**TP : PKI, chiffrement et certificat :   
Durée : 6h**

**Présentation :**

L'objectif de ce TP est de vous aider à comprendre le fonctionnement du chiffrement et d’apprendre à créer, gérer et installer des certificats.  
Pour se faire nous allons utiliser un serveur Web mais il en sera de même pour tout autre élément.

L'accès à un serveur web s’il utilise le protocole HTTP permettra à une personne malveillante positionnée en MITM d'intercepter vos requêtes (login / password, carte bleue, etc.).   
De plus, le site avec lequel vous échangerez s’il n’a pas de certificat prouvant son identité pourra être le site d’une personne malveillante.

**OS :**

Distributions Linux / Unix dans un premier temps et ceux qui auront terminé pourront faire de même sur des OS Windows.

**Questions et actions à réaliser pour les distributions Linux / Unix :**

Votre principale activité va être de créer une documentation vous permettant de savoir comment :

* Chiffrer et déchiffrer des fichiers avec des échanges de clés :
* Créer et installer des certificats ;
* Sécuriser votre serveurs Web.

Pensez donc à bien indiquer toutes les étapes accompagnées de captures d’écran. Vous trouverez ci-dessous quelques éléments qui permettront de vous aiguiller.

**Prérequis :**

1. Indiquer la distribution et version de l’OS utilisé ;
2. Lister les paquets nécessaires et leur version ;

**Chiffrement :**

1. Créer une clé privée RSA :
   1. Générer une clé privée de 2048 bits au format PEM et la stocker dans le fichier « rsaprivatekey.pem ».
   2. Le fichier « rsaprivatekey.pem » contient la partie privée de la clé, et ne peut donc pas être communiqué tel quel (même s’il est chiffré). Avec l’option « -pubout » exporter la clé publique dans le fichier « rsapublickey.pub ».
2. Échanger un fichier chiffré en binôme :
3. Créer un fichier txt contenant un mot, et chiffrez le avec la clé publique de votre partenaire ;
4. Envoyer le à votre partenaire afin qu’il le déchiffre avec sa clé privée.

**Certificat :**

1. Créer une page Web (la page par défaut de votre serveur web sera parfaite) ;
2. Création d’un certificat :
   1. Générer une clé privée de 4096 bits avec l’algorithme de chiffrement AES 256 ;
   2. Créer le fichier de demande de signature de certificat (CSR) ;
   3. Signer le certificat ;
   4. Utiliser le certificat SSL.
3. Tester la configuration / sécurité de votre site :
   1. Dans un premier temps avec la commande OpenSSL ;
   2. Quand vous pensez avoir atteint un niveau satisfaisant testez avec le lien suivant : <https://www.ssllabs.com/ssltest/> ;
   3. Faire une copie d’écran au premier test de la note globale ;
   4. Prendre chaque élément warnings et errors (informations en orange et en rouge) et corrigez les. À chaque élément indiquez ce que vous avez fait pour le corriger.
4. Améliorer la sécurité de votre site :
   1. Autoriser uniquement le TLSv1.2 ;
   2. Autoriser uniquement des cipher suites.