### Tutorial 2: Symmetric Key Crypto

1. Suppose that Alice uses a stream cipher to encrypt plaintext *P,* obtaining ciphertext C, and Alice then sends *C* to Bob. Suppose that Trudy happens to know the plaintext *P,* but Trudy does not know the key *K* that was used in the stream cipher.

a. Show that Trudy can easily determine the keystream that was used to encrypt *P.*

b. Show that Trudy can, in effect, replace *P* with plaintext of her choosing, say, *P'.* That is, show that Trudy can create a ciphertext message C’ so that when Bob decrypts *C'* he will obtain *P'.*

1. The RC4 cipher consists of a lookup table *S,* which contains 256 byte values, and two indices, *i* and *j.*

a. The lookup table *S* is initialized to contain the identity permutation 0,1,2,..., 255 and at each step of the algorithm, *S* contains a permutation. How is this achieved? That is, why does *S* always contain a permutation?

b. Where is RC4 used in the real world? **[homework]**

1. This problem deals with a Feistel Cipher.

a. Give the definition of a Feistel Cipher.

b. Is DES a Feistel Cipher?

c. Is AES a Feistel Cipher?

d. Why is the Tiny Encryption Algorithm, TEA, "almost" a Feistel Cipher?

1. Consider a Feistel cipher with four rounds. Then the plaintext is denoted as *P* = (Lo, Ro) and the corresponding ciphertext is C = (L4, R4). What is the ciphertext C, in terms of *Lo,* Ro*,* and the subkey, for each of the following round functions?

a. **F(Ri-1,Ki) = 0**

b. **F(Ri-1,Ki) = Ri-1**

c. **F(Ri-1,Ki) = Ki**

d. **F(Ri-1,Ki) = Ri-1 Ki**

1. This problem deals with the DES cipher.

a. How many bits in each plaintext block?

b. How many bits in each ciphertext block?

c. How many bits in the key?

d. How many bits in each subkey?

e. How many rounds?

f. How many S-boxes?

g. An S-box requires how many bits of input?

h. An S-box generates how many bits of output? **[homework]**

1. AES consists of four functions in three layers.
2. Which of the four functions are primarily for confusion and which are primarily for diffusion? Justify your answer.
3. Which of the three layers are for confusion and which are for diffusion? Justify your answer.

**[homework]**

1. Implement the Tiny Encryption Algorithm (TEA).

a. Use your TEA algorithm to encrypt the 64-bit plaintext block

0x0123456789ABCDEF

using the 128-bit key

0xA56BABCD00000000FFFFFFFFABCDEF01.

Decrypt the resulting ciphertext and verify that you obtain the

original plaintext.

b. Using the key in part a, encrypt and decrypt the following message

using each of the three block cipher modes discussed in the course.

(ECB mode, CBC mode, and CTR mode).

*Four score and seven years ago our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal.*

**[homework]**

1. The formula for counter mode encryption is

**Ci = Pi E(IV + i, K).**

Suppose instead we use the formula

**Ci = Pi E(K, IV + i).**

Is this secure? If so, why? If not, why not?

1. Suppose that we use a block cipher to encrypt according to the rule

**C0 = IV E(P0, K), C1 = C0 E(P1, K), C2 = C1 E(P2, K), …**

a. What is the corresponding decryption rule?

b. Give two security disadvantages of this mode as compared to CBC mode.

1. Suppose that Alice and Bob decide to always use the same IV instead of choosing IVs at random.

a. Discuss a security problem this creates if CBC mode is used.

b. Discuss a security problem this creates if CTR mode is used.

c. If the same IV is always used, which is more secure, CBC or CTR mode?

1. Suppose Alice uses DES to compute a MAC. She then sends the plaintext, the IV, and the corresponding MAC to Bob. If Trudy alters one block of plaintext before Bob receives it, what is the probability that Bob will not detect the change?
2. Suppose that you know a MAC value *X* and the key *K* that was used to compute the MAC, but you do not know the original message.

a. Show that you can construct a message *M* that also has its MAC equal to *X.* Note that we are assuming that you know the key *K* and the same key is used for both MAC computations.

b. How much of the message *M* are you free to choose?

**[homework]**