Compte-rendus des réunions

Pierre DUBAILLAY

19 janvier 2017

Semaine du 09/01

Introduction

Cette première réunion a permis de poser les bases du projet, en définissant le cadre, les attentes et les limites attendus.

Documents demandés

Les documents suivants sont à rendre à la fin du projet :

. une vidéo de démonstration de l'utilisation du programme à des fins publicitaires pour l'université
. un rapport de projet, décrivant l'ensemble du projet (des choix d'implentation aux problèmes rencontrés)
. le code source du projet

Choix du langage

Le langage choisit est le python. Il est imposé un code robuste (qui peut faire face à une utilisation non prévue) et maintenable.

Fonctionnalités imposées

Le programme doit pouvoir prendre une image dans n'importe quel format et la formatter pour une utilisation. Il doit être possible de fournir une clé pour chiffrer une image.

Fonctionnalités souhaitées

Un mode enfant, simple d'accès, et qui permet de dessiner sa propre image.

DeadLines

Une première échéance est début février, pour une démonstration aux portes ouvertes de l'université de Rouen. La seconde échéance est, pour le moment, début avril.

Structure du programme

La structure n'est pas encore arrêtée, mais certaines pistes on été levées :

. un système de gestion des mises à jour ainsi que des paquets nécessaires
. un système de module (plugin), où chaque fonctionnalité (cryptage, génération de clé ...) est dans son propre module. Cela permettrait de mmodulariser le programme, et permettre de nouvelles fonctionnalités non prévues

. un représentation des-dits modules sous forme d'onglets
. les librairies graphiques et de gestion d'image ne sont pas arrêtées

Réflexions sur les algorithmes

Il a été soulevé deux interrogations sur les algorithmes :
. doit-on diviser chaque pixel en 4 ou bien n'est-ce pas nécessaire
. une possibilité d'effectuer l'algorithme XOR avec des couleurs

Semaine du 18/01

Indroduction

Le but de cette réunion était de présenter nos avancées sur le projet ainsi que faire part d'éventuelles difficultés / questions.

Questions posées

Les questions suivantes ont été posées :

. doit-on diviser chaque pixel en 4 ou bien n'est-ce pas nécessaire ?
. est-il possible d'effectuer les algorithmes sur les images en couleur ?
. pourquoi ne pas ajouter les combinaisons en ligne et en colonne lors de la génération de la clé ?

Réponses apportées

Concernant la nécessité de diviser chaque pixel en 4, il a été montré que par le fait que l'algorithme utilise un XOR, un pixel noir apporterait la certitude que celui-ci est bien noir sur l'image d'origine. En effet, pour qu'un pixel soit noir sur le chiffré, il faut que l'addition modulo 2 soit de la forme noir .. ?

Concernant l'application de l'algorithme sur les couleurs, il semblerait que cela affaiblisse la sécurité, notamment parce qu'on peut deviner la couleur d'origine.

Enfin concernant l'ajout des combinaisons en ligne et en colonne, cela peut créer des distortions sur l'image déchiffrée.

Structure du programme

La structure du programme a été validée lors de la réunion.

Précisions sur les algorithmes

Le phénomène d'apparition des deux images originale lorsque deux imagees chiffrées par la même clé sont supperposées a été expliqué. Le principe repose sur l'associativité à doite et à gauche de l'opérateur XOR.

Documents fournis

De nombreux documents ont été fournis sur la cryptographie, le phénomène de distortion ainsi que sur l'utilisation de LaTeX