Examen du 28 novembre 2013

(durée: 3 heures)

Exercice 1. Soit les polynômes $P, Q \in \mathbb{F}_2[X]$, $P(X) = X^7+X+1$ et $Q(X) = X^6+X^3+1$. les polynômes A et B de $\mathbb{F}_2[X]$ vérifient que $\deg(A) < \deg(P)$ et $\deg(B) < \deg(Q)$. Les séries génératrices des suites (s_n) et t_n vérifient

$$\sum_{n\geq 0} s_n X^n = \frac{A(X)}{P(X)} \; ; \; \sum_{n\geq 0} t_n X^n = \frac{B(X)}{Q(X)} \; .$$

1. Pour chacune de ces deux suites, montrer qu'elles sont récurrentes explicitant la relation de récurrence. Représenter le LFSR qui engendre cette suite récurrente. Donner le polynôme de connexion et le polynôme caractéristique.
2. On suppose que $s_i = 0$ pour $i \leq 5$ et $s_6 = 1$. Calculer A.
3. On suppose que $B(X) = 1$, calculer l'initialisation du registre.
4. Ces deux polynômes sont-ils irréductibles ? Sont-ils primitifs ? (utiliser les algorithmes vu en cours en les justifiant rapidement (sur le cas particulier). Présenter la suite des calculs sous forme d'un tableau.

   Qu'en conclure pour la qualité des LFSR associés ?

Exercice 2. On s'intéresse dans cet exercice aux applications $f : \mathbb{F}_q \mapsto \mathbb{F}_q$, $q = 2^n$, qui sont bijectives et pourraient convenir comme substitution (SBOX) pour un chiffrement par bloc de type SPN, par exemple AES ou le chiffrement pédagogique de Heys vu en cours, en particulier du point de vue de la résistance aux attaques linéaires et différentielles.

1. Soit $f_m : x \mapsto x^m$. Montrer que f est bijective si et seulement si m et $q-1$ sont premiers entre eux.
2. Montrer que les applications $f_{2^k} : x \mapsto x^{2^k}$, $0 < k < n$ sont bijectives, et expliquer pourquoi elles ne peuvent convenir pour une SBOX.
3. Montrer que les applications $f_{2^k+1} : x \mapsto x^{2^k+1}$, $0 \leq k < n$, sont bijectives si [A CORRIGER et seulement si] $\frac{n}{\mathrm{pgcd}(n,k)}$ est impair (indication : soit $e = \mathrm{pgcd}(n,k)$, $a = \frac{n}{e}$, $b = \frac{k}{e}$, étudier la congruence modulo un diviseur d de 2^k+1 de $2^{eab}-1$).
4. Soit k, tel que $0 < k < n$. On pose $e = \mathrm{pgcd}(n,k)$. Soient $\alpha,\ \beta \in \mathbb{F}_q$, $\alpha \neq 0$. L'unique sous-corps de $\mathbb{F}_q$ d'ordre 2^e (pourquoi en existe-t-il un ?) des éléments stables par : $x \mapsto x^{2^e}$ est noté $\mathbb{F}_{2^e}$. On cherche à estimer le nombre de couples solutions de l'équation

$$x^{2^k+1} + (x+\alpha)^{2^k+1} = \beta. \tag{1}$$

   a. Montrer que si x et y sont solutions de (1), alors $\frac{x+y}{\alpha} \in \mathbb{F}_{2^e}$.

   b. Conclure que l'équation (1) a au plus 2^e solutions, et que si k et n sont premiers entre eux l'équation (1) possède 0 ou 2 solutions.
5. On suppose maintenant que $0 < k < n$, k et n sont premiers entre eux et que n est impair. Montrer que pour $\alpha \neq 0$ et β en supposant une distribution uniforme des entrées), la probabilité que la différence (xor) en entrée soit $\alpha \neq 0$ et en sortie β est inférieure ou égale à 2^{1-n}, et que ceci est optimal pour des SBOX avec n bits en entrée et en sortie.

Exercice 3. Le chiffrement étudié est un chiffrement par blocs à 4 tours, le schéma est celui du chiffrement de Heys. La taille du bloc est de 16 bits. La taille de la clef est de 48 bits.

la S-box est modifiée. Un bloc est vu comme un élément du corps $\mathbb{F}_{16}$ lui même 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 $a_3 2^3 + a_2 2^2 + a_1 2 + a_0$, et on note ce dernier en hexadécimal.

La S-box est la transformation obtenue par $s : x \mapsto x^7 + 5$.

– Une substitution `block_t subst(block_t, sbox_t);` obtenue en juxtaposant 4 fois la même substitution s sur 4 bits.

- 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 décrit en fin d'énoncé (le dernier tour n'utilise pas de permutation) :

- 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[3]`

1. Vérifier rapidement que $X^4 + X + 1$ est irréductible et que s est bijective (cf. exercice précédent question 1).

2. La substitution obtenue est donnée par (on ne demande pas de faire le calcul)

```
sbox = {0x5, 0x4, 0xe, 0x8, 0xc, 0xb, 0x3, 0x2,
        0x9, 0x0, 0xd, 0x6, 0xa, 0x7, 0x1, 0xf}
```

Calculer la table de différence (la donnée est disponible sur mon répertoire svn, fichier `exam.c`).

3. 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 ? Repérer parmi ceux-ci ceux qui ont une différence qui est un nombre à un seul bit à 1 en entrée ou en sortie, ainsi qu'une différence d'un seul bit à 1 en entrée *et* en sortie.

4. 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) ?

5. Montrer que si une caractéristique différentielle n'utilise qu'une boîte par tour, la différentielle du second tour a nécessairement des différences en entrée et en sortie avec un seul bit à 1, et que donc elle doit nécessairement utiliser au premier tour $S_{1,4}$.

6. Décrire toutes les caractéristiques différentielles de probabilité maximale.

7. 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 ?

8. Comparer rapidement ce chiffrement et celui vu en cours.