Université de Bordeaux
Collège Sciences et Technologies
Année 2020-2021

Master CSI
Cryptologie

Devoir Surveillé, 25 février 2021
Durée 1h30, documents interdits

La qualité de la rédaction sera un facteur d'appréciation.

Exercice 1 –

1) Proposer un système de chiffrement à clé secrète où l'espace des messages clairs (que l'on supposera équiprobables) est $\mathcal{M} = \{a, b\}$, celui des messages chiffrés est $\mathcal{C} = \{1, 2, 3, 4\}$, celui des clés (équiprobables) est $\mathcal{K} = \{\text{i}, \text{ii}, \text{iii}, \text{iv}, \text{v}, \text{vi}\}$ et qui obéit aux contraintes suivantes :

- Deux clés ne chiffrent pas de la même manière ;
- Tous les éléments de $\mathcal{C}$ sont utilisés ;
- Le système est à confidentialité parfaite ;
- Les probabilités d'imposture P_I et de substitution P_S du système sont strictement inférieures à 1.

Comme d'habitude les variables M et K sont indépendantes. Il est demandé de justifier la confidentialité parfaite et de déterminer P_I et P_S. Le système pourra être décrit par un tableau comme ci-dessous :

$\mathcal{M}$ \ $\mathcal{K}$	i	ii	iii	iv	v	vi
a						
b						

2) Si c'est possible, en utilisant au plus deux clés supplémentaires, améliorer la probabilité d'imposture tout en préservant la confidentialité parfaite. Quelles sont les probabilités d'imposture et de substitution de ce nouveau système ?

Exercice 2 – Soient un entier $\ell \geq 1$ et une application $f : \{0,1\}^\ell \to \{0,1\}^\ell$. Pour tout bloc $[L\|R] \in \{0,1\}^{2\ell}$ (où L et $R \in \{0,1\}^\ell$ sont les parties gauche et droite du bloc), on pose $T_f([L\|R]) = [L \oplus f(L \oplus R)\|R \oplus f(L \oplus R)]$.
1) On chiffre un bloc $[L\|R]$ en appliquant successivement les transformations T_{f_1}, $T_{f_2}, \ldots, T_{f_s}$ où $s \geq 1$ et où les f_i sont des applications de $\{0,1\}^\ell$ dans lui-même. Peut-on distinguer ce schéma d'une transformation aléatoire ? Si oui, comment ?
2) Quel est l'algorithme de déchiffrement ?
3) Montrer qu'une transformation T_f correspond à un schéma de Feistel comportant trois tours $[L\|R] \mapsto [R\|L \oplus g_i(R)]$ $(1 \leq i \leq 3)$, *avec permutation gauche-droite finale*, où les g_i sont des applications de $\{0,1\}^\ell$ dans lui-même que l'on précisera.

Exercice 3 – Soit $E_K : \mathbb{F}_2^{64} \to \mathbb{F}_2^{64}$ une fonction de chiffrement à clé secrète K agissant sur des blocs de 64 bits. Considérons la variante suivante du mode opératoire CFB vu en cours. Le message clair est découpé en blocs de 16 bits : $M = M_1\|M_2\|M_3\|\ldots$, où $M_i \in \mathbb{F}_2^{16}$ pour tout i. On choisit un bloc initial aléatoire V_0 de 64 bits puis pour $i = 1, 2, 3, \ldots$, on pose :

(1) $C_i = M_i \oplus R_{16}(E_K(V_{i-1}))$
(2) $V_i = C_i \| L_{48}(V_{i-1})$

où $L_{48}(X)$ et $R_{16}(X)$ désignent respectivement les 48 premiers bits et les 16 derniers bits de $X \in \mathbb{F}_2^{64}$. Le chiffré est $C = V_0 \| C_1 \| C_2 \| C_3 \| \dots$

1) Décrire l'algorithme de déchiffrement.

2) On chiffre M qui comporte au moins 8 blocs. Au cours de la transmission de C, le bloc C_1 est altéré en $C_1' \neq C_1$, les autres blocs étant correctement transmis, y compris V_0. Quels sont les blocs qui seront probablement erronés à l'issue du déchiffrement ?

3) Même question si c'est V_0 qui est modifié, tous les C_i étant correctement transmis.

Exercice 4 – Soit $(s_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite engendrée par la relation de récurrence

$$s_{i+7} = s_{i+1} + s_i \quad \text{pour tout } i \geq 0$$

et de graine $(1, 0, 0, 0, 0, 0, 1)$.

1) Sans calculer les termes suivants de la suite, déterminer la complexité linéaire et la période de $(s_i)_{i\geq 0}$.

On considère la suite $(t_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ *périodique* de période 15 et dont les 15 premiers termes sont

$$0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0.$$

2) Sans calcul, dire si la suite $(t_i)_{i\geq 0}$ est une MLS ou non. Justifier.

3) À l'aide de sa série génératrice, déterminer la complexité linéaire de $(t_i)_{i\geq 0}$ et une relation de récurrence de plus courte longueur satisfaite par cette suite[1].

4) Quelles sont la complexité linéaire et la période de $(s_i + t_i)_{i\geq 0}$?

5) Même question pour la suite $(t_{2i})_{i\geq 0}$.

[1]On pourra remarquer que dans $\mathbb{F}_2[X]$, $(X^4+X^3+1)(X^4+X^3+X^2+X+1) = X^8+X^4+X^2+X+1$.