Exercise_10

1.

Modern block cipher is only partially one way. More accurately, if given ciphertext and a plaintext, it is hard to find the key, however, if given a ciphertext and a key, the original plaintext can be easily found by decryption function.

In conclusion, if we only use a block cipher as compression function, meet-in-the-middle would be an effective attack techniques.

For target attack without free start, according to birthday paradox, so the complexity is $2^{\frac{m}{2}}$ on average.

For target attack with free start, $C_{FS-target} \leq C_{target}$, so the complexity is $2^{\frac{m}{2}}$.

2.

MAC cannot provide the property of non repudiation. Because sender and receiver share the same key, MAC cannot provide a proof that whether the message was sent by the sender or the message was forged by the receiver.