Master 1 M7 Cryptographie

Examen partiel du 6 novembre 2007, corrigé.

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?*
   p a r t i e l d e c r y p t o
2. *Décrivez précisément la méthode que vous avez utilisée , en justifiant votre réponse à la question 1.*
   Avec la table: Nous surlignons les 6 lignes C,R,Y,P,T,O. Nous savons que, pour chiffrer la première lettre du message en clair inconnu de nous, le chiffreur a parcouru la colonne correspondant à cette lettre, jusqu' à la ligne C et qu'il a pris la lettre dans cette case ; c'était le R.
   Donc, pour retrouver la lettre inconnue, à partir du R et du C (première lettre du mot-clef), nous parcourons la ligne C, jusqu'au R, où nous remontons la colonne, ce qui nous donne la lettre p.
   Pour la deuxième lettre, il faut trouver cette fois l'intersection de la ligne R (deuxième lettre du mot-clef) avec une colonne inconnue qui donne la case R; évidemment, nous trouvons a.
   Pour la troisième lettre, la recherche de la colonne qui rencontre la ligne Y en P nous donne r.
   En utilisant successivement toutes les lettres du mot-clef et les 6 premières lettres du cryptogramme, nous trouvons ainsi les 6 premières lettres du message en clair :
   p a r t i e.
   Pour la septième lettre, nous reprenons la ligne C, correspondant à la première lettre du mot-clef, nous trouvons la case N, nous remontons la colonne, et nous en déduisons que la septième lettre du message en clair est l.
   Nous continuons ainsi, pour déchiffrer tout le message. En fait, nous pouvons trouver les trois dernières lettres sans calcul, par symétrie de la table.
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.*
   Sans la table : Nous mettons en correspondance les 26 lettres de l'alphabet, de A à Z, avec les éléments de $\mathbb{Z}/26\mathbb{Z}$, notés de 0 à 25. Le mot-clef CRYPTO est une chaîne de caractères de longueur 6, qui correspond à la clef (2,17,24,15,19,14) dans $(\mathbb{Z}/26\mathbb{Z})^6$. Le texte en clair inconnu a été décomposé en blocs de messages de 6 caractères. Ainsi l'ensemble de définition de la clef, des messages en clair et des messages chiffrés est $(\mathbb{Z}/26\mathbb{Z})^6$. En notant e la fonction de chiffrement, le premier bloc $(x_1,x_2,x_3,x_4,x_5,x_6)$ du message en clair a éte chiffré par $e(x_1,x_2,x_3,x_4,x_5,x_6) = (x_1+2,x_2+17,x_3+24,x_4+15,x_5+19,x_6+14) = (y_1,y_2,y_3,y_4,y_5,y_6) = (17,17,15,8,1,18)$ dans $(\mathbb{Z}/26\mathbb{Z})^6$, ce qui a éte converti en chaîne de 6 caractères alphabétiques RRPIBS .
   Pour déchiffrer, nous effectuons la démarche inverse:
   (1) convertir la chaîne de 6 caractères alphabétiques RRPIBS en un vecteur de $(\mathbb{Z}/26\mathbb{Z})^6$, $(y_1,y_2,y_3,y_4,y_5,y_6) = (17,17,15,8,1,18)$

(2) appliquer la fonction, notée d, de déchiffrement, définie par $d(y_1,y_2,y_3,y_4,y_5,y_6) = (y_1-2,y_2-17,y_3-24,y_4-15,y_5-19,y_6-14) = (x_1,x_2,x_3,x_4,x_5,x_6)$, ce qui donne ici $(x_1,x_2,x_3,x_4,x_5,x_6) = d(17,17,15,8,1,18) = (15,0,17,19,8,4)$ dans $(\mathbb{Z}/26\mathbb{Z})^6$.
(3) convertir $(x_1,x_2,x_3,x_4,x_5,x_6) = (15,0,17,19,8,4)$ en texte clair, ce qui donne:
p a r t i e.
Nous obtenons ainsi les 6 premières lettres du message en clair, puis nous reprenons l'étape (1), avec de nouvelles valeurs des y_i.

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* $x^{11} = x+2$.
   Calculons $x^3 = -2x^2-1 = x^2+2$, $x^4 = x^3+2x = x^2+2x+2$, $x^5 = x^3x^2 = x^4+2x^2 = 2x+2$, d'où $x^{11} = xx^{10} = x(x^5)^2 = x(x^2+2x+1) = x^3+2x^2+x = x+2$.

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 $\mathbb{F}_{27}^*$.
   $\mathbb{F}_{27}^*$ est un groupe multiplicatif cyclique d'ordre 26, l'ordre de x est 1,13 ou 26. Calculons $x^{12} = xx^{11} = x^2 + 2x$ et $x^{13} = x^3 + 2x^2 = 2$, donc x est d'ordre 26.
3. *Expliquer pourquoi, pour trouver l'inverse de $(x^2+2)^{11}$, on peut calculer $(x^2+2)^{15}$.*
   Parce que 26 est l'ordre du groupe, donc l'ordre de x^2+2 divise 26 et $15 = 26-11$, donc $(x^2+2)^{15} = (x^2+2)^{26}(x^2+2)^{-11} = (x^2+2)^{-11}$.
4. *Vérifier, à l'aide de calculs déjà effectués, que $(2x+2)(x^2+2)^{15} = 2x+1$.*
   D'après les calculs précédents, $(2x+2)(x^2+2)^{15} = x^5(x^3)^{15} = x^{50} = x^{24} = (x^{12})^2 = (x^2+2x)^2 = x^4+x^3+x^2 = 2x+1$.
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.*
   D'après les hypothèses, notre clef secrète est l'entier $a = 11$, et nous avons publié la clef publique de chiffrement $(x+2)$. D'après la question 1), $x^{11} = x+2$, donc, d'après la question 2), notre clef publique est bien de la forme x^a, avec x un générateur de $\mathbb{F}_{27}^*$.
   Nous savons que le couple (K,H) correspond à $(x^2+2{,}2x+2) = (x^k{,}(Claire)(x^a)^k)$, où (Claire) désigne la lettre en clair, masquée par le chiffrement d'El Gamal. Pour enlever le masque, nous utlisons notre clef secrète, en multipliant le deuxième terme par le premier terme élevé à la puissance $(-a)$, ou mieux, d'après la question 3), élevé à la puissance 15. Ici, le calcul a déjà été fait question 4), donc (Claire) $= 2x+1$, ce qui correspond à la lettre 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.*
   (P,X) correspond à $(x^2+2x+1{,}2x^2+2x) = (x^{10}{,}x^6)$, donc, ici, (Claire) $= x^6(x^{10})^{15} = x^{156} = (x^{26})^6 = 1$, ce qui donne pour deuxième lettre du message en clair un a.
   (N,K) correspond à $(x^2+x+2{,}x^2+2) = (x^8{,}x^3)$, donc (Claire)$= x^3(x^8)^{15} = x^{123} = x^{19}$, les exposants se simplifiant modulo 26. Puisque $x^{19} = x^2+x$, la troisième lettre est un l.
   (H,R) correspond à $(2x+2{,}2x^2) = (x^5{,}x^{15})$, donc (Claire)$= x^{15}(x^5)^{15} = x^{90} = x^{12} = x^2+2x$, calcul fait question 2), donc la quatrième lettre est un o.
   (T,F) correspond à $(2x^2+2{,}2x) = (x^{20}{,}x^{14})$, donc (Claire)$= x^{14}(x^{20})^{15} = x^{314} = x^2$, donc la cinquième lettre est un i.
   (V,Y) correspond à $(2x^2+x+1{,}2x^2+2x+1) = (x^{17}{,}x^{21})$, donc (Claire)$= x^{21}(x^{17})^{15} = x^{276} = x^{16} = 2x^2+1$, donc la sixième lettre est un s.
   Le message déchiffré est g a l o i s .
7. *Donner une estimation du coût d'une addition, puis d'une multiplication, dans un corps fini $\mathbb{F}_q$, où $q = p^n$.*
   Comme dans le cas $p = 3$, $q = 3$, on suppose $\mathbb{F}_q$ identifié à $(\mathbb{F}_p)[X]/(Q)$, où Q est un polynôme irréductible unitaire de degré n à coefficients dans $\mathbb{F}_p$. Un élément de $\mathbb{F}_q$ est représenté par un polynôme de degré inférieur ou égal à $n-1$ en x, avec $Q(x) = 0$.
   Pour additionner deux éléments , il faut donc faire n additions dans $\mathbb{F}_p$ et le coût est $O(nlogp) = O(logq)$.
   Pour multiplier deux éléments, il faut faire le produit des polynômes correspondants dans $\mathbb{F}_p[X]$, puis prendre le reste de la division euclidienne par Q. Comme le coût d'une multiplication modulo p est $O(log^2 p)$ et d'une division avec l'algorithme d'Euclide est $O(log^3 p)$, le coût total est $O(n^2 log^2 p + nlog^3 p) = O((nlogp)^3) = O(log^3 q)$.
   Si $p = 2$, $q = 2^n$, on a $O(n^2 log^2 2 + nlog^3 2) = O(n^2) = O((log 2^n)^2) = O(log^2 q)$.