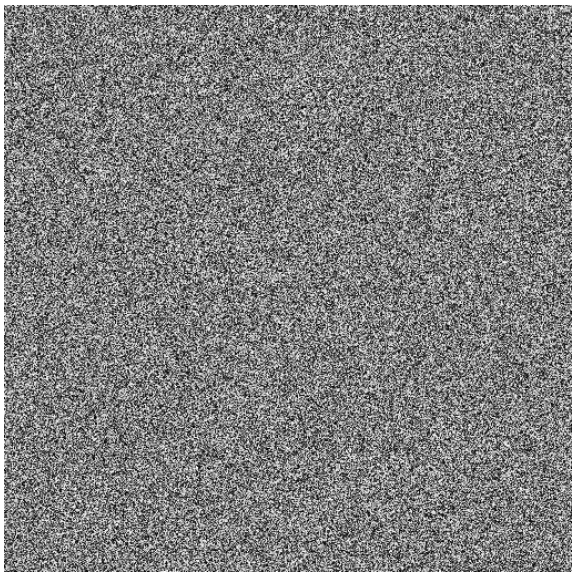
TP1 Chiffrement multimédia

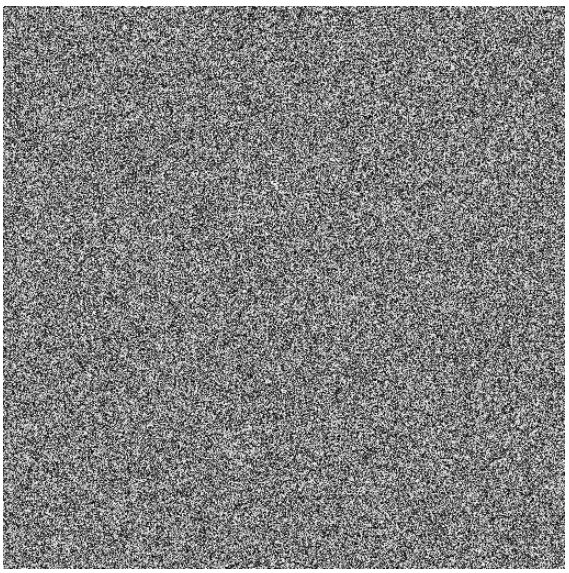
Dubar Axel

Introduction

a)



clef : B28AB097EAEF7CF15D2154F16A6883C



clef : 11111111111111111111111111111111

Quelque soit la clef utilisée, l'image s'apparente a du bruit.

ii) L'image peut être décodée en utilisant le mode CBC

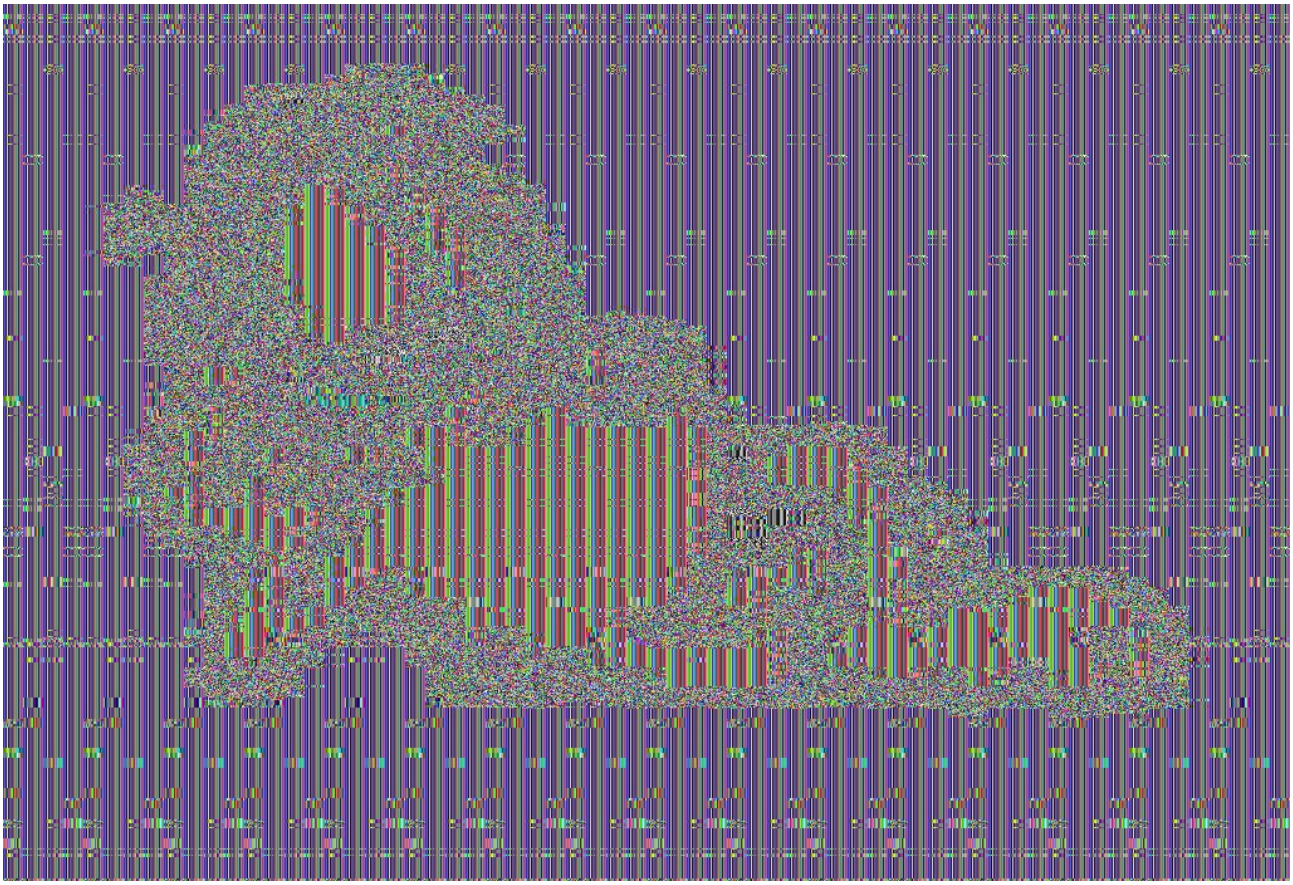
image inconnue en clair

iii)
ECB : « Electronic Code Book », le message à chiffrer est séparé en blocs qui sont chiffrés indépendamment les un des autres, ainsi deux blocs identiques vont former le même message chiffré en sortie, ce mode n'est donc pas sûr.

CBC : « Cipher Block Chaining », aussi un chiffrement par bloc, cependant ici le chiffrement d'un bloc se fait à l'aide des blocs précédents. Un OU Exclusif (XOR) est appliqué entre le bloc précédent chiffré et le bloc à chiffrer en clair avant le chiffrement.

OFB : «Output Feedback » Chiffrement à l'aide d'un flux de clef, les flux est calculé avec à l'aide du précédent flux. Ainsi il est possible de précalculer la suite de flux, mais de la même manière il est plus simple de reconstitué le flux sur une attaque.

iv) Puisque le mode ECB chiffre les blocs de manière indépendante, tout blocs ayant la même valeur donnera la même suite chiffrée. Cette méthode de calcul peut entraîner des problèmes sur les images ayant de grandes suite de pixels similaires comme les images numériques.
Exemple avec garfield.pnm :



On peut voir que le fond étant une suite de pixels de même couleur donne le même chiffrement, la confidentialité visuelle ne peut être complètement garantie.

v)

image casimir_noised en clair

On peut voir que des lignes de bruits apparaissent, cela est du au fait que le bruit généré en mettant les pixels égaux à 60 à 0 empêche le déchiffrement du bloc, ce qui ce répercute sur tous les pixels appartenant au même bloc.

b)

Chiffrement de l'image Chat.png avec le chiffrement JPEG :

ii)Toute les composantes ne sont pas chiffrées sinon nous ne serions pas en mesure de reconnaître l'image en clair.
iii)Cette méthode ne permet pas de garantir la confidentialité visuelle de l'image en clair.

Un exemple de cryptosystème symétrique : le chiffrement XOR

a) ii)

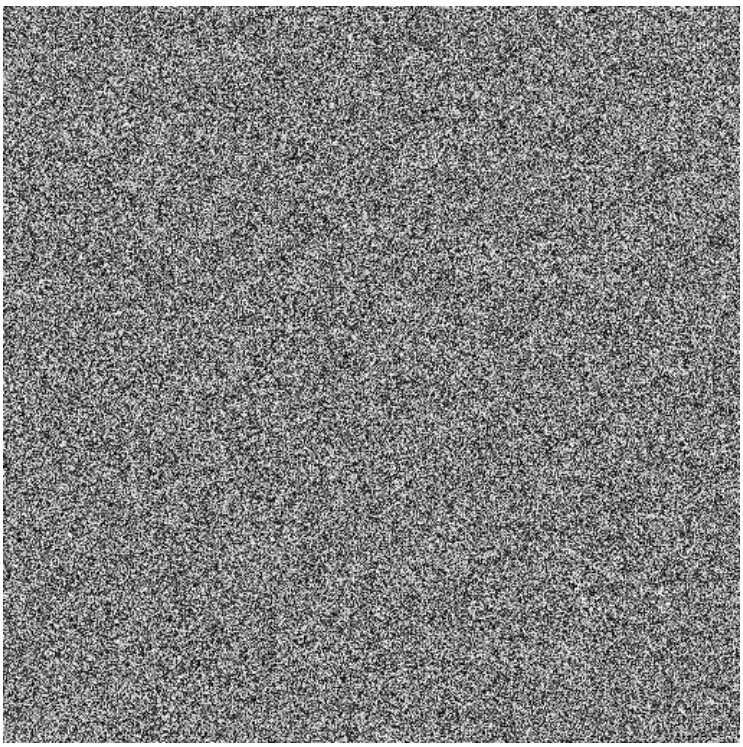


image en clair *image chiffrée avec clef=24*

En réappliquant le chiffrement avec la même clef sur l'image chiffrée, on obtient bien l'image originale.

b)

i) L'entropie de l'image en clair est de 6,72 alors que celle de l'image chiffrée est de 7.999. L'entropie maximale d'une image pgm étant de 8, l'image chiffrée est effectivement très proche de l'entropie maximale.

ii) En attaquant l'image d'un voisin, on est en mesure de retrouver l'image en clair car c'est celle qui dispose de l'entropie la plus basse :