ISEC - Examen

3 septembre 2020 (2ème session)

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

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). Chaque question vaut environ 2 points.

Exercice 1 :

Un mode de chiffrement pour les chiffrements par blocs est le mode CFB (de l'anglais *Cipher Feedback*) décrit dans la figure (1). Il s'agit d'une combinaison des modes CBC et CTR qui consiste à masquer le i-ème bloc du texte clair par le chiffrement du bloc précédent du texte chiffré par un « ou exclusif » bit-à-bit (comme dans le chiffrement de Vernam) :

$$c_1 = m_1 \oplus \mathcal{E}_K(v) \text{ et } c_i = m_i \oplus \mathcal{E}_K(c_{i-1}) \text{ pour } i \in \{2, \ldots, t\}$$

où v désigne un *vecteur d'initialisation* et $\mathcal{E}_K$ désigne un chiffrement par bloc utilisant une clé K. Nous supposons que le chiffrement par blocs $\mathcal{E}$ opére sur des blocs de n bits.

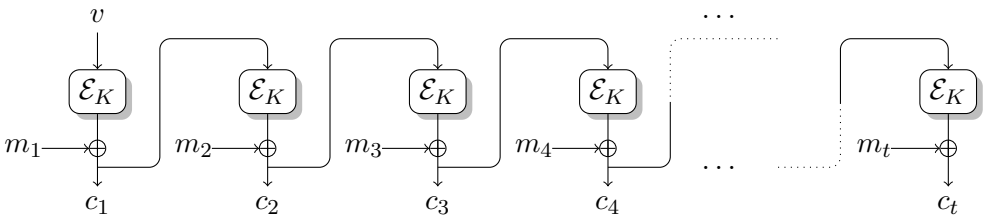

FIGURE 1 – Mode opératoire CFB (*Cipher Feedback*)

1.a] Décrire comment le déchiffrement est effectué pour le mode opératoire CFB.

1.b] Analyser l'efficacité du mode CFB et comparer la à celle des modes ECB, CBC et CTR (notamment en termes de parallélisabilité et de coût d'implantation).

1.c] Montrer que le mode opératoire CFB n'assure pas la sécurité sémantique (sous une attaque à chiffrés connus) pour des messages suffisamment longs (*i.e.* lorsque le nombre de blocs des messages chiffrés est de l'ordre de $2^{n/2}$).

Indication : On pourra étudier le cas où deux blocs du chiffré sont égaux.

Nous considérons maintenant un code d'authentification de messages (MAC) défini à partir du mode CFB (et appelé CFB-MAC). Le MAC τ d'un message formé de t blocs $(m_1, \ldots, m_t)$ est le « ou exclusif » bit-à-bit des blocs de chiffrés obtenus avec le mode CFB en utilisant le vecteur d'initialisation constant v formé de n zéros :

$$\tau = c_1 \oplus \cdots \oplus c_t, \text{ avec } c_1 = m_1 \oplus \mathcal{E}_K(0 \ldots 0) \text{ et } c_i = m_i \oplus \mathcal{E}_K(c_{i-1}) \text{ pour } i \in \{2, \ldots, t\}.$$

1.d] Montrer que si un attaquant peut obtenir le MAC d'un message formé d'un unique bloc, il peut retrouver $\mathcal{E}_K(0 \dots 0)$.

1.e] Montrer que si un attaquant peut obtenir le MAC d'un message $m = (m_1, \dots, m_t)$ formé de t blocs, il peut produire le MAC d'un message m' formé de t blocs avec $m \neq m'$.

1.f] Supposons qu'un attaquant connaisse la valeur de $\mathcal{E}_K(0 \dots 0)$. Montrer que tout chaîne h de n bits, il peut construire un message $m = (m_1, m_2)$ formé de deux blocs tels que

$$\texttt{CFB-MAC}(m_1, m_2) = h.$$

1.g] Qu'en concluez-vous la sécurité de ce MAC ?

Exercice 2 :

Considérons un groupe cyclique $\mathbb{G}$, engendré par un générateur g, dans lequel on suppose que le calcul du logarithme discret est difficile — par exemple, il peut s'agir du groupe des entiers non-nuls modulo un grand nombre premier p pour la multiplication.

Le problème *Diffie-Hellman Calculatoire* (CDH) consiste, étant donné g^x et g^y, à calculer g^z.

Le problème *Diffie-Hellman Décisionnel* (DDH) consiste, étant donné *ou bien* (g^x, g^y, g^{xy}) *ou bien* (g^x, g^y, g^z) avec x, y, z choisis aléatoirement, à déterminer si on est dans le premier cas ou dans le deuxième cas.

2.a] Entre le logarithme discret, CDH et DDH, qui est le plus facile ? Qui est le plus dur ? (justifier en explicitant les réductions).

2.b] Supposons un instant que CDH soit facile à résoudre en pratique dans le groupe $\mathbb{G}$. Quelles en serait les conséquences d'un point de vue cryptographique dans $\mathbb{G}$ (quels schémas classiques seraient cassés) ?

Le problème *Square Diffie-Hellman* (SqDH) consiste, étant donné g^x, à calculer $g^{(x^2)}$.

2.c] Supposons qu'on dispose d'un algorithme efficace pour résoudre CDH. Exhibez un algorithme efficace pour résoudre SqDH.

2.d] Supposons qu'on dispose d'un algorithme efficace pour résoudre SqDH. Exhibez un algorithme efficace pour résoudre CDH. On peut supposer que le calcul des racines carrées dans $\mathbb{G}$ est facile. Indice : qu'obtient-on en donnant $(x + y)$ à l'algorithme qui résoud SqDH ?