TP2 Chiffrement multimédia

Dubar Axel

Algorithme RSA

a)

iv)

image en clair

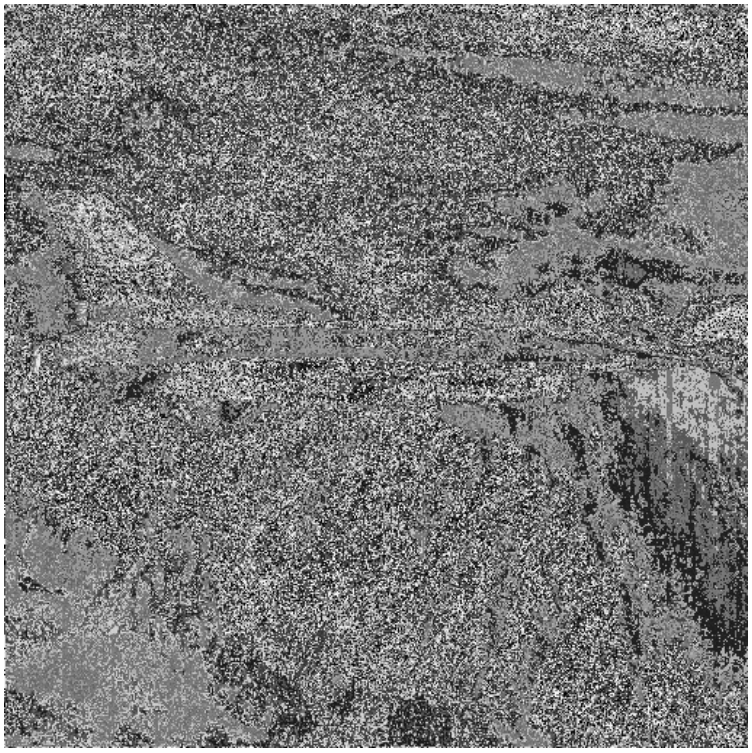


image chiffrée

La clef publique utilisée est le couple (17,p*q=253)

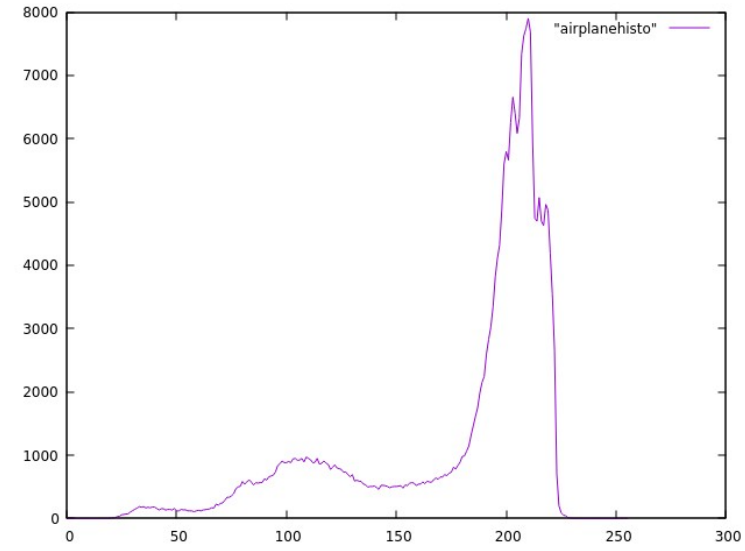
b)

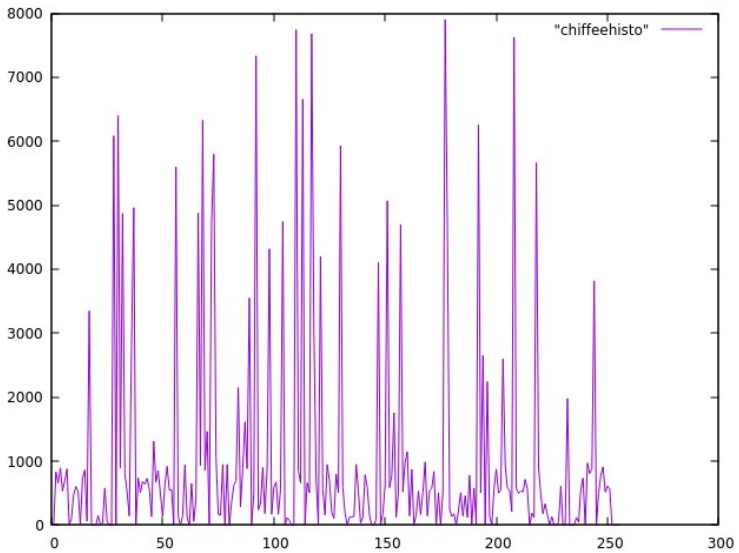
Pour trouver l'inverse modulaire d'un nombre entier, on utilise généralement l'algorithme d'Euclide étendu.

La clef privée utilisée est l'inverse modulaire, ici 13.

c)

i)Les images ont une entropies similaires : 6.677, ça s'explique par le fait que chaque pixels ayant la même intensité vont avoir la même valeur chiffrée.





ii)

En seuillant l’image pour la binariser, on remarque que l’image change de ton mais n’est pas chiffrée, car tout les pixels blancs ont la même valeurs et de manière similaire pour les pixels noirs.

iii)

L’algorithme implémenté ne possède pas un bon niveau de sécurité car il est fragile face à l’analyse de fréquences.