Secure MAC

Input: Key of length seed_size and a message of arbitrary length.

Output: A CBC Mac tag of length seed_size

Algorithm:

Prepend the length of the message in binary format to the message.

Divide the message into blocks of size equal to seed_size.

The initial input to the PRF is the first message block i.e, block having the length of the message.

The subsequent inputs are the result of xor of the previous output and the current message block.

The output last PRF operation is the Message Authentication Code.