Compte Rendu rapide du TP2 ExerciceHashGenerique

Différences des sha-3

Keccak est une fonction de hachage cryptographique créée par la keccak team pour la NIST (National Institute of Standards and Technology) hash function competition. L’objectif de la compétition est de trouver un nouveau standard pour la fonction de hachage qui remplacera sha-02.

Keccak remporte la compétition mais le NIST change le « padding » de la fonction keccak en SHA3-256(M) = KECCAK [512] (M || 01, 256); et donc il y a 2 versions de la fonction, celle proposée par la keccak team (qui est souvent appelée keccak) et la fonction standard du NIST (qui est souvent appelée Sha-3).