Exercise 9

1.

For collision attack, it means that given H_0, find M and $M^{'} \neq M$, but $Hash(H_0, M) = Hash(H_0, M^{'})$.

For target attack, it means that given H_0 and M, find $M^{'} \neq M$, but $Hash(H_0, M) = Hash(H_0, M^{'})$.

As we can see, we can not get any message in collision attack, so all we have to is to find a pair of message whose hash code are the same. Based on birthday paradox, we only need $2^{\frac{m}{2}}$ brute force computations to find this pair. But in target attack, we get massage M, so to find $Hash(H_0, M) = Hash(H_0, M^{'})$, we need $2^{\frac{m}{2}}$ brute force computations to get $M^{'}$.

2.

Incorrect.

There is a concept of effective/actual key strength. For Double DES the effective key strength is 2^{57} even though double DES uses 2^{112} keys. The below example will make it clear.

Assume that you are a cryptanalyst who has access to the plain text and encrypted text. Your aim is to recover the secret key. Assume AAA (plaintext) -> XXX (After 1st encryption) -> ZZZ (after 2nd encryption).

You start with AAA and try all the 2^{56} combinations for secret key by encrypting AAA. This will give you a big list of possible values for XXX. Next you take ZZZ and try all the 2^{56} combinations for secret key by decrypting ZZZ. This will give you a big list of possible values for XXX.

The amount of effort you have put in 2^{56} +2^{56} = 2^{57} .

Now do a simple lookup between the two lists to find a matching value. As soon you see a matching value XXX in both the lists, you have found out the secret key. So this means that with effort of 2^{57} keys you have broken the encryption.

So 2^{57} brute force computations can succeed against double DES. In this case, the birthday attack need one hash function, however, the keys for D and E are different, so we can not just simply apply birthday paradox to this problem.

As proved, incorrect.