Master 1ère année
Initiation à la Cryptographie

Travaux Dirigés

Hachage, Signature et Authentification

Exercice 1 : (Signature RSA)
Bob a construit un cryptosystème RSA dont les données privées sont $p = 23$; $q = 43$ et $d = 683$.

1. Déterminer les données publiques.
2. Quelle opération doit faire Bob pour signer (sans fonction de hachage) un message m? Calculer la signature RSA de Bob pour $m = 123$.
3. La connaissance de p et q accélère le calcul de signature. Signer le même message avec RSA-CRT.
4. Que doit faire une personne qui souhaite vérifier que le message s est bien la signature de Bob?

Exercice 2 : Montrer que le chiffrement RSA ne résiste pas aux attaques à texte chiffré choisi.
En particulier étant donné un texte chiffré y, montrer comment choisir un texte chiffré $\tilde{y} \neq y$ tel que la connaissance du texte clair $\tilde{x} = d_k(\tilde{y})$ permette de calculer $x = d_k(y)$.
(Indication : utiliser le fait que $e_k(x_1)e_k(x_2) \bmod N = e_k(x_1x_2 \bmod N)$).

Exercice 3 : (Signature aveugle)
On s'intéresse à un cas particulier de signature appelé « signature aveugle ». On souhaite pouvoir effectuer une signature sans que le signataire sache ce qu'il signe.

Un exemple d'application est le vote électronique : on peut imaginer qu'un bulletin, pour être valide, doive être validé (signé) par une autorité sans que celle-ci connaisse le contenu du vote.

Trouver un algorithme à partir de la signature R.S.A qui permet de faire un algorithme de signature aveugle. On a un message m qu'on souhaite faire signer sans que le signataire sache ce qu'il signe, et un couple de clés publique/privée.
(Indice : multiplier le message par une valeur adéquate.)

Exercice 4 : (Fonction de hachage)
Soit $h : X \to Y$ une fonction qui possède les deux propriétés suivantes : d'une part $h(x)$ se calcule facilement et d'autre part, pour tout x, le nombre $h(x)$ est de taille fixée. On rappelle les définitions des propriétés suivantes :

(i) (Preimage) La fonction h est dite à sens unique si, pour presque tout y de Y, il est calculatoirement infaisable de trouver x tel que $y = h(x)$.

(ii) (Second Preimage) La fonction h est dite faiblement sans collision si, pour x donné, il est calculatoirement infaisable de trouver $x_0 \neq x$ tel que $h(x_0) = h(x)$.

(iii) (Collision) La fonction h est dite sans collision s'il est calculatoirement infaisable de trouver x et x_0 ($x \neq x_0$) tels que $h(x) = h(x_0)$.

1. Montrer que « sans collision » implique « faiblement sans collision »

2. Montrer que « à sens unique » implique « faiblement sans collision ».

3. Montrer qu'une fonction peut être « sans collision » mais pas « à sens unique ».

Exercice 5 : On suppose que $f : \{0,1\}^m \to \{0,1\}^m$ est une bijection à sens unique (c'est-à-dire Résistante à la préimage). Définissons la fonction $h : \{0,1\}^{2m} \to \{0,1\}^m$ par

$$h(x) = f(x' \oplus x''),$$

où $x \in \{0,1\}^{2m}$ est découpé en deux morceaux de même taille : $x = x'||x''$ avec $x', x'' \in \{0,1\}^m$.

Montrer que h n'est pas faiblement sans collision (c'est-à-dire n'est pas résistante à la seconde préimage)

Exercice 6 : On suppose que $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ est une fonction de hachage sans collision.

a) Soit $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ définie par

   (a) Ecrivons $x \in \{0,1\}^{4m}$ sous la forme $x = x_1||x_2$ avec $x_1, x_2 \in \{0,1\}^{2m}$.
   (b) On pose $h_2(x) = h_1(h_1(x_1)||h_1(x_2))$.

   Prouver que h_2 est sans collision.

b) Pour un entier $i \geq 2$, définissons la fonction de hachage $h_i : \{0,1\}^{2^i m} \to \{0,1\}^m$ récursivement à partir de h_{i-1} par

   (a) Ecrivons $x \in \{0,1\}^{2^i m}$ sous la forme $x = x_1||x_2$ avec $x_1, x_2 \in \{0,1\}^{2^{i-1} m}$.
   (b) On pose $h_i(x) = h_1(h_{i-1}(x_1)||h_{i-1}(x_2))$.

   Montrer que h_i est sans collision.

Exercice 7 : (Authentification de messages (MAC) par blocs)
Soit un message $m = m_1||m_2||\cdots||m_n$ à authentifier avec une clé k. Soit E_k une fonction de chiffrement sûre. Pour authentifier le message m, on calcule le MAC suivant :

$$MAC_k(m) = E_k(m_1) \oplus E_k(m_2) \oplus \cdots \oplus E_k(m_n).$$

1. Expliquer pourquoi ce calcul ne garantit pas l'intégrité du message dès qu'il y a au moins deux blocs.

2. Montrer pourquoi il est simple pour l'attaquant de faire authentifier un message de la forme $m||m$.

3. Que se passe-t-il lorsque deux blocs du message sont échangés?

4. Montrer comment l'attaquant peut authentifier n'importe quel message en ayant accès aux réponses de deux calculs bien choisis.

Afin de contrer les attaques basiques telles que la suppression ou l'échange de blocs, on considère la nouvelle version :

$$MAC_k(m) = E_k(1||m_1) \oplus E_k(2||m_2) \oplus \cdots \oplus E_k(n||m_n).$$

5. Montrer qu'un attaquant peut encore authentifier n'importe quel message mais cette fois à l'aide de la réponse à trois questions.

6. Regarder rapidement si les modifications de blocs des premières questions sont encore valables en utilisant le mode de chaînage CBC.