Merkle Damgard Transformation

Input: A message x of arbitrary length and an initialization vector of length n.

Output: Returns the hash of input message.

Algorithm:

Append length of the message to the input message.

Divide the message into blocks of size n.

For each message block:

Apply the fixed length hash function to the message the block and the initialization vector

Update the vector with the result

Return the output the last fixed length hash function.