Tanner Krebs, Gerardo Lopez, William Thornton
Math 314
10/05/17

COSC/MATH - 314

Assignment 5

Problem 1: Alice and Bob are using 3-DES with 3 keys. That is the encryption algorithm is $C = E_{K1}(E_{K2}(E_{K3}(P)))$ with the keys K1, K2, and K3 having 56 bits each. Suppose that Eve somehow knows K3 and also suppose that Eve can do 2^{56} DES encryptions in 5 hours.

(a.) Describe a meet-in-the-middle type of attack that Eve can mount in an efficient way to determine K1 and K2. You need to describe the 2 tables that Eve has to construct, specifying their entries and how large each table is. (Hint: For the meet-in-the-middle attack for 2-DES in which $C = E_{K2}(E_{K1}(P))$, we have described the 2 tables as follows. Table 1: Contains $D_{K2}(C)$ for all possible K2. Table 1 has size 2^{56} because there are these many K2's. Table 2: Contains $E_{K1}(P)$ for all possible K1. Table 1 has size 2^{56} because there are these many K1's. You need to make a similar description.)

(b.) Estimate the time the attack takes (you can ignore the time for all operations other than DES encryptions/decryptions) and explain how you arrived at your estimation.

Problem 2: Let K = 111...111 be the DES key consisting of all 1's. Show that $D_K(C) = E_K(C)$, for any block C of 64 bits. (Hint: Think of the difference between DES encryption and DES decryption and also of the key scheduling in DES, and then argue that the difference disappears when the key is the above K.)

Modes of operation exercises and AES exercises can be seen in original document FOR practice, solutions are not to be turned in.