Travaux Pratiques : Analyse des modes de chiffrement AES

M1-SI – Module : Sécurité avec Python

Date : 18 Juin 2025

Enseignant : *Arij AZZABI*

June 18, 2025

Objectifs

- Comprendre les modes de chiffrement ECB et CBC.
- Observer les vulnérabilités du mode ECB par l'expérimentation.
- Manipuler le chiffrement d'images et l'analyse des blocs.
- Introduire l'idée d'attaque sans clé (attaque par connaissance partielle).

Exercice 1 — Chiffrement ECB d'une image

1. Télécharger une image (par exemple *Tux*, un QR code ou un logo à motifs).
2. Convertir l'image en octets (bytes).
3. Chiffrer l'image avec AES en mode **ECB** avec une clé de 16 octets.
4. Sauvegarder l'image chiffrée.
5. Comparer visuellement l'image d'origine et l'image chiffrée.

Questions :

- Que remarquez-vous dans l'image chiffrée ?
- Pourquoi peut-on voir la forme d'origine ?
- Quelles données sont restées identifiables malgré le chiffrement ?

Exercice 2 — Chiffrement CBC de la même image

1. Reprendre l'image utilisée dans l'exercice précédent.
2. Chiffrer cette image avec AES en mode **CBC**.
3. Utiliser un vecteur d'initialisation (**IV**) aléatoire de 16 octets.
4. Sauvegarder l'image chiffrée.
5. Comparer visuellement les deux images chiffrées (ECB vs CBC).

Questions :

- Que voyez-vous dans l'image chiffrée en CBC ?
- Pourquoi les motifs ont-ils disparu ?
- Quel est le rôle exact de l'IV dans ce mode ?

Exercice 3 — Analyse des blocs chiffrés

1. Extraire les blocs de 16 octets de l'image chiffrée.
2. Compter combien de blocs sont identiques dans le fichier chiffré.
3. Afficher un histogramme de fréquence des blocs.

Questions :

- Quel mode présente le plus de répétitions ?
- Pourquoi ECB génère-t-il autant de blocs identiques ?
- En quoi cela compromet-il la confidentialité ?

Exercice 4— Déchiffrement sans la clé

1. Proposer un scénario où un attaquant ne connaît pas la clé, mais peut deviner certaines parties du texte clair.
2. Dans un message chiffré en ECB, essayer de retrouver des structures ou du contenu connu.
3. Explorer l'idée d'une attaque par dictionnaire : si un texte connu génère toujours le même bloc chiffré, il peut être identifié sans déchiffrement.

Questions :

- En quoi le mode ECB rend-il ce type d'attaque possible ?
- Que faudrait-il changer pour se protéger contre ce type d'analyse ?