NOM :
PRENOM :
GROUPE :

Contrôle Cryptologie

Octobre 2015

La calculatrice n'est pas autorisée *(désolé)*

Exercice 1

5 min

1. Cette égalité définie-t-elle une division euclidienne $5 = 2 \times 2 + 1$. Justifier (si c'est le cas, donner le dividende, le diviseur, le quotient et le reste). 0.5

2. Cette égalité définie-t-elle une division euclidienne $10 = 2 \times 3 + 4$. Justifier (si c'est le cas, donner le dividende, le diviseur, le quotient et le reste). 0.5

3. Donner la fonction de déchiffrement du cryptosystème affine par paquet de 2 de clef $(5, 0)$. 0.5

Exercice 2

20 min

Donner le reste de la division euclidienne de A par B.

1. $A = 685$, $B = 12$ 1

2. $A = 3078$, $B = 84$ 1

3. $A = 404^{403}$, $B = 405$ 1

4. $A = 3^{1147}$, $B = 26$ 1

5. $A = 333^{33}$, $B = 10$ 1

Exercice 3

10 min

1. Donner la table de multiplication de $\mathbb{Z}/8\mathbb{Z}$.

$\times$	0	1	2	3	4	5	6	7
0								
1								
2								
3								
4								
5								
6								
7								

2. En déduire la liste des éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$.

Exercice 4

25 min

Cryptosystème de César.
Le but de cet exercice est de déchiffrer le message *290-1709-2324* obtenu en appliquant le cryptosystème de César par paquet de 2.

1. Rappelez l'espace des clefs du cryptosystème de César par paquet de 2. 0.5

2. Soit $k \in \mathcal{K}$ la clef utilisée pour chiffrer ce message. Rappelez la forme de la fonction de chiffrement C_k. 0.5

3. On sait que les deux premières lettres claire du message chiffré sont *SP*. En déduire la clef k. 2

4. Déchiffrer le message. 2

Message crypté	290		1709		2324	
Décryptage	1815					
Paquetage	18	15				
Décodage	S	P				

Message claire : _____

Exercice 5

30 min

Cryptosystème affine.
Le but de cet exercice est de déchiffrer le message *XBEURG* obtenu en appliquant le cryptosystème affine par paquet de 1 de clef $(17, 1)$.

1. Appliquer l'algorithme d'Euclide et déterminer $\text{PGCD}(26, 17)$. 1

a	b	r	q	u	v

$$\text{PGCD}(26, 17) = \_\_\_\_\_$$

2. Expliquer pourquoi $(17, 1)$ est bien une clef du cryptosystème affine par paquet de 1. 0.5

3. Déterminer deux entiers relatifs u et v tels que $26u + 17v = 1$. On complètera le tableau précédent. 1.5

$$26 \times (\_\_\_\_) + 17 \times (\_\_\_\_) = 1$$

4. En déduire l'inverse de 17 modulo 26. 1

5. Donner la fonction de déchiffrement $D_{(17,1)}$. 2

6. Déchiffrer le message 2

Message crypté	X	B	E	U	R	G
Codage						
Message clair						

Message claire : _____

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	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

Parce que j'ai pitié :

$26 \times 2 = 52$
$26 \times 3 = 78$
$26 \times 4 = 104$
$26 \times 5 = 130$
$26 \times 6 = 156$
$26 \times 7 = 182$
$26 \times 8 = 208$
$26 \times 9 = 234$