M2-DNR2I TP3-2:
Cryptographie asymétrique

Gaétan Richard

24 octobre 2011

L'objectif de ce TP est la manipulation de clés RSA. Vous devrez être capable de générer une bi-clé RSA (une paire de clés publique, privée) l'aide de openssl, et de l'utiliser pour signer et chiffrer des données.

1 Génération d'une bi-clé RSA

La commande genrsa de openssl permet de générer une bi-clé RSA :
`$ openssl genrsa -out < fichier> <taille>` Les fichiers produits lors de la création des clés sont au format PEM (Privacy-Enhanced Message).

Question 1 *Générez une bi-clé RSA de 1024 bits et stockez la dans un fichier (extension .pem).*

2 Visualisation des clés RSA

La commande rsa permet de visualiser le contenu d'un fichier au format PEM contenant une bi-clé RSA :
`$ openssl rsa -in < fichier> -text -noout` L'option -text demande l'affichage décodé de la bi-clé. L'option -noout supprime la sortie normalement produite par la commande rsa. L'option -pubout permet d'obtenir en sortie une clé publique (distribuable à tous) au lieu de la clé privée obtenue par défaut.

Question 2 *Lisez les informations contenues dans le fichier* `.pem` *avec un éditeur de texte quelconque (par exemple la commande cat sous Linux), puis avec la commande rsa de openssl. Quel est l'apport de la commande rsa ?*

Question 3 *Que vaut votre exposant de chiffrement ? comparez avec ceux de vos voisins. Expliquez.*

Question 4 *Utilisez l'option -pubout pour exporter la partie publique de votre clé et stockez là dans un fichier* `.pub.pem`.

3 Chiffrement d'un fichier de clés RSA

Il n'est pas très prudent de laisser une bi-clé en clair (surtout la partie privée). Il existe deux méthodes pour chiffrer une bi-clé (en utilisant un des algorithmes de chiffrement -des, -des3 ou -idea) :

- Soit lors de la création de la bi-clé :
  `$ openssl genrsa -des3 -out ficher.pem 1024`
- Soit en chiffrant après coup une bi-clé existante avec la commande rsa :
  `$ openssl rsa -in ficher.pem -des3 -out ficher.pem`

Question 5 *Protégez votre clé privée RSA à l'aide d'une clé symétrique ; Visualisez le contenu du fichier* `.pem` *à l'aide d'un éditeur de texte, puis avec la commande rsa ; Quelle différence voyez-vous ?*

4 Chiffrement, déchiffrement avec RSA

La commande rsautl permet de chiffrer et déchiffrer des données.
`$ openssl rsautl -encrypt -in <fichier entree> -inkey <cle> -out <fichier sortie>`

- *fichier entree* est le fichier des données à chiffrer.
- *cle* est le fichier contenant la clé RSA. Si ce fichier ne contient que la clé publique, il faut ajouter l'option -pubin.
- *fichier sortie* est le fichier des données chiffrées.

Pour déchiffrer, on remplace l'option `-encrypt` par `-decrypt`.

Question 6 *Chiffrez le sujet du TP avec votre clé RSA. Que se passe-t-il ? Expliquez. Que devez-vous faire ?*

Le but de cet question est d'échanger des fichiers chiffrés par un moyen de communication "non sûr".

Question 7

- *Répartissez-vous par groupes de deux ou trois et échangez vos clés publiques RSA ; Attention : une fois que vous aurez publié votre clé publique, si vous devez en changer vous devrez avertir tous les autres utilisateurs.*
- *Choisissez un fichier de votre choix et envoyez-le chiffré aux membres de votre groupe. Détaillez les étapes.*
- *Déchiffrez les messages que vous avez reçu.*

5 Signature avec RSA

Pour signer, on utilise l'option `-sign` de la commande rsautl :
`$ openssl rsautl -sign -in <fichier a signer > -inkey <cle > -out <signature >`
et pour vérifier la signature :
`$ openssl rsautl -verify -in <signature > -pubin -inkey <cle > -out <fichier signe>`

Question 8 *Signez un (petit) fichier de votre choix, et faites vérifier votre signature à un autre membre de votre groupe ; quelles clés utilisez-vous ?*

6 Empreinte d'un document

Il est possible de calculer une empreinte d'un document avec la commande dgst :

`$ openssl dgst <hachage > -out <empreinte > <fichier entree >` où hachage est une fonction de hachage, comme MD5 (option -md5) qui calcule des empreintes de 128 bits, ou SHA1 (-sha1) et RIPEMD160 (option -ripemd160) qui calculent toutes deux des empreintes de 160 bits.

Question 9 *Signez le sujet de TP.*