MATH 178 Homework #14

Tamir Enkhjargal

May 2019

Hashes and MACs

HASH 1.

We can use the fact that using AES as a hash is not an one-way function by decrypting first to find out encrypting keys. Here are some of our knowns:

$$aesenc(M1, IV) = c \tag{1}$$
$$aesenc(M2, c) = CT \tag{2}$$

Where IV is a bitstream of all 0s and CT is a bitstream of all 1s. Therefore, we can infer that:

$$aesdec(c, IV) = M1 \tag{1}$$
$$aesdec(CT, c) = M2 \tag{2}$$

Therefore, to find M1 and M2 through decrypting, we can choose an arbitrary c. I chose $c = 0101010101010101$. Therefore:

$$aesdec(c, IV) = \mathbf{0110110101000010} = M1 \tag{1}$$
$$aesdec(CT, c) = \mathbf{0110111100010011} = M2 \tag{2}$$

$$aesenc(M1, IV) = 0101010101010101 = c \tag{3}$$
$$aesenc(M2, c) = 1111111111111111 = CT \tag{4}$$

By choosing a c I was able to find a $M1$ and $M2$ that would work. There is also a check above.

HASH 1.5

If Eve knows both the ciphertext block and the plaintext block, and she is **not** able to determine the key, then rather than using symmetric key cryptography, such as AES, in ECB mode, we can use the IV/key and use that same key on every single block of PT to output the CT.

In other words, use the IV as the key for every single PT$_i$ block, get an output as CT$_i$ block. This blocks the ability for Eve to be able to retrace backwards or forwards from the CT to the PT or vice versa. This is all relying on the fact that if there was a single PT to CT encryption using a key, that it is impossible to find the key.

MAC 1.

```
key = \r mackey.txt
a=ASCII(me)
b=ASCII(mo)
c=ASCII(ry)
x=aesenc(a,key)
y=aesenc(b,x)
z=aesenc(c,y)=[1,0,1,1,0,1,1,0,1,1,1,0,0,1,1,0]
```