POIS ASSIGNMENT 1

TASK 7

USE MERKLE-DAMGARD TRANSFORM TO OBTAIN A PROVABLY SECURE COLLISION RESISTANT HASH FUNCTION

THEORY

Constructing a hash function seems like a challenging task, especially given that it must accept strings of arbitrary length as input. In this section, we'll see one approach for constructing hash functions, called **the Merkle-Damgård construction.**

Instead of a full-fledged hash function, imagine that we had a collision-resistant function (family) whose inputs were of a single fixed length, but longer than its outputs. In other words, suppose we had a family $\mathcal{H}$ of functions $h : \{0,1\}^{n+t} \rightarrow \{0,1\}^{n}$, where $t > 0$. We call such an h a **compression function**.

The idea of the Merkle-Damgard construction is to split the message M into blocks of constant length.
A compression function H takes input x of length b + c bits, and produces output H~(x) of length b bits. From such a function, we can easily create a hash function H. How?

Let x be an arbitrary input of any length.
Let's write x = x1x2x3:::xn , where each xi is c bits (if necessary, pad the last block of x).
Set h1 = 0 (or any other initial value)
define h_{i+1} = H~(h_i; x_i) for i > 1. Then, H(x) = h_n+1 (b bits).
[In H~(h_i; x_i), we mean that the b bits for h_i are concatenated with the c bits for x_i, for a total of b + c bits.]

This construction is known as a MerkleDamgård construction and is used in the design of many hash functions, including MD5 and SHA-1/2