Fiche de TP N° 2 du Module Cryptgraphie

Implémentation d'un Algorithme de Chiffrement par Flot (RC4)

RC4 (Rivest Cipher 4) est un algorithme de chiffrement à flot conçu en 1987 par Ronald Rivest, l'un es inventeurs du RSA, pour les Laboratoires RSA. Il est supporté par différentes normes, par exemple dans TLS (anciennement SSL) ou encore WEP.
RC4 est un générateur de bits pseudo-aléatoires dont le résultat est combiné avec le texte en clair via une opération XOR, le déchiffrement se fait de la même manière (voir chiffrement de Vernam).
Pour générer le flot de bits, l'algorithme dispose d'un état interne, tenu secret, qui comprend deux parties :
une permutation S de tous les 256 octets possibles
deux pointeurs i et j de 8 bits qui servent d'index dans un tableau
La permutation est initialisée grâce à la clé de taille variable, typiquement entre 40 et 256 bits, grâce au key schedule de RC4. L'algorithme RC4 opère en deux phases :

1- L'algorithme de key schedule :

```
pour i de 0 à 255
   S[i] := i
finpour
j := 0
pour i de 0 à 255
   j := (j + S[i] + clé[i mod longueur_clé]) mod 256   // Longueur de clé exprimée en octet
   échanger(S[i], S[j])
finpour
```

2- La génération du flot pseudo-aléatoire

Tant qu'un octet doit être généré pour effectuer le XOR avec le texte clair, le générateur modifie son état interne selon la série d'instructions suivantes :

```
i := 0
j := 0
tant_que générer une sortie:
   i := (i + 1) mod 256
   j := (j + S[i]) mod 256
   échanger(S[i], S[j])
   octet_chiffrement = S[(S[i] + S[j]) mod 256]
   result_chiffré = octet_chiffrement XOR octet_message
fintant_que
```

Cet algorithme garantit que chaque valeur de est échangée au moins une fois toutes les 256 itérations.

Objectif du TP:

1. Implémentation de l'algorithme RC4 (en Java si possible), pour une longueur de clé de 128bit (16 octet) et (256bit 32 octet). L'utilisateur introduit la clé octet par octet, il introduite ensuite la taille du flot désiré et le programme génére une séquence en fonction de ces deux paramètres. (Une fonction Gener_Stream(key: tableau d'octet, size:entier) et qui renvoi un tableau de taille "size" contenant le flot pseudo aléatoire).
2. Utilisation de cette fonction pour chiffré et déchiffré des fichiers de tailles arbitrires.