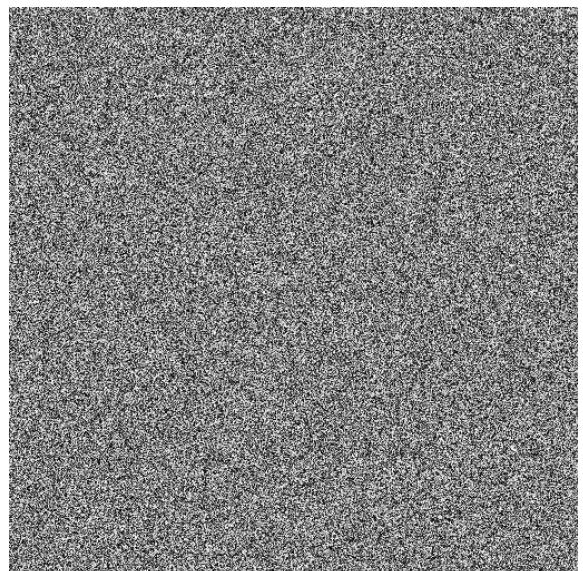
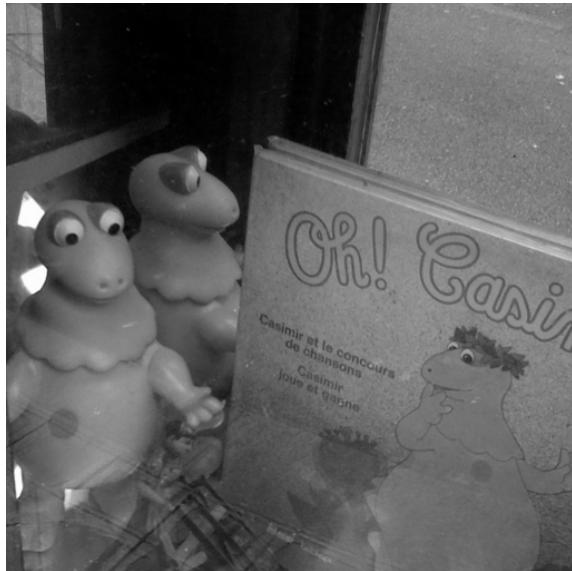


Compte-rendu TP1

Chiffrement multimedia

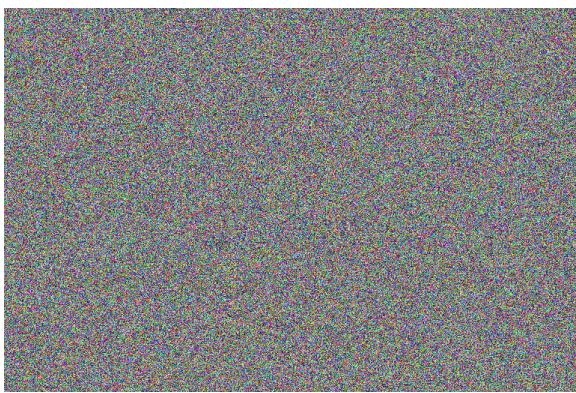
Saffin Alex andre

Q1)



En utilisant le chiffrement CBC on obtiens des images différentes comme on peut le voir ci-dessus.

Q2)

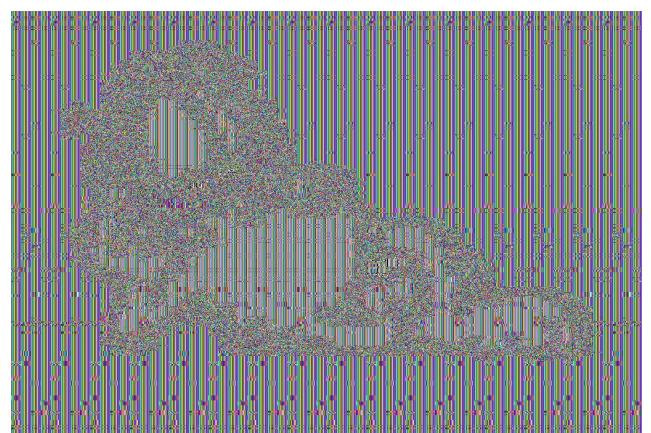


En décryptant l'image à gauche avec le mode « OFB » et la clef 0123ABC4567DEF890123AB-C4567DEF89 on obtiens l'image à droite.

Q3)

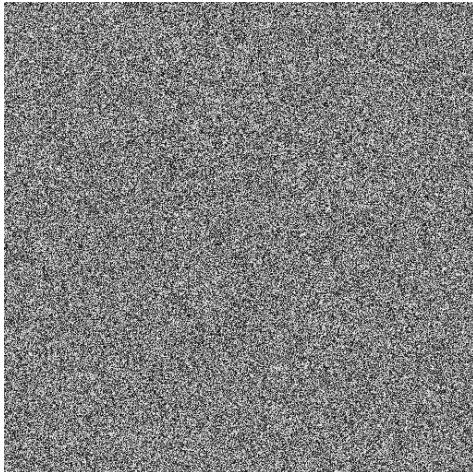
- Avec le chiffrement ECB, on va chiffrer les différents blocs de texte et assembler les résultats les un à la suite des autres afin d'obtenir le texte chiffré.
- Avec le chiffrement CBC on va choisir un vecteur d'initialisation, effectuer un XOR avec notre premier bloc clair et chiffrer ce bloc avec une clef afin d'obtenir le bloc chiffré associé. On va par la suite effectuer la même étape que précédemment pour le second bloc clair en effectuant cette fois-ci le XOR avec le bloc chiffré précédemment.
- Avec OFB on va prendre un vecteur d'initialisation que l'on va chiffrer avec une clef et effectuer un XOR sur le premier bloc clair pour obtenir le bloc chiffré, par la suite on va réutilisé le vecteur d'initialisation chiffré que l'on va rechiffrer et effectuer la même chose que précédemment avec le second bloc clair et ainsi de suite.

Q4)



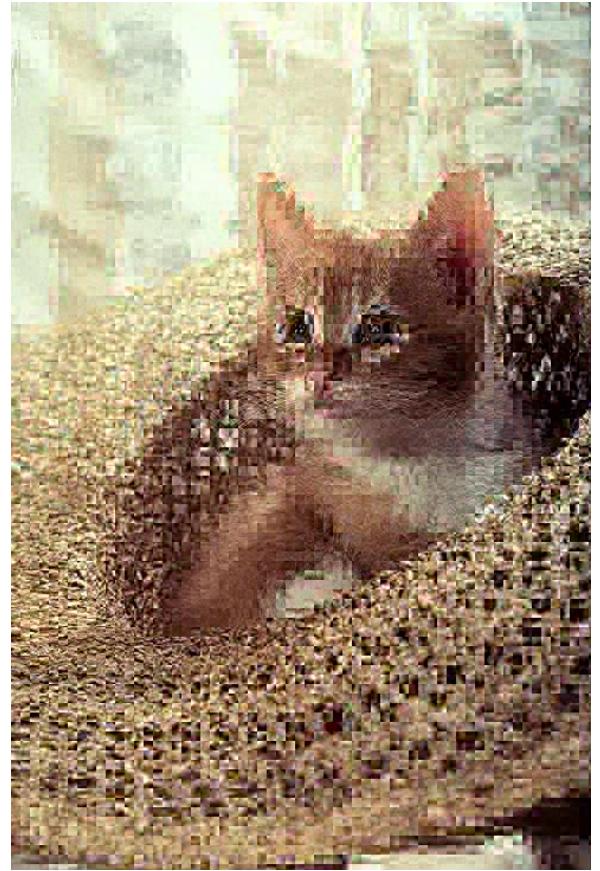
On peut voir effectivement que l'on peut retrouver des informations sur l'image original (ici les contours) dans l'image chiffré avec le mode ECB. Ceci est lié à l'absence de vecteur d'initialisation.

Q5)



On observe des interférences sur l'image, cela est lié aux pixels qui ont été mis à 0 après son chiffrement, il est normal qu'on obtienne des erreurs au déchiffrement.

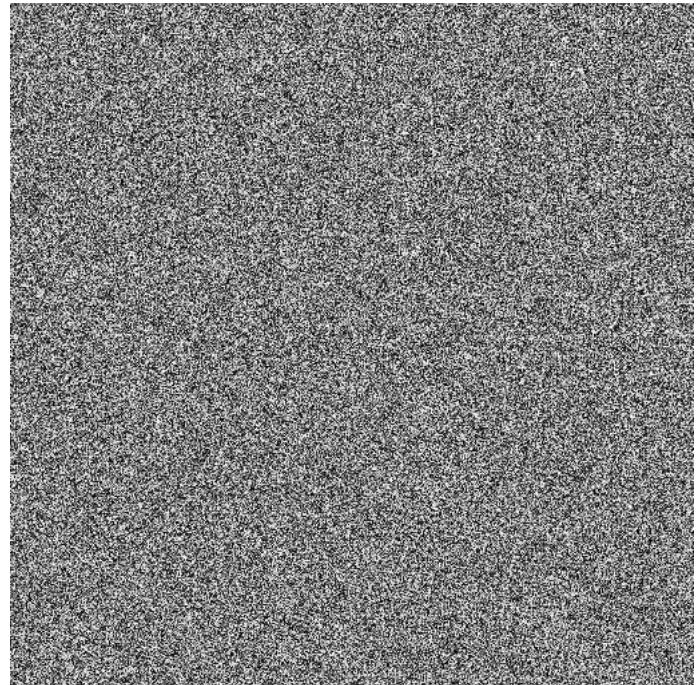
Q6)



L'image obtenue est proche de l'image originale elle est simplement de moins bonne qualité, il semble évident que toutes les composantes n'ont pas été chiffrée.

On pourrait utiliser ce genre de chiffrement pour donner à l'utilisateur un aperçu de ce qu'il pourrait obtenir si on lui donnait la clé qui permet d'obtenir l'image originale de meilleures qualités.

Chiffrement XOR



En utilisant l'algorithme Xor sur l'image de gauche, on obtiens l'image chiffré à droite, si on réapplique le même algorithme alors on obtiens de nouveau l'image de droite (car le Xor est symétrique), j'ai utilisé la seed « 15 ».

Pour le Force brute, on va parcourir toute les seed et déchiffrer l'image avec chacune d'elle, on va prendre l'image avec l'entropie qui se rapproche le moins de l'entropie maximale pour obtenir la seed.