Johns Hopkins ■ CS600.424: Network Security ■ Spring 2012

Homework 2 – Assignment
Due Date – March 2 in class

Instructions: Please do not submit handwritten assignment.

1. This problem provides a numerical example of encryption using a one round version of DES. We use the same bit pattern for the key K and the plaintext at the start which is :

   0000 0001 0010 0011 0100 0101 0110 0111
   1000 1001 1010 1011 1100 1101 1110 1111

   (a) Derive the first round key K_1.

   (b) Derive L_0 and R_0.

   (c) Expand R_0 to get $E[R_0]$, where E[.] is the expansion function of Table 3.2 of your textbook.

   (d) Calculate $A = E[R0] \oplus K_1$.

   (e) Group the 48 bit results of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.

   (f) Concatenate the results of (e) to get a 32 bit result, B.

   (g) Apply the permutation to get P(B)

   (h) Calculate $R_1 = P(B) \oplus L_0$.

   (i) Write down the ciphertext

2 (a) Using RSA, choose p=3, and q=11, and encode the word "dog" by encrypting each letter separately. Apply the decryption algorithm to the encrypted version to recover the original plaintext message. (b) Repeat part (a) but now encrypt "dog" as one message. [Hint – treat each letter as 5 bit number and then concatenate all 15 bits to get the number to encrypt.]

3. Consider RSA with p=5 and q=11.

   (a) what are *n* and *z*.

   (b) Let *e* be 3, why is this an acceptable choice for *e*.

   (c) Find *d* such that $de=1 \pmod z$ and $d<160$.

   (d) Encrypt the message m=8 using the key (n,e). Let *c* denote the corresponding ciphertext. Show all the work. [Hint: To simplify the calculations, use the fact:

   $$[(a \bmod n)\ (b \bmod n)] \bmod n = (a\ b) \bmod n$$