Master 2ème année – SeCReTS

Examen "Cryptographie : compléments et applications

1er décembre 2020

Durée : 2h – Documents interdits, sauf une feuille A4 recto écrite de votre main. Aucun accès à un téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, connectable ou non.

Exercice 1. *Fonction de hachage*

Soit $f : \{0,1\}^{2m} \longrightarrow \{0,1\}^m$ une fonction de hachage. Soit maintenant une deuxième fonction de hachage définie par

$$h : \begin{array}{ccc} \{0,1\}^{4m} & \longrightarrow & \{0,1\}^m \\ x_1||x_2 & \mapsto & f(f(x_1)||f(x_2)) \end{array}$$

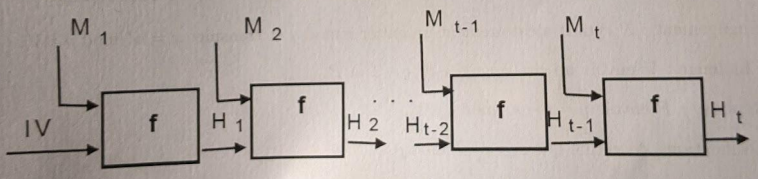
où $||$ désigne l'opération de concaténation. Montrer que si f est à collisions fortes difficiles, alors h est aussi à collisions fortes difficiles.

Exercice 2. *MAC*

Dans cet exercice, on considère plusieurs constructions de MAC à partir d'une fonction de hachage. Soit $h : \{0,1\}^* \to \{0,1\}^n$ une fonction de hachage obtenue en appliquant la construction de Merkle-Damgård à une fonction de compression f à collisions fortes difficiles. Rappel : le principe est de découper le message M en blocs de même taille

$$M = M_1||M_2||\ldots||M_{t-1}||M_t$$

(chaque M_i fait typiquement 512 bits) et de calculer $H_i = f(H_{i-1}||M_i)$ successivement pour $i = 1, 2, \ldots, t$ (avec H_0 =IV). Le haché de M est alors, par définition, $h(M) = H_t$.



1. Montrer que le MAC défini par

$$\mathrm{MAC}_K(M) = h(K||M)$$

n'est pas sûr. En particulier, on montrera qu'étant donné un couple (M, T) où T est un MAC valide de M, un attaquant peut construire un couple (M', T'), où $M' \neq M$ et T' est un MAC valide de M'. On pourra supposer, pour simplifier, que la clé K a la même taille que les blocs M_i du message.

2. On considère maintenant le MAC défini par

$$\mathrm{MAC}_K(M) = h(M||K)$$

Montrer qu'il existe une attaque à messages choisis, de complexité approximativement $\mathcal{O}(2^{n/2})$, permettant une forge existentielle (c'est-à-dire d'obtenir un MAC valide pour un certain message).

9 mars 2021

Durée : 1h – Documents interdits, sauf une feuille A4 recto écrite de votre main. Au téléphone portable, une calculatrice, un PDA ou tout autre dispositif électronique, non.

Exercice 3. *Courbe elliptique et cryptosystème de Menezes-Vanstone*

Le cryptosystème de Menezes-Vanstone est un algorithme de chiffrement défini de la manière suivante. On suppose que sont connus de tout le monde : une courbe elliptique E sur un corps $\mathbb{F}_p$, et un générateur P de la courbe E. Alice possède une clé secrète s qui est un nombre entier, et publie sa clé publique $PK_A = s.P$. Les messages M sont les couples $(M_1, M_2) \in \mathbb{F}_p \times \mathbb{F}_p$. Lorsque Bob veut transmettre un tel message à Alice, il génère un entier aléatoire k, calcule $k.PK_A = (x, y) \in E$, puis envoie à Alice le chiffré, qui est le triplet $(k.P, M_1.x, M_2.y)$.

1. Soit E la courbe définie sur $\mathbb{F}_{11}$ par l'équation
$$y^2 = x^3 + x + 6.$$
Montrer que E est une courbe elliptique sur $\mathbb{F}_{11}$.
2. Déterminer l'ordre du groupe, et trouver tous les points de la courbe elliptique.
3. Montrer que le point $P = (2, 7)$ est un générateur de E.
4. Bob souhaite envoyer le message $M = (9, 1) \in \mathbb{F}_{11} \times \mathbb{F}_{11}$ à Alice (M n'est pas un point de E) en utilisant le cryptosystème de Menezes-Vanstone associé au couple public (E, P). La clé secrète d'Alice est l'entier $s = 7$. Calculer la clé publique d'Alice.
5. Bob choisit aléatoirement l'entier $k = 6$. Quel est le message chiffré envoyé par Bob à Alice et comment Alice retrouve-t-elle le message M ?

Exercice 4. *Protocole de Schnorr*

Dans un protocole d'authentification, 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'authentification 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 mod 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'authentification se déroule en quatre étapes :

1. Engagement : P choisit aléatoirement un entier r mod 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 authentification auprès de V si la vérification est positive.

1. Montrer que P réussit toujours son authentification 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'authentifier 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 authentification 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.