Master 2ème année – SeCReTS

Examen "Cryptologie industrielle"

24 novembre 2015

Consignes :

- Durée : 3h.
- 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. Que dit le paradoxe des anniversaires ? (donner une réponse la plus précise possible, avec si possible une formule)

3. Soit $h : \{0,1\}^* \longrightarrow \{0,1\}^n$ une fonction de hachage (qui est en particulier à collisions faibles difficiles, et à collisions fortes difficiles). Soit $h' : \{0,1\}^* \longrightarrow \{0,1\}^{n+1}$ définie par :

$$h'(x) = \begin{cases} 0||x & \text{si } x \in \{0,1\}^n \\ 1||h(x) & \text{sinon} \end{cases}$$

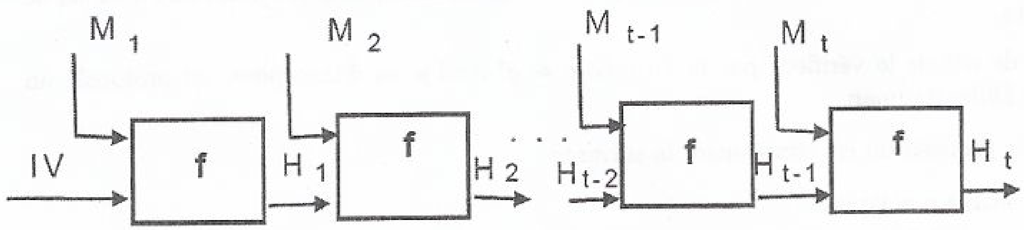
Montrer que h' n'est pas à sens unique, mais est encore à collisions faibles difficiles et à collisions fortes difficiles

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

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

(chaque M_i fait typiquement 512 bits) et de calculer $H_i = f(H_{i-1}||M_i)$ successivement pour $i = 1, 2, \dots, t$ (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).

Exercice 3. *Courbes elliptiques*

1. Pour une courbe elliptique E définie par une équation de la forme $y^2 = x^3 + ax + b$ sur le corps $\mathbb{F}_p$ (avec $p > 3$), retrouver les formules d'addition sur E, à partir de la définition géométrique de l'addition. Pour $R = P + Q$, on donnera les coordonnées de $R = (x_R, y_R)$ en fonction des coordonnées de $P = (x_P, y_P)$ et de $Q = (x_Q, y_Q)$ en précisant les conditions dans lesquels la formule est valable.
2. Vérifier que $E : y^2 = x^3 + x + 3$ définit bien une courbe elliptique sur $\mathbb{F}_7$.
3. Donner (sous la forme d'un tableau) l'ensemble des points $(x, y) \in \mathbb{F}_7 \times \mathbb{F}_7$ de cette courbe. Montrer que le cardinal du groupe G issu de cette courbe est de 6.
4. Montrer que le point $(4, 1)$ est d'ordre 6 dans G. Exhiber un point d'ordre 2 dans G
5. Terminer de remplir le tableau suivant représentant la table d'addition de G.

$+$	$\mathcal{O}$	$(4,1)$				
$\mathcal{O}$	$\mathcal{O}$	$(4,1)$	$(6,6)$			
$(4,1)$	$(4,1)$	$(6,6)$				$\mathcal{O}$
$(6,6)$	$(6,6)$				$\mathcal{O}$	
				$\mathcal{O}$		
			$\mathcal{O}$			
		$\mathcal{O}$				

Exercice 4. *Protocole d'authentification*

On cherche à construire un protocole d'authentification par mot de passe, où Alice détient un secret s (déduit de son mot de passe), et Bob un vérifieur v (calculé à partir de s), tel que :

- un intrus passif, qui enregistre les messages échangés entre Alice et Bob, n'obtient aucune information utile, et ne peut pas, en particulier, monter d'attaque de dictionnaire ;
- un intrus actif, qui tente de se faire passer pour Alice auprès de Bob en devinant s, obtient comme seule information que son choix n'est pas le bon (ou, par un hasard extraordinaire, qu'il est bon) ;
- un attaquant qui dérobe v ne peut pas usurper l'identité d'Alice, sauf à travers une attaque de dictionnaire.

Le principe est de définir le vérifieur par la formule $v = g^s \bmod p$, et d'incorporer au protocole un échange de type Diffie-Hellman.

1. La première proposition est simplement la suivante :
   - Alice choisit a aléatoire
   - Alice envoie à Bob : "Je suis Alice" et $A = g^a \bmod p$
   - Bob choisit b aléatoire
   - Bob envoie à Alice : $B = g^b \bmod p$

   Alice (qui connaît s) et Bob (qui connaît v) calculent une clef commune (tous les calculs sont effectués mod$p$) :

$$K = B^{a+s} = (Av)^b$$

(a) Quel message, noté M, Alice peut-elle ensuite envoyer à Bob pour prouver qu'elle a bien calculé la clef K correcte (et qu'elle connaît donc s) ? *Note :* donner plusieurs réponses si possible, en comparant avantages et inconvénients.

(b) Montrer que ce protocole a les deux premières propriétés souhaitées (un intrus, passif ou actif, n'obtient aucune information utile).

(c) Par contre, si Charlie dérobe v, il peut se faire passer pour Alice : expliquer quelle valeur truquée de A Charlie peut envoyer, pour être capable de calculer la même clef que Bob.

2. Pour remédier au défaut constaté, on modifie le protocole comme suit : Bob envoie à Alice, en même temps que B, un défi aléatoire u, et la clef à calculer devient :

$$K = B^{a+us}.$$

Donner la formule qui permet à Bob de calculer K. Expliquer pourquoi Charlie, même en connaissant v, ne peut plus usurper l'identité d'Alice ; montrer en particulier qu'il est essentiel que Bob n'envoie pas le défi u avant d'avoir reçu A.

3. (Question subsidiaire) Malgré les apparences, le protocole précédent possède une faille : si Charlie, sans connaître v, arrive à se faire passer pour Bob, il peut, à la fin du protocole (qui s'est donc déroulé entre Alice et Charlie), rompre la connexion, et monter une attaque de dictionnaire "hors ligne". Expliquer comment. Indication : ne pas oublier qu'Alice calcule, en fin de protocole, une valeur M qui prouve sa connaissance de K, et l'envoie à Charlie.