Université Bordeaux 1 — **MHT203 – Cryptologie**
Mathématiques — Année 2012–2013

Correction du Devoir Surveillé 1

1) Lorsqu'on calcule le pgcd de 257 et de 2357 on obtient 1, donc 257 est inversible modulo 2357. Pour calculer l'inverse on applique l'agorithme d'Euclide étendu qui permet d'obtenir une identité de Bezout :

	2357	257		
2357	1	0		
257	0	1	9	$(2357 = 257 * 9 + 44)$
44	1	-9	5	$(257 = 44 * 5 + 37)$
37	-5	46	1	$(44 = 37 * 1 + 7)$
7	6	-55	5	$(37 = 7 * 5 + 2)$
2	-35	321	3	$(7 = 2 * 3 + 1)$
1	111	-1018		

Ceci nous montre bien que le pgcd est égal à 1. De plus, on peut ensuite vérifier par le calcul que

$$2357 \times 111 - 257 \times 1018 = 1.$$

Par conséquent l'inverse de 257 modulo 2357 est $-1018 \equiv 1339 \bmod 2357$.

Exercice 1 –

1) Soit $m > 0$ un entier et $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}/26\mathbb{Z})^m$. Pour toute clef $K = (k_1, k_2, \ldots, k_m)$, on définit

$$e_K(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m),$$
$$d_K(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 + k_2, \ldots, y_m + k_m).$$

2) Par soustraction de la valeur du message en clair à la valeur du message chiffré on obtiendra la clef. En pratique on a

c	c	z	g	g	v	a	b	s	w	v	a	q	s	h	z	g	...
2	2	25	6	6	21	0	1	18	22	21	0	16	18	7	25	6	...
l	o	n	g	t	e	m	p	s	j	e	m	e	s	u	i	s	...
11	14	13	6	19	4	12	15	18	9	4	12	4	18	20	8	18	...
17	14	12	0	13	17	14	12	0	13	17	14	12	0	13	17	14	...
R	O	M	A	N	R	O	M	A	N	R	O	M	A	N	R	O	...

En vérifiant le calcul sur tout le texte on constate que le mot clef est **ROMAN**

Exercice 2 –

1) L'équation à résoudre est équivalente à l'équation $2x \equiv 1 \pmod{26}$. Comme le pgcd de 2 et de 26 est égal à 2 et qu'il ne divise pas 1, l'équation n'a pas de solution.

2) L'équation à résoudre est équivalente à l'équation $2x \equiv 4 \pmod{26}$. Comme le pgcd de 2 et de 26 est égal à 2 et qu'il divise 4, l'équation a exactement deux solutions. En divisant toute l'équation par 2 on obtient $x \equiv 2 \pmod{13}$. Finalement les solutions modulo 26 sont

$$x \equiv 2 \pmod{26} \quad \text{et} \quad x \equiv 15 \pmod{26}.$$

3) L'équation à résoudre est équivalente à l'équation $3x \equiv a-2 \pmod{26}$. Comme le pgcd de 3 et de 26 est égal à 1, l'équation a une unique solution. L'inverse de 3 modulo 26 est égal à 9 (car $3 \times 9 = 27$). Par conséquent on obtient l'unique solution :

$$x \equiv 9 \times (a-2) \bmod 26.$$

4) Pour la clef donnée, le chiffrement affine est défini par $y \equiv 3 \times x + 2 \bmod 26$. C'est exactement la troisième équation ci-dessus. Donc pour déchiffrer le message on applique le procédé suivant :

$$x \equiv 9 \times (y-2) \bmod 26.$$

On obtient **Le joueur d'échecs**. Comme on a un chiffrement monoalphabétique, une même lettre dans le message chiffré sera déchiffrée par la même lettre dans le message clair : ceci permet de diminuer vos calculs.