**Fonctions** **de Hachage** (Hash Functions)

Une valeur *h* d’une fonction de hachage H est de la forme *h*=H(*M*) où M est un message de longueur variable et H(M) de longueur fixe. La valeur h est jointe au message lors de la transmission de ce dernier. Le receveur de M authentifie (Vérifie l’intégrité) du message en recalculant *h.*

**Exigences d’une fonction H**.

1. H est applicable à un bloc de données de taille quelconque
2. H fournit une sortie de taille fixe
3. H(x) est relativement facile à calculer pour tout x donné. En pratique, H est implémentée matériellement (Hard : algorithme câblé) ou logiquement (Programme soft).
4. Pour tout *h* donné, il est calculatoirement infaisable de trouver x tel que H(x)=h, c’est la propriété de fonction à sens unique (one-way property).
5. Pour tout bloc de données x, il est calculatoirement infaisable de trouver un bloc y tel que H(y)=H(x) : propriété de faible résistance aux collisions
6. Il est calculatoirement infaisable de trouver une paire (x, y) tel que H(x)=H(y). propriété de résistance forte aux collisions.

* Les propriétés 1, 2, 3 sont nécessaires pour qu’une fonction Hash soit appliquée à l’authentification de messages.
* La propriété 4 de ‘sens unique’ stipule qu’il est facile de générer un code à partir d’un message mais impossible de générer un message à partir d’un code.
* La propriété 5 garantie qu’on ne peut pas trouver deux messages avec la même valeur h. Ce qui évite les falsifications de messages.

**Exercice 9.**

La plupart des virus infectent les systèmes en s’implantant dans les fichiers exécutables sur disques. Expliquez comment utiliser un algorithme d’une fonction de Hashing pour détecter les fichiers infectés par un virus informatique.

**Exercice 10**

Expliquez comment un système multi-usagers vérifie de manière sure les demandes d’accès, sachant que ces dernières doivent fournir un code d’identification et un mot de passe.

**Exercice 11.**

Considérons la fonction Hash

Les messages sont sous forme d’une séquence de nombre décimaux : M = (a1, a2,….ai). La valeur h est calculée en fonction de la valeur prédéfinie de n.

1. Quelle sont les propriétés satisfaites par H ?
2. Même question qu’en a pour la fonction H’ en remplaçant ai par (ai)2
3. Calculer la valeur h pour *M* = (189, 632, 900, 722, 349) et *n* = 989