# Sécurité Appliquée
# Fonctions de hachage

Jean-François COUCHOT
couchot[arobase]femto-st[point]fr

1er février 2021

## 1 Fonction de hachage : introduction

**Exercice 1.1 (Congruence modulo 1024).** *On considère la fonction de hachage qui étant donné un nombre retourne son reste dans la division par 1024.*

1. *Formaliser cette fonction $H : B^* \to B^n$.*
2. *Calculer les empreintes de 156 ; 1224 ; 10240.*
3. *Est-elle résistante aux collisions ? Justifier.*
4. *Est-elle résistante à la première préimage ? Justifier.*
5. *Est-elle résistante à la seconde préimage ? Justifier.*

**Exercice 1.2 (Relation entre la résistance à la seconde préimage et la résistance aux collisions).** *Montrer que la résistance aux collisions implique la résistance à la seconde préimage.*

**Exercice 1.3 (Résistance aux collisions, mais pas à la préimage.).** *Soit $G : \{0,1\}^* \to \{0,1\}^n$ une fonction de hachage résistante aux collisions. On construit $H : \{0,1\}^* \to \{0,1\}^{n+1}$ définie par*

$$H(x) = \begin{cases} 0||x & \text{si } x \text{ est de longueur } n \\ 1||G(x) & \text{sinon} \end{cases}$$

1. *Montrer que $H$ est résistante aux collisions. On prendra par hypothèse $x$ et $x'$ deux chaînes de bits distincts telles que $H(x) = H(x')$. Raisonner alors sur la taille de $x$ et de $x'$.*
2. *Montrer que $H$ n'est pas résistante à la seconde préimage.*
3. *Montrer que $H$ n'est pas résistante à la première pré-image.*

## 2 Bourrage pour le procédé de Merkle-Damgård

Supposons que les messages à hacher ont une longueur qui n'est pas un multiple de la longueur du bloc $l$. Les messages doivent complétés.

**Exercice 2.1 (stratégies de bourrage).**

1. *On complète le message $m$ par une chaîne de zéros jusqu'à ce que la longueur soit un multiple de $l$. Montrer que la fonction obtenue n'est pas résistante aux collisions.*
2. *Supposons maintenant que le processus de bourrage ajoute d'abord un 1 avant de compléter par des zéros comme à la question précédente. Montrer qu'il est aussi possible de trouver des collisions pour la fonction de hachage.*

*Soit $\tau_m$ la longueur de $m$ encodée en binaire sur $l$ bits. On considère le processus de bourrage de la question précédente auquel on ajoute $\tau_m$. On pourrait montrer que la fonction obtenue est résistante aux collisions si la fonction de hachage basée sur le procédé de Merkle-Damgård l'est.*