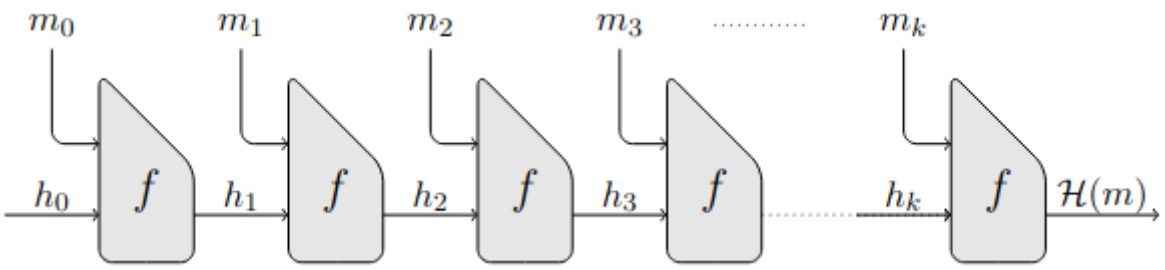
TD4



Considérons une *fonction de compression* $f : \{0,1\}^{n+\ell} \longrightarrow \{0,1\}^n$ avec $\ell \geq 2$ et $h_0 \in \{0,1\}^n$ un vecteur d'initialisation (utilisée pour le premier bloc). Nous considérons un processus de remplissage $\mathcal{R}$ défini sur $\{0,1\}^*$ et vérifiant $|\mathcal{R}(m)| \equiv 0 \bmod \ell$ pour tout message $m \in \{0,1\}^*$ (*i.e.* qui transforme le message à hacher en un message dont la longueur est un multiple de ℓ). La valeur de la fonction de hachage itérée $\mathcal{H}$ construite à partir de f et R est définie par $\mathcal{H}(m) = f(h_k, m_k)$ où

— la valeur $\mathcal{R}(m)$ en $(k+1)$ blocs de ℓ bits $\mathcal{R}(m) = (m_0, \ldots, m_k) \in \left(\{0,1\}^\ell\right)^k$;

— $h_i = f(h_{i-1}, m_{i-1})$ pour tout $i \in \{1, \ldots, k\}$.

R. Merkle et I. Damgård ont montré que si la fonction de compression est résistante aux collisions et si le processus de bourrage est bien construit, alors la fonction de hachage itérée $\mathcal{H}$ obtenue à partir de f est résistante aux collisions.

Exercice 1 : Construction de Merkle-Damgård

1.a] Supposons que les messages dont la longueur n'est pas un multiple de la longueur du bloc ℓ sont complétés par une chaîne de zéros jusqu'à ce que la longueur soit un multiple de ℓ (*i.e.* en posant $i = |m| \bmod \ell$, $\mathcal{R}(m) = m \| 0^{\ell - i}$).
Montrer que la fonction itérée obtenue à partir de f et $\mathcal{R}$ n'est pas résistante aux collisions.

- Trouvez un exemple simple pour lequel deux messages différents donnent le même haché pour ce type de padding.

1.b] Supposons désormais que le processus de bourrage est défini de la façon suivante :

$$\mathcal{R}(m) = m \| 10^{\ell - i - 1} \text{ avec } i = |m| \bmod \ell$$

Montrer que si l'on dispose d'un bloc de message z tel que $f(h_0, z) = h_0$ alors il est possible de trouver des collisions pour la fonction itérée obtenue à partir de f et $\mathcal{R}$.

- Faire passer ces deux messages dans R puis H, montrer que les deux empreintes obtenues sont bien égales.

1.c] Supposons enfin qu'un dernier bloc contenant la longueur binaire du message est concaténé au procédé de bourrage de la question précédente (*i.e.* en notant τ_m un encodage binaire de la longueur $|m|$ de m, nous avons $\mathcal{R}(m) = (m \| 10^{\ell - i - 1} \| \tau_m)$ avec $i = |m| \bmod \ell$).
Montrer que la fonction itérée obtenue à partir de f et $\mathcal{R}$ est résistante aux collisions si f est résistante aux collisions.

Considérez deux messages m et m' tels que H(m)=H(m'). Traitez deux cas : l'un ou m et m' sont de même longueur, puis le cas où ils sont de longueur différente. Dans les deux cas prouvez que vous obtenez bien une collision !

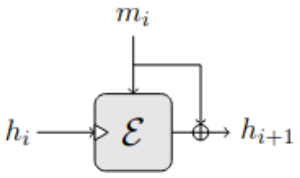
Exercice 2 : Cryptographie Asymétrique

2.2. Quel niveau de sécurité (= taille de clef secrète équivalente) offrent les clefs de 2048 bits recommandées aujourd'hui ?

2.3. Quelle taille de clef RSA faut-il choisir pour s'assurer un niveau de sécurité équivalent à des clefs secrètes de 128 bits ?

2.4. Le meilleur code publiquement disponible de factorisation, CADO-NFS, a besoin de 90 jours pour factoriser un nombre de 512 bits sur un coeur à 2Ghz. On peut estimer qu'un serveur qui contient 36 coeurs comparables coûte 4000 euros, et consomme 400W. Quel budget est nécessaire pour casser RSA-1024 en 3 mois ?

2.5. Quelle puissance électrique est nécessaire ? (un serveur qui contient 36 coeurs comparables coûte 4000 euros, et consomme 400W)



Une construction de fonction de compression à partir d'un système de chiffrement par bloc et résistante aux collisions a été proposée par Matyas, Meyer et Oseas. La fonction de compression $f : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n$ est définie par $f(h,m) = \mathcal{E}_h(m) \oplus m$ où $\mathcal{E}$ est un système de chiffrement par blocs de n bits. Il est conjecturé qu'il n'existe aucune attaque plus efficace que les attaques génériques sur cette construction ou sur la construction duale connue sous le nom de construction de Davies-Meyer (*i.e.*, une attaque en collision nécessite environ $2^{n/2}$ évaluations de la fonction f et une attaque en (seconde) pré-image nécessite environ 2^n évaluations de la fonction f). Cette conjecture a été démontrée sous l'hypothèse que la primitive de chiffrement par bloc utilisée a un comportement idéal. En pratique, les systèmes de chiffrement par bloc n'ont pas les mêmes propriétés que les fonctions aléatoires et l'exercice suivant montre que si le chiffrement par bloc utilisé a des propriétés spécifiques alors la fonction de compression peut ne pas être sûre.

Exercice 3 : Sécurité de la construction de Matyas-Meyer-Oseas avec le DES

Montrer que la fonction de compression f n'est pas résistante aux collisions lorsque $\mathcal{E} = \text{DES}$ dans la construction de Matyas-Meyer-Oseas.

- Utilisez la propriété de complémentation du DES pour prouver la non résistance aux collisions.

Exercice 4 : Attaque en collision contre fonctions de hachage concaténées

Soient $\mathcal{H}_1$ et $\mathcal{H}_2$ deux fonctions de hachage de même domaine qui produisent des empreintes de n bits et considérons la fonction de hachage $\mathcal{H}$ définie pour tout message m par $\mathcal{H}(m) = \mathcal{H}_1(m)\|\mathcal{H}_2(m)$ (en particulier $\mathcal{H}$ produit des empreintes de $2n$ bits).

4.a] Montrer que $\mathcal{H}$ est résistante aux collisions dès que l'une des fonctions $\mathcal{H}_1$ ou $\mathcal{H}_2$ est résistante aux collisions.

- Considérer deux messages différents m_1 et m_2 tels que $H(m_1)=H(m_2)$. Déduisez en qu'une collision de H fournit une collision pour H_1 et H_2.

4.b] En supposant que $\mathcal{H}_1$ est une fonction de hachage itérée vulnérable à l'attaque des multicollisions de l'exercice précédent, proposer un algorithme pour construire une collision pour la fonction $\mathcal{H}$ en environ $2^{n/2}(n/2)$ évaluations de la fonction de hachage $\mathcal{H}_1$ et $2^{n/2}$ évaluations de la $\mathcal{H}_2$.

- Reprenez le résultat du TD_3 sur le coût des multi-collisions. Quel est ce coût pour une 2^t-multicollision **?**
- Appliquez cela à H_1, a combien d'évaluations de H_1 cela correspond-il **?**
- Combien de couples sont obtenus **?** A combien de messages en collision cela correspond-il **?**
- Grâce à quoi peut-on évaluer la fonction H2 **?**
- Que venez vous de démontrer **?**