TP2 Chiffrement Multimédia

Durant la majeure grande partie de ce TP,

$$p = 11 \quad q = 23 \qquad e = 17$$

Ici la clef publique est donc:

$$K_{pub} = (e, n)$$

avec

$$e = 17 \text{ et } n = 253$$

Et la clef privée est:

$$K_{priv} = (n, d)$$

avec

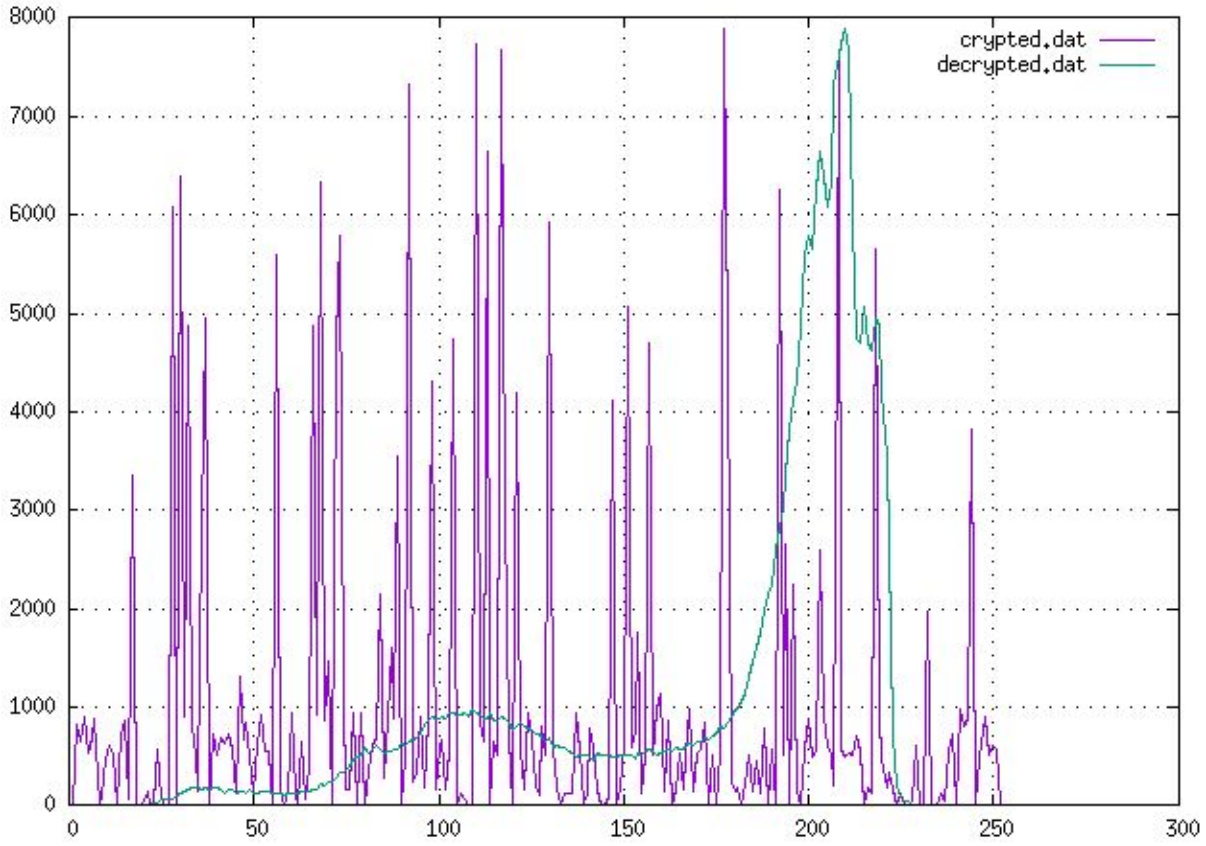
$$n = 253 \text{ et } d = 13$$

Image Chiffrée

Image en Clair

On note que toute l'information visuelle n'a pas été protégée par le chiffrement de l'image.

L'algorithme généralement utilisé pour calculer l'inverse modulaire d'un nombre est l'algorithme d'Euclide étendu.



Les entropies des deux images représentées sur les histogrammes ci-dessus ont une valeur identique de 6.67765 bpp.

Image Binarisée *Image chiffrée*

Une fois encore les entropies des deux images sont identiques avec une valeur de 0.999905 bpp mais cette fois ci l'information est clairement visible sur l'image cryptée, n'offrant quasiment aucune sécurité.

Le problème est, je pense, que pour une valeur donnée en clair, il n'existe qu'une seule valeur possible en chiffré.

Ainsi une solution serait de quantifier l'image en clair afin d'augmenter la plage des valeur correspondantes :

$0 \rightarrow [0,7]$ $128 \rightarrow [1016,1023]$ $255 \rightarrow [2040,2047]$

(toute modification pré-chiffrement permettant d'empêcher les suites de nombres identiques et étant réversibles seraient une solution)