Patrick Austin

2/25/2018

CS 491 1001 Homework 1

1. Use of a DES calculator program available online that traces rounds produced the following output:

Thus the 64-bit output is L = 10011100011101111110100101111000 and 

R = 11000010010000100011000100111000. In hexadecimal, L = 9C77E978 and R = C2423138.

2. By using the provided tool, the plaintext is “MOTHER: WHAT DID YOU LEARN IN SCHOOL TODAY SON: HOW TO WRITE MOTHER: WHAT DID YOU WRITE? SON: I DON'T KNOW, THEY HAVEN'T TAUGHT US HOW TO READ YET!” and the key is 3.

3. Both of the primitive operations achieve one of the necessary elements of a strong cryptography system. Substitution increases confusion and transposition increases diffusion. By combining and repeating these two primitives in it is possible to create more and more confusion and diffusion. This ultimately achieves the avalanche effect, where small changes in plaintext cause large changes in ciphertext. In this fashion the relationship between the plaintext and the ciphertext becomes very difficult to decipher without the secret key and a high degree of security is maintained.

4. An entire 16 round cycle of DES will first require 8 time units for the initial permutation. Each of the 16 rounds will require 8 S-box permutations, a single P-box permutation, and a single expansion permutation. Therefore the 16 rounds will require 16(8\*8 + 4 + 8) = 1216 time units. The final permutation will require an additional 8 time units. Therefore the total number of time units needed for a full 16 round cycle of DES is equal to 8 + 1216 + 8 = 1232 time units.