TD 3

Exercice I. Chiffrement avec blanchiment

1. On s'intéresse à la complexité des recherches exhaustives.
   - Pour un chiffrement par bloc E avec des clefs de k bits pour chiffrer des blocs de n bits, quelle est la complexité de la brute force ?
   - Quel intérêt d'appliquer un blanchiment ?
   - Avec deux clefs de dimension k et n, quelle est la complexité de la brute force pour un chiffrement avec blanchiment ?
   - En ayant un couple de clairs/chiffrés, comment faire diminuer cette complexité ? (Exprimez vos clairs en fonction des chiffrés puis essayez de trouver comment diminuer la complexité.)
   - A combien s'élève la complexité ?

Exercice II. Double Chiffrement

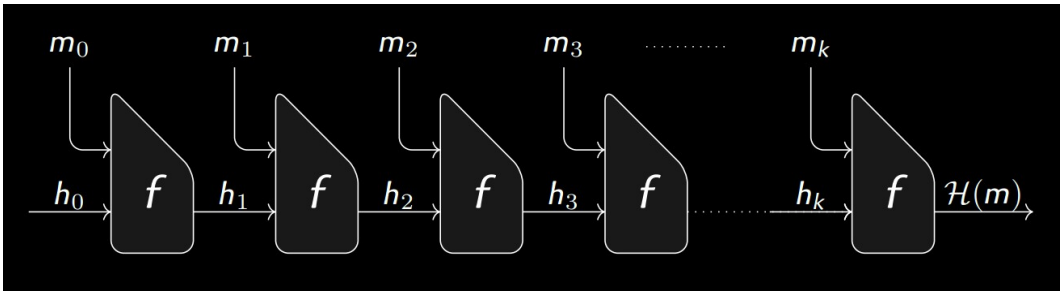
1. Montrer que le double chiffrement n'apporte pas toujours un gain de sécurité par rapport au chiffrement simple.
   - Pouvez-vous citer un exemple simple de chiffrement pour lequel le chiffrement double revient à un chiffrement simple ?

2. Exprimer la taille de l'espace des clefs du chiffrement double en fonction de la taille k des clefs du système de chiffrement sous-jacent. Donner l'accroissement de la complexité d'une recherche exhaustive de la clef.
   - A combien s'élève la complexité d'un chiffrement double dans le cas ou il ne correspond pas à un chiffrement simple ?

3. Montrer que le double chiffrement est vulnérable à une attaque à clairs connus si l'attaquant dispose de quelques couples clair/chiffré et calcule Ek(m) et Dk(c) pour toutes les clefs k en mémorisant les résultats obtenus une table.
   - Schématiser le chiffrement double pour un couple (m, c) avec deux clefs K1 et K2.
   - Par quelle astuce peut-on obtenir les clefs avec moins de calculs en utilisant une table de hachage ?
   - Donner la complexité en temps et la complexité en espace de la table de hachage obtenue.

Exercice III. Multicollisions pour les fonctions de hachage itérées

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



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

1. En cherchant deux collisions bien choisis pour la fonction de compression, montrer comment obtenir une 4-multicollision pour H2.

- Qu'est-ce qu'une collision ?
- En vous intéressant au problème pour H2, choisissez deux clairs différents mais provoquant une collision dès la première étape pour h1. Faites de la même manière pour la seconde étape pour h2. Aidez-vous d'un schéma.
- En déduire la 4-multicollision.

2. Expliquer comment transformer cette 4-multicollision pour H2 en une 4-multicollision pour H. (Quelle différence entre H2 et H ? Comment parer à cela?)

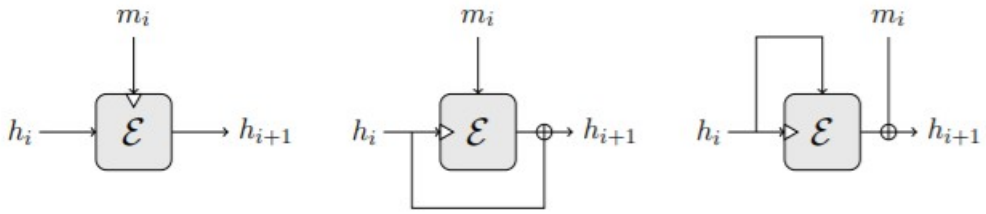
3. Généraliser en montrant qu'on peut obtenir une 2t -multicollision pour H pour le coût de t collisions sur f.

Combien de t couples au total ? Quel coût pour une collision si f se comporte comme une fonction aléatoire ? Et donc quel coût pour une 2t-multicollision ?

Exercice IV. Chiffrement par bloc et fonction de compression

Soit E : $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ un système de chiffrement par blocs qui utilise des clefs de n bits pour chiffrer des messages de n bits. Montrer que les trois fonctions de compression f1, f2 et f3 ne sont pas résistantes à la pré-image.

1. f1 : $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$, $f1(h, m) = E_m(h)$
2. f2 : $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$, $f2(h, m) = E_h(m) \oplus h$
3. f3 : $\{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$, $f3(h, m) = E_h(h) \oplus m$



- Qu'est ce que la résistance à la pré-image ?
- Observez le lien entre les schémas proposés et la paramétrisation des fonction de compression. Qu'en déduisez-vous ?
- En notant h* la sortie des fonctions retrouver h* à partir de votre entrée : essayez d'exprimer chaque fonction par son déchiffrement (on connaît E^{-1}) en partant de h ou m en fonction du paramètre et de la variable de la fonction.