Cryptanalyse — 4TCY902U
Responsable : G. Castagnos

Examen — mardi 18 décembre 2018

Durée 3h
Documents non autorisés
Les exercices sont indépendants

$\boxed{1}$ Soit $a, b, \mathrm{K}, \mathrm{M} \in \mathbf{N}^*$, des entiers positifs non nuls tels que $a < \mathrm{M}$ et $b < \mathrm{M}$. On considère le réseau $\mathscr{L}$ de $\mathbf{R}^3$ de base donnée par les lignes de la matrice suivante

$$\begin{pmatrix} 1 & 0 & \mathrm{K}a \\ 0 & 1 & \mathrm{K}b \end{pmatrix}.$$

(a) Soit $w = (w_1, w_2, w_3)$ un vecteur de $\mathscr{L}$. Montrer que si w_3 est non nul alors $\|w\| \geqslant \mathrm{K}$.

(b) Soit b_1 le premier vecteur d'une base LLL réduite. On rappelle que $\|b_1\| \leqslant \sqrt{2}\|w\|$ pour tout $w \in \mathscr{L}$. Montrer que $\|b_1\| \leqslant 2\mathrm{M}$.

(c) On suppose $\mathrm{K} > 2\mathrm{M}$. En utilisant le fait que la réduction agit sur la base du réseau par des opérations élémentaires, montrer que la base LLL réduite de $\mathscr{L}$ est de la forme

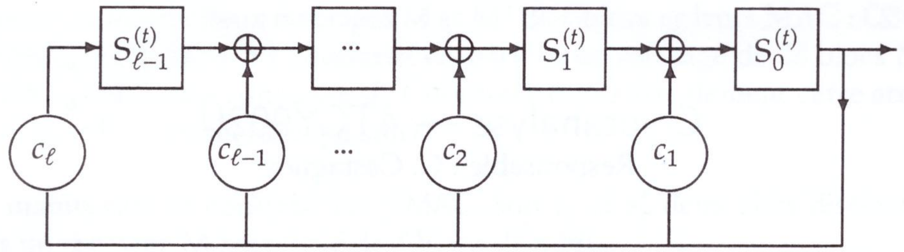
$$\begin{pmatrix} x_1 & x_2 & 0 \\ u & v & \pm \mathrm{K}g \end{pmatrix}$$

où $g = pgcd(a, b) = \pm(ua + vb)$.

$\boxed{2}$ Soit $f(\mathrm{X}) \in \mathbf{F}_2[\mathrm{X}]$ un polynôme de degré ℓ avec $f(\mathrm{X}) = 1 + c_1\mathrm{X} + \cdots + c_\ell \mathrm{X}_\ell$. On considère un automate constitué d'un registre de ℓ bits et produisant une suite de bits. On note $\mathrm{S}^{(t)} = (\mathrm{S}_0^{(t)}, \mathrm{S}_1^{(t)}, \dots, \mathrm{S}_{\ell-1}^{(t)})$ l'état du registre à l'instant $t \geqslant 0$. À l'instant t, on sort le bit d'indice 0 du registre, $\mathrm{S}_0^{(t)}$, et on met à jour l'état du registre de la façon suivante (calculs dans $\mathbf{F}_2$) :

$$\mathrm{S}_i^{(t+1)} = \mathrm{S}_{i+1}^{(t)} + c_{i+1}\mathrm{S}_0^{(t)}, \text{ pour } 0 \leqslant i \leqslant \ell - 2 \text{ et } \mathrm{S}_{\ell-1}^{(t+1)} = c_\ell \mathrm{S}_0^{(t)}$$

Le polynôme $f(\mathrm{X})$ est son polynôme de rétroaction. On représente l'automate par le schéma suivant :



(a) Donner les 5 premiers bits produits par cet automate dans le cas $\ell = 3$, avec le polynôme de rétroaction $1 + X + X^3$ de registre initial $S^{(0)} = (S_0^{(0)}, S_1^{(0)}, S_2^{(0)}) = (1, 1, 0)$.

(b) On considère maintenant le cas général. Pour tout entier t, on désigne par $S^{(t)}(X)$ le polynôme de $\mathbf{F}_2[X]$ de degré au plus $\ell - 1$ correspondant au registre au temps t : c'est à dire $S^{(t)}(X) = S_0^{(t)} + S_1^{(t)}X + \cdots + S_{\ell-1}^{(t)}X^{\ell-1}$. On note z_t le bit sorti au temps t (c'est à dire $S_0^{(t)}$).

Montrer que pour tout entier $t \geqslant 0$, $X \times S^{(t+1)}(X) = S^{(t)}(X) + z_t \times f(X)$.

(c) On note $Z^{(0)}(X) = 0$ et pour tout $t \geqslant 1$, $Z^{(t)}(X) := z_0 + z_1X + \cdots + z_{t-1}X^{t-1}$. Montrer que pour tout $t \geqslant 0$, $S^{(0)}(X) = f(X) \times Z^{(t)}(X) + X^t \times S^{(t)}(X)$.

(d) On note $Z(X)$ la série génératrice de la suite produite par cet automate, c'est à dire que $Z(X) = \sum_{t\geqslant 0} z_t X^t$. Déduire de la question précédente que $Z(X) = S^{(0)}(X)/f(X)$. Montrer que toute suite récurrente linéaire produite par un LFSR peut l'être par cet automate et réciproquement.

(e) Soit $z = (z_t)_{t\geqslant 0}$ la suite produite par cet automate avec les paramètres de la question (a). Quel LFSR permet de produire la même suite z ? Avec quelle initialisation ?

Réciproquement, soit $s = (s_t)_{t\geqslant 0}$ la suite produite par un LFSR de longueur 4, de polynôme de rétroaction $1 + X^3 + X^4$, initialisé par $(1, 1, 1, 1)$. Quel polynôme de rétroaction et quelle initialisation choisir pour que l'automate de cet exercice produite la même suite s ?

(f) Pour des implantations matérielles on préfère parfois représenter les LFSR comme introduit dans cet exercice plutôt qu'en mode classique. Pourquoi ?

$\boxed{3}$ Attaque différentielle

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.

On considère un chiffrement par bloc de 64 bits employant 2 clefs de tours K_0 et K_5 de 64 bits et 4 sous clefs de 16 bits, K_1, K_2, K_3 et K_4. Soit F_{K_i} avec $1 \leqslant i \leqslant 4$ une fonction de tour définie plus bas, prenant en entrée 32 bits et ressortant 32 bits. Soit M un bloc de 64 bits à chiffrer. On pose $X_0 = M \oplus K_0$, puis on effectue 4 tours de schéma de Feistel avec la fonction F_{K_i} : On note $X_0 = L_0 || R_0$ avec L_0 et R_0 de 32 bits, puis pour $i \in \{1, \ldots 4\}$,

$$L_i = R_{i-1}, \qquad R_i = L_{i-1} \oplus F_{K_i}(R_{i-1})$$

Le chiffré est $C = (R_4 \| L_4) \oplus K_5$.

La fonction de tour utilise deux boîtes S, S_0, S_1 prenant en entrée 16 bits et ressortant 8 bits définie comme suit :

$$S_i(x, y) = (x + y + i \quad mod\ 256) << 2,$$

pour $i \in \{0, 1\}$, en identifiant les entiers entre 0 et 255 et leur représentation binaire sur 8 bits (bit de poids faible à droite), et où $<< 2$ désigne la rotation circulaire de deux bits vers la gauche.

La fonction de tour $F_K(X)$ pour X de 32 bits et K une sous clef de 16 bits est définie ainsi : on note $X = x_0 \| x_1 \| x_2 \| x_3$ avec les x_i de 8 bits, et $K = K^L \| K^R$ avec K^L, K^R de 8 bits. On calcule :

$$u = S_1(x_0 \oplus x_1 \oplus K^L, x_2 \oplus x_3 \oplus K^R),$$

et

$$v = S_0(x_2 \oplus x_3 \oplus K^R, u)$$

Enfin $F_K(X) = S_0(x_0, u) \| u \| v \| S_1(x_3, v)$.

(a) Montrer que pour tout $(x, y) \in \{0, 1\}^8 \times \{0, 1\}^8$,

$$S_0(x \oplus 1000\ 0000, y) = S_0(x, y) \oplus 0000\ 0010.$$

(b) Soit $M, M^\star \in \{0, 1\}^{64}$ deux messages clairs, tel que $M \oplus M^\star =$

$$1000\ 0000\ 1000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000\ 0000.$$

On note $(L_2 \| R_2)$ (resp. $(L_2^\star \| R_2^\star)$) l'entrée du troisième tour lors du chiffrement de M (resp. de $M^\star$).

Que vaut la différence à l'entrée du troisième tour, c'est à dire $(L_2 \| R_2) \oplus (L_2^\star \| R_2^\star)$?

(c) Soit $O = 0 \ldots 0$ la chaîne nulle de 16 bits. Soit $K = K^L \| K^R$ une sous clef de 16 bits avec K^L, K^R de 8 bits. Montrer que pour tout X de 32 bits,

$$F_K(X) = F_O(X \oplus (0000\ 0000 \| K^L \| K^R \| 0000\ 0000)).$$

(d) On note $K_5 = K_5^L \| K_5^R$ avec K_5^L, K_5^R de 32 bits.

Déduire des deux questions précédentes une attaque utilisant 2 clairs choisis permettant de retrouver la valeur de $K_5^R \oplus (0000\ 0000 \| K_4^L \| K_4^R \| 0000\ 0000)$. Quelle est sa complexité ?

4 Constructions de MAC

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) Rappeler ce qu'est un MAC (*Message authentication code*). Quelles propriétés de sécurité apporte-t-il ? Quelles sont les différences avec une signature numérique ?

Soit $\mathsf{Encrypt}_{sk}(m) = c$ un algorithme de 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. Le schéma CBC – MAC, dont la description suit, utilise le mode opératoire CBC pour construire un MAC.

On considère un message M constitué de ℓ blocs de n bits : $M = M_1, M_2, \ldots, M_\ell$.

On pose $C_1 = \mathsf{Encrypt}_{sk}(M_1)$, puis $C_i = \mathsf{Encrypt}_{sk}(M_i \oplus C_{i-1})$ pour $2 \leqslant i \leqslant \ell$.

Le MAC de M noté $\mathsf{CBC}-\mathsf{MAC}_{sk}(M)$, est la valeur C_ℓ.

(b) On suppose connaître deux messages M et M′ de ℓ blocs et leurs MAC : $\mathsf{CBC-MAC}_{sk}(M)$ et $\mathsf{CBC-MAC}_{sk}(M')$. Montrer comment construire un message de 2ℓ blocs M″ et son MAC, $\mathsf{CBC-MAC}_{sk}(M'')$ sans connaître sk. Comment éviter simplement cette attaque (autrement qu'en utilisant la construction qui suit) ?

On considère maintenant la construction EMAC. Soit s_k et s'_k deux clefs distinctes de k bits. On considère toujours un message M constitué de ℓ blocs de n bits.

Le MAC de M par EMAC, noté $\mathsf{EMAC}_{sk,sk'}(M)$, est la valeur $\mathsf{Encrypt}_{sk'}(\mathsf{CBC-MAC}_{sk}(M))$, c'est à dire que l'on surchiffre le résultat obtenu par CBC – MAC avec une deuxième clef sk'.

(c) On suppose dans cette question que les deux clefs sont choisies égales, c'est à dire $sk = sk'$. Montrer que cela revient à une construction de type CBC – MAC. En déduire que comme dans la question précédente, à partir de deux messages M et M′ de ℓ blocs et leurs MAC, $\mathsf{EMAC}_{sk,sk}(M)$ et $\mathsf{EMAC}_{sk,sk}(M')$, il est possible de construire un message plus long M″ et son MAC, $\mathsf{EMAC}_{sk,sk}(M'')$ sans connaître sk.

(d) On revient au cas général de EMAC avec $sk \neq sk'$. On suppose connaître $2^{n/2}$ messages $M^{(i)}$ avec $1 \leqslant i \leqslant 2^{n/2}$ et leurs MAC, $\mathsf{EMAC}_{sk,sk'}(M^{(i)})$. Montrer qu'avec une bonne probabilité, il existe deux entiers distincts i et j avec $1 \leqslant i,j \leqslant 2^{n/2}$, tel que connaissant de plus $\mathsf{EMAC}_{sk,sk'}(M^{(i)}\|R)$ pour un R quelconque, on puisse construire $\mathsf{EMAC}_{sk,sk'}(M^{(j)}\|R)$, sans connaître les clefs sk et sk'.

On considère maintenant une légère variante de cette construction, notée EMAC – TDES utilisant le DES avec une clef sk de 56 bits pour la partie CBC puis pour le chiffrement final, la variante Triple-DES à deux clefs de 56 bits. Pour ces deux clefs, on prend la clef sk utilisée pour la partie CBC et une autre clef sk' avec $sk' \neq sk$. On rappelle que l'on a alors $\mathsf{Triple-DES}_{sk,sk'}(X) := \mathsf{DES}_{sk}(\mathsf{DES}^{-1}_{sk'}(\mathsf{DES}_{sk}(X)))$.

Plus précisément, soit un message M constitué de ℓ blocs de 64 bits, notés $M_1, \dots, M_\ell$.

On pose $C_1 = \mathsf{DES}_{sk}(M_1)$, puis $C_i = \mathsf{DES}_{sk}(M_i \oplus C_{i-1})$ pour $2 \leqslant i \leqslant \ell$, et le MAC de M est $\mathsf{EMAC-TDES}_{sk,sk'} = \mathsf{Triple-DES}_{sk,sk'}(C_\ell)$.

(e) On suppose connaître $2^{n/2}$ messages $M^{(i)}$ avec $1 \leqslant i \leqslant 2^{n/2}$ et leur MAC, c'est à dire les valeurs $\mathsf{EMAC-TDES}_{sk,sk'}(M^{(i)})$. Montrer qu'avec une bonne probabilité, il est possible de retrouver les clefs sk et sk' en 2×2^{56} opérations.