THIERRY MEYER
SÉCURITÉ INFORMATIQUE

INTRODUCTION A LA CRYPTOGRAPHIE APPLIQUÉE
Travaux pratiques : 2h

Manipulation des grands principes de la cryptographie
Utilisation de OpenSSL

---

1 Aperçu du lab :

A travers ce TP, vous allez approfondir vos connaissances sur les mécanismes de cryptographie. Pour cela vous chiffrerez et signerez des documents que vous vous échangerez. Vous utiliserez la suite d'outils du logiciel ***OpenSSL***[1] dans sa version linux en ligne de commande.

Bien que dans un contexte réel, l'échange des clefs soit source de vulnérabilité, nous ne nous attarderons pas, dans ce cas, sur les risques liés à cette étape. Vous pourrez donc les transmettre soit par mail, clefs USB, …

Vous travaillerez seul et de façon totalement autonome, vous devrez donc consulter toute la documentation officielle à votre disposition pour comprendre les options que vous utiliserez et les décrire. Je vous invite vivement à consulter les ***manpages*** de ***OpenSSL***[2].

Normalement vous avez largement le temps de faire toutes les manipulations dans le temps imparti, mais ne perdez pas trop de temps.

2 Objectifs du lab :

Ce TP a été réalisé avec en tête plusieurs objectifs :

- Tout d'abord il est une bonne illustration du cours théorique sur les mécanismes de cryptographie en systèmes et réseaux, puisqu'il reprend la majeure partie des notions abordées.
- Il va vous permettre de manipuler de façon concrète les grands principes de la cryptographie contemporaine à savoir, les fonctions de hachage, le chiffrement symétrique et le chiffrement asymétrique.
- Pour finir, il vous fait découvrir un outil complexe et très puissant qu'est ***OpenSSL***.

1 https://www.openssl.org
2 Un bon point de départ sera la commande ***man openssl***

3 Les consignes :

3.1 Utilisation d'un algorithme de hachage :

3.1.1 Rappels théoriques :

- Expliquez moi à quoi peut servir une fonction de hachage ? Dans le cas du téléchargement d'un fichier sur un site internet, quel risque cela permet-il de prévenir ?

3.1.2 Contrôle d'intégrité d'un téléchargement :

- Téléchargez depuis le site internet officiel[3] la dernière version de ***GNUPG***[4] pour linux.
- A l'aide de ***OpenSSL*** et de l'empreinte ***SHA1*** de l'archive de ***GNUPG*** affichée sur son site officiel, vérifiez que le fichier n'a pas été altéré pendant le téléchargement. Comment avez vous procédé ? Expliquez en détail vos manipulations.

3.2 Chiffrement de fichier à l'aide du chiffrement symétrique AES :

3.2.1 Rappels théoriques :

- Rappelez moi les grands principes du chiffrement symétrique.

3.2.2 Chiffrement de fichier :

- A partir de votre éditeur de texte favori[5] générez un fichier simple contenant le texte de votre choix.
- A l'aide de ***OpenSSL*** chiffrez le contenu de ce fichier en utilisant l'algorithme AES-256-CBC. Expliquez en détail votre manipulation. Transmettez ensuite ce fichier à votre voisin, puis la clef utilisée pour le chiffrer.
- Votre voisin vous aura transmis un fichier chiffré. Éditez son contenu et constatez que celui-ci est bel et bien chiffré. A l'aide de la clef que vous aurez reçue avec ce fichier, déchiffrez son contenu. Expliquez en détail vos manipulations. Vérifiez avec votre voisin que le contenu que vous avez obtenu est bien celui qu'il a rédigé au départ.

3.3 Manipulation des protocoles de chiffrement asymétrique :

3.3.1 Rappels théoriques :

- Rappelez moi les deux applications principales du chiffrement asymétrique. Expliquez leurs principes de fonctionnement respectifs.

Note : Pour chacun des points suivants vous expliquerez en détail vos manipulations. Vous indiquerez les commandes que vous avez utilisées en les commentant.

3.3.2 Préparation de la biclef :

- Générez pour chacun d'entre vous une paire de clefs RSA 2048. Repérez le répertoire où sont stockées vos clefs, puis sauvegardez les.
- Pour communiquer avec un interlocuteur vous allez devoir transmettre une de vos clefs. De laquelle s'agit-il ? Échangez alors cette clef avec toutes les personnes avec qui vous allez vouloir communiquer.

3.3.3 Chiffrement et déchiffrement de fichiers :

- A l'aide de la clef adéquat, chiffrez un fichier texte. Vérifiez à l'aide d'un éditeur le contenu du fichier obtenu. Transmettez le à l'un de vos interlocuteur.
- Récupérez un fichier chiffré par l'un de vos interlocuteur, puis déchiffrez le.

3 http://www.gnupg.org/
4 La dernière version stable au 03/09/2020 est la 2.2.23
5 A votre convenance, nano, vi, vim, ...

3.3.4 Signature électronique :

- A l'aide de la clef adéquat, signez un fichier texte. Transmettez ce fichier et sa signature à l'un de vos interlocuteur.
- Récupérez un fichier signé par un de vos interlocuteur, ainsi que sa signature, puis déchiffrez le à l'aide de la clef qu'il vous aura transmise et de la signature qu'il vous a fournie. Essayez avec la clef d'un autre interlocuteur puis avec la bonne clef.

4 Les livrables :

A l'issue du TP, vous devrez me remettre un rapport détaillé de votre travail. Ce rapport devra être correctement rédigé.
Pour chacun des points à traiter vous fournirez l'explication détaillée des manipulations que vous avez effectuées (commandes et résultats). Vous joindrez les résultats que vous avez obtenus, votre interprétation, ainsi que vos éventuelles remarques et constats. N'hésitez pas également à indiquer vos interrogations sur des résultats.

Pour finir, la note tiendra compte de votre analyse et de la qualité de la rédaction.