Master 2ème année – SeCReTS

Examen "Cryptologie industrielle"

22 novembre 2016

Consignes :

- Durée : 2h.
- Documents interdits. Aucun accès à un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non.

Exercice 1. *Fonctions de hachage*

1. Rappeler la définition d'une fonction à sens unique, d'une fonction à collisions faibles difficiles et d'une fonction à collisions fortes difficiles.

2. Soit une fonction de hachage h donnant en sortie une chaîne de n bits. On considère k messages choisis aléatoirement, notés x_1, x_2, ..., x_k, et on note $y_1 = h(x_1)$, $y_2 = h(x_2)$, ..., $y_k = h(x_k)$. Retrouver, en fonction de n et k, la probabilité P que ces k messages donnent une collision sur la sortie de n bits.

3. Une méthode classique pour construire une fonction de hachage $h : \{0,1\}^* \longrightarrow \{0,1\}^n$ consiste à itérer une *fonction de compression* $f : \{0,1\}^\ell \longrightarrow \{0,1\}^n$, avec $\ell > n$. L'idée est de décomposer le message m en blocs $m_1, m_2, \ldots, m_k$ de longueur $\ell - n$, puis de poser $y_0 =$IV pour une valeur IV$\in \{0,1\}^n$, puis

$$y_i = f(y_{i-1}||m_i) \qquad (1 \leq i \leq k)$$

On pose alors $h(m) = y_k$. Pour que la longueur de m soit divisible par $\ell - n$, on utilise un schéma de "padding" standard.

Soit $g : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ un algorithme de chiffrement par blocs, avec une clé de longueur n bits, et une taille de bloc de n bits (la clé est le premier paramètre, le bloc est le second paramètre). On définit alors une fonction de compression $f : \{0,1\}^{2n} \longrightarrow \{0,1\}^n$ par :

$$f(\check{y}||m) = g(y,m)$$

Montrer comment on peut trouver une collision pour la fonction h.

Exercice 2. *Courbes elliptiques*

On considère la courbe elliptique définie par $y^2 = x^3 + 4x + 3$ sur $\mathbb{F}_7$.

1. Vérifiez que les coefficients de cette équation satisfont la condition qui permet d'affirmer que la courbe elliptique décrit un groupe.

2. Donnez des bornes sur le nombre de points de la courbe.

3. Déterminez tous les éléments de $\mathbb{F}_7$ qui sont des carrés. Déduisez-en tous les points de la courbe. Quel est l'ordre du groupe défini par la courbe elliptique?

4. Si $P = (1, -1)$, calculez $2P$, $3P$, $4P$, $5P$, $6P$, $7P$, $8P$, $9P$ et $10P$.

5. Rappeler l'algorithme "Double and Add", et expliquez pourquoi il donne bien le bon rsultat.

6. Avec l'algorithme "Double and Add", calculez $5P$.

Exercice 3. *Protocole d'authentification*

Dans un protocole d'identification, un vérificateur V veut vérifier l'identité d'un prouveur P. Pour cela P doit convaincre V qu'il est en possession d'un certain secret s. Les deux objectifs essentiels d'un tel protocole sont d'une part qu'un usurpateur U ne connaissant pas s ne puisse pas convaincre V, et d'autre part que P puisse convaincre V qu'il possède s sans lui révéler la valeur de s (sinon V pourrait devenir à son tour un usurpateur de l'identité de P).

Nous décrivons maintenant le protocole d'identification de Schnorr :

p et q sont des nombres premiers tels que q divise $p-1$ et α est un élément d'ordre q du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$. Un nombre $s \bmod q$ est le secret de P, tandis que les valeurs de p, q, α, et $v := \alpha^{-s} \bmod p$ sont publiques. Le protocole d'identification se déroule en quatre étapes :

1. Engagement : P choisit aléatoirement un entier $r \bmod q$ et transmet $x = \alpha^r \bmod p$ à V.
2. Challenge : V envoie un challenge $e \in [0, q-1[$ à P.
3. Réponse : P envoie $y = r + es \bmod q$ à V.
4. Vérification : V vérifie que $x = \alpha^y v^e \bmod p$.

P a réussi son identification auprès de V si la vérification est positive.

1. Montrer que P réussit toujours son identification auprès de V.
2. Comment doit-on choisir les nombres premiers p et q pour que personne d'autre que P ne puisse calculer s en un temps raisonnable ?
3. U tente de s'identifier auprès de V. Pour cela il répond un y aléatoire à l'étape 3. Quelles sont ses chances de succès ?
4. Supposons que le protocole précédent soit mal exécuté, et que l'ordre des étapes 1 et 2 soit inversé. Montrer que U peut alors réussir son identification auprès de V.
5. Montrer que, si pour un engagement r, U est capable de répondre correctement à deux questions e et e' distinctes posées par V, alors il connaît s.