CRYPTOGRAPHIE
TD N°1

Objectif du TD: Se familiariser avec les protocoles

ENONCE :

Exercice 1 :
L'objectif est un protocole de confidentialité/intégrité sur une base de cryptographie hybride très simple :
Protocole Version 1 :

1. Alice choisit une clef secrète Ks , la chiffre avec la clef publique de Bob.
2. Bob déchiffre Ks avec sa clef privée.
3. Ils communiquent en chiffrant avec la clefs Ks.

Questions :
- Que vaut notre protocole ?

Protocole Version 2 :
Alice et Bob connaissent leurs clefs publiques respectives.

4. Alice choisit une clef secrète Ks , la chiffre avec la clef publique de Bob, signe le tout avec sa clef privée (elle signe un digest) et envoie.
5. Bob vérifie l'origine et déchiffre avec sa clef privée.
6. Ils communiquent en chiffrant avec la clefs Ks.

Questions :
- Que vaut notre protocole ?
- Imaginons que Mallory ait stocké tous les messages échangés et cassé en force brute une vieille clef Ks.
  - Que peut il faire ?
  - Comment y remédier ?

Exercice 2 :
Voici un protocole d'authentification (nommé SKEY) : Il se base sur l'existence d'une fonction a sens unique sans trappe.
Initialisation :

1. Initialiser, Alice entre un nombre aléatoire r.
2. Bob calcule n nombres x(i) = fofofof....of(r) (i fois) et donne cette liste a Alice
3. Dans un fichier, Bob conserve le couple Alice/x(n+1) et jette la liste

Fonctionnement à la ieme authentification :

1. Alice fournit s= x(n-i+1).
2. Bob calcule f(s) et le compare à son contenu dans la base.
3. En cas de non-match, il stoppe.
4. En cas de match, il authentifie, place s dans son fichier associé a Alice. Alice supprime cette clef de sa liste.

Questions :
On supposera la partie initialisation effectuée de façon sûre .

- Pour une authentification de personne en local sur une machine, que pensez vous de la méthode décrite ci dessus ? En particulier, qu'apporte-t-elle par rapport au simple password ?

- Mêmes questions pour une authentification de personne sur le réseau.

- Qu'en pensez vous d'un point de vue pratique ?

Exercice 3

Il n'existe en fait qu'une seule technique véritablement sure de chiffrement. Cette méthode est appelée Tampon unique ou « one time pad ». Elle suit la méthode suivante : Pour un message M de n bits, générer un message aléatoire R de n bits égalements.
R est la clef (symétrique) permettant de chiffrer.
Le chiffrement se fait de la manière suivante : C = M . XOR . R
Le déchiffrement se fait de la manière suivante : E = C. XOR . R

Ce qui rend cette méthode résistante a toute attaque est le fait que chaque clef ne sert qu'une seule fois (il paraît que les communications par le téléphone rouge entre le Kremlin et la Maison blanche étaient cryptées ainsi...)

- Montrer qu'aucune attaque par cryptanalyse ne peut fonctionner...

Exercice 4

Secret Splitting :
Vous voulez partager un secret (une carte au trésor) avec votre meilleur ami...la règle est simple : il faudra que les deux soient présents pour pouvoir reconstituer la carte.
Questions :

- Comment utiliser le principe du One Time Pad pour cela ?
- Qu'est ce que cela apporte par rapport a découper la carte en deux ?
- Pouvez vous généraliser ceci a N participants ?