M1 2015 - 2016

Introduction à la Sécurité **TD1**

L'AES est, comme son nom l'indique, un standard de chiffrement symétrique qui à remplacer le DES (Data Encryption Standard), devenu trop faible au regard des attaques actuelles. Le but de ce TD est de comprendre sa structure.

L'AES opère sur des blocs de 128 bits qu'il transforme en blocs chiffrés de 128 bits par une séquence de N_R opérations ou *tours*, à partir d'une clé de 128, 192 ou 256 bits. Suivant la taille de celle-ci, le nombre de tours diffère : respectivement 10, 12 et 14 rounds. L'état interne de 128 bits est vu comme une matrice 4×4 d'octets, où chaque octet représente un élément du corps fini à 256 éléments $\mathbb{F}_{256}$. Un tour d'AES consiste en 4 opérations appliquées successivement à l'état interne :

- *SubBytes :* la même boite-S est appliquée en parallèle aux 16 octets de l'état interne,
- *ShiftRows :* chaque ligne de l'état interne est décalée selon son indice,
- *MixColumns :* l'état interne est multiplié à gauche par une matrice inversible,
- *AddRoundKey :* l'état interne est XORé avec une sous-clé.

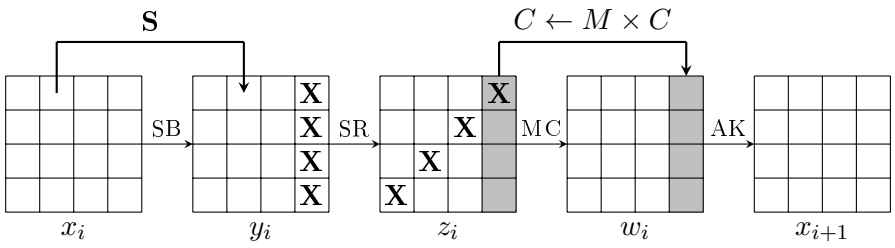

FIGURE 1 – Description d'un tour d'AES.

Dans les exercices suivants on supposera que les sous-clés utilisées sont indépendantes.

Exercice 1 - MixColumns

Soit AES-MC une version modifiée de l'AES dans laquelle on omet l'opération MixColumns.

1. Quel est le problème de ce chiffrement ?
2. On suppose que l'adversaire a en sa possession $N_r + 1$ couples clair/chiffré. Décrire une attaque permettant de retrouver les $N_r + 1$ sous-clés.
3. Décrire une méthode permettant de déchiffrer n'importe quel message à partir de 16×2^8 couples clair/chiffré.

4. Est-il possible de n'utiliser que 2^8 couples ?

Exercice 2 - ShiftRows

Soit AES-SR une version modifiée de l'AES dans laquelle on omet l'opération ShitRows.

1. Quel est le problème de ce chiffrement ?
2. Décrire une méthode permettant de déchiffrer n'importe quel message à partir de 2^{32} couples clair/chiffré.

Exercice 3 - SubBytes

Soit AES-SB une version modifiée de l'AES dans laquelle on omet l'opération SubBytes.

1. Quel est le problème de ce chiffrement ?
2. Montrer que l'on peut trouver 2 clés différentes k_1 et k_2 telles que
$$\text{AES-SB}(k_1, \bullet) = \text{AES-SB}(k_2, \bullet).$$
3. Trouver une clé k telle que
$$\text{AES-SB}(k, 0) = 0.$$

Exercice 4 - Chiffrement de Hill

Dans le chiffrement de Hill, chaque lettre de l'alphabet est représentée par un entier compris entre 0 et 25. L'algorithme 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 :

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

où A est une matrice carrée d'ordre m à coefficients dans $\mathbb{Z}_{26}$, 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

$$(10, 21) \cdot A = (10 \times 5 + 21 \times 12, 10 \times 1 + 21 \times 3) = (16, 21).$$

Le déchiffrement d'un bloc se fait en multipliant le bloc chiffré par la matrice inverse de A. Une matrice carrée à coefficient dans $\mathbb{Z}_{26}$ est inversible si et seulement si son déterminant est inversible modulo 26.

1. Quelle est la formule donnant la matrice inverse lorsque $m = 2$?
2. Calculer la matrice inverse de celle donnée en exemple.
3. Décrire une méthode permettant d'attaquer le chiffrement de Hill à clair connu.
4. Application : on dispose des couples clair/chiffré $((2, 9), (11, 11))$ et $((7, 3), (11, 23))$.