Cryptographie – Feuille d'exercices 5

Advanced Encryption Standard

M1 Informatique – 2014-2015

1 Exercice 1

Combien y a-t-il :

1. de permutations de 128 bits sur 128 bits ?
2. de fonctions de 128 bits sur 128 bits ?

2 Exercice 2 : Représentation matricielle vs. Représentation polynomiale

1. On considère, comme dans l'AES, le corps à 2^8 éléments, défini au moyen du polynôme irréductible $m(X) = X^8 + X^4 + X^3 + X + 1$. Calculer l'octet obtenu en calculant le produit suivant :
$$\{e1\} \times \{05\}.$$
2. On considère maintenant l'opération
$$\text{MixColumn} : \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} \mapsto \begin{pmatrix} a'_0 \\ a'_1 \\ a'_2 \\ a'_3 \end{pmatrix}$$
qui agit sur chaque colonne de la représentation "carrée" de l'AES.
Dans le cours, on a défini cette transformation par
$$\begin{pmatrix} a'_0 \\ a'_1 \\ a'_2 \\ a'_3 \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$
Montrer que l'opération MixColumn peut se définir de manière équivalente par la formule
$$a'_3X^3 + a'_2X^2 + a'_1X + a'_0 =$$
$$(a_3X^3 + a_2X^2 + a_1X + a_0) \cdot (\{03\}X^3 + \{01\}X^2 + \{01\}X + \{02\}) \bmod (X^4 + 1).$$
3. Vérifier que la matrice utilisée pour MixColumn a pour inverse la matrice
$$\begin{pmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{pmatrix}.$$
4. A votre avis, d'un point de vue implémentation, quand faut-il privilégier la représentation polynomiale ou la représentation matricielle ?

3 Exercice 3 : Fonction de hachage

Soit $f : \{0,1\}^{2m} \longrightarrow \{0,1\}^m$ une fonction de hachage. Soit maintenant une deuxième fonction de hachage définie par

$$h : \begin{array}{ccc} \{0,1\}^{4m} & \longrightarrow & \{0,1\}^m \\ x_1||x_2 & \mapsto & f(f(x_1)||f(x_2)) \end{array}$$

où $||$ désigne l'opération de concaténation. Montrer que si f est à collisions fortes difficiles [1], alors h est aussi à collisions fortes difficiles.

4 Exercice 4 : Fonction de hachage basée sur AES

Soit $m = m_1 m_2 \dots m_n$ une chaîne de bits dans laquelle pour chaque $i = 1 \dots n$, m_i est un bloc de 128 bits. On définit une fonction de hachage H qui opère sur les mots binaires de cette forme en posant

- h_0 est un bloc de 128 bits tous nuls ;
- pour chaque $i = 1 \dots n$, $h_i = \mathrm{AES}_{m_i}(h_{i-1})$, où $\mathrm{AES}_K(m)$ est le résultat du chiffrement du bloc m avec la clé K ;
- $H(m) = h_n$.

1. Montrer comment on peut trouver des collisions pour H en appliquant approximativement $c.2^{64}$ fois l'AES, où c est une constante.
2. Étant donnée une chaîne m, montrer comment trouver une chaîne différente m' telle que $H(m) = H(m')$, en appliquant approximativement 2^{64} fois l'AES. [Indication : s'inspirer de l'attaque sur le double DES - voir Feuille 4, Exercice 1.]

1. C'est-à-dire qu'il est calculatoirement difficile d'obtenir deux messages différents x et x' tels que $f(x) = f(x')$.