Université Paris Descartes – UFR de mathématiques et Informatique

Licence 3 Informatique – Sécurité et Réseaux

TD/TP n°5

OpenSSL

Exercice 1 : Codage en base64

1. Encoder un fichier texte contenant un mot de passe de votre choix en base64 et envoyer le résultat par courriel à votre binôme. Donner la commande pour coder le fichier.
2. Est-ce que votre binôme est capable de décoder ? donner la commande associée.
3. Est-ce que le codage en base64 est un moyen sûr pour protéger un mot de passe ?

Exercice 2 : Deffie-Hellman

Bob et Alice se sont mis d'accord sur les valeurs suivantes : g = 2879, n = 9929. Bob a choisi ″b = 6″, et Alice a choisi ″a = 9″. Les valeurs de g et n sont la partie publique et ″a″ est la clé privé d'Alice et ″b″ est la clé privée de Bob.

1. En utilisant une calculatrice, calculer :
   $A=g^a \bmod n$
   $B=g^b \bmod n$
2. Alice envoi ″A″ à Bob. Ce dernier utilise sa clé privée pour calculer ″A^b″. Bob envoi ″B″ à Alice, qui l'utilise pour calculer ″B^a″. Donner les valeurs de A^b et B^a.
3. Est-ce que la valeur de A^b est égale à la valeur de B^a?
4. Que peut-on conclure sur l'objective de l'algorithme Deffie-Hellman ?

Exercice 3 : RSA

1. Générer votre paire de clé RSA en la stockant dans un fichier et ensuite visualiser le contenu du fichier avec la commande ″`openssl rsa`″.
   Génération : `openssl genrsa -out private.pem 1024`
   Affichage : `openssl rsa -in private.pem -text`
2. Quelle clé se trouve dans le fichier ″private.pem″ ? publique ou privée ?
3. Quel est le type du codage du fichier ″private.pem″ ?
4. Il n'est pas prudent de laisser une clé en clair, surtout avec un intrus qui risque de causer beaucoup de dégâts. Pour cela, OpenSSL offre la possibilité de protéger la paire des clés en la chiffrant avec un mot de passe.
   Protéger la clé précédemment générée avec chiffrement 3DES et une phrase de passe, en utilisant la commande suivante :
   ```
   openssl rsa -in private.pem -des3 -out key3des.pem
   ```
5. Visualiser le contenu avec une de ces commandes : more ou cat ou less. Est-ce que vous avez besoin de votre mot de passe ? pourquoi ? Noter la différence avec le contenu du fichier ″private.pem″
6. Utiliser de nouveau la commande d'affichage de la clé RSA pour visualiser le contenu de la clé. Que constatez-vous ?
7. Extraire la partie publique de votre clé en utilisant la commande suivante :
   ```
   openssl rsa -in key3des.epm -pubout -out public_key.pem
   ```
8. Pouvez-vous extraire la partie privée de la clé ?

9. Utiliser la commande `rsa` pour visualiser le contenu du fichier *public_key.pem* (n'oublier pas d'utiliser l'option `-pubin`, puisque seule la clé publique est contenue dans le fichier *public_key.pem*).
10. Créez un document texte dans un fichier nommé message.txt, dont le contenu est la phrase suivante :
    `Ceci est un message confidentiel!`
11. Chiffrer le message avec votre clé publique et donner la commande.
12. Déchiffrer le message avec votre clé privée et donner la commande.

PS : la majorité des commandes d'OpenSSL sont disponibles online en cherchant sur google ou sur le site : https://github.com/fracasula/openssl-lab

Exercice 4 : Déchiffrement avec RSA

1. Le fichier ″encrypted.bin″ (disponible sur moodle) contient le résultat de chiffrement d'un texte en clair avec l'algorithme aes-256-cbc. Le mot de passe (″encrypted_sym_key.bin″) est chiffré avec ma clé publique. Par ailleurs, ma clé privée (la paire de mes clés est dans le fichier ″rsaprivkey.pem″) a été chiffrée avec le mot de passe ″secres″. Saurez-vous déchiffrer le fichier ″encrypted.bin″ ?
2. Après le déchiffrement du fichier ″encrypted.bin″, dériver la signature du fichier en clair texte et donner la commande. Quelles sont les opérations à réaliser pour signer un fichier ? quelle clé est utilisé pour la signature ?
3. Quelles sont les étapes nécessaires pour vérifier la signature à la réception ? quelle clé est utilisée pour la vérification de la signature ?

Exercice 5 : Passwd

1. Dans quel fichier sont stockés les mots de passe sous Linux ?
2. Ajouter un utilisateur user1 au système avec un mot de passe azerty. Contempler le résultat stocké sur votre machine
3. Le résultat est composé de 3 parties séparées par $. Noter le contenu de chaque partie.
4. Expliquer la signification de chaque partie.
5. En utilisant l'outil OpenSSL et le ″salt″, régénérer l'empreinte du mot de passe stocké sur votre machine
6. (Optionnel) Est-ce possible d'écrire un script (langage de votre choix) pour déchiffrer le mot de passe ?