Compte-rendu TP2

Chiffrement multimedia

Saffin Alexandre

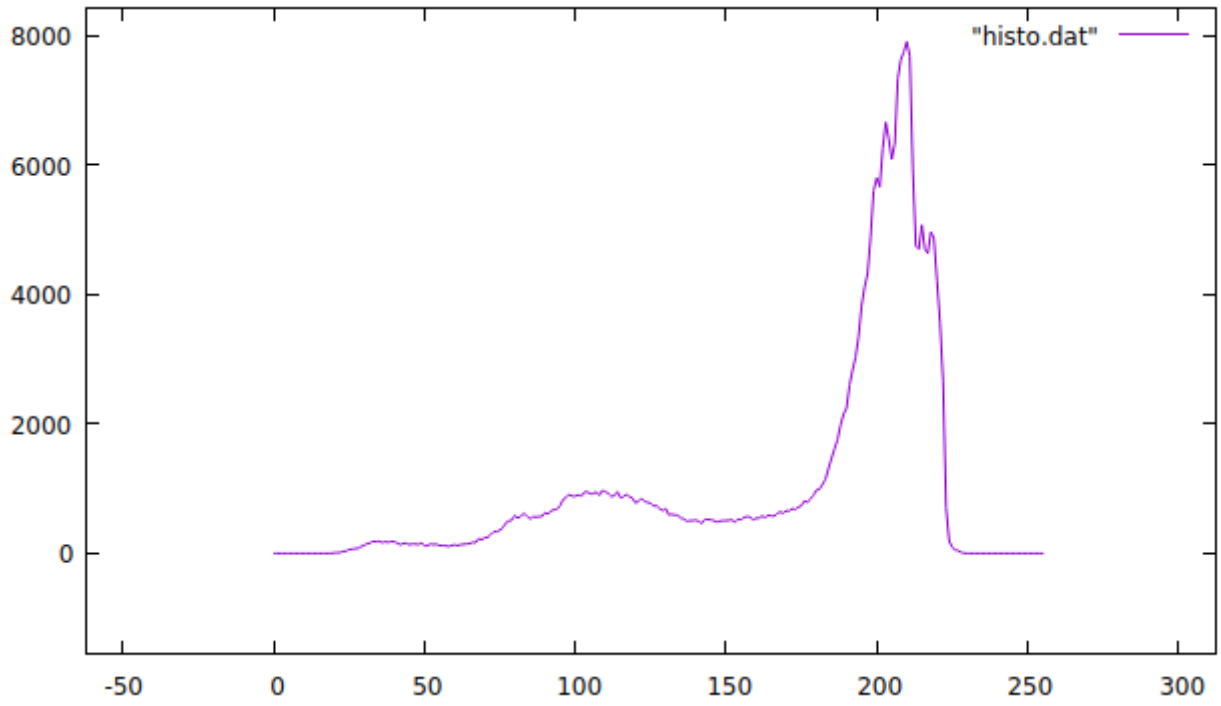
Pour chiffrer cette image on a utilisé la clef publique (17,253) (e=17 et n = 253).

image originale

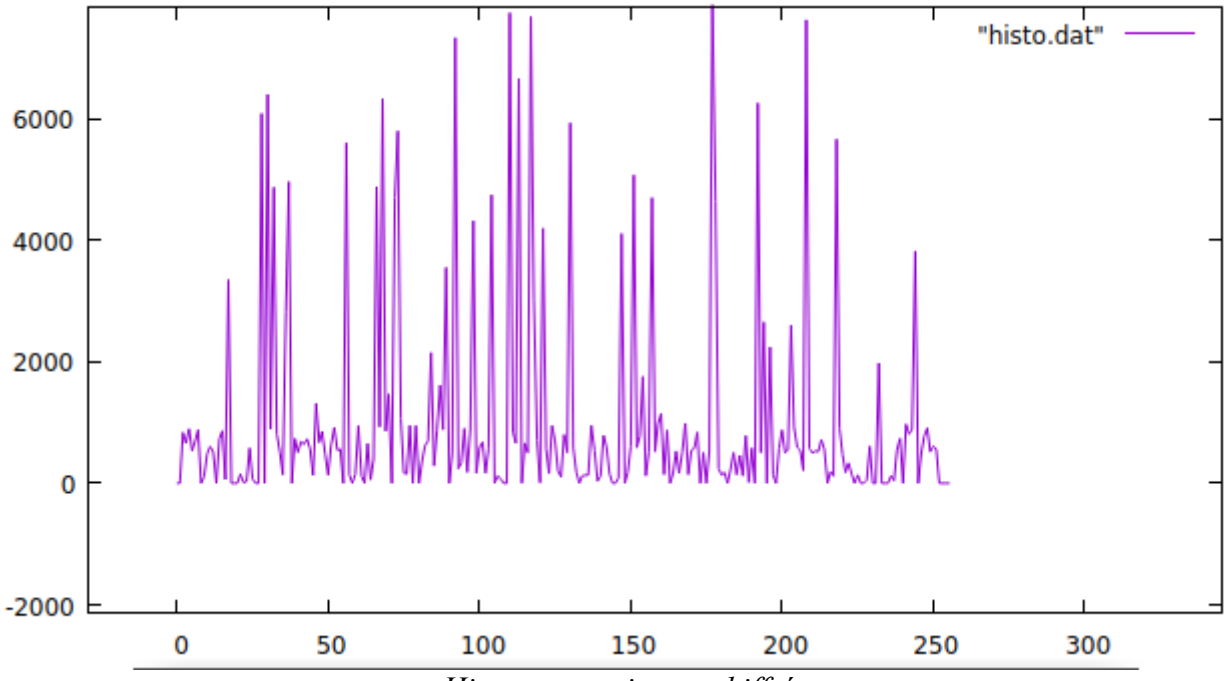
image chiffrée

En utilisant l'inverse modulaire on peut déchiffrer l'image. L'algorithme utilisé pour calculer l'inverse modulaire est l'algorithme d'Euclide étendu. La clef privé utilisé est (13) (d=13).

On obtiens une entropie de 6.67765 bits/pixels pour l'image chiffré et également la même chose pour l'image déchiffré.



Histogramme image originale



Histogramme image chiffré

Image originale binarisé

Image binarisé chiffré

En chiffrant l'image binarisé on constate que l'on peut apercevoir de nombreux détails de l'image originale, cela montre que l'algorithme implémenté n'est pas sûre car la confidentialité n'est pas conservé, le probléme est lié au fait que l'ont utilise seulement 2 niveaux de gris.