DS du 28 mai 2009

Durée 1h30 - documents non autorisés

Exercice 1. *Corps à 256 éléments*

Question 1. Quel système de chiffrement fait appel à l'arithmétique sur le corps $\mathbb{F}_{256}$ à 256 éléments ?

Dans ce système, les éléments du corps sont considérés comme des polynômes à coefficients dans le corps à 2 éléments modulo le polynôme $P(X) = X^8 + X^4 + X^3 + X + 1$.

Question 2. Parmi les polynômes qui suivent, un seul aurait pu être un autre candidat pour définir l'arithmétique du corps $\mathbb{F}_{256}$. Lequel et pourquoi ?

1. $X^8 + X^2 + X + 1$;
2. $X^7 + X + 1$;
3. $X^8 + X^7 + X^3 + X^2 + 1$;
4. $X^8 + X^2 + 1$.

Les éléments du corps $\mathbb{F}_{256}$ sont des polynômes de degré au plus 7 que l'on peut représenter par des octets dont le bit de poids faible (le plus à droite) représente le coefficient du terme de degré 0, le bit qui suit celui du terme de degré 1, ... et enfin le bit de poids fort est le coefficient du terme de degré 7.

Question 3. Avec l'arithmétique du corps définie par le polynôme trouvé dans la question précédente, calculez le produit des deux octets `0x0F` et `0x28`.

Exercice 2. *Chiffrement affine*

On considère dans cet exercice un alphabet de 30 symboles, constitué des 26 lettres de l'alphabet latin auxquelles on ajoute quatre symboles de ponctuation : l'espace, la virgule, le point-virgule et le point. Ces 30 symboles sont codés numériquement par les entiers de 0 à 29, en commençant par les lettres dans l'ordre alphabétique usuel `A` → 0, ..., `Z` → 25, puis les quatre symboles de ponctuation `ESP` → 26, , → 27, ; → 28 et . → 29.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		,	;	.
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

Le système envisagé ici pour chiffrer des messages écrits à l'aide de cet alphabet est le chiffrement affine dans lequel chaque caractère est chiffré par la formule

$$c = (a \cdot m + b) \pmod{30},$$

où m désigne le code associé à un caractère clair du message, c le code associé au caractère chiffré correspondant et les entiers a et b constituent la clé secrète.

Question 1. Quelle(s) condition(s) doivent vérifier les entiers a et b pour qu'un message chiffré par ce procédé soit déchiffrable. Donnez alors l'opération de déchiffrement. Donnez aussi le nombre de clés de chiffrement possibles.

Question 2. On utilise ce système en mode CBC. C'est-à-dire que l'on utilise un nombre entier arbitraire iv compris entre 0 et 29 comme vecteur d'initialisation, et que l'on chiffre le i-ème caractère d'un message par le calcul

$$c_i = (a \cdot (m + c_{i-1}) + b) \pmod{30},$$

en considérant que $c_0 = iv$.

Q 2–1. De manière générale quel est l'intérêt du mode CBC ?

Q 2–2. Codez les trois premières lettres de votre nom avec la clé $(a, b) = (17, 20)$ et le vecteur d'initialisation $iv = 3$.

Q 2–3. Déchiffrez le message chiffré « `ZB.S Q` » obtenu avec la même clé mais le vecteur $iv = 22$.

Exercice 3. *LFSR*

On veut construire un LFSR produisant une suite binaire de période 127.

Question 1. Donnez une minoration de la longueur d'un tel LFSR ? Justifiez !

Question 2. Construisez un LFSR de longueur minimale produisant une suite binaire de période 127. Donnez sa longueur et un polynôme de rétroaction.

Question 3. Comment faut-il initialiser votre LFSR pour qu'il produise une telle suite ?

Question 4. Que dire de deux suites de période 127 produites par votre LFSR ? Sont-elles très différentes ?

Question 5. Combien y a-t-il de bits nuls dans une période ?