SORBONNE UNIVERSITÉ

Cryptographie Appliquée – `OpenSSL`

Version du 22 janvier 2024

TME

Exercice 1 – *Modus Operandi*

Non cet exercice ne s'intéressera pas aux manières d'opérer des criminels sortis des Experts Cyber ! Ici nous nous intéresserons aux modes opératoires utilisés en cryptographie symétrique.

1. L'image `UniKorn.ppm` est dans un format où il est très facile de distinguer les donnés de l'image de l'entête. Gimp ou Emacs peut afficher un tel fichier. Ecrire un script shell qui permette, à partir d'un tel fichier, de créer deux fichiers, l'un correspondant à l'entête, l'autre aux données binaires. (indication : google est ton ami)
2. Écrire un script shell qui chiffre des fichiers de données binaires comme construits dans la question précédente. Utiliser OpenSSL pour réaliser des chiffrements AES en mode ECB et en mode CBC.
3. Écrire un script shell qui reconstruit des images à partir des données chiffrées réalisées à la question précédente et de l'entête construite précédemment.
4. Comparer toutes les images construites. Qu'en déduisez-vous sur le mode opératoire ECB. Expliquer les phénomènes observés. Qu'en déduisez-vous comme technique pour mettre à mal la stéganographie.

Exercice 2 – Comparaison des algorithmes de chiffrement

1. Écrire un script shell ou un programme en C ou en Python qui permette de mesurer le temps de calcul d'un processus.
2. À l'aide du programme de la question précédente, mesurer le temps de calcul pris par différents cryptosystèmes proposés par `OpenSSL` pour le chiffrement (vous utiliserez le même fichier en entrée qui devra être suffisamment gros pour que les mesures aient du sens).
3. Construire un tableau de records de vitesse et nommer le gagnant de la compétition !

