TD8 – Sécurité et protocoles cryptographiques (2ème partie)

{Emmanuel.Godard, Yann.Esposito}@lif.univ-mrs.fr

1 décembre 2005

☞ Le but de ce TD va être de se familiarisé avec les crypto-systèmes et en particulier les cryptosystèmes à clef publique comme PGP et son équivalent Gnu, GPG.
Ce TD s'inspire grandement du How To de GPG.

1 Cryptosystèmes à clef publique 1

1.1. Sans systèmes à clef publique, quels sont les deux préalable nécessaire à l'établissement d'une connexion sécurisée utilisant des clef symétriques ?

1.2. Quels sont les trois missions d'un cryptosystème ?

(a) Quelles sont les utilisations pour lesquelles un tel cryptosystème est particulièrement adapté (donnez au moins trois exemples) ?

1.3. Donnez le schéma d'encryption d'un cryptosystème à clef publique.

1.4. Quel est le rôle d'une signature numérique ?

(a) Comment signer numériquement un document ? Donnez un exemple schématique.

1.5. Dans le cryptosystème décrit jusqu'ici ; quel est le maillon de la chaîne qui semble le plus faible.

(a) Expliquez comment un intrus peu lire les messages d'une personne utilisant un cryptosystème en ayant très peu de chance d'être détecté.

(b) Comment éviter ce problème ?

1.6. Expliquez à quoi peut servir certificat de révocation.

1.7. Est-il possible de lire mes messages chiffrés sans mon accord lorsque j'utilise un cryptosystème ?

1.8. Les client de mail récent intègrent des cryptosystèmes. Vous remarquerez que beaucoup de certificats sont déjà intégrés à l'intérieur de ceux-ci. Pourquoi ? Peut-on leur faire une confiance absolue ?

1.9. Lorsque vous surfez sur internet, il vous est parfois dit que le certificat est introuvable. Le site que vous allez visiter est-il celui d'une personne malhonnête ?

❦