# SÉCURISATION DES DONNÉES - EXERCICES

## Exercice 0

1. Ouvrez un terminal puis connectez-vous au serveur ssh avec votre compte lfclt*x*, en mettant votre numéro à la place du *x*.
2. Créez le répertoire « tpSECU » dans votre « home directory ». Puis, mettez-vous dans ce répertoire.
3. Tous les fichiers que vous allez créer ou déplacer sont à mettre dans ce répertoire tout au long du TP.

## Intégrité des données : algorithmes de hachage

### Exercice 1

1. Copiez les fichiers texte messsagehappy.txt et messagesad.txt qui se trouvent suivant le chemin /home/lfcltpartage/tpSECU/
2. Quel message est inscrit dans chacun de ces fichiers ?

3. Grâce à la commande openssl, calculez les empreintes de ces deux fichiers (voir partie 3.1 du cours pour la commande exacte). Vérifiez entre vous que vous trouvez la même chose pour le même fichier.
4. Comparez les empreintes des deux fichiers : que remarque-t-on ?

*Pour les plus en avance : vous pouvez refaire les questions 3 et 4 avec -md5 ou -sha256 ou -sha512 à la place de -sha1. Expliquez la différence entre chacun de ces paramètres. Quels sont les avantages et désavantages de chacun d'entre eux ?*

### Exercice 2

Dans cet exercice, nous allons télécharger un logiciel et vérifier son intégrité grâce à son empreinte.

1. A partir d'un navigateur internet, connectez-vous à : putty.org
2. Cliquez sur le premier lien pour accéder à la page de téléchargement du logiciel.
3. Le fichier téléchargeable au premier lien « putty.exe » est sur le serveur au chemin /home/lfcltpartage/tpSECU/putty.exe : calculez son empreinte avec l'algorithme MD5.
4. Revenez sur la page de téléchargement du logiciel et ouvrez la page contenant les empreintes MD5 de tous les fichiers téléchargeables du site (en bas de la page).
5. Retrouvez l'empreinte MD5 du fichier putty.exe que vous venez de télécharger, et vérifiez que c'est la bonne.

*Pour les plus en avance : vous pouvez refaire les questions 5 et 6 avec -sha1 ou -sha256 ou -sha512 et vérifier dans la page adéquate.*

## Confidentialité des données : algorithmes de chiffrement symétrique

### Exercice 3

Dans cet exercice, nous allons chiffrer puis déchiffrer un document grâce à l'algorithme de chiffrement symétrique AES.

1. Choisissez une clé de chiffrement de 64 chiffres (sans espace).
2. Pour cette question, référez-vous à l'exemple du cours de la partie 3.2. Dans le terminal connecté au serveur ssh, chiffrez le fichier messagehappy.txt avec la clé de chiffrement choisie et stockez le résultat dans le fichier « messagehappyc ».
3. Affichez le contenu du fichier messagehappyc : est-ce lisible ?

4. Toujours à l'aide de l'exemple du cours de la partie 3.2, déchiffrez le fichier « messagehappyc » et stockez le résultat dans « messagehappydc ».

5. Vérifiez que vous retrouvez bien votre message initial.

## Authentification : algorithmes de chiffrement asymétrique

### Exercice 4

Dans cet exercice, nous allons chiffrer puis déchiffrer un document grâce à l'algorithme de chiffrement asymétrique RSA. Vous devrez vous inspirer de l'exemple de la partie 3.3. du cours pour réaliser cet exercice.

1. Créez votre clé privée que vous stockez dans le fichier « privkey.pem ».
2. Observez ce que contient le fichier privkey.pem.
3. A partir de votre clé privée, créez votre clé publique que vous stockez dans pubkey.pem.
4. Observez ce que contient le fichier pubkey.pem.
5. Chiffrez le document messagesad.txt avec votre clé publique et stockez le fichier de sortie dans messagesadc.txt
6. Vérifiez que le document obtenu est illisible.
7. Déchiffrez le document messagesadc.txt avec votre clé privée : retrouvez-vous bien le message de départ ?

# Authentification : certificats électroniques

## Exercice 5

Cherchez la liste des autorités de certification dans les paramètres de sécurité du navigateur internet de votre choix et notez le chemin pour y accéder :

## Exercice 6

1. Connectez-vous au site w3schools.com
2. En cliquant avec le bouton droit juste à gauche de l'adresse du site dans la barre d'adresse du navigateur, affichez le certificat du site.
3. a. Cherchez l'autorité de certification : qui a signé ce certificat ?
   b. Retrouvez-la dans le magasin des autorités de certification (voir exercice 5)
4. Quelle est la période de validité du certificat ?
5. Avec quel algorithme asymétrique la clé publique disponible dans ce certificat fonctionne-t-elle ?
6. a. Trouvez les empreintes disponibles du certificat.
   b. Grâce à quelle famille d'algorithmes a-t-on pu obtenir ces empreintes ?
   c. Grâce au bouton « Exporter », on peut télécharger le certificat. Il est accessible sur le serveur au chemin /home/lfcltpartage/tpSECU/putty.exe : vérifier son empreinte grâce à la commande suivante :
   > openssl x509 -fingerprint -sha256 -noout -in NomDuFichier
   … et comparez-la à celle contenue dans la certificat dans votre navigateur. Quel élément de sécurité vient-on de vérifier ?
   d. Pourquoi ne trouve-t-on pas la clé privée dans le certificat ?

*Pour les plus en avance : vous pouvez refaire la question 6 avec -sha1 au lieu de -sha256.*

# Protocole HTTPS

## Exercice 7

1. Téléchargez puis ouvrez avec le logiciel Wireshark le fichier « EchangeHTTPS.pcapng » disponible sur classroom.

2. Dans ce fichier, on voit les paquets lors de l'échange d'un ordinateur avec le site marion.szpieg.fr. Commentez les 10 premières lignes.

## Exercice 8 : garder une trace de son travail

**Avant de vous déconnecter,** tapez la commande suivante :

> history>/home/lfcltx/tpSECU/historytpSECU.txt

Si vous voulez aller voir toutes les commandes tapées sur ce TP, il suffira de taper :

> cat /home/lfcltx/tpSECU/historytpSECU.txt

Pour quitter le serveur « marion.szpieg.fr » tapez « exit » (à faire pour éviter de faire tourner la session « pour rien » svp).