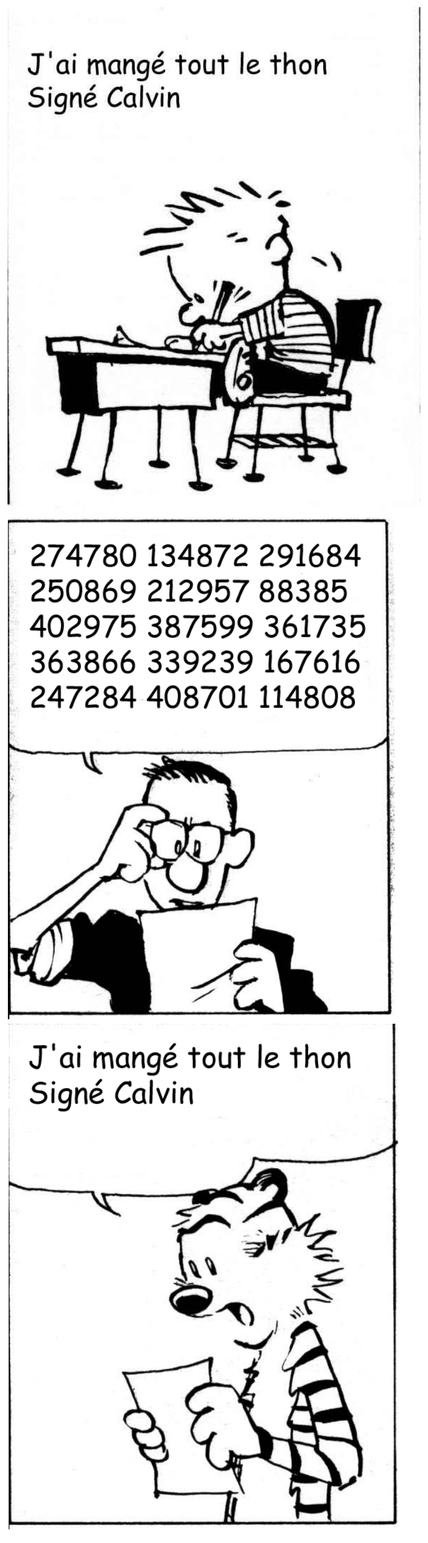
FACULTE DES SCIENCES

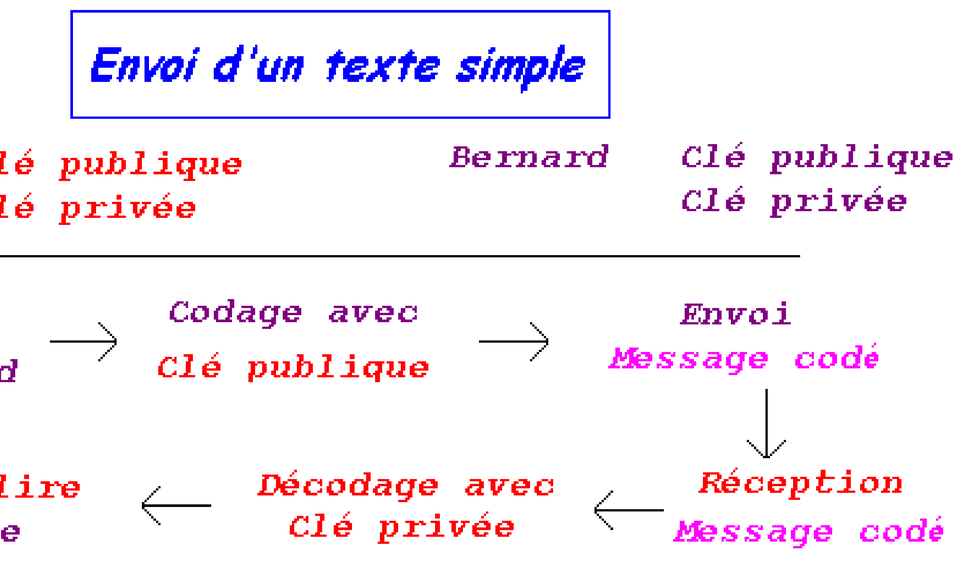
LE CODAGE AVEC RSA

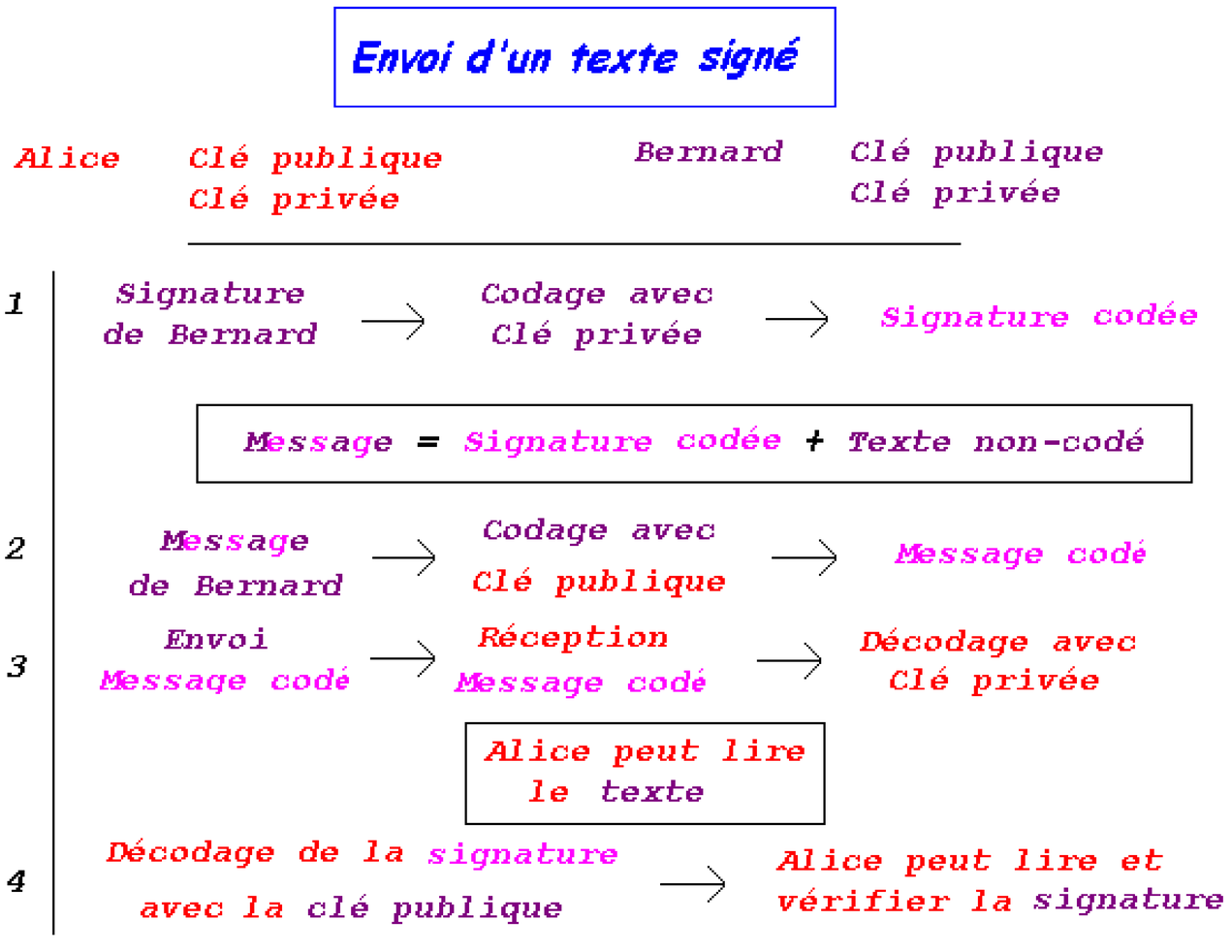
Exemple simple de codage

Soient $p = 659$ et $q = 673$.
On trouve donc $n = 443507$.
On choisit $e = 97$; alors $d = 291745$.
Codons, par exemple "J'ai mangé tout le thon Signé Calvin"
par groupe de 2 caractères.

"J'aimang" $\overset{ASCII}{\longrightarrow}$ 074 039 097 105 109 097 110 103
Il faut donc coder les séquences 074039 097105 109097 110103
Coder: $(074039)^{97}\ mod\ 443507 = 274780$
Décoder: $(274780)^{291745}\ mod\ 443507 = 74039 = 074\ 039$.







Cryptanalyse et RSA

Le RSA est basé sur la difficulté de factoriser un "grand" nombre.