OpenSSL

OpenSSL est une boîte à outils cryptographiques implémentant les protocoles SSL et TLS qui offre

1. Une bibliothèque de programmation en C permettant de réaliser des applications client/serveur sécurisées s'appuyant sur SSL/TLS.

2. Une commande en ligne (OpenSSL) permettant :

– la création de clés RSA, DSA (signature)

– la création de certificats X509

– le calcul d'empreintes (MD5, SHA, RIPEMD160, ...)

– le chiffrement et déchiffrement (RSA, DES, IDEA, RC2, RC4, Blowfish, ...)

– la réalisation de tests de clients et serveurs SSL/TLS

– la signature et le chiffrement de courriers (S/MIME)

EXERCICE

1. Générez-vous votre clé privée avec une longueur de 1024 bits.

2. Dériver la clé publique associée à la clé privée.

3. Générer une clé de 256 bits comme une clé de cryptage symétrique pour une utilisation ultérieure.

4. Créer un fichier cigale.txt contenant un message secret.

5. Chiffrer le fichier cigale.txt avec l'algorithme AES 256 bits.

6. Chiffrer la clé de la session (étape 3) avec l'algorithme RSA, en utilisant la clé publique de votre binôme.

7. Générer un digest (hashage) pour le fichier cigale.txt avec md5 et sha1.

8. A quoi sert le digest en général ?

9. Envoyer la clé chiffrer à votre binôme (via : FTP, Telnet, scp, email, clé usb, etc.).

10. Envoyer le fichier chiffré à votre binôme, ainsi que sa signature.

11. Traiter les fichiers reçus par votre binôme (déchiffrer la clé et le fichier), après la vérification de la signature. Extraire le message original.