TD 3 Cryptographie CSI 2024–2025

Léo Colisson Palais

Exercice 1: Adaptation non sécurisée de Merkle-Damgård

Soit $h : \{0,1\}^{n+t} \to \{0,1\}^n$ une fonction de compression à taille fixe. Supposons que nous avons oublié certaines des caractéristiques importantes de la transformation de Merkle-Damgård, et construisons une fonction de hachage H à partir de h comme suit :

- Soit x l'entrée.
- Découper x en $y_0, x_1, x_2, \ldots, x_k$, où y_0 fait n bits, et chaque x_i fait t bits. Le dernier morceau x_k doit être complété avec des zéros si nécessaire.
- Pour $i = 1$ à k, définir $y_i \coloneqq h(y_{i-1} \| x_i)$.
- Retourner y_k.

Cela ressemble à Merkle-Damgård, sauf que nous avons perdu le vecteur d'initialisation (IV) et le bloc de padding final.

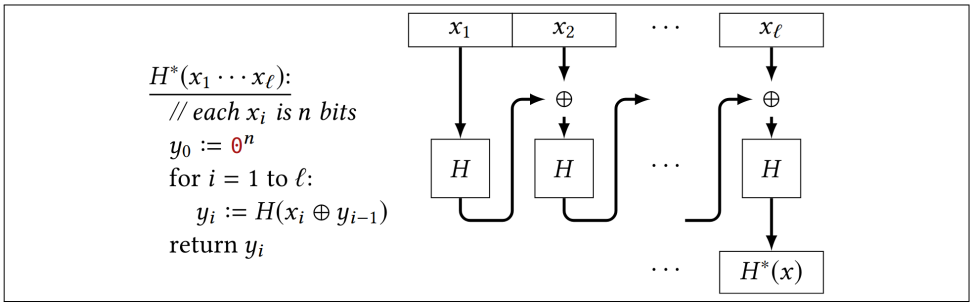
1. Décrire une méthode simple pour trouver deux messages découpés en le même nombre de blocs, qui ont la même valeur de hachage sous H.
2. Décrire une méthode simple pour trouver deux messages découpés en un nombre différent de blocs, qui ont la même valeur de hachage sous H.

   Indice : Choisissez une chaîne de longueur $u + 2t$, puis trouvez une chaîne plus courte qui entre en collision avec elle.

Aucune des collisions ci-dessus ne doit impliquer de trouver une collision dans h.

Exercice 2: Attaque contre "CBC-HASH"

Soit H une fonction de hachage résistante aux collisions, de sortie de longueur n. Soit H^* la fonction obtenue en itérant H d'une manière similaire à CBC-MAC :



Montrer que H^* n'est pas résistante aux collisions. Décrire une attaque réussie.

Exercice 3

1. Supposons qu'une fonction $H : \{0,1\}^* \to \{0,1\}^n$ possède la propriété suivante. Pour toutes chaînes x et y de même longueur, on a $H(x \oplus y) = H(x) \oplus H(y)$. Montrer que H n'est pas résistante aux collisions (décrire comment trouver efficacement une collision dans une telle fonction).
2. Montrer qu'une PRP seule n'est pas résistante aux collisions. Autrement dit, si F est une PRP sécurisée, montrer comment trouver efficacement des collisions dans $H(x\|y) \coloneqq F(x, y)$.

* Exercice 4

Soit F une PRF sécurisée prenant des entrées de n bits, et soit H une fonction de hachage (salée) résistante aux collisions, produisant des sorties de n bits. Définissons la nouvelle fonction $F'((k,s),x) \coloneqq F(k,H(s,x))$, où (k,s) est interprété comme la clé. Montrer que F' est une PRF sécurisée prenant des entrées de longueur arbitraire.