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 $H_i = h(H_{i-1}, M_i) = e_{M_i}(H_{i-1})$? Estimate the complexity of target attack with and without free-start.

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， since it will be easy to broke.

For target attack without free-start, if we use brute force to try all the $l-bit$ messages, It follows from the usual birthday argument that brute force collision attacks require about $2^{l/2}$ computations of hash values. So the complexity is $2^{l/2}$ on average.

The target attack with free-start is never harder than the one without free-start. The complexity is less than $2^{l/2}$.

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.

However, non-repudiation can be provided by systems that securely bind key usage information to the MAC key; the same key is in possession of two people, but one has a copy of the key that can be used for MAC generation while the other has a copy of the key in a hardware security module that only permits MAC verification. This is commonly done in the finance industry.