Exercice

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 $c=97$

Correction :

$p=3089$ 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

$irem(0704162 \wedge 97, 12\,581\,497)$

On obtient : 6380601

On écrit huit chiffres y=**06380601**

$x=004$

On utilise le logiciel Xcas

$irem(4 \wedge 97, 12\,581\,497)$

On obtient : 417801

On écrit huit chiffres y=**00417801**

On obtient comme codage :

078305250837755506380601004178 01

Pour le décryptage, il faut déterminer d avec :

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

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, $97\times 388897\equiv 1\left(12\,574\,336\right)$ et 1<388897<12 574 336

donc, $\boxed{d=388897}$

$y=0208130$

On utilise le logiciel Xcas

$irem\left(7830525\wedge 388897,12\,581\,497\right)$

On obtient : 208130

On écrit huit chiffres x=**0208130**

$y=0208130$

On utilise le logiciel Xcas

$irem\left(8377555\wedge 388897,12\,581\,497\right)$

On obtient : 4120019

On écrit huit chiffres x=**4120019**

$y=06380601$

On utilise le logiciel Xcas

$irem\left(6380601\wedge 388897,12\,581\,497\right)$

On obtient : 704162

On écrit huit chiffres x=**0704162**

$y=00417801$

On utilise le logiciel Xcas

$irem(00417801 \wedge 388897,12\,581\,497)$

On obtient : 4

On écrit huit chiffres x=**004**

(il nous faut un renseignement pour le nombre de zéro à ajouter)