Université de Bordeaux
Collège Sciences et Technologies
Année 2017-2018

Master CSI
Cryptologie

Corrigé du devoir surveillé du 28 Février 2018

Exercice 1 – On a $\Pr(M = 0|C = 0) = 1$, et si $c \neq 0$ $\Pr(M = 0|C = c) = 0$. Mais $\Pr(M = 0) = 1/26^n$.

Exercice 2 –

1) Soient $m \in \mathcal{M}$ et $c \in \mathcal{C}$. Pour fixer les idées, prenons $m = a$ et $c = 1$. Alors

$$\begin{aligned}
\Pr(M = a|C = 1) &= \frac{\Pr(M = a, C = 1)}{\Pr(C = 1)} \\
&= \frac{\Pr(M = a, K = \mathrm{i})}{\Pr(C = 1)} \\
&= \frac{\Pr(M = a)\Pr(K = \mathrm{i})}{\Pr(C = 1)} \\
&= \frac{1/3 \times 1/6}{3/18} \\
&= 1/3 \\
&= \Pr(M = a)
\end{aligned}$$

Les autres cas sont similaires par permutation. Le système est donc à confidentialité parfaite.

2) Un attaquant envoie par exemple 1. Ce message sera accepté si la clé est i, v ou vi. Dans les autres cas, on a toujours trois clés sur six compatibles. La probabilité d'imposture est donc de $3/6 = 1/2$.

Cette fois-ci, il intercepte un chiffré et cherche à lui substituer un autre chiffré. Admettons qu'il intercepte par exemple 1. La clé utilisée est donc i, v ou vi. Il lui substitue un chiffré $\neq 1$ qui a le plus de chance d'être accepté. Facilement on voit que c'est 2 ou 6 car parmi ces trois clés, deux font que le chiffré 2 ou 6 sera accepté, à savoir les clés i et vi pour 2, les clés v et vi pour 6. Pour 3 et 5 une seule clé convient (i et v respectivement). Pour 4, aucune. Les autres cas se traitent de la même façon. La probabilité de substitution est donc de 2/3.

Exercice 3 – La fonction inverse de F_i est $G_i : A\|B \mapsto B + f_i(A)\|A$ et le déchiffrement correspond à $G_1 \circ G_2 \circ G_3$. Si on note F la fonction de chiffrement et G celle de déchiffrement, on a

$$F : A\|B \mapsto B \oplus f_2(A \oplus f_1(B))\|A \oplus f_1(B) \oplus f_3(B \oplus f_2(A \oplus f_1(B))),$$
$$G : A\|B \mapsto B \oplus f_3(A) \oplus f_1(A \oplus f_2(B \oplus f_3(A)))\|A \oplus f_2(B \oplus f_3(A)).$$

Si on déchiffre $0\|0$ on obtient

$$X^L\|X^R = f_3(0) \oplus f_1(f_2(f_3(0)))\|f_2(f_3(0)).$$

Remarquons que

$$X^L = f_3(0) \oplus f_1(X^R).$$

On chiffre $0\|X^R$ et on obtient

$$Y^L\|Y^R = X^R \oplus f_2(f_1(X^R))\|f_1(X^R) \oplus f_3(X^R \oplus f_2(f_1(X^R))).$$

On a alors

$$X^L \oplus Y^R = f_3(0) \oplus f_3(X^R \oplus f_2(f_1(X^R))).$$

Déchiffrons $Y^L\|X^L \oplus Y^R$. Le bloc de droite est

$$Z^R = Y^L \oplus f_2(X^L \oplus Y^R \oplus f_3(Y^L)).$$

Or

$$f_3(Y^L) = f_3(X^R \oplus f_2(f_1(X^R))) = Y^R \oplus f_1(X^R).$$

On a donc

$$Z^R = Y^L \oplus f_2(X^L \oplus f_1(X^R)) = Y^L \oplus f_2(f_3(0)) = Y^L \oplus X^R.$$

Exercice 4 –

1) L'algorithme de déchiffrement est

(1) $m_1 = D_K(c_1) \oplus c_0 = D_K(c_1) \oplus IV$;
(2) $I_1 = (0, 0, \ldots, 0) \in \mathbb{F}_2^k$;
(3) Pour $2 \leqslant i \leqslant n$, $I_i = I_{i-1} \oplus c_{i-1}$ et $m_i = D_K(c_i) \oplus I_i$.

2) Si $i > 0$ et si c_i est altéré, $m_i = D_K(c_i) \oplus I_i$ (où I_i est correct) sera faux. De plus, I_{i+1} sera faux, et donc m_{i+1} aussi. De même I_{i+2} sera faux et m_{i+2} aussi. On voit en fait que tous les m_j obtenus pour $j \geqslant i$ seront erronés.
Si c'est c_0 qui est faux, m_1 sera erroné mais les m_j avec $j > 1$ seront exacts (c_0 n'intervient qu'en (1)).

Exercice 5 –

1) Les premiers termes de la suite u sont $1011011011\ldots$ On voit que $u_{i+3} = u_i$ pour $0 \leqslant i \leqslant 4$ et pour $i \geqslant 5$ on procède par récurrence sur i en appliquant la relation de récurrence linéaire suivant le schéma $u_{i+3} = u_{i+2} + u_{i-2} = u_{i-1} + u_{i-5} = u_i$. La période de u vaut donc 3.

2) Si $P(X) = X^5 + X^4 + 1$ qui est le polynôme caractéristique de u est irréductible, la période de u (de vecteur initial non nul) est l'ordre de n'importe quelle racine de $P(X)$ dans $\mathbb{F}_{2^5}^\times$. Elle doit donc diviser 31. Absurde.

3) Les premiers termes de v sont $10010111001011\ldots$ On voit que $v_{i+7} = v_i$ pour $0 \leqslant i \leqslant 4$ et pour $i \geqslant 5$ on procède par récurrence sur i en appliquant la relation de récurrence linéaire suivant le schéma $v_{i+7} = v_{i+6} + v_{i+2} = v_{i-1} + v_{i-5} = v_i$. La période de v vaut donc 7.

4) On utilise la périodicité de u et v.

$$\begin{aligned} U(X) &= 1 + X^2 + (1+X^2)X^3 + (1+X^2)X^6 + \cdots \\ &= (1+X^2)(1 + X^3 + X^6 + \cdots) \\ &= \frac{1+X^2}{1+X^3}. \end{aligned}$$

On obtient de même

$$\begin{aligned} V(X) &= 1 + X^3 + X^5 + X^6 + (1 + X^3 + X^5 + X^6)X^7 + (1 + X^3 + X^5 + X^6)X^{14} + \cdots \\ &= (1 + X^3 + X^5 + X^6)(1 + X^7 + X^{14} + \cdots) \\ &= \frac{1 + X^3 + X^5 + X^6}{1 + X^7}. \end{aligned}$$

5) On met les fractions précédentes sous forme irréductible. On obtient

$$U(X) = \frac{(1+X)^2}{(1+X)(1+X+X^2} = \frac{1+X}{1+X+X^2},$$

$$V(X) = \frac{(1+X)^3(1+X+X^3)}{(1+X)(1+X+X^3)(1+X^2+X^3)} = \frac{(1+X)^2}{1+X^2+X^3}.$$

La complexité linéaire de u vaut 2, celle de v vaut 3.

6) Par la question précédente on connaît les polynômes de connexion minimaux de u et v, à savoir $1 + X + X^2$ et $1 + X^2 + X^3$. On en déduit que u et v vérifient

$$u_{i+2} = u_{i+1} + u_i \quad \text{et} \quad v_{i+3} = v_{i+1} + v_i \quad \text{pour tout } i \geqslant 0.$$

En outre ces relations sont les plus courtes vérifiées par u et v.

7) Les polynômes $X^2 + X + 1$ et $X^3 + X^2 + 1$ sont premiers entre eux. La complexité linéaire de $u + v$ vaut donc $2 + 3 = 5$.
De plus on a évidemment $(u + v)_{i+21} = u_{i+21} + v_{i+21} = u_i + v_i = (u + v)_i$. La période de $u + v$ divise donc 21. Comme ce n'est ni 1, ni 3 (car $v_{i+3} = v_i$ pour tout i est faux), ni 7 (car $u_{i+7} = u_i$ pour tout i est faux), la période de $u + v$ est 21.