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 $10 = 2 \times 3 + 4$. 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 $5 = 2 \times 2 + 1$. 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 de César par paquet de 2 de clef 1234. 0.5

Exercice 2

20 min

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

1. $A = 555$, $B = 12$ 1

2. $A = 3078$, $B = 487$ 1

3. $A = 123^{122}$, $B = 124$ 1

4. $A = 2^{1147}$, $B = 7$ 1

5. $A = 133^{39}$, $B = 10$ 1

Exercice 3

10 min

Déterminer $\mathrm{PGCD}(4626, 1083)$. A cette fin, appliquer l'algorithme d'Euclide et remplissez le tableau suivant où chaque ligne (est une division euclidienne $a = bq + r$) représente une étape de l'algorithme. 1.5

a	b	r	q

$\mathrm{PGCD}(4626, 1083) =$ _____

Exercice 4

25 min

Cryptosystème de César.
Le but de cet exercice est de déchiffrer le message *1213-1607-387* 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 *CO*. En déduire la clef k. 2

4. Déchiffrer le message. 2

Message crypté	1213		1607		387	
Décryptage	214					
Paquetage	02	14				
Décodage	C	O				

Message claire : _____

Exercice 5

30 min

Cryptosystème affine.
Le but de cet exercice est de déchiffrer le message *NITOTK* obtenu en appliquant le cryptosystème affine par paquet de 1 de clef $(19, 13)$.

1. Appliquer l'algorithme d'Euclide et déterminer $\text{PGCD}(26, 19)$. 1

a	b	r	q	u	v

$$\text{PGCD}(26, 19) = \_\_\_\_\_$$

2. Expliquer pourquoi $(19, 13)$ est bien une clef du cryptosystème affine par paquet de 1. 0.5

3. Déterminer deux entiers relatifs u et v tels que $26u + 19v = 1$. On complètera le tableau précédent. 1.5

$$26 \times (\_\_\_\_) + 19 \times (\_\_\_\_) = 1$$

4. En déduire l'inverse de 19 modulo 26. 1

5. Donner la fonction de déchiffrement $D_{(19,13)}$. 2

6. Déchiffrer le message 2

Message crypté	N	I	T	O	T	K
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 :

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