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

Enseignant : Pauline Puteaux
pauline.puteaux@lirmm.fr
A rendre le 19 octobre 2020

TP2 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] TP2 Chiffrement multimedia - Nom Prénom`
Compte-rendu : `CR_TP2_ChiffrementMultimedia_NomPrénom`
Archive des sources : `Code_TP2_ChiffrementMultimedia_NomPrénom`

(1) Un exemple de cryptosystème asymétrique : l'algorithme RSA (1h30)

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

(a) Implémentation de la méthode de chiffrement

i) Implémentez une fonction permettant de vérifier qu'un nombre est premier. On choisit $p = 11$ et $q = 23$: vérifiez, à l'aide de cette fonction, que ces deux nombres sont premiers.

ii) Implémentez une fonction testant si deux nombres sont premiers entre eux.

iii) Implémentez une fonction permettant d'obtenir tous les exposants de chiffrement e possibles. On choisit, pour la suite, $e = 17$.

iv) Implémentez la fonction de chiffrement du système RSA. Dans cette version simplifiée, vous chiffrerez chaque pixel de l'image séparément, *i.e.* la version chiffrée d'un pixel $p(i, j)$ de l'image originale est obtenue en calculant $p(i, j)^e \mod n$ (avec $n = pq$). Quelle est la clef publique utilisée ? Chiffrez l'image `Airplane.pgm` et présentez les résultats obtenus dans votre rapport.

(b) Implémentation de la méthode de déchiffrement

i) Implémentez une fonction pour calculer l'inverse modulaire d'un nombre entier. Vous vous en servirez pour obtenir d, l'inverse de e modulo $\Phi(n)$ dans la question suivante. Quel est le nom de l'algorithme généralement utilisé ?

ii) Implémentez la fonction de déchiffrement du système RSA. Déchiffrez l'image chiffrée que vous avez obtenue à la question (a). Quelle est la clef privée utilisée ?

(c) Analyse de sécurité

i) Calculez l'entropie de l'image chiffrée que vous avez obtenue à la question (a) et celle de l'image en clair. Tracez leurs histogrammes. Que constatez-vous ?

ii) Binarisez l'image en clair, puis chiffrez la avec l'algorithme RSA que vous venez d'implémenter. Que constatez-vous ?

iii) L'algorithme ainsi implémenté offre t-il un bon niveau de sécurité ? Quel est le problème ici ? Expliquez en quelques lignes une solution pour y remédier.

(2) Bonus

Adaptez l'algorithme RSA implémenté dans la partie précédente en prenant en compte la solution proposée à la question 1.c.iii.