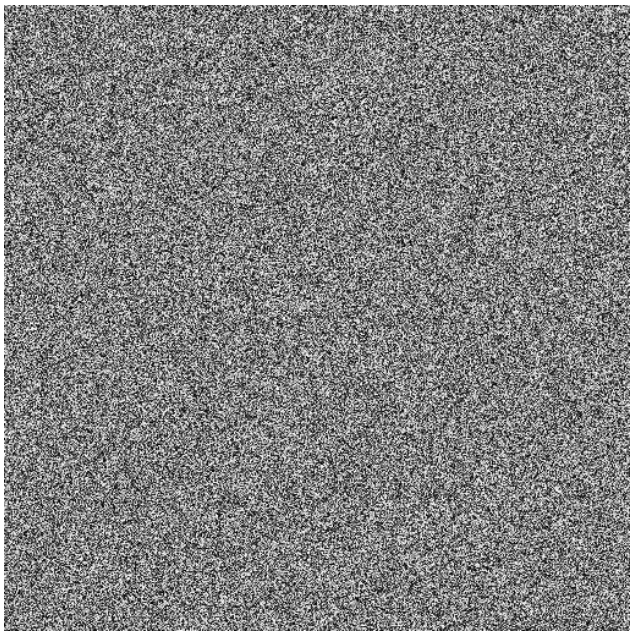
Jandot Julien
Codage et Compression multimédia

Chiffrement - Compte rendu du TP 1

I. Introduction

Image originale



Chiffrée avec la clé :
2B28AB097EAEF7CF15D2154F16A6883C

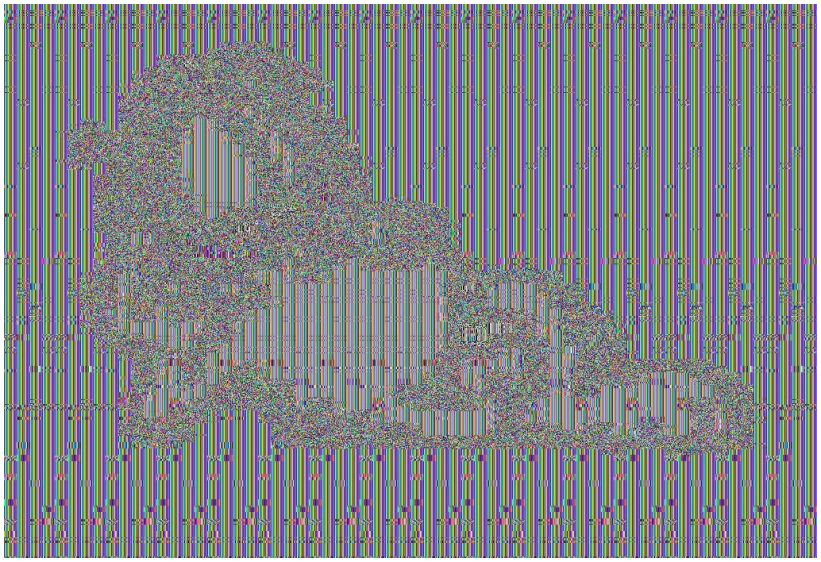
On est censé obtenir des images différentes si la clé change.

Déchiffrement d'Inconnue.pnm avec OFB

Différentes modes de chiffrement :

- **ECB :** on découpe les données en blocs qui sont chiffrés les uns à la suite des autres
- **CBC :** on découpe les données en blocs, puis on applique un XOR sur le bloc avant qu'il soit chiffré, puis on code les blocs suivant en prenant pour base le précedent.
- **OFB :** chiffrement précalculable, on crée le bloc chiffré à appliqué sur le texte, puis ce bloc sera recalculé pour le prochain bloc.

ECB n'est pas sécurisé car deux blocs identiques seront chiffrés de la même manière, ce qui rend sont déchiffrage « facile ». Dans l'image suivante, on reconnaît les contours, même après le chiffrement.



Chiffrement ECB de Garfield

Reconstruction ECB :

On remarque la présence de bruit sur l'image. Cela est du aux pixels de l'image chiffrée qui ont été mis à 60, et n'ont pas pu être décodé de manière correcte, car le bloc était différent.

Clé
0123ABC4567DEF890123ABC4567DEF89

JPEG :

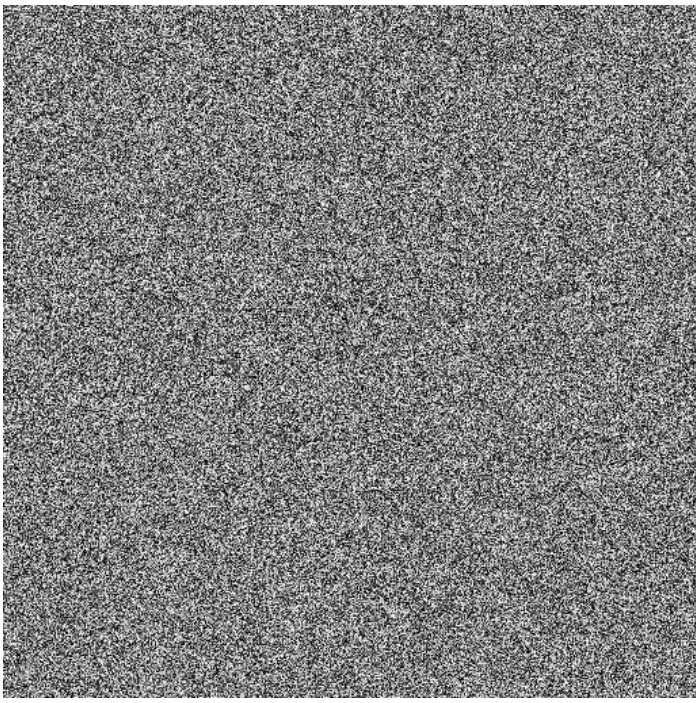
La luminance n'a pas été changée, mais les composantes de chrominance, ont été réduites en bloc, ce qui donne cet effet de découpage marqué. Pour gagner de la place, l'algorithme a étendu, un pixel sur ses voisins, ou fait des moyennes.

Cette méthode ne garantit pas la confidentialité de l'image, mais peut être utilisée si l'on veut flouter l'image, ou l'afficher en préchargement pour permettre une aperçu plus rapide.

Clé
2B28AB097EAEF7CF15D2154F16A6883C

II. XOR

Image originale : airplane.pgm



Chiffrage XOR avec la clé 42

En réappliquant XOR avec la même clé, on retrouve bien l'image de base.

Pour l'attaque bruteforce, le programme fonctionne de la manière suivante : on prend l'image chiffrée, et pour chaque clé possible, on la décode, et on calcule l'entropie de l'image décodée. On affiche ensuite la liste de toutes les entropies, et celle qui est grandement différente des autres et celle de notre clé.