

## R4.Cyber.10 - Cryptographie

### Exercice 1

Parmi les propositions, lesquelles sont vraies.

1.  $15 \equiv_8 7$

3.  $654 \equiv_3 0$

5.  $873 \equiv_5 555$

7.  $-8 \equiv_9 1$

2.  $99 \equiv_2 -1$

4.  $3 \equiv_3 3$

6.  $8704 \equiv_{13} 791$

8.  $-984 \equiv_{19} 17$

### Exercice 2

Dans chacun des cas, déterminer  $x$  modulo  $n$  (donner un représentant dans  $\mathbb{Z}/n\mathbb{Z}$ ).

1.  $x = 555, n = 12$

2.  $x = 983, n = 45$

3.  $x = 3078, n = 487$

4.  $x = 573, n = 159$

### Exercice 3

Crypter le mot *MATHEMATIQUES* par la méthode de César avec 19 comme clef.

### Exercice 4

On a utilisé la méthode de César avec 25 comme clef pour obtenir *BDRSBGZTCBZAQTKD*. Quel était le message original ?

### Exercice 5

Vous ne connaissez pas la clef de ce message chiffré par la méthode de César. Quel est le message clair.

VTZTEXKXHNJNHB

### Exercice 6

Dans chacun des cas, donner l'inverse de  $a$  modulo  $n$  lorsque cela est possible.

1.  $a = 13, n = 7$

2.  $a = 4, n = 17$

3.  $a = 2, n = 8$

4.  $a = 54, n = 17$

### Exercice 7

Déchiffrer le message *EROONBOONN* obtenue par le cryptosystème affine avec  $(3, 1)$  comme clef.

### Exercice 8

Déchiffrer le message *CBLXD* obtenue par le cryptosystème affine avec  $(7, 1)$  comme clef.

### Exercice 9

Voici un texte chiffré par la méthode affine. Quel est le message clair ?

V G W C S W A P U Z M N Z C H E K D G B G D  
G Z T U S Z G E G H Z U C Z K E U Z S Q C G  
D C B U H M U M G D G F G B K N N G N U T K  
N G H U S V U S G Z G J K T E G G H C Z S B  
S W U H Z C H M T U H D H K E X T G D G D K  
H H G G W Z G L Z C G B B G W G Z V G W C S  
W A U N U X B G D G A K E N T G H D T G G Z  
D G M G H G T G T D G W N P T U W G W G H C  
Z S B S W U H Z D S J J G T G H Z W A K H Z  
G L Z G W G Z Z P G E G W E G W J K H A Z S  
K H H U B S Z G W S H A B C G H Z B U A K E  
N T G P G H W S K H D G B U B U H M C G H U  
Z C T G B B G B U M G H G T U Z S K H D G Z  
G L Z G W B U Z T U D C A Z S K H U C Z K E  
U Z S Q C G G Z B U T G N K H W G U D G W Q  
C G W Z S K H W V G N G C L G M U B G E G H  
Z G Z T G C Z S B S W G N K C T D G W Z U A  
P G W Z G B B G W Q C G B U T G A K H H U S  
W W U H A G D G B U F K S L B U A K E N T G  
P G H W S K H D G B S E U M G G Z B U M G H  
G T U Z S K H D G A K H Z G H C V G W C S W  
A K H W Z U E E G H Z E S W U V K C T G Z U  
E G B S K T G N K C T J K C T H S T D G W T  
G W C B Z U Z W D G E G S B B G C T G Q C U  
B S Z G G Z N K C T T G B G F G T D G H K C  
F G U C L D G J S W E K H K X V G A Z S J G  
W Z D U S D G T B G W M G H W U U A A K E N  
B S T D G W Z U A P G W N B C W T U N S D G  
E G H Z G Z N B C W G J J S A U A G E G H Z  
G H C Z S B S W U H Z B G W D G T H S G T G  
W U F U H A G G W G H E U Z S G T G D S U

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequence	3.08%	5.73%	5.14%	4.41%	3.38%	0.73%	19.24%	7.93%	0.0%	1.32%	5.14%	0.88%	1.62%
Frequence	2.79%	0.0%	1.03%	0.73%	0.0%	6.31%	5.43%	8.08%	1.03%	7.05%	0.44%	0.0%	8.52%
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

### Exercice 10

Compléter le tableau suivant sachant que  $p < q$  sont deux nombres premiers,  $n = pq$ ,  $\varphi = (p - 1)(q - 1)$  et  $e$  et  $d$  sont des nombres premiers à  $\varphi$  inverse l'un de l'autre.

p	q	n	$\varphi$	e	d
3	13			11	
7	41			13	
101	139				43
2		202			19
		77		47	
		437			23
			32	7	
			16		5
		3599	3480	1001	
		1341517	1339200		433

### Exercice 11

Calculer les nombres suivants.

1.  $71^{21}$  modulo 65
2.  $33^{19}$  modulo 130
3.  $123^{43}$  modulo 98
4.  $301^{17}$  modulo 59
5.  $1000^{55}$  modulo 99
6.  $2^{666}$  modulo 2015

### Exercice 12

On considère dans le système RSA, la clef publique (1763, 929).

1. Déterminer deux entiers  $p$  et  $q$  tel que  $p < q$  et  $1763 = pq$ .
2. Justifier que (1763, 929) est une clef publique valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 929 en binaire.  
(b) Calculer  $18^{929}$  modulo 1763.  
(c) Quel est le message chiffré de  $M = 18$ .
4. Déterminer la clef privé associée à la clef publique (1763, 929).
5. Déchiffrer le message  $M' = 884$

### Exercice 13

On considère dans le système RSA, la clef publique (1189, 1031).

1. Déterminer deux entiers  $p$  et  $q$  tel que  $p < q$  et  $1189 = pq$ .
2. Justifier que (1189, 1031) est une clef publique valide du cryptosystème RSA.
3. (a) Déterminer la décomposition de 1031 en binaire.  
(b) Calculer  $44^{1031}$  modulo 1189.  
(c) Quel est le message chiffré de  $M = 44$ .
4. Déterminer la clef privé associée à la clef publique (1189, 1031).
5. Déchiffrer le message  $M' = 583$