Examen Partiel – Cryptographie

vendredi 10 novembre 2006

Toutes les réponses devront être soigneusement justifiées

Exercice 1

Un message binaire de type GM consiste en un premier bloc de formatage de 8 bits suivi de plusieurs blocs de 32 bits.
Le protocole SP code un message binaire en des blocs de 63 bits. Si le message n'est pas de longueur divisible par 63, alors le protocole ajoute à la fin du message des bits de remplissage.
Quelle est la longueur minimale d'un message de type GM qu'on peut crypter avec le protocole SP de telle sorte qu'exactement 5 bits de remplissage soient nécessaires ?

Solution. Notons l la longueur du message recherché. Puisque ce message est de type GM, il doit être constitué d'un bloc de 8 bits, puis de plusieurs blocs, disons s blocs, de longueur 32 bits. Donc on a $l = 8 + 32s$, ou encore $l \equiv 8 \pmod{32}$.

En ajoutant 5 bits à ce message, on doit pouvoir le coder avec le protocole SP, c'est-à-dire qu'on obtient alors un nouveau message qui peut se couper en blocs de longueur 63 bits, disons t blocs. Donc on a $l + 5 = 63t$, ou encore $l \equiv -5 \pmod{63}$. Ainsi, l vérifie le système

$$\begin{cases} l \equiv 8 & \pmod{32} \\ l \equiv -5 & \pmod{63} \end{cases}$$

En utilisant le théorème des restes chinois, on voit que ce système équivaut à l'unique congruence

$$l \equiv 1192 \pmod{2016}$$

et donc la plus petite longueur possible est 1192 bits.

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

1. Crypter le mot 1111 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 0000 :

$$1000\,1101\,0011\,1110$$

Solution. On rappelle les formules suivantes du cours : si $w = w_1 \cdot w_2$ est le mot d'entrée alors le diagramme de Feistel renvoie le mot de sortie $w' = w'_1 \cdot w'_2$ avec

$$\begin{cases} w'_1 &= f_2(f_1(w_1) \oplus w_2) \oplus w_1 \\ w'_2 &= f_1(w_1) \oplus w_2 \end{cases}$$

1. On a

$$w'_1 = f_2(f_1(11) \oplus 11) \oplus 11 = f_2(00 \oplus 11) \oplus 11 = f_2(11) \oplus 11 = 00,$$

et

$$w'_2 = f_1(11) \oplus 11 = 00 \oplus 11 = 11.$$

Donc l'image du mot 1111 par ce diagramme est le mot 0011.

2. On veut $w'_1 = w_1$ et $w'_2 = w_2$ donc il faut avoir $f_2(f_1(w_1) \oplus w_2) = 00$ et $f_1(w_1) = 00$. La deuxième formule donne $w_1 = 01$ ou $w_1 = 11$. En remplaçant $f_1(w_1) = 00$ dans la première, on trouve qu'on doit avoir $f_2(w_2) = 00$ et donc $w_2 = 10$. Donc les deux mots invariants par ce diagramme sont 0110 et 1110.

3. On pose

$$M_1 = 1000,\ M_2 = 1101,\ M_3 = 0011,\ M_4 = 1110,$$

et on note $E(m)$ l'image du mot m par le diagramme de Feistel. On obtient les blocs de sortie :

$$\begin{aligned} C_1 &= E(M_1 \oplus IV) = E(1000) = 0111, \\ C_2 &= E(M_2 \oplus C_1) = E(1010) = 1101, \\ C_3 &= E(M_3 \oplus C_2) = E(1110) = 1110, \\ C_4 &= E(M_4 \oplus C_3) = E(0000) = 1111. \end{aligned}$$

et donc la réponse est

$$0111\,1101\,1110\,1111.$$

On peut aussi partir avec $E(IV) = 1111$ à la place de IV et on obtient alors le message crypté suivant

$$1011\,0110\,0001\,0011.$$

Exercice 3
Soient a et b deux entiers non nuls avec a pair et non divisible par 3, et b impair.

1. Montrer que $a^2 + b^2 \equiv 1 \pmod 4$.
2. Montrer qu'il existe un entier u tel que $au \equiv b \pmod 3$, puis que
$$\left(\frac{a^2+b^2}{3}\right) = \left(\frac{1+u^2}{3}\right).$$
3. En déduire la formule suivante :
$$\left(\frac{3}{a^2+b^2}\right) = \begin{cases} 1 & \text{si 3 divise } b, \\ -1 & \text{sinon.} \end{cases}$$

Solution.

1. On écrit $a = 2a'$ et $b = 2b' + 1$ avec a' et b' entiers. On calcule
$$a^2 + b^2 = 4a'^2 + 4b'^2 + 4b' + 1 \equiv 1 \pmod 4.$$
2. Puisque a n'est pas divisible par 3, il est inversible modulo 3 et donc il existe un entier c tel que $ac \equiv 1 \pmod 3$. Il suffit donc de prendre $u = bc$. On calcule
$$\left(\frac{a^2+b^2}{3}\right) = \left(\frac{a^2+a^2u^2}{3}\right) = \left(\frac{a^2(1+u^2)}{3}\right) = \left(\frac{a^2}{3}\right)\left(\frac{1+u^2}{3}\right) = \left(\frac{1+u^2}{3}\right).$$
3. On utilise la loi de réciprocité quadratique
$$\left(\frac{3}{a^2+b^2}\right) = (-1)^{(3-1)(a^2+b^2-1)/4}\left(\frac{a^2+b^2}{3}\right).$$
Pour l'exposant, on a $(a^2 + b^2 - 1)/2$ pair par la question 1. et donc
$$\left(\frac{3}{a^2+b^2}\right) = \left(\frac{a^2+b^2}{3}\right) = \left(\frac{1+u^2}{3}\right)$$
par la question 2. Si b est divisible par 3, On trouve que $u \equiv 0 \pmod 3$, et $\left(\frac{1+u^2}{3}\right) = 1$. Sinon $u^2 \equiv 1 \pmod 3$ et $\left(\frac{1+u^2}{3}\right) = -1$ car 2 n'est pas un carré modulo 3.

Exercice 4
On identifie les lettres avec les entiers $A = 0, B = 1, \ldots, Z = 25$.

On définit une multiplication $*$ sur les entiers de la manière suivante : pour calculer le produit de deux lettres, on transforme les lettres en entiers, on multiplie ces deux entiers et on réduit le résultat modulo 26, puis on le retransforme en une lettre. Par exemple, pour le produit de G et Y, on a $G = 6$ et $Y = 24$ et $6 \times 24 \mod 26 = 14$, donc $G * Y = O$.

Le cryptogramme de César multiplicatif consiste à multiplier toutes les lettres du message par un lettre fixé qui sert de clé.

1. Coder en utilisant le cryptogramme de César multiplicatif le message suivant avec la clé N
$$QUOI$$

2. En déduire que certaines clés donnent des messages cryptés non décryptables. Déterminer toutes ces mauvaises clés.

3. Coder le message ci-dessus avec une clé, de votre choix, permettant un décryptage.

Solution.

1. On a
$$N * Q = A, \quad N * U = A, \quad N * O = A, \quad N * I = A.$$
Donc le codage du message $QUOI$ avec la clé N donne le message $AAAA$. On voit donc que la clé N n'est pas convenable car elle ne permet pas un décodage.

2. Pour qu'une lettre c donne une clé convenable, il faut qu'il existe une lettre d telle que pour toute lettre l, on ait $d*(c*l) = l$. Ceci équivaut à demander que le nombre correspondant à la lettre c doit être inversible modulo 26. Les nombres non inversibles modulo 26 sont ceux qui ne sont pas premiers avec 26, c'est-à-dire ceux qui sont divisibles par 2 ou par 13. Ainsi les mauvaises lettres sont
$$A, C, E, G, I, K, M, N, O, Q, S, U, W, Y.$$

3. On choisit une clé qui n'est pas dans la liste ci-dessus, par exemple H (correspondant à 7). On trouve le message crypté suivant
$$IKUE$$
La clé de décodage est P correspondant à l'inverse de 7 modulo 26, c'est-à-dire 15.