TD2 - Chiffrement par bloc

(INSMAC2fr) **Exercise 1.** *Insecure MAC*

Soit $F : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ une fonction pseudo-aléatoire (PRF) sûre. Montrez que chacun des MAC suivants ne sont pas sûrs:

1. Pour authentifier un message $m = m_1 \| \ldots \| m_d$ où $m_i \in \{0,1\}^n$ pour tout i, calculer $t = F(k, m_1) \oplus \ldots \oplus F(k, m_d)$.

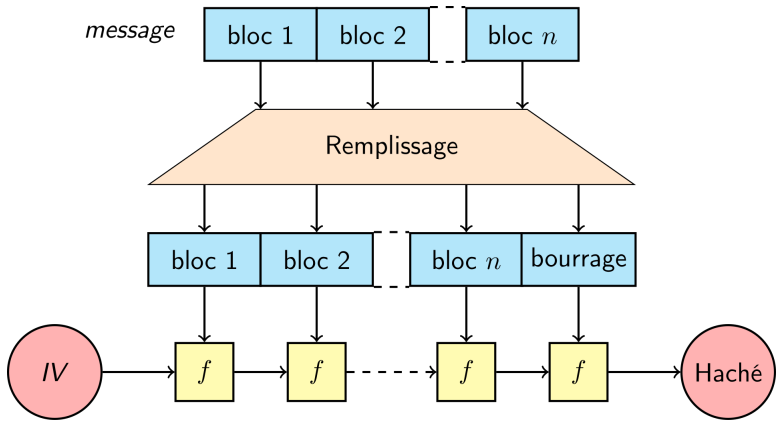
2. Pour authentifier un message $m = m_1 \| \ldots \| m_d$ avec $d < 2^{n/2}$ et $m_i \in \{0,1\}^{n/2}$ pour tout i, calculer

$$t = F(k, \underline{1} \| m_1) \oplus \ldots \oplus F(k, \underline{d} \| m_d),$$

où $\underline{i}$ est la représentation de taille $n/2$-bit de i, pour tout $i \leqslant d$.

(MultiColfr) **Exercise 2.** *Multi Collision*

On considère une fonction de hachage $H : \{0,1\}^r \to \{0,1\}^n$ construite sur une fonction de compression $f : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^n$ via la transformation de Merkle-Damgård (avec $\ell > n$). Soit $H_2 : \{0,1\}^{c \cdot \ell} \to \{0,1\}^n$ une fonction construite sur f via la transformation de Merkle-Damgård (rappelée ci-dessous) mais sans padder et utilisée seulement pour des message de taille fixe multiple de ℓ.



On rappelle qu'une fonction de collision H est une paire d'entrées distinctes x_1 et x_2 telles que $H(x_1) = H(x_2)$. Pour tout $m \geqslant 2$, une m-multi-collision pour une fonction H est un m-tuple d'entrées distinctes $x_1, \ldots, x_m$ telles que $H(x_1) = \ldots = H(x_m)$.

1. Montrez comment obtenir une 4-multi-collision pour H_2.

   Hint: Chercher deux collisions bien choisies pour la fonction f.

2. Expliquez comment transformer cette 4-multi-collision pour H_2 en une 4-multi-collision pour H.

3. Généralisez la méthode: montrez qu'on peut trouver une 2^t-multi-collision pour H avec un coût de t collisions pour f.

(TwoHashfr) **Exercise 3.** *Two-hash*

Soient H_1 et H_2 deux fonctions de hachage de même domaine, et de sortie $\{0,1\}^n$. On considère la fonction de Hachage H définie pour un message m par $H(m) = H_1(m)\|H_2(m)$.

1. Montrez que si H_1 ou H_2 est résistante aux collisions alors H l'est aussi.

2. On suppose que H_1 soit une fonction de hachage vulnérable aux attaques par multi collisions de l'exercice précédent. Donnez un algorithme pour construire des collisions sur H avec $2^{n/2}(n/2)$ évaluations de la fonction H_1 et $2^{n/2}$ évaluations de H_2.