CS381 Exercise 10

Name: Zhang Yupeng

Student ID: 5130309468

1. What would happen if we use a block cipher directly (i.e. without DM) as compress function $H_i = h(H_{i-1}, M_i) = e_{M_i}(H_{i-1})$?

Solution:

Block ciphers take (like one-way compression functions) two fixed size inputs (the key and the plaintext) and return one single output (the ciphertext) which is the same size as the input plaintext.

However, modern block ciphers are only partially one-way. That is, given a plaintext and a ciphertext it is infeasible to find a key that encrypts the plaintext to the ciphertext. But, given a ciphertext and a key a matching plaintext can be found simply by using the block cipher's decryption function.

So, it's not proper to only use block cipher directly without some extra operations.

2. Can we use a MAC to provide non-repudiation, and why?

Solution:

MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption.

So MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages.