TP : OpenSSL

Utilisez le matériel donné pour les routines OpenSSL.

Exercices:

1. Générez des clés RSA de 1024 bits dans un fichier: Cles.pem
2. Utilisez la commande *cat* ou la commande *less* pour lire le fichier au format .pem. Est-ce que le contenu du fichier est chiffré ou pas ?
3. Utilisez la commande *openssl rsa* pour visualiser le contenu du fichier Cles.pem (comme dans la section 2.2). Quelle est la longueur (en bits) des deux facteurs premiers du module ?
4. Utilisez l'internet pour répondre à l'exercice 1 du matériel donné. Pourquoi est-ce qu'on veut que l'exposant public soit petit ?
5. Chiffrez le fichier Cles.pem avec l'algorithme des3. Pourquoi est-ce que le fichier en entrée est le même que le fichier en sortie ?
6. Faites les exercices 2 et 3.
7. Comparez maintenant les deux fichiers (Cles.pem et le fichier où vous avez exporté la clé publique) avec une adresse e-mail et son mot de passe. Si vous voulez que quelqu'un puisse vous envoyé des messages chiffrés, quel de ce deux fichiers est-ce que vous devez faire public ?
8. Créez un fichier text avec un contenu de votre choix, avec le nom Plaintext.txt. Chiffrez le fichier avec votre clé publique, en utilisant la commande *rsautl*. Nommez le fichier en sortie Ciphertext.txt. Puis déchiffrez-le et vérifiez le résultat.
9. Tapez la commande *openssl enc*. Vous trouverez une liste de mécanismes de chiffrement symétrique. La commande pour chiffrer un fichier avec un protocole de chiffrement symétrique de votre choix est : *openssl enc -<méthode> -in <fichier entrée> -out <fichier sortie> -pass:<MotDePasse>*.
   Maintenant chiffrez le texte Plaintext.txt avec une méthode de chiffrement de votre choix et avec un mot de passe de votre choix. Nommez le fichier en sortie Symctext.txt. Répétez le processus avec une autre méthode de chiffrement avec le fichier en sortie Symctext2.tex (avec un autre mot de passe).
10. Maintenant déchiffrez les deux chiffrés obtenus. Pour déchiffrer un fichier chiffré avec une clé symétrique la commande est :
    openssl *enc -<méthode> -in <fichier entrée> -out <fichier sortie> -pass:<MotDePasse> -d.*
    Essayez de déchiffrer les chiffres avec la fausse clé (utilisez pour le déchiffrement de Symctext.txt la clé utilisée pour Symctext2.txt et l'inverse). Quelle est votre conclusion ?
11. (À faire en paires) Envoyez le fichier avec votre clé publique à votre partenaire et recevez sa clé publique. Puis, chiffrez, avec la clé RSA de votre partenaire, la clé symétrique que vous avez utilisée pour le chiffrement symétrique, dans un fichier : Password.txt. Envoyez les fichiers Symctext.txt et Password.tex à votre partenaire et recevez ses fichiers. Déchiffrez-les et vérifiez le résultat.

12. Calculez une empreinte du fichier Plaintext.txt comme enseigné dans le paragraphe 2.6, avec l'algorithme SHA1. Quelle longueur a votre empreinte ? Essayez maintenant avec un autre fichier, plus long. Quels sont vos résultats en utilisant l'algorithme sha256 ?
13. Pour voir l'empreinte en *–hex* il faut ajouter cette option-ci avant le nom du fichier de sortie. Essayez ceci avec un de vos empreintes.
14. Faites l'exercice 6.
15. Répétez l'exercice 9, mais signez les fichiers que vous avez envoyés aussi. Vérifiez la signature de votre partenaire.