Master 1 M7 Cryptographie

Examen partiel du 6 novembre 2007

Exercice 1

1. Sachant que le message a été chiffré par la méthode de Vigenère, en utilisant le mot-clef CRYPTO, quel est le message en clair obtenu en déchiffrant le cryptogramme suivant: R R P I B S N U C R K M R K M?
2. Décrivez précisément la méthode que vous avez utilisée , en justifiant votre réponse à la question 1.
3. Indiquez brièvement une méthode, sans (ou avec) l'aide de la Tabula Recta, différente de celle que vous avez utilisée, qui permettrait aussi de trouver la réponse à la question 1.

Exercice 2

On intercepte le message "RT?UMQT):L!!IBSS!!BIJE D" (il y a bien un espace entre E et D). On sait que ce message a été chiffré dans un alphabet de 36 lettres identifiées à
$A = 0$, $B = 1$, $C = 2$,..., $Z = 25$, $! = 26$, $espace = 27$, $' = 28$, $? = 29$, $. = 30$, $; = 31$, $(= 32$, $) = 33$, $:= 34$, $* = 35$, à l'aide d'une matrice 2×2, notée ξ, à coefficients dans $\mathbb{Z}/36\mathbb{Z}$. Les blocs de deux lettres sont donc des vecteurs de $(\mathbb{Z}/36\mathbb{Z})^2$.
On sait que les six dernières lettres du message chiffré correspondent à " itu.p" (il y a un espace au début), qui est la signature en clair de notre adversaire.
Traduisez matriciellement ces informations et vérifiez qu'on ne peut pas calculer la matrice ξ^{-1} de déchiffrement directement, mais, qu'en calculant ξ^{-1} modulo deux entiers bien choisis, on peut en déduire ξ^{-1} modulo 36 par le lemme chinois.
Déchiffrez le message.

Exercice 3

On note 0,1,2, les éléments du corps $\mathbb{F}_3$. Le polynôme $Q = X^3 + 2X^2 + 1$ est irréductible sur $\mathbb{F}_3$, ce qui nous permet d'identifier le corps fini $\mathbb{F}_{27}$au quotient $(\mathbb{F}_3)[X]/(Q)$ de l'anneau de polynômes par l'idéal engendré par Q. On note x la classe de X dans ce quotient. On rappelle que $\mathbb{F}_{27} \simeq \mathbb{F}_3[x]$: tout élément de $\mathbb{F}_{27}$ s'écrit de manière unique comme un polynôme de degré inférieur ou égal à 2 en x et les multiplications dans ce corps se font modulo Q.
Vous devez déchiffrer le message (K,H) (P,X) (N,K) (H,R) (T,F) (V,Y), où chaque couple de ce cryptogramme cache une lettre à trouver.
Le message en clair a été chiffré en utilisant un chiffrement d'El Gamal sur le corps fini $\mathbb{F}_{27}$, votre clef secrète de déchiffrement est l'entier $a = 11$, la clef publique de chiffrement est $(x+2)$ et les 26 lettres de l'alphabet sont en correspondance avec les 26 éléments non nuls du corps, de la manière suivante:

A	$=$	1	B	$=$	2	C	$=$	x
D	$=$	$x+1$	E	$=$	$x+2$	F	$=$	$2x$
G	$=$	$2x+1$	H	$=$	$2x+2$	I	$=$	x^2
J	$=$	x^2+1	K	$=$	x^2+2	L	$=$	x^2+x
M	$=$	x^2+x+1	N	$=$	x^2+x+2	O	$=$	x^2+2x
P	$=$	x^2+2x+1	Q	$=$	x^2+2x+2	R	$=$	$2x^2$
S	$=$	$2x^2+1$	T	$=$	$2x^2+2$	U	$=$	$2x^2+x$
V	$=$	$2x^2+x+1$	W	$=$	$2x^2+x+2$	X	$=$	$2x^2+2x$
Y	$=$	$2x^2+2x+1$	Z	$=$	$2x^2+2x+2$			

1. Vérifier rapidement que $x^{11} = x + 2$.
2. Exprimer x^{12} et x^{13} comme des polynômes de degré inférieur ou égal à 2 en x.
   En déduire que x engendre le groupe multiplicatif $\mathbb{F}_{27}^*$.
3. Expliquer pourquoi, pour trouver l'inverse de $(x^2 + 2)^{11}$, on peut calculer $(x^2 + 2)^{15}$.
4. Vérifier, à l'aide de calculs déjà effectués, que $(2x + 2)(x^2 + 2)^{15} = 2x + 1$.
5. Décrire le système de chiffrement d'El Gamal et le déchiffrement que vous devez appliquer, pour justifier que la première lettre du message en clair cherché est un g.
6. Sachant de plus que $x^{14} = 2x$, $x^{16} = 2x^2 + 1$, $x^{19} = x^2 + x$, $x^{21} = 2x^2 + 2x + 1$, déchiffrer les cinq lettres suivantes et donner le mot de six lettres que vous avez trouvé.
7. Donner une estimation du coût d'une addition, puis d'une multiplication, dans un corps fini $\mathbb{F}_q$, où $q = p^n$.