Université Clermont 1
IUT Info 1A
Arithmétique et Cryptographie

Année 2010-2011
Semestres décalés
Malika More

Devoir à la maison

à rendre le lundi 21 février 2011

Exercice 1 (3 points)**.**

1. En utilisant les propriétés des congruences, déterminez successivement les restes de la division euclidienne par 17 des entiers suivants : 100 ; 61 ; 161 ; 6100 ; 61^2 ; 33^{343}.

2. Calculez le PGCD de 385 et 1365.

3. Calculez l'inverse de 125 modulo 242.

Exercice 2 (3 points)**.**

1. Montrez que pour tout entier naturel n, $12n + 1$ et $30n + 2$ sont premiers entre eux.

2. En supposant que $n \geq 1$, en est-il de même pour $4n$ et $n + 1$?

3. Donnez un couple d'entiers relatifs (x, y) solution de l'équation diophantienne

$$345x + 714y = 3$$

Exercice 3 (3 points)**.**

1. Donnez tous les nombres inversibles dans $\mathbb{Z}/25\mathbb{Z}$. Justifiez votre réponse.

2. Résoudre l'équation $5x \equiv 11$ dans $\mathbb{Z}/77\mathbb{Z}$.

3. Quel est le nombre de solutions dans dans $\mathbb{Z}/77\mathbb{Z}$ de l'équation $11x \equiv 6$? Justifiez votre réponse.

Exercice 4 (5 points)**.** On rappelle la correspondance habituelle entre les lettres de l'alphabet $\{A, B, C, \ldots, Z\}$ et les nombres $\{0, 1, 2, \ldots, 25\}$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

1. On utilise la clé de chiffrement $f_1(x) \equiv 17x + 5 \mod 26$.

   (a) Chiffrer le message EXAMEN.

(b) Vérifier que la clé de déchiffrement associée à f_1 est $g_1(x) \equiv 23x + 15 \mod 26$.

(c) Déchiffrer le message WLEHKV.

2. La fonction $f_2(x) \equiv 13x + 18 \mod 26$ est-elle une clé de chiffrement valide ? Pourquoi ?

3. Calculer la clé de déchiffrement g_3 associée à la clé de chiffrement $f_3(x) \equiv 15x + 11 \mod 26$

4. Sachant que dans un chiffrement affine inconnu, la lettre E est chiffrée par O et que la lettre H est chiffrée par J, déterminer la fonction de chiffrement f_4 correspondante.

Exercice 5 (6 points)**.** Il s'agit dans cet exercice de déterminer un entier naturel n dont l'écriture décimale du cube se termine par 2009, c'est-à-dire tel que $n^3 \equiv 2009 \mod 10000$.

1. Déterminer le reste de la division euclidienne de 2009^2 par 16. En déduire que $2009^{8001} \equiv 2009 \mod 16$.

2. On considère la suite (u_n) définie sur $\mathbb{N}$ par $\begin{cases} u_0 = 2009^2 - 1 \\ u_{n+1} = (u_n + 1)^5 - 1 \end{cases}$. Calculer u_1, u_2 et u_3.

3. Vérifier que $u_{n+1} = u_n \times \left(u_n^4 + 5 \times \left(u_n^3 + 2u_n^2 + 2u_n + 1\right)\right)$ pour tout $n \in \mathbb{N}$.

4. Montrer que u_0 est divisible par 5, u_1 est divisible par 25, u_2 est divisible par 125 et u_3 est divisible par 625.

5. En déduire que $2009^{8001} \equiv 2009 \mod 625$

6. Conclure, c'est-à-dire déterminer un entier naturel n dont l'écriture décimale du cube se termine par 2009.

Partie facultative : Chiffrement par substitution

- Un chiffrement par substitution simple consiste à remplacer chaque lettre par une autre, selon une méthode décidée à l'avance.
- Un chiffrement affine correspond à un cas particulier où la substitution se calcule à l'aide d'une fonction affine.

Exercice 6 (Chiffrer/Déchiffrer)**.** Dans le cas général, il n'y a pas de fonction mathématique simple permettant de chiffrer chaque lettre, c'est pourquoi on donne la table de chiffrement en entier. On utilise la substitution suivante :

A	B	C	D	E	F	G	H	I	J	K	L	M
S	C	W	U	D	X	B	F	Y	T	G	Z	I

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
H	O	J	N	K	A	M	L	P	E	Q	R	V

1. Chiffrer le message : FACILE.
2. Écrire la table de déchiffrement correspondante.
3. Déchiffrer le message DAASY.

Exercice 7 (D'où vient ce nom ?)**.** Expliquer pourquoi les chiffrements par substitution font partie des méthodes dites *à clé secrète*.

Exercice 8 (Cette fois, ce n'est pas faible)**.** Combien y-a-t-il de chiffrements par substitution simples différents ?

Exercice 9 (Décryptage)**.** Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement par substitution simple inconnu :

> RC IZQKOGJZCKVYD DTO SUD PDT PYTIYKRYUDT PD RC IZQKOGRGJYD T'COOCIVCUO C KZGODJDZ PDT XDTTCJDT (CTTSZCUO IGUBYPDUOYCRYOD, CSOVDUOYIYOD DO YUODJZYOD) DU T'CYPCUO TGSLDUO PD TDIZDOT GS IRDT. DRRD DTO SOYRYTDD PDKSYT R'CUOYWSYOD, XCYT IDZOCYUDT PD TDT XDOVGPDT RDT KRST YXKGZOCUODT, IGXXD RC IZQKOGJZCKVYD CTQXDOZYWSD, U'GUO WSD WSDRWSDT PYMCYUDT P'CUUDDT P'DHYTODUID. AYDU WS'DXYUDXXDUO TOZCODJYWSD, RC IZQKOGJZCKVYD DTO ZDTODD KDUPCUO OZDT RGUJODXKT SU CZO, KGSZ UD PDLDUYZ SUD TIYDUID WS'CS HHD TYDIRD. CLDI R'CKKCZYOYGU PD R'YUBGZXCOYWSD, TGU SOYRYTCOYGU TD PDXGIZCOYTD PD KRST DU KRST.

1. Que deviennent les méthodes de décryptage utilisées précédemment ?
2. Décrypter le message proposé.
3. Décrire la méthode utilisée.