Cryptographie.

1. Introduction

La cryptographie permet à 2 personnes de correspondre de manière confidentielle.
Ainsi toute personne interceptant un message ne comprend pas la signification de ce message.
On note E l'algorithme de cryptage, si m est un message, $E(m)$ est le message chiffré.
On note D l'algorithme de décryptage donc $D(E(m))=m$.
On distingue deux types de d'algorithmes de cryptographie.

1.1. Les algorithmes à clés secrètes

C'est dans le cas où l'algorithme de déchiffrement se déduit facilement de l'algorithme de chiffrement (dans ce cas l'algorithme de chiffrement doit être secret.)

1.2. Les algorithmes à clés publiques

C'est dans le cas où il n'est pas possible de déduire (facilement) l'algorithme de déchiffrement connaissant l'algorithme de chiffrement. (dans ce cas, l'algorithme de chiffrement peut être connu de tout le monde.)

2. Algorithmes à clés secrètes

2.1. Codage des lettres de l'alphabet

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

Chaque lettre des 26 de l'alphabet est codée par un nombre à deux chiffres.

Exemple : A:00

2.2. Décalage affine

b est un entier relatif non nul fixé.

$00 \leqslant x \leqslant 25$

$E(x)$ est le reste de la division euclidienne de $x+b$ par 26, donc :

$E(x) \equiv x+b(26)$ et $00 \leqslant E(x)=y \leqslant 25$

$x \equiv y-b(26)$ et $00 \leqslant x \leqslant 25$

Donc, $D(y)$ est le reste de la division euclidienne de $y-6$ par 26 .

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

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

Exemple : $b=10$

	E	S	S	A	I
x	04	18	18	00	08
x+10	14	28	28	10	18
y	14	02	02	10	18
	O	C	C	K	S
y-10	04	-8	-8	00	08
D(y)	04	18	18	00	08

message m	ESSAI
	04 18 18 00 08
chiffrement de m	14 02 02 10 18
	OCCKS

2.3. Chiffrement affine

a est un entier naturel non nul fixé.

b est un entier naturel fixé.

$00 \leqslant x \leqslant 25$

$E(x)$ est le reste de la division euclidienne de $ax+b$ par 26, donc :

$E(x) \equiv ax+b(26)$ et $00 \leqslant E(x)=y \leqslant 25$

Pour le déchiffrement, connaissant y il faut être capable de déterminer x .
$y=ax+b+26k \quad (k \in \mathbb{Z})$
Donc, $ax+26k=y-b$
a et b sont donnés et on doit déterminer x pour toutes valeurs possibles de y $(00 \leqslant y \leqslant 25)$.

Rappel sur les équations diophantiennes :
Si a et 26 ne sont pas premiers entre eux, il existe des solutions à l'équation si et seulement si le pgcd de a et 26 divise $y-b$ (ceci n'est pas possible pour toutes les valeurs de y)
Conséquence : pour pouvoir calculer x quelque soit y il faut que a et 26 soient premiers entre eux.
Exemple : on choisit $a=7$ et $b=3$

Pgcd(7;26)=1

On détermine une solution de l'équation :

$7u+26v=1$

(-11;3) est une solution particulière.

On utilise l'algorithme d'Euclide, ou, pour le logiciel Xcas l'instruction iabcuv(7,26,1).

Une solution de l'équation $ax-26k=y-b$ est donc :

$(-11(y-b);-3(y-b))$

$x\equiv -11(y-b)(26)$

$x\equiv -11y+11b(26)$

Or, $b=3$

$x\equiv -11y+33(26)$

$x\equiv 15y+7(26)$ (15+11=26)

$D(y)$ est le reste de la division euclidienne de $15y+7$ par 26.

$D(y)\equiv 15y+7(26)$ $(00\leqslant D(y)\leqslant 25)$

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

	E	S	S	A	I
x	04	18	18	00	08
7x+3	31	129	129	03	59
y	05	25	25	03	07
	F	Z	Z	D	H
15y+7	82	382	382	52	112
D(y)	04	18	18	00	08

3. Propriétés (compléments d'arithmétique)

3.1. Propriété 1

p est un nombre premier.
Si k est un entier naturel tel que $k\equiv 1(p-1)$ alors pour tout entier naturel a :
$\boxed{a^k\equiv a(p)}$.

- Si p est un nombre premier ne divisant pas a alors $a^{p-1}\equiv 1(p)$ (théorème de Fermat)
  Pour tout entier naturel q :
  $(a^{p-1})^q\equiv 1^q(p)$

$a^{q(p-1)} \equiv 1(p)$
$a^{q(p-1)} \times a \equiv a(p)$
$a^{q(p-1)+1} \equiv a(p)$

- Si p est un nombre premier divisant a , alors :
  $a \equiv 0(p)$
  $a^{q(p-1)+1} \equiv 0(p)$
  Donc, $a^{q(p-1)+1} \equiv a(p)$

- Conséquence :
  On pose $k = q(p-1)+1$ (k est un entier naturel)
  $k \equiv 1(p-1)$
  Et, $a^k \equiv a(p)$
  (q est le quotient de la division euclidienne de k par $(p-1)$)

3.2. Propriété 2

p et q sont deux nombres premiers distincts.
Si k est un entier naturel tel que $k \equiv 1((p-1)(q-1))$ alors pour tout entier naturel a :
$\boxed{a^k \equiv a(pq)}$.

p et q sont deux nombres premiers distincts donc p et q sont premiers entre eux.
k est un entier naturel tel que $k \equiv 1((p-1)(q-1))$, on a :
$k = \alpha(p-1)(q-1)+1$ avec α entier naturel
Donc, $k \equiv 1(p-1)$ et $k \equiv 1(q-1)$.
On utilise la propriété 1, pour tout entier naturel a , $a^k \equiv a(p)$.
Donc, $a^k - a = \beta p$ (β entier naturel)
De même, $a^k - a = \gamma q$ (γ entier naturel)
Conséquence :
$\beta p = \gamma q$
Donc, p divise γq et p et q sont premiers entre eux, donc d'après le théorème de Gauss p divise γ .
Donc, $\gamma = \delta p$ (δ entier naturel)
Conclusion :
$a^k - a = \delta pq$ et $a^k \equiv a(pq)$

3.3. Remarque

p et q sont deux nombres premiers distincts. Si c est un entier naturel premier avec $(p-1)(q-1)$ tel que $1 < c < (p-1)(q-1)$ alors il existe un entier naturel d tel que :
$1 < d < (p-1)(q-1)$ et $c.d \equiv 1((p-1)(q-1))$.

c et $(p-1)(q-1)$ sont premiers entre eux.
Le théorème de Bezout nous permet d'affirmer qu'il existe deux entiers relatifs u et v tels que :
$uc + v(p-1)(q-1) = 1$
Donc, $uc \equiv 1((p-1)(q-1))$
Soit d le reste de la division euclidienne de u par $(p-1)(q-1)$

$u=\alpha(p-1)(q-1)+d$
α est un entier relatif et d est un entier naturel tel que $1\leqslant d\leqslant(p-1)(q-1)$
($d\neq 0$ car u n'est pas divisible par $(p-1)(q-1)$ et dans ce cas, on aurait $uc\equiv 0((p-1)(q-1))$)
$cu=c[\alpha(p-1)(q-1)+d]$
Donc, $cu\equiv cd((p-1)(q-1))$
Donc, $cd\equiv 1((p-1)(q-1))$

Si $d=1$ alors $c\equiv 1((p-1)(q-1))$
Or, $1<c<(p-1)(q-1)$ donc, c n'est pas congru à 1 modulo $(p-1)(q-1)$

Donc $d\neq 1$ et $1<d<(p-1)(q-1)$

3.4. Propriété 3

p et q sont deux nombres premiers distincts. Soient c et d deux entiers naturels tels que $1<c<(p-1)(q-1)$; $1<d<(p-1)(q-1)$; c est premier avec $(p-1)(q-1)$ et $c.d\equiv 1((p-1)(q-1))$.
Pour tous entiers naturels a et b, si $b\equiv a^c(p.q)$ alors $b^d\equiv a(p.q)$

$c.d=k\equiv 1((p-1)(q-1))$
En utilisant la propriété 2, on a $a^{cd}\equiv a(p.q)$.
Si on pose $b=a^c$ alors $b^d=a^{cd}$
Et, $b^d\equiv a(p.q)$

4. Exemple d'algorithme à clés publiques. Cryptage RSA

4.1. Généralités

- L'algorithme R.S.A (du nom des trois auteurs RIVEST, SHAMIR, ADLEMEN) est un exemple d'algorithme à clés publiques utilisé par les services secrets.
- On choisit deux nombres premiers distincts « très grands » p et q et on considère le nombre $N=pq$.

Connaissant N, il est très difficile même pour les ordinateurs actuels de retrouver p et q lorsque N a plus de 200 chiffres.
On choisit un entier naturel c tel que c soit premier avec $(p-1)(q-1)$ et $1<c<(p-1)(q-1)$.
On peut alors déterminer, en connaissant p et q, d tel que $c.d\equiv 1((p-1)(q-1))$ et $1<d<(p-1)(q-1)$.
La partie publique est N et c nécessaire pour le cryptage.
La partie secrète est $p;q;d$ nécessaire pour le décryptage.

4.2. Principe de cryptage et du décryptage

$N=pq$ $\quad$ $c.d\equiv 1((p-1)(q-1))$

- Cryptage

x est un entier naturel.
$0\leqslant x\leqslant N-1$
$C(x)$ est le reste de reste de la division euclidienne de x^c par N.
$C(x)\equiv x^c(pq)$ et $0\leqslant C(x)=y\leqslant N-1$

- Décryptage

$D(y)$ est le reste de la division euclidienne de y^d par N .
$D(x)\equiv y^d\,(pq)$ et $0\leqslant D(y)\leqslant N-1$.
Or, $y^d\equiv(x^c)^d\,(pq)$ On utilise la propriété 3.
$y^d\equiv x^{cd}\,(pq)$
$y^d\equiv x\,(pq)$
et $0\leqslant x\leqslant N-1$
Donc, $D(y)=x$

4.3. Exemple

Pour les calculs, on utilisera le logiciel Xcas en choisissant des nombres premiers permettant l'utilisation de ce logiciel.
$p=3559$ $q=4049$
(p et q ne sont pas des nombres premiers très grands)
$N=pq=14\,410\,391$
$(p-1)(q-1)=3558\times4048=14\,402\,784$
$c=71$ est un nombre premier ne divisant pas pas $(p-1)(q-1)$.
On considère le mot CHRONOLOGIQUE

C	H	R	O	N	O	L	O	G	I	Q	U	E
02	07	17	14	13	14	11	14	06	08	16	20	04

On obtient le nombre :
02071714131411140608162004 (26 chiffres)
x doit être compris entre 0 et $N-1$. Or, N a huit chiffres, mais tout nombre de huit chiffres n'est pas nécessairement inférieur ou égal à $N-1$.
On considère donc des nombres de 7 chiffres. (on pourrait prendre des nombres de 6 chiffres, …).
On sépare le nombre donné, en commençant à gauche par des nombres de sept chiffres sauf le dernier de 5 chiffres.
0207171 4131411 1406081 62004

$x=0207171$ et $c=71$
Avec Xcas :
$irem(207171\wedge71,14410391)$
On obtient : $1140879=C(x)=y$
On écrit nécessairement y avec huit chiffres (car y est un reste d'une division euclidienne par N donc pour certaine valeur de x on peut obtenir un nombre à huit chiffres)
$y=01140879$

$x=4131411$ et $c=71$
$irem(4131411\wedge71,14410391)$
On obtient : $4389312=C(x)=y$
$y=04389312$

$x=1406081$ et $c=71$

$irem(1406081 \wedge 71,14410391)$
On obtient : $12080504 = C(x) = y$
$y = 12082504$

$x = 62004$ et $c = 71$
$irem(62004 \wedge 71,14410391)$
On obtient : $12380403 = C(x) = y$
$y = 12380403$

On obtient comme codage :
011408790438931212082504 12380403

Pour le décryptage, il faut déterminer d avec $1 < d < (p-1)(q-1) = 14402784$.
On détermine alors une solution de l'équation :
$uc + v \times 14402784 = 1$
On considère alors l'instruction :

iabcuv(71,14402784,1)
On obtient (-1825705,9)
d est compris entre 1 et 14402784
d=14402784-1825705=12577079
$\boxed{d = 12577079}$
La solution de l'équation que l'on choisit est (d,8)

- $y = 01140879$

$irem(1140879 \wedge 12577079,14410391)$
On obtient $x = D(y) = 207171$
Il faut 7 chiffres : $x = 0207171$

- $y = 04389312$

$irem(4389312 \wedge 12577079,14410391)$
On obtient $x = D(y) = 4131411$
$x = 4131411$

- $y = 12080504$

$irem(12080504 \wedge 12577079,14410391)$
On obtient $x = D(y) = 1406081$
Il faut 7 chiffres : $x = 1406081$

- $y = 12380403$

$irem(12380403 \wedge 12577079,14410391)$
On obtient $x = D(y) = 62004$
Il faut 7 chiffres : $x = 62004$

On obtient bien le nombre initial.