

Compte Rendu

TP1 Chiffrement Multimédia

Thomas Duprat

Introduction

A. Chiffrement AES


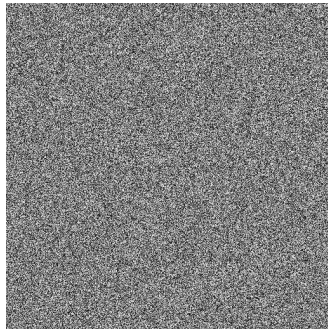
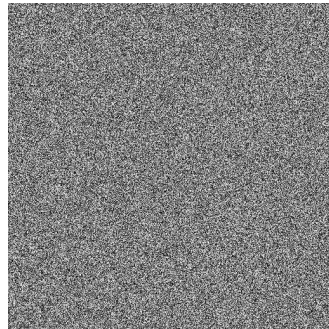
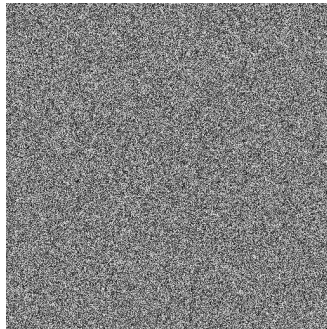
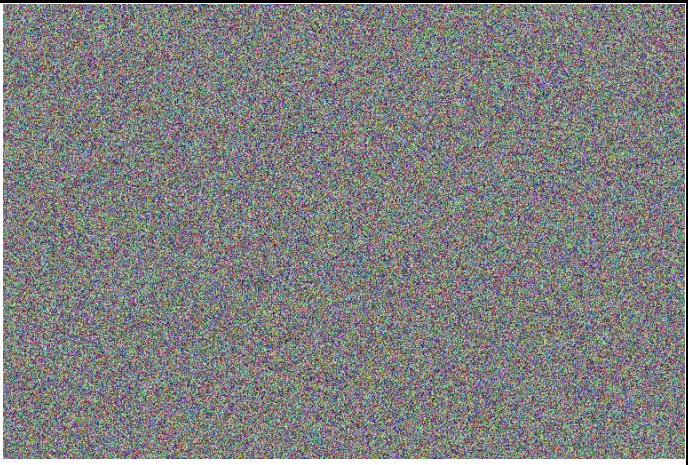

<p>Image en Clair</p>			
<p>Image Chiffrée Obtenue</p>			
<p>Clef Utilisée</p>	<p>2B28AB097EAEF7CF15 D2154F16A6883C</p>	<p>00000000000000000000 00000000000000</p>	<p>FFFFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFF</p>

Image Chiffrée	
Image en Clair	
Mode Utilisé	<i>OFB</i>

Comparaison entre ECB, CBC, et OFB

	Chiffrement par Bloc	Vecteur d'Initialisation	Parallélisable	Fonctionnement
ECB	Oui	Non	Oui	Crée un dictionnaire des codes des différentes valeurs de blocs
CBC	Oui	Oui	Non	Applique l'opération XOR entre le bloc chiffré précédent (respectivement le vecteur d'initialisation) avant d'utiliser le résultat et la clef pour chiffrer le bloc courant.
OFB	Non	Oui	Non	Génère un texte chiffré à partir de la clef et du texte chiffré précédent (respectivement le vecteur d'initialisation). Applique ensuite l'opération XOR entre le texte chiffré obtenu et le texte en clair.

Ces trois modes présentent des failles de sécurité mais ECB est moins sécurisé que les deux autres.

Pour argumenter la phrase précédente sur la sécurité de ECB, voici un petit exemple de sa mise en application:



Image en clair



Image Chiffrée

On note tout de suite que des informations ne sont pas cachées par l'image chiffrée :

- On remarque qu'il y a un fond et un personnage principal
- On peut deviner que le personnage principal est couché sur le côté

Etude de Casimir_noised_ECB.pnm

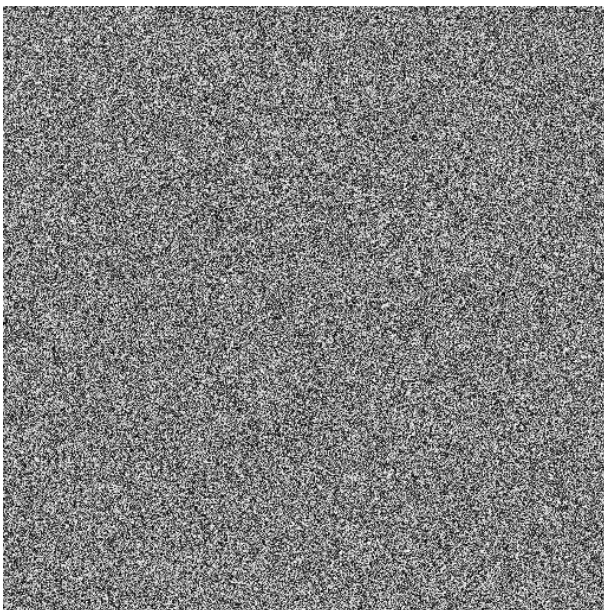


Image Chiffrée



Image en Clair

On constate des artefacts présents sur l'image reconstruite. Certains des pixels ayant été modifiés après chiffrement, on leur a appliqué le code de leur nouvelle valeur, ce qui a modifié l'image en clair.

B. Chiffrement d'images JPEG



Image en Clair



Image Chiffrée

Il ne semble pas que toutes les composantes aient été chiffrées, certains endroits comme la zone crème en bas à droite de l'image sont quasiment identiques, impliquant que certains blocs n'aient pas été chiffrés.

Cette méthode ne garantit absolument pas la confidentialité visuelle de l'image en clair, on dirait plus qu'une compression avec perte quelconque lui a été appliquée (sans chiffrement), dégradant sa qualité.

On pourrait peut-être utiliser cette méthode pour effectuer des effets visuels ? (dans l'esprit level of detail)

Le Chiffrement XOR

A. Implémentation de la méthode de déchiffrement



Image de base en clair

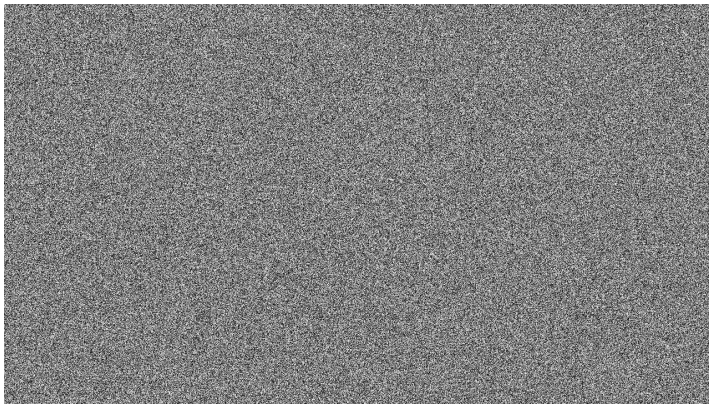


Image chiffrée

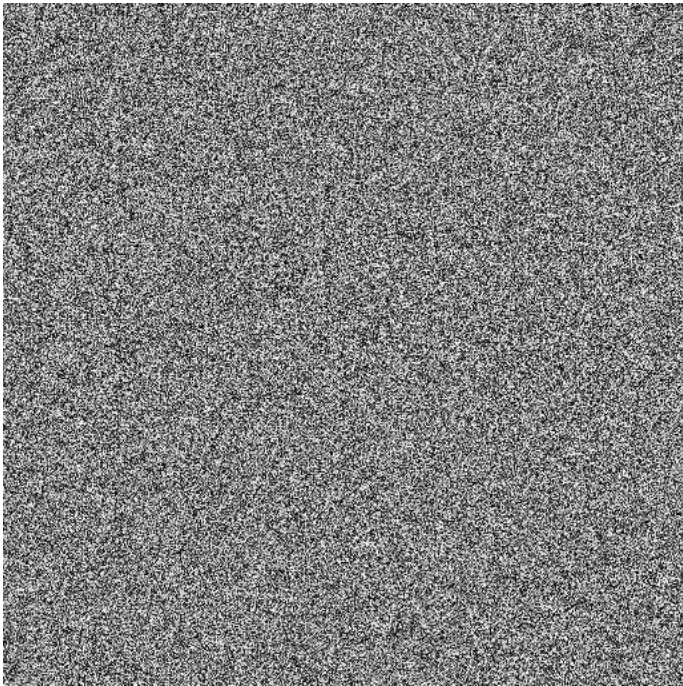


Image déchiffrée

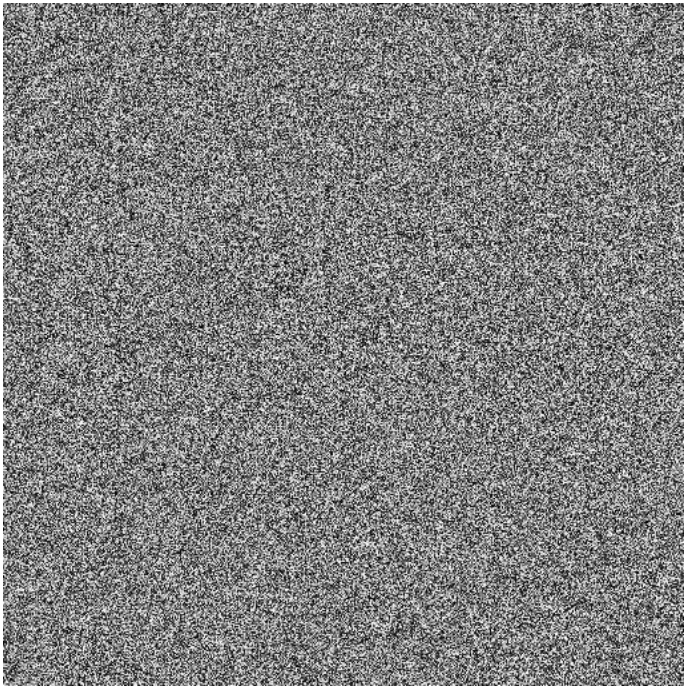
B. Attaque pour retrouver l'image en clair

J'ai échoué...

Bonus



F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0



0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F0F



Carte des différences