Université de Montpellier
Master 2 - Imagina
TP Codage et compression (HMIN322)

Enseignant : Pauline Puteaux
pauline.puteaux@lirmm.fr
A rendre le 12 octobre 2020

TP1 Chiffrement multimédia

Le but de ce TP est de manipuler différents algorithmes de chiffrement pour comprendre leur fonctionnement. Il sera aussi important de prendre conscience des enjeux de sécurité relatifs à ces méthodes. Vous devrez rendre le compte-rendu de ce TP et vos sources à la fin de la séance. Le compte-rendu doit être constitué de vos réponses aux questions et éventuellement de remarques sur vos choix d'implémentation. Le code doit être commenté.

Ci-dessous, vous trouverez les conventions de nommage (à respecter pour être évalué...) :
Sujet du mail : `[M2-IMAGINA] TP1 Chiffrement multimedia - Nom Prénom`
Compte-rendu : `CR_TP1_ChiffrementMultimedia_NomPrénom`
Archive des sources : `Code_TP1_ChiffrementMultimedia_NomPrénom`

(1) Introduction (0h30)

Allez sur le site de démonstration http://www.lirmm.fr/icar-ancien/en_ligne/.

(a) Chiffrement d'images avec l'AES
Allez dans la partie `Image encryption > Full encryption`. Vous utiliserez l'algorithme symétrique AES.

i) En utilisant le mode de chiffrement CBC, chiffrez l'image en clair `Casimir.pgm`. Obtient-on la même image chiffrée avec différentes clefs ? Vous mettrez dans votre rapport différentes images obtenues.

ii) Déchiffrez l'image chiffrée `Inconnue.pnm` avec la clef `0123ABC4567DEF890123ABC4567DEF89`. Vous mettrez dans votre rapport l'image en clair retrouvée et indiquerez le mode utilisé lors du chiffrement de l'image.

iii) Effectuez des recherches sur le fonctionnement des modes ECB, CBC et OFB. Dans votre rapport, expliquez brièvement leurs différences.

iv) Le mode ECB est-il sécurisé ? Argumentez votre réponse. Pour répondre à cette question, chiffrez l'image `Garfield.pnm` en utilisant ce mode de chiffrement.

v) L'image `Casimir_noised_ECB.pnm` a été chiffrée en utilisant le mode ECB et la clef `0123ABC4567DEF890123ABC4567DEF89`. Après son chiffrement, tous les pixels égaux à 60 ont été mis à zéro. Déchiffrez cette image. Que constatez-vous ? Pourquoi ? Vous mettrez dans votre rapport l'image reconstruite.

(b) Chiffrement d'images JPEG
Allez dans la partie `Image encryption > Compression with encryption > Selective encryption with compression`. Vous utiliserez l'algorithme symétrique AES, avec le mode de chiffrement CBC.

i) Appliquer l'algorithme de crypto-compression sur l'image en clair `Chat.png`. Mettre dans votre rapport l'image obtenue.

ii) Toutes les composantes ont-elles été chiffrées ? Argumentez.

iii) Cette méthode de chiffrement permet-elle de garantir la confidentialité visuelle de l'image en clair ? Donnez une application possible.

(2) Un exemple de cryptosystème symétrique : le chiffrement XOR (1h)

On s'intéressera ici au chiffrement d'images en niveaux de gris (`.pgm`). Vous utiliserez l'image `.pgm` de votre choix pour vos tests (à présenter dans votre rapport).

(a) Implémentation de la méthode de (dé)chiffrement

On rappelle le fonctionnement du chiffrement XOR :

Définition Le chiffrement XOR est une méthode de chiffrement symétrique. Soit I une image de taille $m \times n$ pixels $p(i, j)$ avec $0 \leq i < m$ et $0 \leq j < n$. L'image chiffrée I_e est obtenue en effectuant un ou-exclusif entre les pixels de l'image en clair et une séquence binaire générée pseudo-alétoirement.

i) Implémentez une fonction qui prend en entrée un nombre entier dans l'intervalle $[0, 100]$ considéré comme clef de chiffrement pour initialiser un générateur pseudo-aléatoire. Ce générateur sera utilisé pour obtenir une séquence pseudo-aléatoire de la même taille que l'image.

ii) A l'aide de la fonction précédente, implémentez la fonction de chiffrement. Chiffrez l'image que vous avez choisie et présentez le résultat obtenu dans votre rapport. Vous indiquerez aussi la clef de chiffrement utilisée.

NB : L'opération XOR étant symétrique, la fonction de déchiffrement est identique. Vérifiez que vous réussissez à reconstruire l'image originale en ré-appliquant votre fonction.

(b) Attaque pour retrouver l'image en clair

On rappelle que l'espace des clefs est réduit aux nombres entiers dans l'intervalle $[0, 100]$.

i) Implémentez une fonction qui calcule l'entropie de Shannon d'une image. On rappelle sa définition ci-dessous :

Définition : Soit I une image de taille $m \times n$ pixels avec l niveaux de gris α_i $(0 \leq i < l)$, de probabilité associée $P(\alpha_i)$. L'entropie d'ordre zéro d'une image X, exprimée en bit par pixel (bpp) est :

$$H(I) = -\sum_{i=0}^{l} P(\alpha_i) \log_2(P(\alpha_i)).$$

ii) Proposez une attaque par force brute. En d'autres termes, essayez de déchiffrer l'image chiffrée en utilisant toutes les clefs possibles. Pour retrouver l'image en clair (et donc la clef de chiffrement), utilisez le théorème suivant :

Théorème : Si un algorithme de chiffrement est efficace, la valeur de l'entropie de l'image chiffrée doit être proche de l'entropie maximale et donc, plus grande que l'entropie mesurée dans l'image en clair.

Pour tester votre algorithme, vous échangerez l'image chiffrée obtenue à la question 2.a.ii avec votre voisin et essayerez de reconstruire l'image originale qu'il a choisi.

(3) Bonus

Pour étayer votre réponse à la question 1.a.i, calculez la carte des différences entre deux images chiffrées avec deux clefs différentes, mais similaires. Vous indiquerez les deux clefs utilisées, et présenterez cette carte des différences dans votre rapport.