CS381 Exercise 9

Name: Zhang Yupeng

Student ID: 5130309468

1. What are the differences between collision attack and target attack?

Solution:

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

We can get one message, and try to find the same hash code of this message. We should use brute-force to find another message which has the same hash code with it. The attack requires about 2^m computations.

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

We cannot get any message, and try to find two message with the same hash code. It is like to find a pair of messages rather than one message. This is the main difference with the target attack. Thus, using brute-force just need $2^{m/2}$ computations because of the birthday paradox.

2. For double DES $E_{k_2}(E_{k_1}M) = C$, using the birthday argument, by meeting-in-the-middle, one can

-Compute $E_{k_1}(M) = S$ for 2^{32} choices of k_1

-Compute $D_{k_2}(C) = T$ for 2^{32} choices of k_2

-because $|\{S\}||\{T\}| \simeq 2^{64}$, we find k_1, k_2, s.t. $E_{k_2}(E_{k_1}M) = C$

-i.e. the complexity of break double DES is about 2^{32}, not 2^{56}.

Is this correct, and why?

Solution:

It's not correct.

For meet-in-the-middle attack, for any given plaintext P, there are 2^{64} possible ciphertexts produced by Double DES.

But Double DES effectively has 112 bit key, so there are 2^{112} possible keys.

On average then, for a given plaintext, the number of different 112 bit keys that will produce a given ciphertext is $2^{112}/2^{64} = 2^{48}$

Thus the bottom line: a known plaintext attack will succeed against Double DES with an effort on order of 2^{56}.

In this case, the birthday paradox need one hash function, however, D and E are different functions because there subkey is different, so we cannot apply birthdat paradox in this case.

In conclusion, it's incorrect.