Examen du 10 décembre 2015

(durée: 3 heures)

Exercice 1. Soit un LFSR dont le polynôme caractéristique (polynôme caractéristique de la matrice) est $P \in \mathbb{F}_2[X]$:

$$P(X) = X^8 + X^5 + X^4 + X^3 + 1$$

1. Donner le schéma du LFSR, la relation de récurrence vérifiée par une suite engendrée, et son polynôme de connexion.

2. Calculer $X^{17} \pmod{P}$, et en déduire que P est un produit de polynôme irréductibles dont le degré divise 8.

3. Le polynôme P est-il primitif ? Est-il irréductible (justifier, on peut utiliser la question précédente) ?

4. Quelle peut être la plus petite période d'une suite engendrée par ce LFSR ? Qu'en conclure sur la qualité du LFSR (justifier) ?

Exercice 2. Soit $(s_i)_{i\in\mathbb{N}}$ une suite engendrée par un LFSR sur $\mathbb{F}_2$ de longueur m dont la période est de longueur maximale $p = 2^m - 1$.

1. On pose $S_i = (s_i, s_{i+1}, \ldots, s_{i+m-1})$. Rappeller pourquoi, si $0 \le i < j < p$, alors $S_i \neq S_j$. Qu'en déduire pour $\{S_i \ / \ 0 \le i < p\}$?

2. Montrer que :

$$\sum_{i=0}^{p-1} (-1)^{s_i} = -1 \ .$$

3. Montrer que si deux suites sont engendrées par un LFSR de même polynôme caractéristique χ, alors toute combinaison linéaire de ces deux suites est engendrée par un LFSR de polynôme caractéristique χ.

4. En déduire que la fonction d'auto-corrélation de la suite (s_i), soit :

$$C(r) = \sum_{i=0}^{p-1} (-1)^{s_i + s_{i+r}}$$

ne prend que deux valeurs, p et -1.

Exercice 3. On se propose de construire une substitution sur 4 bits obtenue de façon analogue à la transformation subByte de l'AES (qui est sur 8 bits). Dans tout l'énoncé, sauf précision, « + » désigne l'addition sur $\mathbb{F}_2$ (le `xor`).

Le corps $\mathbb{F}_{16}$ est vu comme $\mathbb{F}_2[X]/(X^4+X+1)$. Un élément de $\mathbb{F}_{16}$, soit $a_3X^3+a_2X^2+a_1X+a_0$ est représenté par l'entier $a_3 2^3 + a_2 2^2 + a_1 2 + a_0$ (où l'addition est sur $\mathbb{N}$), et on note ce dernier en hexadécimal.

1. Calculer pour cette représentation la table de la fonction inverse complétée en 0 :

$$\begin{array}{rccl} \mathrm{inv} : & \mathbb{F}_{16} & \to & \mathbb{F}_{16} \\ & 0 & \mapsto & 0 \\ & x & \mapsto & x^{-1} \ . \end{array}$$

sous la forme d'une liste, de façon que l'image de i soit le i-ème élément de cette liste (la numérotation commence à 0).

2. On note $j \bmod n$ le reste de la division de j par n dans $\mathbb{N}$. Soit l la transformation de $\mathbb{F}_2^4$ dans $\mathbb{F}_2^4$ qui à (x_3, x_2, x_1, x_0) associe (y_3, y_2, y_1, y_0) défini par (au niveau des indices l'addition est bien-sûr celles des entiers) :

$$y_i = x_i + x_{(i+2) \bmod 4} + x_{(i+3) \bmod 4} \ .$$

Vérifier que l est une transformation linéaire sur $\mathbb{F}_2^4$ (donner son expression matricielle), et montrer qu'elle est inversible.

3. On note également l l'application de $\mathbb{F}_{16}$ dans $\mathbb{F}_{16}$ qui à $a_3X^3 + a_2X^2 + a_1X + a_0$ associe $b_3X^3 + b_2X^2 + b_1X + b_0$, où $(b_3, b_2, b_1, b_0) = l(a_3, a_2, a_1, a_0)$. Donner, sous la forme d'une liste comme précédemment, la table de la fonction $s = l \circ \mathrm{inv}$.

4. Soit : $\begin{array}{rccl} s_u : & \mathbb{F}_{16} & \to & \mathbb{F}_{16} \\ & x & \mapsto & s(x) + u \ . \end{array}$

Rappeler quel peut être le nombre de solutions de l'équation en x, $\mathrm{inv}(x) + \mathrm{inv}(x + a) = b$, $\mathbb{F}_{16}$ pour $(a, b) \neq (0, 0)$, puis Montrer que l'équation $s_u(x) + s_u(x + a) = b$ a même nombre de solutions que la précédente. Interpréter ce résultat du point de vue de la résistance à une attaque différentielle pour un chiffrement où s_u intervient comme substitution.

5. On cherche $u \in \mathbb{F}_{16}$ tel que la transformation s_u n'ait pas de point fixe, c'est-à-dire que pour tout $x \in \mathbb{F}_{16}$, $s_u(x) \neq x$ Calculer les valeurs possibles pour u.

La substitution s_3 est celle utilisée à l'exercice suivant.

Exercice 4. Le chiffrement étudié est un chiffrement par blocs à 4 tours, le schéma est celui du chiffrement de Heys, la S-box est modifiée.

La taille du bloc est de 16 bits. La taille de la clef est de 48 bits.

— Une substitution `block_t subst(block_t, sbox_t);` obtenue en juxtaposant 4 fois la même substitution s sur 4 bits. L'image par la substitution s d'un entier `i` de 4 bits est `sbox[i]`, avec :
```
sbox = {0x3, 0x4, 0xf, 0xb, 0x2, 0x1, 0x7, 0x0,
        0xc, 0xd, 0x5, 0x9, 0x6, 0xe, 0xa, 0x8};
```
— La même permutation sur 16 bits `block_ tperm(block_t)` que celle du chiffrement de Heys :
```
pbox = {0x0, 0x4, 0x8, 0xc, 0x1, 0x5, 0x9, 0xd,
        0x2, 0x6, 0xa, 0xe, 0x3, 0x7, 0xb, 0xf};
```
— Les clefs de tour sont de 16 bits chacune, et numérotées de 0 à 4. La clef numéro i est obtenue en sélectionnant les bits de la clef principale (numérotés de 0 à 47) de la position $8i$ à la position $8i + 15$.

Le schéma du chiffrement est celui du chiffrement de Heys.

— Initialisation
```
block_t m; // clair
block_t r; // chiffré
r = m ^ key[0]
```
— 1er tour
```
r =subst(r)
r =perm(r)
r = r ^ key[1]
```
— 2nd tour
```
r =subst(r)
r =perm(r)
r = r ^ key[2]
```
— 3ème tour
```
r =subst(r)
r =perm(r)
r = r ^ key[3]
```
— 4ème tour

— `r =subst(r)`

— `r = r ^ key[4]`

1. Calculer la table des différences de la S-box. Chaque ligne doit indiquer, pour une différence d'entrée δx à entre deux entrées n et $n \oplus \delta x$, le nombre d'occurrences de la différence de sortie $\delta y = s(n) \oplus s(n \oplus \delta x)$, pour n variant de 0 à 15 (utiliser la notation hexadécimale pour les entrée et sorties) (déposer le programme produisant la table et le résultat dans votre répertoire svn, répertoire exam déjà créé).
2. Quelles sont les valeurs prises par la probabilité d'apparition d'une différence en sortie (en supposant l'équidistribution des différences en entrée) ? Quelle est, hors cas triviaux, la probabilité maximale, et combien y-a-t-il de couples de différence de probabilité maximale ? donner parmi ceux-ci d'une part ceux qui ont une différence d'un seul bit en entrée, d'autre part ceux qui ont une différence d'une seul bit en sortie.
3. Quelle est le nombre minimum de S-boxes que doit utiliser une caractéristique différentielle pour ce chiffrement ? Quelle probabilité maximale peut-on espérer pour cette caractéristique différentielle (sous les hypothèses d'indépendances usuelles que l'on précisera) ?
4. Montrer qu'une caractéristique différentielle qui utilise ce nombre minimum de S-boxes, doit nécessairement utiliser au second tour la différence $(4, 1)$.
5. En déduire qu'il y a exactement 4 caractéristiques différentielles de probabilité maximale et les décrire toutes.
6. Comment utiliser ces caractéristiques pour une attaque différentielle : de quoi doit-on disposer, comment programmer l'attaque, quels bits de la clef de tour chacune d'entre elle permet-elle de retrouver ?
7. Comparer rapidement ce chiffrement et celui étudié en TP.