Nom: Prénom:

L3 informatique. Sécurité. Partie J.-F. COUCHOT.

Seule une fiche manuscrite recto-verso de format A4 est autorisée. Tout moyen de communication est interdit. Toutes les réponses doivent être justifiées. Sans justification, une réponse est considérée comme fausse.

1 AES et MixColomns

On rappelle que d'un point de vue pratique, AES représente chaque octet (8 bits) sous la forme d'un mot de deux chiffres hexadécimaux. Théoriquement, AES code chaque octet à l'aide d'un polynome de degré inférieur ou égal à 7, où chaque coefficient est 0 ou 1 et les calculs se font modulo le polynome de de Rijndael $R(X) = X^8 + X^4 + X^3 + X + 1$. L'addition correspond au "ou exclusif" sur les mots binaires.

L'opération Micolumns opère colonne par colonne. Pour un vecteur (a_0, a_1, a_2, a_3) elle effectue le calcul

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

1. Représenter les paires d'hexadécimaux $B2$ et 03 à l'aide de polynômes de degré inférieur ou égal à 7.

2. Montrer que $B2 \times 03 = CD$?

3. Trouver une paire de deux chiffres hexadécimaux XY telle que $03 \times XY = 03$.

4. Même question avec l'équation $03 \times XY = CD$.

Nom: Prénom:

A	B	C	D	E		Q	Y	A	L	S
F	G	H	I	K		Z	C	R	X	E
L	M	N	O	P		F	O	M	W	B
Q	R	S	T	U		V	I	T	G	U
V	W	X	Y	Z		P	D	K	N	H
L	W	D	A	K		A	B	C	D	E
B	C	G	N	H		F	G	H	I	K
O	I	X	E	M		L	M	N	O	P
Z	U	P	Q	R		Q	R	S	T	U
S	T	V	Y	F		V	W	X	Y	Z

FIGURE 1 – Illustration du codage-décodage dans le chiffre des 4 carrés

5. Quelles conséquences cela aurait-il sur l'algorithme AES s'il y avait plusieurs solutions à la question précdente.

2 Chiffre bigraphique des 4 carrés

Le chiffre des 4 carrés se présente sous la forme de 4 tableaux carrés s_1, s_2 et s_3 (5×5) que l'on écrit dans un tableau carré plus grand (voir FIGURE 1). Chaque carré ne contient que 25 lettres de l'alphabet (on considère $I = J$). Dans les carrés en haut à gauche s_1 et en bas à droite (s_1 à nouveau) ces 25 lettres sont écrites dans l'ordre alphabétique. Dans les deux autres carrés (s_2 en haut à droite et s_3 en bas à gauche), elles sont écrites dans un autre ordre. On obtient un tableau qui ressemble à ce qui est donné en FIGURE 1.

On rappelle qu'un bigramme est une paire de lettres. Pour être chiffré, le message $M = M_0M_1M_2M_3$ est découpé en une liste de bigrammes $[M_0M_1, M_2M_3, \dots]$. Le mot *VITESSE* donnerait par exemple $[VI, TE, SS, \dots]$. Chaque bigramme $M_{2k}M_{2k+1}$ est traité comme suit. La position $P_{2k} = (l_{2k}, c_{2k})$ de la première lettre M_{2k} du bigramme est extraite du carré en haut à gauche. La position $P_{2k+1} = (l_{2k+1}, c_{2k+1})$ de la seconde lettre M_{2k+1} du bigramme est extraite du carré en bas à droite.

Dans le carré en haut à droite, la lettre C_{2k} est celle à l'intersection de la ligne de M_{2k} et de la colonne de M_{2k+1}. Dans ce carré, sa position est (l_{2k}, c_{2k+1}). Similairement, dans le carré en bas à gauche, la lettre C_{2k+1} est celle à l'intersection de la colonne de M_{2k} et de la ligne de M_{2k+1}. Dans ce carré, sa position est (l_{2k+1}, c_{2k}). Le bigramme $C_{2k}C_{2k+1}$ est le chiffré de $M_{2k}M_{2k+1}$. Par exemple VI serait chiffré en NB dans la FIGURE 1. La méthode de déchiffrement est à trouver.

1. Chiffrer le couple BP et déchiffrez IQ en considérant les carrés de la FIGURE 1. On pourra justifier en laissant apparents les traits sur la FIGURE 1

Nom: Prénom:

2. On considère les fonctions suivantes :
   — *position*(s, v) : pour une lettre donnée v et un carré s retourne la paire (l, c), position de la lettre v dans le carré s où l est le numéro de ligne et c est le numéro de colonne ;
   — *lettre*(s, l, c) : pour un quarré s, un numéro de ligne l, et un numéro de colonne c retourne la lettre v qui est à la position (l, c) dans s.

   Dans le langage de votre choix, donner le code de la fonction *dechiffre4s*(C) qui dechiffre le bigramme C, chiffré selon cet algorithme.

3. Le chiffre est-il à clef publique ? à clef privée ?

4. Combien existe-t-il de manières de construire s_2, le tableau en haut, à droite.

5. Combien de clés différentes existe-t-il ?

6. Supposions que vous obteniez un message chiffré par ce chiffre sans en connaître la clef. Vous souhaitez le déchiffrer par force brute, c'est à dire obtenir un message lisible à partir d'une clé et, ce, en testant toutes les clefs possibles. On affirme que $25! \approx 1.55 \times 10^{25} \approx 2^{84}$. En moyenne, combien d'essais doit-on faire pour trouver la clef ?

7. Est-ce réaliste sur un ordinateur récent ? Quelle alternative proposeriez-vous ?

Nom: Prénom:

3 Codes correcteurs d'erreurs de Hamming $(2^k - 1, 2^k - k - 1)$

Dans ce qui suit, on considère le code de Hamming systématique $(2^k - 1, 2^k - k - 1)$.

1. Donner le code d'une fonction java ou python qui prend en paramètre k et qui retourne H_k une matrice de contrôle.

2. Donner le code d'une fonction java ou python qui prend en paramètre une matrice de contrôle H_k et v un vecteur binaire de taille $2^k - 1$ et qui retourne le mot de code associé à v.