Homework 8 – Due Tuesday, April 3

1. Draw and label a picture that illustrates the Merkle-Damgard hash function construction. Make sure you clearly label the input to the hash function and the output (the hash value).

2. Since a MAC is conceptually like adding a key to a hash function, let's try taking the key away from a MAC and seeing if it makes a good hash function. In particular, consider the Data Authentication Algorithm (sometimes called CBC-MAC) using DES, which is described in Section 12.6, where the input consists of an integer number of 64-bit blocks: $D_1, \ldots, D_N$. We then "take away" the key by setting it to zero, and computing

$$\begin{aligned} O_1 &= DES(0, D_1) \\ O_2 &= DES(0, D_2 \oplus O_1) \\ &\cdots \\ O_N &= DES(0, D_N \oplus O_{N-1}) \end{aligned}$$

   The hash output is O_N. Is this preimage resistant? (*Justify your answer, giving an attack algorithm if appropriate.*)

3. For the hash function in the previous problem, can you find collisions efficiently (given $D_1, D_2, \ldots, D_N$ can you find a different input that gives the same hash value)? (*Justify your answer, giving an attack algorithm if appropriate.*)