Cryptanalyse — 4TCY902U
Responsable : G. Castagnos

Examen — mardi 19 décembre 2017

Durée 3h
Documents non autorisés
Les exercices sont indépendants

$\boxed{1}$ Soit $z = (z_t)_{t\geqslant 0}$ une suite binaire non constante produite par un LFSR de longueur ℓ de polynôme de rétroaction $f(X) \in \mathbf{F}_2[X]$ de degré ℓ. Soit s la suite binaire définie par $s_t = z_t \oplus 1$ pour tout $t \geqslant 0$.

(a) Dans cette question on suppose f primitif. Quel est la période de la suite s ?

(b) Soit $Z(X)$ la série génératrice définie par $Z(X) = \sum_{t\geqslant 0} z_t X^t$. Rappeler sans démonstration la formule reliant $Z(X)$ et $f(X)$.

(c) Donner un polynôme $h(X)$ tel que s soit produite par un LFSR de polynôme de rétroaction $h(X)$ (Justifier le résultat).

(d) On suppose que le polynôme $f(X)$ est le polynôme de rétroaction minimal pour la suite z. Quelle est le complexité linéaire de la suite s ?

$\boxed{2}$ On considère le corps à 256 éléments, $\mathbf{F}_{2^8}$, dans la représentation $\mathbf{F}_{2^8} = \mathbf{F}_2[\alpha]$, avec $\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$, comme dans l'AES. On identifie de la manière usuelle l'espace vectoriel $\mathbf{F}_2^8$ et le corps $\mathbf{F}_{2^8}$ en associant à $v = (v_1, \dots, v_8) \in \mathbf{F}_2^8$, l'élément $v_1 + v_2\alpha + \cdots + v_8\alpha^7 \in \mathbf{F}_{2^8}$.

(a) Rappeler la définition du degré d'une fonction booléenne.

(b) On considère l'application $s : \mathbf{F}_2^8 \to \mathbf{F}_2^8$, $x \mapsto x^2$, où le carré est effectué dans $\mathbf{F}_{2^8}$. Pour $i = 1, \dots, 8$, on note $s_i : \mathbf{F}_2^8 \mapsto \mathbf{F}_2$ les fonctions booléennes coordonnées de telle sorte que $s(x_1, \dots, x_8) = (s_1(x_1, \dots, x_8), \dots, s_8(x_1, \dots, x_8))$.

Quel est le degré des s_i pour $i = 1, \dots, 8$? Donner leur expression.

(c) Soit u un entier. On considère maintenant l'application $t_u : \mathbf{F}_2^8 \to \mathbf{F}_2^8$, $x \mapsto x^{2^u}$, où le calcul est effectué dans $\mathbf{F}_{2^8}$. On note de même $t_{u,i}$ pour $i = 1, \dots, 8$, les fonctions booléennes coordonnées.

Quel est le degré des $t_{u,i}$ pour $i = 1, \dots, 8$? Donner un algorithme (en pseudo code) pour trouver leur expression.

Dans la suite de l'exercice, on considère l'application suivante

$$\begin{aligned} \mathrm{I} : \mathbf{F}_2^8 &\to \mathbf{F}_2^8 \\ x &\mapsto \mathrm{I}(x) = \begin{cases} 0 \text{ si } x = 0 \\ x^{-1} \text{ si } x \neq 0 \end{cases} \end{aligned}$$

où l'inversion x^{-1} est celle du corps $\mathbf{F}_{2^8}$. On note $\mathrm{I}_1, \dots, \mathrm{I}_8$ les fonctions booléennes coordonnées.

(d) Montrez que $\mathrm{I}(x) = x^{2^8-2} = x^{2^7+2^6+2^5+2^4+2^3+2^2+2}$.

(e) En déduire le degré des fonctions booléennes $\mathrm{I}_1, \dots, \mathrm{I}_8$.

(f) Soit k un entier. Quel est, en fonction de k, le degré des fonctions coordonnées associées à la fonctions $x \mapsto x^k$ dans $\mathbf{F}_2^8$? Que pensez vous du choix fait pour la boîte S de l'AES (On rappelle que cette boîte S est la composition d'une fonction affine et de I) ?

Dans la suite de l'exercice, on considère un chiffrement par flot additif, en utilisant les fonctions booléennes $\mathrm{I}_1, \dots, \mathrm{I}_8$ définies précédemment et un LFSR de ℓ bits. On note $\mathrm{S}^{(t)} = (\mathrm{S}_0^{(t)}, \dots, \mathrm{S}_{\ell-1}^{(t)})$, l'état interne du LFSR au temps t. À l'initialisation, la clef secrète sk de ℓ bits est simplement chargée dans l'état interne : $\mathrm{S}^{(0)} = sk$. On fixe 8 cases du registres $\ell - 1 \geqslant i_1 \geqslant i_2 \geqslant \cdots \geqslant i_8 \geqslant 0$.

À chaque instant $t \geqslant 0$, on sort le bit $z_t = \mathrm{I}_{j(t)}(\mathrm{S}_{i_1}^{(t)}, \mathrm{S}_{i_2}^{(t)}, \dots, \mathrm{S}_{i_8}^{(t)})$ avec $j(t) = (t \mod 8) + 1$, puis le LFSR est mis à jour.

(g) Donner une attaque particulièrement bien adaptée contre ce système. Bien détailler la description de l'attaque, en particulier donner sa complexité et le nombre de bits de suite chiffrante nécessaires.

$\boxed{3}$ On considère le chiffrement par bloc suivant. On utilise une clef de 64 bits K ainsi que des blocs de clairs et de chiffrés de 64 bits. Ces éléments de 64 bits sont vus comme 8 éléments de $\mathbf{Z}/256\mathbf{Z}$. On note S une permutation de $\mathbf{Z}/256\mathbf{Z}$.

On désigne par + l'addition modulo 256 de $\mathbf{Z}/256\mathbf{Z}$ et par <<< 1 une rotation de 1 bit vers la gauche. Étant donné un message clair, $\mathrm{M} = (\mathrm{M}_0, \dots, \mathrm{M}_7) \in (\mathbf{Z}/256\mathbf{Z})^8$ et une clef $\mathrm{K} = (\mathrm{K}_0, \dots, \mathrm{K}_7) \in (\mathbf{Z}/256\mathbf{Z})^8$, l'algorithme de chiffrement est défini comme suit :

```
Pour r de 0 à 31 faire
    M8 ← M0
    Pour i de 0 à 7 faire
        M(i+1) ← (M(i+1) + S(Mi + Ki)) <<< 1
    Fin Pour
    M0 ← M8
Fin Pour
Retourner M0, ..., M7
```

On notera dans la suite f_{K} la fonction de tour correspondant à la boucle sur r appliquée 32 fois.

(a) Soit $\mathrm{M}, \mathrm{M}' \in (\mathbf{Z}/256\mathbf{Z})^8$ deux messages clairs et C, C' les chiffrés correspondant en utilisant une même clef K. Montrer que si $f_{\mathrm{K}}(\mathrm{M}) = \mathrm{M}'$ alors $f_{\mathrm{K}}(\mathrm{C}) = \mathrm{C}'$.

(b) Montrer que si un tel couple M, M' est connu alors on peut retrouver facilement la clef K.

(c) En déduire une attaque à textes clairs connus, retrouvant la clef secrète K meilleure que la recherche exhaustive. Préciser sa complexité en équivalent de nombres de chiffrements complets.

(d) Améliorer l'attaque précédente en faisant une recherche exhaustive sur 16 bits de la clef K.

$\boxed{4}$ Construction de fonction de hachage et fonction de compression

Dans cet exercice, on note comme d'habitude par $||$ la concaténation de deux chaînes de bits, et par $\oplus$ l'addition bit à bit modulo 2 de deux chaînes de bits.

(a) On note f une fonction dite de compression de $\{0,1\}^{n+k}$ dans $\{0,1\}^n$, avec n et k deux entiers strictement positifs. Rappeler la construction de Merkle-Damgård qui permet de construire à partir d'une telle fonction f une fonction de hachage h de $\{0,1\}^*$ dans $\{0,1\}^n$. Si f est résistante aux collisions, que peut on dire de h ? Rappeler la démonstration de ce résultat.

(b) On note dans la suite de l'exercice, $\mathsf{Encrypt}_{sk}(m) = c$ un chiffrement par bloc prenant en entrée un clair m de n bits et une clef sk de k bits et produisant un chiffré c de n bits. Montrer que les trois fonctions de compression f_1, f_2 et f_3 suivantes ne sont pas à sens-unique :

- f_1 qui a une chaîne de bits $m \in \{0,1\}^k$ et une chaîne de bits $z \in \{0,1\}^n$ associe $f_1(m||z) = \mathsf{Encrypt}_m(z)$
- f_2 qui a une chaîne de bits $m \in \{0,1\}^n$ et une chaîne de bits $z \in \{0,1\}^n$ associe $f_2(m||z) = \mathsf{Encrypt}_z(m) \oplus z$, en supposant $n = k$
- f_3 qui a une chaîne de bits $m \in \{0,1\}^n$ et une chaîne de bits $z \in \{0,1\}^n$ associe $f_3(m||z) = \mathsf{Encrypt}_z(z) \oplus m$, en supposant $n = k$

(c) Ces fonctions sont elles résistantes aux collisions ?

(d) On considère maintenant la fonction de compression f qui a une chaîne de bits $m \in \{0,1\}^n$ et une chaîne de bits $z \in \{0,1\}^k$ associe $f(m||z) = \mathsf{Encrypt}_z(m) \oplus m$. On note pour toute chaîne de bits x, $\overline{x} = x \oplus (11 \dots 1)$, la chaîne de bits de même longueur que x constituée des bits complémentaires de ceux de x. On suppose de plus que le chiffrement par bloc vérifie la propriété suivante : $\mathsf{Encrypt}_{\overline{z}}(\overline{m}) = \overline{\mathsf{Encrypt}_z(m)}$ pour tout $m \in \{0,1\}^n$ et $z \in \{0,1\}^k$. Montrer que f n'est pas résistante aux collisions.