# Fiche exercices

## EXERCICE 1

En utilisant le décalage affine avec $b=-11$ .
Donner le codage et le décodage du mot :
BONJOUR

## EXERCICE 2

En utilisant le chiffrement affine avec $a=17$ et $b=-2$ , donner le codage et le décodage du mot :
BONJOUR

## EXERCICE 3

En utilisant le cryptage R.S.A et en utilisant le logiciel Xcas, donner le codage et le décodage du mot :
CINEMATHEQUE
avec $p=3089$ et $q=4073$ et $c=97$

## EXERCICE 4

En utilisant le décalage affine avec $b=7$ .
Donner le codage et le décodage du mot :
VOYANCE

## EXERCICE 5

En utilisant le chiffrement affine avec $a=9$ et $b=5$ , donner le codage et le décodage du mot :
VOYANCE

## EXERCICE 6

En utilisant le cryptage R.S.A et en utilisant le logiciel Xcas, donner le codage et le décodage du mot :
CRYPTOGRAPHIE
avec $p=3491$ et $q=4643$ et $c=89$

## CORRECTION

### EXERCICE 1

$b=-11$
$E(x)=y$ est le reste de la division euclidienne de $x-11$ par $26$.
$E(x)\equiv x-11(26)$
$0\leqslant E(x)\leqslant 25$

$D(y)$ est le reste de la division euclidienne de $y+11$ par $26$.
$D(y)\equiv y+11(26)$
$0\leqslant D(y)\leqslant 25$
$\boxed{D(y)=D[E(x)]=x}$

Exemple :

| | B | O | N | J | O | U | R |
|---|---|---|---|---|---|---|---|
| x | 01 | 14 | 13 | 09 | 14 | 20 | 17 |
| x-11 | -10 | 03 | 02 | -02 | 03 | 09 | 06 |
| y | 16 | 03 | 02 | 24 | 03 | 09 | 06 |
| | Q | D | C | Y | D | J | G |
| y+11 | 27 | 14 | 13 | 35 | 14 | 20 | 17 |
| D(y) | 01 | 14 | 13 | 09 | 14 | 20 | 17 |

### EXERCICE 2

Correction :
$a=17$ et $b=-2$
$E(x)=y$ est le reste de la division euclidienne de $17x-2$ par $26$.
$E(x)\equiv 17x-2(26)$
$0\leqslant E(x)\leqslant 25$
Pgcd(17;26)=1
On détermine une solution particulière de l'équation : $17u+26v=1$
En utilisant le logiciel Xcas :
iabcuv(17,26,1)
On obtient (-3;2).
On a, $y\equiv ax+b(26)$ $a=17$
$17x\equiv y-b(26)$
$17x-26k=y-b$
Une solution particulière de cette équation est (-3(*y*-*b*) ;-2(*y*-*b*)).
Donc, $x\equiv -3(y-b)(26)$ $b=-2$

$x\equiv -3y-6(26)$

ou $x\equiv 23y+20(26)$

$D(y)$ est le reste de la division euclidienne de $23y+20$ par $26$.
$D(y)\equiv 23y+20(26)$

$0 \leqslant D(y) \leqslant 25$

$\boxed{D(y)=D[E(x)]=x}$

Exemple :

| | B | O | N | J | O | U | R |
|---|---|---|---|---|---|---|---|
| x | 01 | 14 | 13 | 09 | 14 | 20 | 17 |
| 17x-2 | 15 | 236 | 219 | 151 | 236 | 338 | 287 |
| y | 15 | 02 | 11 | 21 | 02 | 00 | 01 |
| | P | C | L | V | C | A | B |
| 23y+20 | 365 | 66 | 273 | 503 | 66 | 20 | 43 |
| D(y) | 01 | 14 | 13 | 09 | 14 | 20 | 17 |

## EXERCICE 3

$p=3089$ et $q=4073$

$N=p\times q=12\,581\,497$

$(p-1)(q-1)=12\,574\,336$

$c=97$ est un nombre premier ne divisant pas $(p-1)(q-1)$ donc $c$ est premier avec $(p-1)(q-1)$.

On considère le mot : CINEMATHEQUE

| C | I | N | E | M | A | T | H | E | Q | U | E |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 02 | 08 | 13 | 04 | 12 | 00 | 19 | 07 | 04 | 16 | 20 | 04 |

On obtient le nombre :

020813041200190704162004

N est un nombre de huit chiffres, on sépare le nombre obtenu à partir de la gauche en nombres de sept chiffres (pour les premiers).

0208130 4120019 0704162 004

$x=0208130$

On utilise le logiciel Xcas

$irem(0208130\wedge 97,12\,581\,497)$

On obtient : 7830525

On écrit huit chiffres $y$=07830525

$x=4120019$

On utilise le logiciel Xcas

$irem(4120019\wedge 97,12\,581\,497)$

On obtient : 8377555

On écrit huit chiffres $y$=08377555

$x=0704162$

On utilise le logiciel Xcas

$irem(0704162 \wedge 97, 12581497)$

On obtient : 6380601

On écrit huit chiffres $y$=**06380601**

$x = 004$

On utilise le logiciel Xcas

$irem(4 \wedge 97, 12581497)$

On obtient : 417801

On écrit huit chiffres $y$=**00417801**

On obtient comme codage :

**078305250837755506380601004178 01**

Pour le décryptage, il faut déterminer $d$ avec :

$1 < d < (p-1)(q-1) = 12574336$

On détermine alors une solution de l'équation :

$uc + v \times 12574336 = 1$

On utilise l'instruction :

iabcuv(97,12574336,1)

On obtient **(388897,-3)**

Donc, $97 \times 388897 \equiv 1 (12574336)$ et 1<388897<12 574 336

donc, $\boxed{d = 388897}$

$y = 0208130$

On utilise le logiciel Xcas

$irem(7830525 \wedge 388897, 12581497)$

On obtient : 208130

On écrit huit chiffres $x$=**0208130**

$y = 0208130$

On utilise le logiciel Xcas

$irem(8377555 \wedge 388897, 12581497)$

On obtient : 4120019

On écrit huit chiffres $x$=**4120019**

$y = 06380601$

On utilise le logiciel Xcas

$irem(6380601 \wedge 388897, 12581497)$

On obtient : 704162

On écrit huit chiffres $x$=**0704162**

## EXERCICE 4

$b = 7$

$E(x)=y$ est **le reste de la division euclidienne** de $x+7$ par $26$.

$E(x)\equiv x+7(26)$

$0\leqslant E(x)\leqslant 25$

$D(y)$ est **le reste de la division euclidienne** de $y-7$ par $26$.

$D(y)\equiv y-7(26)$

$0\leqslant D(y)\leqslant 25$

$\boxed{D(y)=D[E(x)]=x}$

Exemple :

| | V | O | Y | A | N | C | E |
|---|---|---|---|---|---|---|---|
| x | 21 | 14 | 24 | 00 | 13 | 02 | 04 |
| x+7 | 28 | 21 | 31 | 07 | 20 | 09 | 11 |
| y | 02 | 21 | 05 | 07 | 20 | 09 | 11 |
| | C | V | F | H | U | J | L |
| y-7 | -05 | 14 | -02 | 00 | 13 | 02 | 04 |
| D(y) | 21 | 14 | 24 | 00 | 13 | 02 | 04 |

## EXERCICE 5

$a=9$ et $b=5$

$E(x)=y$ est **le reste de la division euclidienne** de $9x+5$ par $26$.

$E(x)\equiv 9x+5(26)$

$0\leqslant E(x)\leqslant 25$

Pgcd(9;26)=1

On détermine **une solution particulière** de l'équation : $9u+26v=1$

En utilisant le logiciel Xcas :

iabcuv(9,26,1)

On obtient **(3;-1)**.

On a, $y\equiv ax+b(26)$ $a=9$

$9x\equiv y-b(26)$

$9x-26k=y-b$

Une solution particulière de cette équation est **(3(*y*-*b*) ;(*y*-*b*))**.

Donc, $x\equiv 3(y-b)(26)$ $b=5$

$x\equiv 3y-15(26)$

$D(y)$ est **le reste de la division euclidienne** de $3y-15$ par $26$.

$D(y)\equiv 3y-15(26)$

$0\leqslant D(y)\leqslant 25$

$\boxed{D(y)=D[E(x)]=x}$

Exemple :

| | V | O | Y | A | N | C | E |
|---|---|---|---|---|---|---|---|
| x | 21 | 14 | 24 | 00 | 13 | 02 | 04 |
| 9x+5 | 194 | 131 | 221 | 05 | 122 | 23 | 41 |
| y | 12 | 01 | 13 | 05 | 18 | 23 | 15 |
| | M | B | N | F | S | X | P |
| 3y-15 | 21 | -12 | 24 | 00 | 39 | 54 | 30 |
| D(y) | 21 | 14 | 24 | 00 | 13 | 02 | 04 |

## EXERCICE 6

$p=3491$ et $q=4643$
$N=p\times q=16\,208\,713$
$(p-1)(q-1)=16\,200\,580$
$c=89$ est un nombre premier ne divisant pas $(p-1)(q-1)$ donc $c$ est premier avec $(p-1)(q-1)$.
On considère le mot : CRYPTOGRAPHIE

| C | R | Y | P | T | O | G | R | A | P | H | I | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 02 | 17 | 24 | 15 | 19 | 14 | 06 | 17 | 00 | 15 | 07 | 08 | 04 |

On obtient le nombre :
02172415191406170015070804
N est un nombre de huit chiffres, on sépare le nombre obtenu à partir de la gauche en nombres de sept chiffres (pour les premiers).
0217241 5191406 1700150 70804
$x=0217241$
On utilise le logiciel Xcas
$irem(217241\wedge 89,16\,208\,713)$
On obtient : 3376241
On écrit huit chiffres $y$=**03376241**

$x=5191406$
On utilise le logiciel Xcas
$irem(5191406\wedge 89,16\,208\,713)$
On obtient : 933503
On écrit huit chiffres $y$=**00933503**

$x=1700150$
On utilise le logiciel Xcas
$irem(1700150\wedge 89,16\,208\,713)$
On obtient : 9951366
On écrit huit chiffres $y$=**09951366**
$x=70804$
On utilise le logiciel Xcas

$irem(70804 \wedge 89, 16\,208\,713)$
On obtient : 14692302
On écrit huit chiffres $y$=**14692302**

On obtient comme codage :
**033762410093350309951366 14692302**

Pour le décryptage, il faut déterminer $d$ avec :
$1<d<(p-1)(q-1)=16\,200\,580$
On détermine alors une solution de l'équation :
$u \times 89 + v \times 16\,200\,580 = 1$
On utilise l'instruction :
iabcuv(89,16 200 580,1)
On obtient **(182029,-1)**
Donc, $89 \times 182029 \equiv 1 (16\,200\,580)$
donc, $\boxed{d = 182029}$
$x$ est le reste de la division euclidienne de $y^{182029}$ par 16 208 713

$y$=03376241
On utilise le logiciel Xcas
$irem(03376241 \wedge 182029, 16\,208\,713)$
On obtient : 217241
On écrit huit chiffres $x$=**0217241**

$y$=0208130
On utilise le logiciel Xcas
$irem(00933503 \wedge 182029, 16\,208\,713)$
On obtient : 5191406
On écrit huit chiffres $x$=**5191406**

$y$=06380601
On utilise le logiciel Xcas
$irem(09951366 \wedge 182029, 16\,208\,713)$
On obtient : 1700150
On écrit huit chiffres $x$=**1700150**

$y$=14692302
On utilise le logiciel Xcas
$irem(14692302 \wedge 182029, 16\,208\,713)$
On obtient : 70804
On écrit huit chiffres $y$=**70804**