POIS ASSIGNMENT 1

TASK 6

USE DLP TO BUILD A FIXED LENGTH COLLISION RESISTANT HASH FUNCTION

THEORY

Hash functions are extremely useful and appear in almost all information security applications.
A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.
Values returned by a hash function are called message digest or simply hash values.

COLLISION RESISTANCE HASH FUNCTION :
Consider a hash function H from M → T where M is the message space and T is the tag space where |T | ≪ |M|. Then, a collision for H is a pair such that m0 6= m1 ∈ M such that H(m0) = H(m1).

One application of collision resistant hash functions is the distribution of software packages. Suppose we have software packages F1, F2, F3 and in a public read-only space, we write H(F1), H(F2), H(F3). Then, when you download one of the packages, you can compute H(F1) to verify the integrity of the package F1. Note that an attacker cannot change the contents of the file without being detected. Note that in this example, we do not need a key to verify integrity; it is universally verifiable, but we need a public read-only space to ensure security.