Examen Partiel – Cryptographie

vendredi 24 octobre 2008, 14h – 15h30

Documents de cours autorisés
Toutes les réponses devront être soigneusement justifiées

Exercice 1 (Chiffre affine)
On identifie les lettres avec les entiers modulo 26 de la manière usuelle :

$$A = 0,\ B = 1,\ \ldots,\ Z = 25.$$

Pour a, b deux entiers, on considère la fonction affine $f_{a,b}$ sur les lettres définies par $f_{a,b}(\ell) = a\ell + b \mod 26$. Par exemple $f_{5,4}(B) = J$ puisque $B = 1$ et $5 \cdot 1 + 4 = 9 = J$.

1. Calculer l'image du message `BONJOUR` par la fonction $f_{2,5}$.
   Que peut-on en conclure sur l'utilisation de la fonction $f_{2,5}$ comme fonction de cryptage ?

2. Montrer que si $f_{a,b}$ et $f_{a',b'}$ sont deux fonctions affines, alors la composée $f_{a',b'} \circ f_{a,b}$ est aussi une fonction affine.

3. En déduire que l'inverse de la fonction $f_{a,b}$, si elle existe, est la fonction $f_{a',b'}$ où a' et b' vérifie
$$\begin{cases} a'a = 1 \mod 26 \\ a'b + b' = 0 \mod 26. \end{cases}$$

4. Utilisant la question précédente et le fait que $3 \cdot 9 = 27$, décrypter le message suivant qui a été crypté avec la fonction $f_{3,2}$:
   `IJCAB`

Exercice 2
On considère un diagramme de Feistel sur des mots binaires de 4 bits à deux rondes où les fonctions f_1 et f_2 sont les suivantes :

f_1	$00 \mapsto 10$,	$01 \mapsto 10$,	$10 \mapsto 00$,	$11 \mapsto 01$
f_2	$00 \mapsto 11$,	$01 \mapsto 01$,	$10 \mapsto 00$,	$11 \mapsto 10$

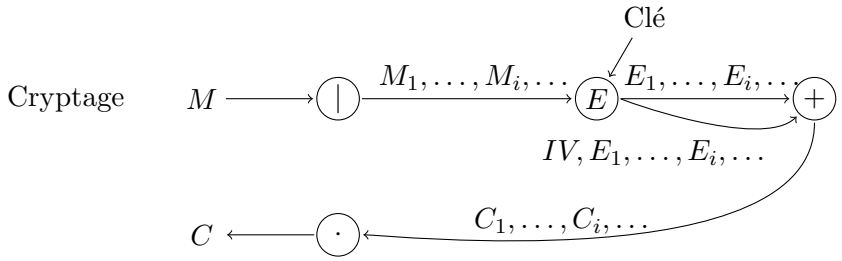
1. Crypter le mot 1101 en utilisant ce diagramme.

2. Trouver tous les mots de 4 bits qui sont invariants par ce diagramme de Feistel.

3. Encrypter le message binaire suivant par ce diagramme de Feistel en utilisant le mode CBC avec pour IV le mot 1111 :

   1000 1001 1111

4. On considère un nouveau mode de codage par blocs défini de la manière suivante



où le cryptage s'effectue, contrairement au mode CBC, *avant* de faire le 'ou exclusif' qui est effectué la première fois avec le mot IV.

(a) Encrypter le message binaire de la question 3. avec ce nouveau mode et le même IV.

(b) Donner l'expression des blocs $C_1, C_2, C_3, \ldots$ en fonction des blocs IV, $E_1, E_2, \ldots$.

(c) Expliquer comment on peut retrouver facilement les blocs $E_1, E_2, E_3, \ldots$ à partir de C et de IV.
En déduire que la sécurité de ce mode est équivalente à celle du mode ECB.

Exercice 3

On considère la fonction f de $\{0,1\}^2$ dans $\{0,1\}^2$ définie par

$$f(a,b) = (a \oplus b, a \wedge b)$$

1. Construire la table de vérité de la fonction f.

Soit w un mot binaire, on note $w_0, w_1, \ldots$ les chiffres binaires de w *en commençant par la droite*. Ainsi, pour $w = 100$, on a $w_0 = w_1 = 0$ et $w_2 = 1$.

On considère l'algorithme suivant qui prend $a, b \in \{0,1\}^n$ en entrée et renvoie $c \in \{0,1\}^{n+1}$.

(1) `Poser` $r \leftarrow 0$, $i \leftarrow 0$.

(2) `Poser` $(s, t_1) \leftarrow f(a_i, r)$, `puis` $(c_i, t_2) \leftarrow f(b_i, s)$.

(3) `Poser` $r \leftarrow t_1 \vee t_2$ `et` $i \leftarrow i + 1$.

(4) `Si` $i < n$ `alors retourner en (2).`

(5) `Poser` $c_n = r$ `et retourner en` $c = c_n c_{n-1} \ldots c_0$.

2. Montrer qu'avec les entrées $a = 10100$ et $b = 10110$, l'algorithme renvoie $c = 101010$. Détaillez les différentes étapes du calcul.

On identifie les mots de n bits et les entiers positifs $\leq 2^n - 1$ de la manière usuelle.

3. Soient $a = 13$ et $b = 9$. Calculer la sortie c renvoyée par l'algorithme en utilisant a et b comme entrées (en détaillant les différentes étapes du calcul).
Vérifier que $a + b = c$.

4. Soit $n \geq 0$ et soient $a_1, a_2 \in \{0,1\}$. Montrer que

$$a_1\, 2^n + a_2\, 2^n = b_1 2^n + b_2 2^{n+1}$$

où $(b_1, b_2) = f(a_1, a_2)$.

5. [Question bonus] Montrer, à l'aide de la question précédente, que l'algorithme calcule la somme de a et de b.