ISEC - TD 2
2019

Énoncé

Exercice 1 : Propriété de complémentation du chiffrement DES

1.a] Montrer que le DES a la *propriété de complémentation* :

$$\forall k \in \{0,1\}^{56}, \forall m \in \{0,1\}^{64}, \mathsf{DES}_k(m) = \overline{\mathsf{DES}_{\overline{k}}(\overline{m})},$$

où pour toute chaîne de bits ω, $\overline{\omega}$ désigne la chaîne formée des bits complémentaires de ceux de ω (*i.e.* $\overline{\omega} = (11\ldots1) \oplus \omega$).

1.b] En déduire une amélioration de la recherche exhaustive de la clé lors d'une attaque à deux clairs choisis.

Exercice 2 : Chiffrement DES avec blanchiment

Nous considérons une variante de DES (dite avec *blanchiment*) qui utilise une clé de 120 bits de la forme $K = (K_1, K_2) \in \{0,1\}^{56} \times \{0,1\}^{64}$ et qui chiffre un bloc m de 64 bits sous la forme

$$c = \mathsf{DES}_{K_1}(m) \oplus K_2.$$

Montrer qu'il existe une attaque à deux clairs connus contre cette variante de DES qui demande 2^{57} évaluations de la fonction DES (*i.e.* que cette variante ne ralentit la recherche exhaustive que d'un facteur 2).

Exercice 3 : Double chiffrement

3.a] Montrer que le double chiffrement n'apporte pas toujours un gain de sécurité par rapport au chiffrement simple.

3.b] Exprimer la taille de l'espace des clés du chiffrement double en fonction de la taille ℓ des clés du système de chiffrement sous-jacent. Donner l'accroissement de la complexité d'une recherche exhaustive de la clé.

3.c] Montrer que le double chiffrement est vulnérable à une attaque à clairs connus si l'attaquant dispose de quelques couples clair/chiffré (m, c) et calcule $\mathcal{E}_k(m)$ et $\mathcal{D}_k(c)$ pour toutes les clés k en mémorisant les résultats obtenus une table. Analyser la complexité en temps et en mémoire de cette attaque et expliquer comment l'attaquant retrouver le couple de clés effectivement utilisé pour le double chiffrement.

Exercice 4 : Multicollisions pour les fonctions de hachage itérées

Nous considérons une fonction de hachage $\mathcal{H} : \{0,1\}^r \to \{0,1\}^n$ construite à partir d'une fonction de compression $f : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n$ par la méthode de Merkle-Damgård (avec $\ell > 2n$).

Soit $\mathcal{H}_c : \{0,1\}^{c\cdot\ell} \to \{0,1\}^n$ une fonction construite à partir de f par la méthode de Merkle-Damgård mais sans ajouter de bourrage et utilisée uniquement pour les messages de longueur fixe égale à un multiple de ℓ.

4.a] En cherchant deux collisions bien choisis pour la fonction de compression, montrer comment obtenir une 4-multicollision pour $\mathcal{H}_2$.

4.b] Expliquer comment transformer cette 4-multicollision pour $\mathcal{H}_2$ en une 4-multicollision pour $\mathcal{H}$.

4.c] Généraliser en montrant qu'on peut obtenir une 2^t-multicollision pour $\mathcal{H}$ pour le coût de t collisions sur f.

Exercice 5 : Chiffrement par bloc et fonction de compression

Soit $\mathcal{E} : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$ un système de chiffrement par blocs qui utilise des clés de n bits pour chiffrer des messages de n bits.

Montrer que les trois fonctions de compression f_1, f_2 et f_3 ne sont pas résistantes à la pré-image.

1. $f_1 : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$, $f_1(h,m) = \mathcal{E}_m(h)$
2. $f_2 : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$, $f_2(h,m) = \mathcal{E}_h(m) \oplus h$
3. $f_3 : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n$, $f_3(h,m) = \mathcal{E}_h(h) \oplus m$