Sécuriser les données

Exercices

Titre
Objectif(s) :
A la fin des exercices, l'élève doit être capable de :

- Comprendre le principe de la stéganographie
- Chiffrer en AES256
- Récupérer une chaine de caractères cachée dans une image
- Récupérer une image dans 3 autres images (stégano.)
- Dissimuler un texte dans une image (stégano.)
- Dissimuler une information de droits d'auteurs (watermarking)

Durée prévue : Selon UD

1 Un peu de stéganographie

1.1 Cache-cache

A l'aide de la page de démonstration de stéganographie du cours, cachez du texte dans 2 ou 3 images et placez-les dans :

- **Selon les consignes de votre enseignant** :
  - un dossier commun ou
  - une conversation Teams ou
  - un dossier Teams ou
  - un autre emplacement mais **demander à votre prof** !

Ensuite regardez ce que les autres ont caché !

Selon vous, ces données (texte caché) sont elles bien protégées de tous les regards indiscrets ? Développez votre réponse :

Non pas complétement car n'importe qui peut les lire avec le bon outil.

1.2 Ça passe, ou ça casse

Toujours sur la même page de démo, utilisez comme couverture le fichier « smiley.png » pour dissimuler le contenu du fichier « texte_secret.txt ».

Tout s'est-il passé correctement ?

Non le message a été tronqué.

Pouvez-vous en donner la raison ?

L'image de couverture est trop petite pour un texte aussi long.

2 Un peu de chiffrement AES256

Avec le site de démonstration de chiffrement AES256, chiffrez quelques messages et placez-les dans une conversation Teams ou un chat Impero ou ailleurs selon les instructions de votre enseignant.

Utilisez la clé « toto123 » pour que tout le monde puisse déchiffrer les messages des autres.

Ces messages chiffrés sont-ils à l'abri des regards indiscrets ?

Oui car sans connaître la clé il est impossible de les déchiffrer.

3 Recherche d'un mot caché dans une image

Dans l'image « fleur.bmp » que vous avez reçu, retrouvez le mot de 4 caractères caché dans les derniers octets du fichier, soit les derniers pixels de l'image en haut à droite.

Utilisez HexEd.it en ligne ou un outil comme HxD pour vous aider.

💡 *Ces deux outils affichent le code binaire des octets !*

1. Combien de bits doit-on cacher pour quatre caractères (octets) selon la table ASCII ?

   4 caractères (octet) sur 8 bits correspondent à 32 bits (4x8)

2. Décodez l'image avec HexEd.it ou HxD et donnez ces 4 caractères :

   a. Code hexa complet des 4 derniers pixels :

   08 09 04 09 08 04 08 08 04 09 09 04 09 09 05 09

   08 03 09 08 03 08 09 01 08 09 01 08 08 01 00 01

   b. Code binaire du mot caché :

   💡 *Si vous faites à la main, pensez que les octets impairs on le LSB à 1 alors que les pairs à 0 !*

   01010000 01101111 01101011 01100101

   c. Révélez le mot caché en ASCII avec un outil comme « RapidTables » ou manuellement en convertissant allez dans la table ASCII du cours :

   Mot caché : Poke

0101 0000	50	P
0110 1111	6F	o
0110 1011	6B	k
0110 0101	65	e

4 Stegano des pros !

4.1 Récupération d'une image cachée dans 3 images

OpenPuff est un outil très complet de stéganographie. Cet exercice va nous le démontrer.

Une image secrète a été dissimulée non pas dans une image mais dans trois images (couverture). Cela rend la dissimulation encore plus efficace. De plus, cette image secrète a été chiffrée (il faut connaître le mot de passe) avec 3 clés (mot de passe). En général une seule clé suffit.

Dans OpenPuff, sous « Steganography » choisissez « Unhide » (révéler) puis utilisez les paramètres suivants :

- Mots de passe (clés)
  - (A) Bf%h7W;k18
    (B) pAinaRmoirecUisine
    (C) Toto1234
- Fichiers de couverture dans cet ordre
  - brocoli.jpg
    carrotte.jpg
    patate_douce.jpg
- Paramètres de sélection de bits par défaut
  - Jpeg 1/5 (20%) medium

Maintenant cliquez sur « Unhide ! » et patientez quelques secondes… Enregistrez l'mage quelque part.

Que représente l'image que vous venez de révéler ?

Une carte indiquant l'emplacement d'un colis secret

Il n'est pas possible d'avoir une image de meilleure qualité dans notre cas, pourquoi ?

La couverture doit être suffisamment grande pour couvrir ce que l'on cache,
on est donc limité par la taille de la couverture.

4.2 Exercice 2

Prenez une des 3 images du point précédent et dissimulez-y un **petit** fichier texte de votre conception.

Désactivez les mots de passe (B) et (C) et renseignez le (A) avec celui que vous voulez. Ne changez pas les paramètres (4).

Une fois que c'est fait contrôlez que vous pouvez révéler votre fichier texte et garantir que tout s'est bien passé. Si ce n'est pas le cas réessayer ou demander de l'aide à votre enseignant.

Suite de l'exercice sur la page suivante…

4.3 Watermarking

Révélez l'artiste qui est en vous et faites un petit dessin sur Paint ou n'importe quel outil similaire pour créer un fichier JPEG, BMP ou PNG.

Maintenant vous allez tatouer numériquement votre dessin, c'est-à-dire que vous allez procéder à un « digital watermark » en anglais. Pour rappel, cela consiste à dissimuler une information de droits d'auteurs à l'intérieur pour prouver, en cas d'utilisation non autorisée, que l'on est bien le propriétaire de l'œuvre tatouée.

A l'aide du logiciel OpenPuff ou un autre outil qui offre cette fonctionnalité, insérez une information avec votre nom et la date de création de votre dessin.

Placez votre dessin une fois tatoué dans un dossier commun ou une conversation Teams ou ailleurs selon les instructions de votre enseignant et allez voir qui sont les auteurs de quelques-unes des œuvres de vos collègues.