Université de Bordeaux
Collège Sciences et Technologies
Année 2022-2023

Master CSI
Cryptologie

Devoir Surveillé, 22 février 2023

Durée 1h30, documents interdits

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

Exercice 1 – On considère un cryptosystème symétrique dans lequel l'espace des clairs et l'espace des chiffrés sont finis de même cardinal : $|\mathcal{M}| = |\mathcal{C}|$. Quelles sont les probabilités d'imposture et de substitution de ce système ?

Exercice 2 – On considère un système de chiffrement symétrique où l'espace des messages clairs est $\mathcal{M} = \{a, b, c\}$, l'espace des messages chiffrés est $\mathcal{C} = \{1, 2, 3, 4, 5, 6\}$ et celui des clés est $\mathcal{K} = \{\text{i}, \text{ii}, \text{iii}, \text{iv}, \text{v}, \text{vi}, \text{vii}, \text{viii}, \text{ix}\}$. Le système est décrit par le tableau suivant dont certaines cases ont été effacées :

$\mathcal{M}$ \ $\mathcal{K}$	i	ii	iii	iv	v	vi	vii	viii	ix
a		1		5		4	2	6	6
b	2			1	6	3	5	2	4
c	6	5		4	1	1		3	

On suppose, comme d'habitude, que la clé est indépendante du message clair. On suppose également que les clés sont équiprobables et, pour simplifier, que les messages clairs le sont aussi.

(1) Remplir les cases vides de manière à rendre le système à confidentialité parfaite. Justifier.
(2) Quelles sont les probabilités d'imposture et de substitution du système ?

Exercice 3 – On s'intéresse ici au mode opératoire dit PCBC (Plaintext Cipher Block Chaining) utilisé pour un chiffrement par bloc à clé secrète. Le fonctionnement en est le suivant. Alice désire envoyer à Bob le clair $M = m_1 \| m_2 \| \dots \| m_s$ où les m_i sont des blocs de l bits et $s \geq 2$. Leur clé secrète est K, la fonction de chiffrement qui va de $\{0,1\}^l$ dans $\{0,1\}^l$ est notée E_K et celle de déchiffrement D_K.

- Elle prend un bloc aléatoire initial de l bits $IV = c_0$;
- Elle calcule $c_1 = E_K(m_1 \oplus c_0)$;
- Pour $2 \leq i \leq s$ elle calcule $c_i = E_K(m_i \oplus m_{i-1} \oplus c_{i-1})$;
- Le chiffré envoyé à Bob est $C = c_0 \| c_1 \| \dots \| c_s$.

(1) Décrire l'algorithme de déchiffrement.
(2) Un attaquant intercepte C et le transforme en substituant à un c_i un $c'_i \neq c_i$. Que se passera-t-il au cours du déchiffrement ?
(3) Alice et Bob veulent exploiter cette propriété en terminant toujours les messages clairs à envoyer par un bloc m_s fixé d'avance et connu d'eux seuls. Ainsi, si une attaque de ce type a lieu, Bob le saura car il ne retrouvera pas m_s lors du déchiffrement. Montrer que malgré tout, si $s \geq 4$, l'attaquant peut intervertir

deux blocs chiffrés consécutifs, c_j et c_{j+1} avec $1 < j < j+1 < s$, sans que Bob s'en aperçoive.

Exercice 4 – Soit $s = (s_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ une suite périodique de période 7 et dont les 7 premiers termes sont $0, 1, 0, 1, 1, 0, 0$. Soit $t = (t_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite engendrée par la relation de récurrence linéaire $t_{i+8} = t_{i+7} + t_{i+4} + t_{i+3} + t_i$ pour tout $i \geq 0$ et de graine $1, 1, 0, 1, 0, 1, 0, 0$. Soit enfin $u = (u_i)_{i\geq 0} \in \mathbb{F}_2^{\mathbb{N}}$ la suite définie par $u_i = s_i + t_{2i}$ pour tout $i \geq 0$.

(1) Expliquer pourquoi s n'est pas une MLS.
(2) Déterminer la complexité linéaire de s et la plus courte relation de récurrence linéaire satisfaite par s.
(3) Montrer que X^5+X^2+1 est irréductible dans $\mathbb{F}_2[X]$ et en déduire la décomposition en produit d'irréductibles de $X^8 + X^7 + X^4 + X^3 + 1$.
(4) Déterminer la plus courte relation de récurrence linéaire satisfaite par t.
(5) Quelle est la période de t ? La suite t est-elle une MLS ?
(6) Déterminer la complexité linéaire de u et la plus courte relation de récurrence linéaire satisfaite par u.
(7) Quelle est la période de u ?

Exercice 5 – Soit le premier $p = 503$. Est-ce que 202 est un carré modulo p ?