypter, Bob calcule $C^d \bmod n$ et obtient M.

En utilisant :
- $p = 17$,
- $q = 13$,
- $d = 77$,
- $e = 5$.

Question 1. Calculez $(p-1)(q-1)$ et vérifiez que d est bien l'inverse de e modulo $(p-1)(q-1)$.

Question 2. Codez la suite de bits `1101011101` en utilisant les paramètres si dessus.
Décodez la suite obtenue.

Remarque : il s'agit du système RSA (Rivest - Shamir - Adleman).