Département informatique **USTHB Le 14/04/2013**
Faculté Electronique et Informatique **Master SSI 1ère année**
USTHB

Contrôle Continu
Durée 1h30

Exercice 1(6 pts)

Le texte suivant a été chiffré à l'aide d'un chiffrement affine :

J U H K W J Q J E T W

1. Les deux premières lettres du texte en clair sont R et A. Donnez deux équations (mod 26) qui vous permettra de trouver la clé de cryptage.
2. Donnez deux équations qui vous permettent de trouver la clé de déchiffrement.
3. Quel est le message déchiffré?

Exercice 2 (9 pts)

Une autre manière de coder consiste à choisir un entier n, à coder le message comme un entier naturel inferieur à n et à calculer des puissances de cet entier modulo n. Ce codage est basé sur le fait qu'il existe un entier $\Phi(n)$ tel que pour tout entier a premier avec n, on ait $a^{\Phi(n)} \equiv 1 \mod n$.

1. On code comme précédemment les lettres par leurs places dans l'alphabet et on code l'espace par 27, le point par 28. On rappelle que 29 est un nombre premier et que donc pour tout entier m compris entre 1 et 28, on a $m^{28} \equiv 1 \mod 29$.
   (a) Montrer que 19 est inversible dans Z/28Z et trouver son inverse.
   (b) Pour tout entier a premier avec 28, on définit une fonction de codage

   $$f_a : Z/29Z \rightarrow Z/29Z$$
   $$m \rightarrow m^a$$

   Montrer que f_{19} est bijective et que la fonction f_3 est son inverse.
   (c) Décoder le message "I NCI N" (9.27.14.3.9.27.14) qui a été codé avec la fonction f_{19}.
2. (a) Soient p et q deux nombres premiers distincts, n = pq
   Montrer que pour tout entier m premier avec p et q, on a $m^{\Phi(n)} \equiv 1 \mod n$.
   Indication : On pourra utiliser que $m^{p-1} \equiv 1 \mod p$ et $m^{q-1} \equiv 1 \mod q$.
   (b) Pour tout entier e premier avec $\Phi(n)$, on définit une fonction de codage

   $$g_{e,n} : (Z/29Z)^* \rightarrow (Z/29Z)^*$$
   $$m \rightarrow m^e$$

   Montrer que $g_{e,n}$ est bijective de bijection réciproque $g_{d,n}$ où d est un représentant de la classe inverse de la classe de e dans Z/'(n)Z.

3. (c) Application :
   On choisit p = 5, q = 7, donc n = 35. On code l'espace par 34 et chaque lettre de l'alphabet suivant le tableau suivant

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	6	8	9	11	12	13	16	17	18
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
19	22	23	24	26	27	29	31	32	33	33	33	33

   Calculer $\Phi(35)$ et vérifier que 5 est premier avec $\Phi(35)$. Calculer l'inverse de 5 modulo $\Phi(35)$ et en déduire la fonction de décodage associée à la fonction de codage $g_{5,35}$.
   Décoder la phrase "IA MEUSEBEUAQXE MALE" en sachant qu'elle a été codée avec $g_{5,35}$.

Corrige contrôle continu

Exercice 1 :

1

57x+44=249 mod 365
57x=205 mod 365
57^{-1} = 32 mod 365
x=32*205mod 365
x= 10 mod 365
la date est le 11 janvier

2

y = a x+b mod 365
x= a^{-1}(y-b) mod 365 $\rightarrow$a inversible pgcd(a,365))=1
la fonction de déchiffrement est
x= a^{-1}(y-b) mod 365
55x+1=221 mod 365 $\rightarrow$ 55x= k*365+220
Or 55 n'est pas premier avec 365, on divise alors l'équation 55x= k*365+220 par 5 ce qui donne 11x=k*73+44 cette équation est équivalente à
11x= 44 mod 73
11-1 = 20 mod 73
x= 20*44 mod 73= 4 mod 73
les valeurs de x possible sont 4, 4+73, 4+2*73, 4+3*73, 4+4*73
4, 77,150,223,296

Exercice 2 :

1

a- 19*3=57= 1+ 2*28
3 est l'inverse de 19 modulo 28
b- F_{19} o f_3 (m)= m^{19*3} mod 29= m*m^{28} mod 29 = m
c- 'I NCI N' dont le code numérique est 9 27 14 3 9 27 14 auquel on appliqué f_3 devient 4 21 18 27 4 21 18 ce qui correspond à DUR DUR

2

a- Soit m premier avec p et q. On a m^{p-1} = 1 mod p donc $m^{\Phi(n)}$=(m^{p-1})$^{q-1}$=1 mod p . De même m^{q-1} = 1 mod q donc $m^{\Phi(n)}$=(m^{q-1})$^{p-1}$=1 mod q. Ainsi p et q divisent $m^{\Phi(n)}$-1 et p et q premiers entre eux donc n =p*q divise $m^{\Phi(n)}$-1 donc $m^{\Phi(n)}$=1 mod n
b- e premier avec Φ(n) donc e est inversible modulo Φ(n), soit d son inverse ; il existe k tel que e*d= 1+k*Φ(n)
$g_{e,n}$ o $g_{d,n}$(m)= $g_{e,n}$(m^d)= m^{e*d}= $m^{1+k*\Phi(n)}$
$m^{\Phi(n)}$=1 mod n donc m^{e*d}= 1 mod n

3

c- p=5, q=7, n=35
Φ(35)=(5-1)*(7-1)=24 qui est premier avec 5
5*5=25= 1+24 donc 5 est l'inverse de 5 modulo 24la bijection de $g_{5,35}$ est $g_{5,35}$
Les message à coder est 12 1 18 6 31 27 6 2 31 1 24 33 6 18 1 17 6 qui devient 17 1 23 6 26 27 6 32 6 26 1 19 3 6 23 1 12 6 ce qui correspond à LA PERSEVERANCE PAIE