Principes et Algorithmes de Cryptographie

DS du 6 avril 2004

Durée 1 heure - documents autorisés
Toute réponse devra être justifiée

Exercice 1 : *Chiffrement de Hill*

Dans le chiffrement de Hill, chaque lettre de l'alphabet est représentée par un entier compris entre 0 et 25 (l'alphabet latin est traduit en l'ensemble $\mathbb{Z}/26\mathbb{Z}$ des entiers modulo 26). C'est un chiffrement par blocs de m lettres, qui transforme un bloc $(x_1, x_2, \ldots, x_m)$ en un bloc $(y_1, y_2, \ldots, y_m)$ défini par la relation algébrique :

$$(y_1, y_2, \ldots, y_m) = (x_1, x_2, \ldots, x_m)A$$

où A est une matrice carrée d'ordre m à coefficient dans $\mathbb{Z}/26\mathbb{Z}$, tous les calculs étant faits modulo 26.

Par exemple avec $m = 2$ et $A = \begin{pmatrix} 5 & 1 \\ 12 & 3 \end{pmatrix}$, le message $(10, 21)$ est chiffré en

$$(10, 21).\begin{pmatrix} 5 & 1 \\ 12 & 3 \end{pmatrix} = (10 \times 5 + 21 \times 12, 10 \times 1 + 21 \times 3) = (16, 21)$$

Le déchiffrement d'un bloc se fait en multipliant le bloc chiffré par la matrice inverse de A.

Une matrice carrée à coefficient dans $\mathbb{Z}/26\mathbb{Z}$ est inversible si et seulement si son déterminant est inversible modulo 26. De plus, lorsque $m = 2$, l'inverse est donné par la formule :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Q 1 . Vérifiez que la matrice de l'exemple ci–dessus est inversible et calculez son inverse.

Q 2 . Décrivez comment mener une attaque à clair connu sur le chiffrement de Hill.

Q 3 . Dans le cas où $m = 2$ et où le message clair est d'une langue naturelle comme le français, décrivez comment mener une attaque à chiffré seul sur le chiffrement de Hill.

Exercice 2 : *AES*

Dîtes pourquoi on opère, en début de chiffrement avec l'AES, un ou-exclusif entre le bloc clair et la clé de tour.

TSVP ☞

Exercice 3 : *LFSR*

Quel est le plus petit LFSR produisant la suite périodique de période `1010011` ?

Exercice 4 : *Transformation d'un LFSR*

Q 1 . Quelle est la période de la suite $(s_n)_{n\geq 0}$ produite par un LFSR de polynôme de rétroaction $f(X) = X^7 + X + 1$, initialisé à un état non nul ?

Q 2 . Écrivez la relation de récurrence donnant le bit s_{i+7} en fonction des sept bits précédents.

Q 3 . Modifiez la relation trouvée à la question précédente en lui ajoutant une fonction non linéaire des sept bits du registre de façon à obtenir un registre à décalage de longueur 7, à rétroaction non linéaire produisant une suite de période 128.