CRYPTOGRAPHIE
TD N°3

Objectif du TD: Avoir quelques notions sur la sécurité en cryptographie
Ce TD rassemble des questions qui pourraient figurer dans un énoncé d'examen.

ENONCE :

Exercice 1 :
On appelle attaque a clair connu une attaque dans laquelle l'attaquant connait le texte en clair ET le texte codé. Son objectif est alors de trouver la clef.

- Si l'algorithme de chiffrement est un XOR entre le message et la clef et le mode opératoire est de l'ECB, une attaque a clair connu est elle faisable ? (et comment obtenez vous la clef ?)
- Si l'algorithme de chiffrement est un XOR et le mode opératoire est le CBC, une attaque à clair connu est elle faisable ? (et comment obtenez vous la clef ?) Que pouvez vous conclure ?
- Quelle propriété du XOR le rend inutile face à des attaques a clair connu ?
- Utiliseriez vous un XOR pour sécuriser des échanges réseaux (http, ftp....) ? Justifiez.

Exercice 2 :
On appelle clef de session une clef déterminée lors d'échanges groupés dans le temps. La distribution de ces clefs de session se fait à l'aide de méthodes cryptographiques classiques (chiffrement symétrique ou asymétrique).

Quel est l'intérêt d'utiliser une clef de session plutôt que les clefs de chaque intervenant ?
Distinguer le cas de la cryptographie symétrique et de la cryptographie asymétrique.

Exercice 3 :
Quel est le contenu d'un certificat X509 ? A quoi cela sert il ?
Donner deux exemples d'applications simples.

Exercice 4 :
Imaginez un protocole permettant de sécuriser un serveur ftp (Bob est le serveur). L'objectif est surtout d'éviter que Eve ou Mallory puisse récupérer le mot de passe d'Alice. Vous pouvez utiliser au plus 1 certificat X509.

Exercice 5 :
Imaginez un protocole permettant de faire un tirage a pile ou face entre deux joueurs par mail sans qu'aucun des deux joueurs ne puisse tricher.