CS355: Cryptography **Fall 2005**

Homework #3

Due date & time: 10:30am on October 7, 2005. Hand in at the beginning of class (preferred), or email to the TA (wangq@purdue.edu) by the due time.

The Late Policy and Additional Instructions for HW1 still apply. Ask for clarifications if you have questions about them.

Problem 1 (15 pts) Suppose that a plaintext message of length 640 bits is encrypted using DES with one of the encryption modes, yielding a ciphertext of length 640 bits. The ciphertext is then sent to the receiver, who will decrypt the ciphertext. Now suppose that during the transmission bit 203 is flipped.

(a) How many **bits** MAY be incorrect after the decryption when using ECB?

(b) when using CBC?

(c) when using CFB with 8-bit blocks (8 bits are encrypted each round)?

(d) when using CFB with 16-bit blocks?

(e) when using CTR?

Problem 2 (12 pts) Recall that in a Feistel-network based block cipher, the round function $F(X, K_i)$ takes an input X and a round key K_i. Suppose that X is 32-bits and the Feistel network has 4 rounds. Furthermore, suppose that all round keys are 32 bits and the round function is defined as $F(X, K_i) = X \oplus K_i$, where $\oplus$ denotes bit XOR. We assume that the key for the entire cipher is a concatenation of the 4 round keys, i.e., the cipher key is 4*32 = 128 bits long.

a (6 pts) Let the plaintext be $L_0||R_0$, where L_0 and R_0 are 32-bit blocks, and $||$ denotes concatenation. Let the key be $K_1||K_2||K_3||K_4$. Let L_i and R_i be the output of the i'th round; then $L_4||R_4$ is the ciphertext. Write L_4 and R_4 in terms of $L_0, R_0, K_1, K_2, K_3, K_4$.

b (6 pts) Show that the resulting cipher is insecure again known-plaintext attack by describing an efficient algorithm that can decrypt any encrypted message given one plaintext/ciphertext pair.

Hint: You do not have to recover the key completely to be able to decrypt encrypted messages.

Problem 3 (10 pts) Exercise 7.(a) in Section 4.9 of the Textbook (On Pages 147–148). Note: You are only asked to do Part (a).

Problem 4 (13 pts) (This is essentially Exercise 6 in Section 4.9 with hints.)

Triple DES may be defined to use 2 keys, rather than 3 keys. Let E, D be the DES encryption/decryption algorithm. $\text{3DES}_{K_1,K_2}(M) = E_{K_1}(D_{K_2}(E_{K_1}(M)))$.

We now describe a chosen-plaintext attack against this version of 3DES. In this attack, we are first given two pairs $(M_1, C_1), (M_2, C_2)$, our goal is to recover the key (K_1, K_2), and we are allowed to issue additional chosen-plaintext queries during the attack.

Let $B_0 = \{0\}^{64}$ be a 64-bit block consisting of all 0's. We first build a table that has 2^{56} entries, one for each key $K \in \{0, 1\}^{56}$. Each entry in the table is a pair $(K, D_K(B_0))$. The table is sorted using

More on the back. Turn Over.

the second component of each entry, and we assume that it takes constant time to find an entry that a given value as the second component.

Then for each key $K \in \{0,1\}^{56}$, we request the ciphertext of $D_K(B_0)$, i.e., $3\text{DES}_{(K_1,K_2)}(D_K(B_0))$, we denote this ciphertext T_K.

a. (3 pts) Use the definition of 3DES in this problem, write out the equation involving T_K and $D_K(B_0)$.

b (5 pts) Finish the description of the attack. Hint: The main idea of the attack is as follows: when we are testing a K that happens to be K_1, then we need to quickly determine what are possible values of K_2 such that (K_1, K_2) can encrypt $D_K(B_0)$ into T_K.

f (2 pts) What is the worst-case running time of the attack?

g (3 pts) Assuming that we have enough storage, is this attack better than an exhaustive key search attack in practice? Why or why not?