Fiche de TP N° 4 du Module Cryptgraphie

Implémentation d'une fonction de hachage cryptographique

SHA-1 (*Secure Hash Algorithm*) est une fonction de hachage cryptographique conçue par la *National Security Agency* des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information (*Federal Information Processing Standard* du *National Institute of Standards and Technology* (NIST)). Elle produit un résultat (appelé « *hash* » ou *condensat*) de 160 bits.

Pour plus de détails : https://fr.wikipedia.org/wiki/SHA-1.

Objectifs du TP:
Implémenatation de la fonction SHA1: le programme prenden entré un texte aléatoire de taille quelconque, ou bien un tabeal d'octet (flot binaire), et donne en sortie la valeur du hache sur 256bit.