République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Béjaia
Faculté des Sciences Exactes

Département d'Informatique
Module : Sécurité 1
Niveau : Master1

Série de TD N°4

Exercice1

Soit une fonction de chiffrement symétrique E_k : $\{0,1\}^n$--->$\{0,1\}^n$, k∈$\{0,1\}^n$
Comment peut-on utiliser la fonction E_k pour définir des fonctions de hachage ?

A partir de e_k, une fonction de chiffrement à clé secrète,

$$e_k : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$$

on peut construire g une *fonction de compression*, identique à la fonction de chiffrement, dont la taille de l'image par est n :

$$g : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \qquad \text{pour } n \in \mathbb{N}$$

La fonction de chiffrement e_k est utilisée soit directement, si elle est résistante aux collisions, soit en la «perturbant» un peu en utilisant par exemple une des perturbations ci-dessous :

$$g(k,x) = e_k(x) \oplus x$$
$$g(k,x) = e_k(x) \oplus x \oplus k$$
$$g(k,x) = e_k(x \oplus k) \oplus x$$
$$g(k,x) = e_k(x \oplus k) \oplus x \oplus k$$

Exercice2

Soit le protocole de chiffrement suivant : **E_{k1}(x||H(x||k2))=y**, tel que :
y le résultat de chiffrement du message clair **x** en utilisant la fonction de chiffrement **E()** avec une clé **k1** ;
H() : une fonction de hachage ;
|| : indique une concaténation ;
K1,**k2** : sont les clés symétriques du chiffrement.

1. Décrire les étapes que doit suivre le destinataire pour déchiffrer le message **y**.
2. Indiquer si le protocole permet de garantir les quatre services de sécurité suivants : *Authentification, Confidentialité, intégrité et non-répudiation.*

Sol

Soit D() la fonction de déchiffrement correspondant à E() ;
Le destinataire commence par $D_{k1}(y)$ il obtient x||H(x||k2). Il prend le x pour lui appliquer la fonction H() comme suite H(x||k2) et il le compare avec le H(x||k2) reçu. Si les hachés sont égaux donc x est le bon message.
Authentification non (pas de signature); confidentialité oui (cryptage) ; intégrité oui (hachage), non-répudiation non(pas de signature).

Exercice3

Un cryptosystème a beau se baser sur des principes mathématiques très forts, il suffit que le cryptosystème soit mal utilisé pour que la sécurité escomptée soit mise à mal. C'est ce que nous allons voir sur la signature RSA.

Cette attaque se place dans le cadre de la signature de documents avec RSA. Pour signer un document **1 < m < n**, Alice associe à m la signature $\mathbf{m_s = m^d \bmod n}$ (**d** est l'exposant de déchiffrement qui fait parti de sa clé privée RSA) et ses interlocuteurs peuvent vérifier l'authenticité de m en vérifiant que $\mathbf{m = m_s^e \bmod n}$ (la paire de clés publiques RSA d'Alice étant (e; n)).
1. Soit **c** un message chiffré $\mathbf{c=m^e \bmod n}$ par Alice. L'attaquant Boualem obtient **c** et veut pouvoir retrouver le message de départ **m**.
Montrer que si Boualem sait qu'Alice utilise les mêmes clés **(e; n)**; **(d; n)** pour signer ses messages et qu'il est capable de la persuader de lui envoyer un message personnel **r** qu'elle aura signé (avec les clés **(d; n)**) alors il pourra retrouver le message de départ **m**.
2. Qu'en déduisez vous sur l'utilisation de RSA ?
Sol

Boualem prend un r telle que r=c * s^e avec s est un éliment connu choisi par Boualem

Alice signe r par $r^d \Rightarrow r^d = (c * s^e)^d$ on a $c = m_s^e \Rightarrow r^d = (m_s^e * s^e)^d \Rightarrow r^d = (m_s * s)^{ed}$

on $a\,ed = 1\,mod\,[?][?](n)\ on\ aussi\ a^{k*[?][?](n)+1}$ ***mod n=a*** (la démonstration se fait par le théorème de Fermat)

alors $(m_s * s)^{ed} = m_s * s$

on $r^d = m_s * s \Rightarrow m_s = \frac{rd}{s}$

Exercice4

Montrer que : dans un système RSA, disposant de deux signatures(produites avec la même clé privée) de deux messages différents, on peut facilement produire une autre signature valide, **sans posséder la clé privée**.

Solution :soit s_1 (respectivement s_2) la signature du message m_1 (respectivement m_2) avec la clé privée **(d,n)** soit maintenant s la signature du message $m = m_1.m_2$.

On a $s_1.s_2 = (m_1^d \bmod n).(m_2^d \bmod n) = (m_1.m_2)^d \bmod n = s$ .Ceci prouve que le produit des signatures des deux messages (réalisés avec la même clé privée) est égale à la signature du produit des deux messages, ce qui permet de créer des signatures valides sans posséder la clé privée

Exercice 5

Discuter les trois scénarios suivants en terme de sécurité :

1-Deux certificats différents sont signés par la même clé privée.

2- Deux certificats différents contiennent la même clé publique.

3- Deux certificats différents ont la même signature.

Solution

1. Deux certificats différents qui sont signés par la même clef privée.

Le fait que deux certificats soient signés par la même clef ne pose aucun problème. C'est tout simplement le cas quand une autorité de certification signe des certificats suivant la norme X.509 ou lorsque qu'une personne signe des certificats PGP de plusieurs autres personnes.

2. Deux certificats différents qui contiennent la même clef publique.

C'est ici une situation très problématique puisque deux personnes différentes possèdent des clefs publique identiques : d'une part chacune d'entre elles peut lire les messages chiffrés destinés a l'autre personne ; d'autre part il sera impossible de différencier les signatures des deux personnes.

3. Deux certificats différents qui ont la même signature.

Si deux certificats différents ont la même signature, cela signifie que la fonction de hachage utilisée pour la signature a crée une collision. La signature de l'un des deux certificats peut avoir été faite par un pirate qui a constaté une collision sur la fonction de hachage.