Sytème de codage ASCII

Chaque caractère a un numéro: A: 65, B 66...

ToCharacterCode@"A"D

865<

In[47]:= **ToCharacterCode@"GENTILLY"D**

Out[47]= 871, 69, 78, 84, 73, 76, 76, 89<

Sytème de codage élémentaire J. César (-50)

décalage d'un caractère

CodeJC@cD:= FromCharacterCode@ToCharacterCode@cD + 1D

General::spell1 : Possible spelling error: new symbol name "CodeJ" is similar to existing symbol "Code".

CodeJC@"a"D

b

DCodeJC@cD:= FromCharacterCode@ToCharacterCode@cD - 1D

General::spell :
Possible spelling error: new symbol name "DCodeJ" is similar to existing symbols 8CodeJ, DCode<.

CodeJC@"Expression à coder: café des sciences"D

Fyqsfttjpo!á!dpefs;!dbgê!eft!tdjfodft

DCodeJC@%D

Expression à coder: café des sciences

Sytème de codage à clef publique dit RSA (Rivest Shamir Adleman 78)

Construction

p et q sont deux grands nombres premiers, la détermination de p et q connaissant M est un travail trop compliqué.

$M = p\,q$

p q

On construit e, clef cachée

$e = \frac{1}{3}\,(2\,(p - 1)\,(q - 1) + 1)\,3$

$\frac{1}{3}\,(1 + 2\,(-1 + p)\,(-1 + q))$

p et q sont deux grands nombres premiers dont le reste de la division par 3 est 2

p = Prime@13D

```
41
```

Mod@Prime@13D, 4D

```
2
```

q = Prime@15D

```
47
```

Mod@Prime@15D, 4D

```
2
```

Le codage consiste à calculer le reste de la division par M du nombre associé au caractère élevé au cube

CodeRSA@c_D := Mod@ToCharacterCode@cD^3, MD

Le décodage consiste à calculer le reste de la division par M du nombre codé élevé à la puissance e, il suffit de connaître e pour décoder le message. Un tiers ne peut décoder le message même s'il connait M.

DCodeRSA@d_D := FromCharacterCode@Mod@d^e, MDD

CodeRSA@"A"D

```
8991<
```

DCodeRSA@%D

```
A
```

CodeRSA@"Expression à coder."D

```
8919, 1408, 145, 1608, 1283, 472, 472, 1425,
 1388, 1370, 9, 1160, 9, 1018, 1388, 1814, 1283, 1608, 986<
```

DCodeRSA@%D

```
Expression à coder.
```