Cryptographie – Feuille d'exercices 6

Message Authentication Codes (MAC)

M1 Informatique – 2014-2015

1 Exercice : Un mauvais MAC

Considérons le schéma de MAC suivant. Soit E un algorithme de chiffrement par bloc, la taille des blocs étant de n bits, et soit h une fonction de hachage (à collisions fortes difficiles) dont la sortie fait n bits. Alors, pour tout message m de longueur $N > n$, on obtient le MAC en calculant $E_k(h(m))$. Par ailleurs, pour tout message m de taille n, le MAC est $E_k(m)$. (Pour simplifier, on suppose que tous les messages font au moins n bits).

1. Montrer que ce MAC n'est pas sûr.
2. Comment modifier la construction du MAC pour le rendre sûr ?

2 Exercice : CFB-MAC

Dans cet exercice, on étudie un schéma de MAC basé sur le mode de chiffrement CFB. On considère un algorithme de chiffrement par blocs

$$E : \{0,1\}^{64} \times \{0,1\}^{64},$$

où $E_k(x) = E(k,x)$ désigne le résultat du chiffrement du message x avec la clé k. Le CFB-MAC d'un message donné $m \in \{0,1\}^*$ avec la clé k est obtenu en chiffrant tout d'abord m par E_k en mode CFB, puis en calculant le XOR de tous les blocs obtenus en sortie.
Plus précisément, pour un message $m = x_1 x_2 \dots x_n$,

$$\text{CFB-MAC}_k(m) = y_1 \oplus y_2 \oplus \dots \oplus y_n,$$

où $y_i = E_k(y_{i-1}) \oplus x_i$ pour $i = 2, \dots, n$ et $y_1 = E_k(IV) \oplus x_1$, IV étant une "valeur d'initialisation". Pour simplifier, on supposera que tous les messages ont une longueur multiple de 64 bits. On suppose également dans toutes les questions de l'exercice, que IV est constante et connnue.

1. Supposons qu'on ait accès à un oracle $\mathcal{O}$ qui calcule le CFB-MAC décrit ci-dessus, pour une clé secrète k donné et une valeur IV fixée et connue. Montrer que l'on peut retrouver $E_k(IV)$ en faisant un seul appel à l'oracle.
2. Supposons qu'un attaquant ait accès à un oracle $\mathcal{O}$ qui calcule le CFB-MAC décrit ci-dessus, pour une clé secrète k donné et une valeur IV fixée et connue. L'attaquant voudrait trouver une collision pour CFB-MAC, pour 2 messages différents ayant 192 bits chacun. Combien de messages de 192 bits l'attaquant doit-il envoyer à $\mathcal{O}$ pour obtenir une collision avec une probabilité proche de 0.9996 ($\simeq 1 - e^{-8}$) ?
3. Étant donné un message m de n blocs et $h = \text{CFB-MAC}_k(m)$, montrer comment on peut construire un nouveau message m' de n blocs, et $h' \in \{0,1\}^{64}$, tels que $m' \neq m$ et CFB-MAC$_k(m') = h'$.

4. Supposons qu'on connaisse IV, $E_k(IV)$, et $h \in \{0,1\}^{64}$. Montrer comment il est possible de construire un message m de deux blocs, tel que CFB-MAC$_k(m) = h$.
5. Peut-on étendre l'attaque de la question précédente à des messages m de plus que deux blocs ? Expliquer votre réponse.