Daniel Frey

CS 4920-001

Assignment 6

4/25/18

**Problem 1: Hash Function DES**

DES already includes a one-way function, f, and an XOR: Ri = Li–1  f(Ri–1, Ki).

The function f maps a 32-bit R and a 48-bit K into a 32-bit output (i.e., an 80-bit input into a 32-bit output). This is a one-way function. Any hash function that produces a 32-bit output could be used for f. Decryption will still be valid for any one-way function f.

**Problem 2: One-Way Hash using RSA**

Given a two-block message B1, B2 and its hash RSAH(B1, B2), then it can be attacked by choosing an arbitrary block C1, and choose C2 such that:

C2 = RSA(C1) RSA(B1)  B2

then

RSA(C1)  C2 = RSA(C1)  RSA(C1)  RSA(B1)  B2

= RSA(B1)  B2

so

**RSAH(C1, C2)** = RSA[RSA(C1)  C2)] = RSA[RSA(B1)  B2]

= **RSAH(B1, B2)**

Which does not satisfy the weak collision resistance.

**Problem 3: CBC MAC**

For a one-block message, the MAC using CBC-MAC is *T* = E(*K*, *X*), where K is the key and X is the message block. For the two-block message, consider the first block is X and the second block is *X* ⊕ *T*. Then the MAC is E(*K*, [*T* ⊕ *X* ⊕ *T*]) = E(*K*, *X*) = *T*.

**Problem 4: CMAC**

1. Constants for block size 64-bits and 128-bits are R128 = 012010000111 and R64 = 05911011
2. Algorithm for left shift and XOR:  
   **1.** Let *L* = E(*K*, 0b).

**2.** If MSB1(*L*) = 0, then *K1* = *L* << 1;

Else *K*1= (*L* << 1) ⊕ *Rb*;

**3.** If MSB1(*K*1) = 0, then *K*2= *K*1<< 1;

Else *K*2= (*K*1<< 1) ⊕ *Rb*.

**Problem 5:**

1. A believes that she shares K`AB with B since her nonce came back in message 2 encrypted with a key only known to B.

B believes that he shares K`AB with A since NA was encrypted with K`AB, which could only be retrieved from message 2 by someone who knows K`AB.

A believe that K`AB is fresh since it is included in message 2 together with NA.

B believe that K`AB is fresh since he chose it himself.

1. Consider the following protocol:

*C*(*B*) →*A*: *E*(*Kbs* : *K’ab*;*A*)

*A*→*C*(B): *E*(*K’ab* : *Nb*)

*C*(B) →*A*: *E*(*K’ab* : *Nb* -1)

The adversary C will have fooled A into thinking she has communicated with B.

1. A possible solution is to include timestamps.