Title: CSCI 55500 Homework #2 report
Name: Zhihao Cao
Data: 9/28/2016
Instructor: Xukai Zou

Programming language: Java

Development software: Eclipse

Problem 1. DES

First, convert key and cypher text into binary. Then use a key generator function to produce 16 keys. Dividing the cypher bits into 64 bit block. Input blocks one by one into the decrypt function to retrieve decrypted bits. Then convert bits back into letter by every 8 bits. The decrypt function will do:

1. Perform the IP

2. Divide into L and R, each with 32 bit length

3. Perform 16 rounds manipulation

    a. $L_i = R_{i-1}$

    b. R_i ->Expand permutation to 48 bits

    c. R_i XOR K_{16-i}

    d. Divide R_i into 8 blocks and perform substitution using 8 parameter boxes

    e. Perform P permutation on R_i

    f. R_i XOR L_{i-1}

4. Combine $R_{16}L_{16}$

5. Perform inverse IP

6. Get output

Problem 2. RAS

Perform Pollard p-1 algorithm to find p. Then, find q by n/p, find phi-n by (p-1)(q-1), find a by b^{-1} mod n. Once all the parameters are derived, fetch the cipher text line by line and perform $x = y^a \bmod n$. x should be padding to even length and use digits from left to right to lookup the matrix table to retrieve normal English text.

Problem 3. Rabin

1. a) $e_k(x) = 32767^2 \bmod n$ to calculate y = 17559.
   b) Use CRT to find four possible decryptions.
   $a_1 = y^{(p-1)/4}$
   $a_2 = -y^{(p-1)/4}$
   $a_3 = y^{(q-1)/4}$
   $a_4 = -y^{(q-1)/4}$
   $M = p*q = n$
   $m_1 = p = 199$
   $m_2 = q = 211$
   $M_1 = M / m_1$
   $M_2 = M / m_2$
   $y_1 = M_1^{-1} \bmod m_1$
   $y_2 = M_2^{-1} \bmod m_2$
   $x_1 = (a_1 M_1 y_1 + a_3 M_2 y_2) \bmod M = 32767$
   $x_2 = (a_1 M_1 y_1 + a_4 M_2 y_2) \bmod M = 20827$
   $x_3 = (a_2 M_1 y_1 + a_3 M_2 y_2) \bmod M = 21162$
   $x_4 = (a_2 M_1 y_1 + a_4 M_2 y_2) \bmod M = 9222$

   Then do the encryption again using these for x to verify.

2. a) $e_k(x) = x(x + B) = 16027$
   b)