ISEC - Examen
23 mai 2019

Énoncé

Notes manuscrites et documents du cours autorisés à l'exclusion de toute autre document
L'utilisation de tout matériel électronique (en dehors d'une montre non connectée) est interdite

Les exercices sont indépendants. Une rédaction claire et concise sera appréciée. Toute affirmation devra être justifiée. Une question non résolue n'empêche pas de faire les suivantes (dans ce cas indiquez clairement que vous admettez le(s) résultat(s) de la question non faite).

Exercice 1 :

Nous considérons un algorithme de chiffrement par blocs $\mathcal{E}$ où la taille des blocs est un entier $n \geq 1$. Pour un message formé de t blocs de n bits, le mode opératoire de chiffrement CBC, décrit dans la figure (**??**), consiste à chiffrer le i-ème bloc préalablement combiné par un « ou exclusif » avec le chiffré du bloc précédent : $c_i = \mathcal{E}_K(m_i \oplus c_{i-1})$ pour $i \in \{2, \ldots, t\}$ et $c_1 = \mathcal{E}_K(m_1 \oplus v)$ où v désigne un *vecteur d'initialisation*.

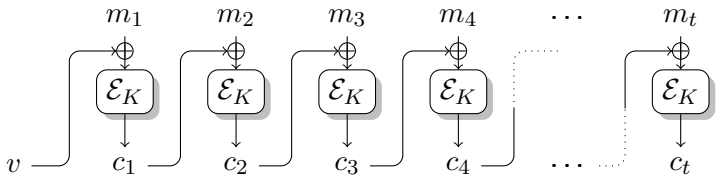

FIGURE 1 – Mode opératoire CBC (*Cipher Block Chaining*)

Le but de ce mode est d'assurer la confidentialité du message mais nous avons vu la variante CBC-MAC pour assurer l'authenticité d'un tel message qui utilise toujours le vecteur d'initialisation $v = 00 \ldots 0 = 0^n$ et retourne la valeur c_t comme code d'authentification de $(m_1, \ldots, m_t)$. Nous avons vu en cours que ce mode n'est pas sûr si on l'utilise pour des messages ayant un nombre de blocs différents (et nous supposons donc que t est fixé dans la suite).

1.a] Montrer que la variante probabiliste où un vecteur d'initialisation est tiré uniformément aléatoirement dans $\{0,1\}^n$ par l'émetteur du message et le code d'authentification est alors le couple $\tau = (v, c_t)$ n'est pas résistante à la contrefaçon existentielle sous une attaque à un message connu.

1.b] Dans certains protocoles, il est cependant parfois utile d'ajouter un vecteur d'initialisation qui sert de compteur pour dater les messages (et éviter les attaques par rejeu). Proposer une variante de CBC-MAC qui permet d'utiliser un compteur mais qui résiste à l'attaque de la question précédente.

1.c] Nous considérons la variante CBC-MAC1 (avec le vecteur d'initialisation constant $v = 0^n$) du mode CBC1 décrit dans la figure (**??**) qui consiste à chiffrer le i-ème bloc puis à le combiner par un « ou exclusif » avec le bloc précédent : $c_i = \mathcal{E}_K(m_i) \oplus m_{i-1}$ pour $i \in \{2, \ldots, t\}$ et $c_1 = \mathcal{E}_K(m_1) \oplus v = \mathcal{E}_K(m_1)$ puis à retourner la valeur c_t comme code d'authentifcation de message.
Montrer que CBC-MAC1 n'est pas résistant à la contrefaçon universelle sous une attaque à un message choisi pour tout $t \geq 2$.

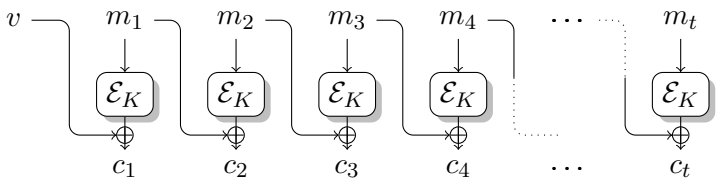

FIGURE 2 – Mode opératoire CBC1

1.d] Nous considérons désormais la variante CBC-MAC2 (avec le vecteur d'initialisation constant $v = 0^n$) du mode CBC2 décrit dans la figure (**??**) qui consiste à chiffrer le i-ème bloc puis à le combiner par un « ou exclusif » avec le chiffré du bloc précédent $c_i = \mathcal{E}_K(m_i) \oplus c_{i-1}$ pour $i \in \{2, \ldots, t\}$ et $c_1 = \mathcal{E}_K(m_1) \oplus v = \mathcal{E}_K(m_1)$ puis à retourner la valeur c_t comme code d'authentifcation de message.

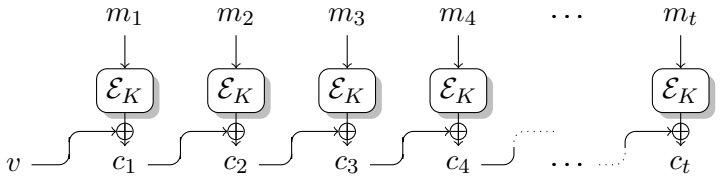

FIGURE 3 – Mode opératoire CBC2

Montrer que CBC-MAC2 n'est pas résistant à la contrefaçon universelle sous une attaque à trois messages choisis pour tout $t \geq 2$.

1.e] Montrer que les modes operatoires de chiffrement CBC1 et CBC2 associés (avec un vecteur d'initialisation tiré uniformément aléatoirement) n'assurent pas la sécurité sémantique.

Exercice 2 :

Une *signature de Lamport* est une méthode pour construire un protocole de signature numérique dont la sécurité repose sur une fonction à sens-unique $f : X \longrightarrow Y$.

2.a] Proposer un choix de fonction f pour que le schéma de signature de Lamport vu en cours assure un niveau de sécurité de 128 bits (*i.e.* la meilleure attaque en contrefaçon contre le schéma demande de l'ordre de 2^{128} opérations élémentaires). Donner les tailles des clés publiques, des clés secrètes et des signatures pour ce choix (pour signer un message de 256 bits).

2.b] Considérons une variante de la signature de Lamport où le signataire révèle dans les signatures uniquement les pré-images secrètes correspondant aux positions des bits du message égaux à 1 (et la vérification consiste simplement à vérifier ces valeurs). Montrer que cette variante n'est pas résistante à la contrefaçon existentielle sous une attaque à un message choisi.

2.c] Justifier que si le signataire utilise en plus de cette variante, le schéma de Lamport classique (avec des clés indépendantes) pour signer le nombre de 1 qui apparaît dans le message, alors cette variante est sûre. Donner la taille des signatures produites pour un niveau de sécurité de 128 bits (pour signer un message de 256 bits).