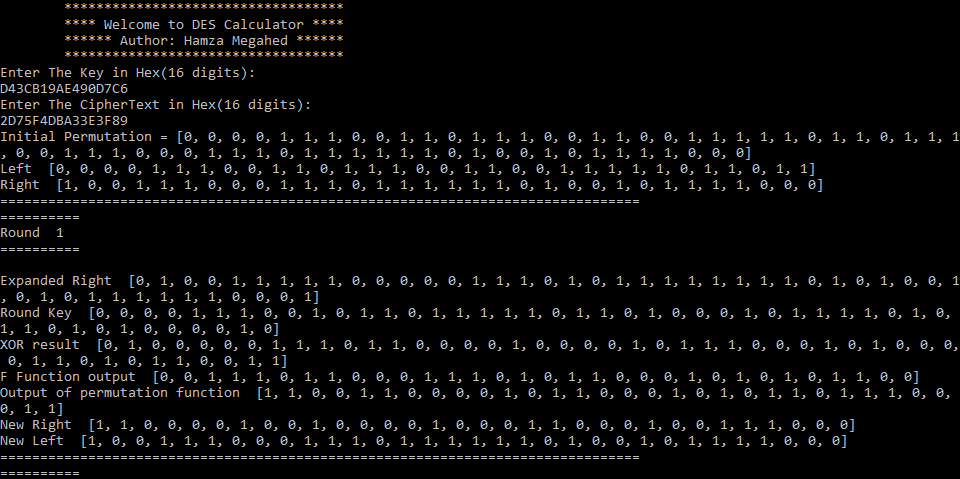
Patrick Austin

10/2/2017

CS 450 Homework 2

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. If we assume a current ordinary computer has a 3GhZ processor, and it takes 50 processor cycles to test one DES key, then it would take ( 256 \* 50 ) cycles / ( 3 x 109 ) cycles per second, or approximately 1.2 x 109 seconds to test every key. This equals about 38 years.

Likewise, with the same assumptions about the processor and cycles needed to test a key, it would take ( 2128 \* 50 ) cycles / ( 3 x 109 ) cycles per second, or approximately 5.7 x 1030 seconds to test every key. This equals about 1.8 x 1023 years.

4. Each round requires 6 P-box substitutions, 4 P-box permutations, and 1 expansion permutation. Thus each round requires 6\*8 + 4\*6 + 8 = 48 + 24 + 8 = 80 units of time. There are 16 rounds. Thus the 16 rounds take 80 \* 16 = 1280 units of time. 8 units of time are also used for the initial permutation and the final permutation, bringing the total number of units of time up to 8 + 1280 + 8 = 1296 units of time.