**CSC2056 Cybersecurity Fundamentals Practical 2 – S-DES**

1. Implement the S-DES algorithm in Java.
2. Using the key K = 1111011000 encrypt the plaintext ”ENIGMACODE”.
3. Output binary string for each major stage of algorithm and record your answers.

The correct output for the first letter E of the plaintext is:

k1 = 11010101

k2 = 01100101

Plain Text = E

Plain Text Binary = 01000101

Initial permutation = 11000100

F(R,K1) = 0001

fk1 = 11010100

swap fk1 = 01001101

F(R,K2) = 0000

fk2 = 01001101

Cipher Binary = 00010111

**Guidance for S-DES Cipher**

1. Declare and assign key and P10
2. Declare and initialise array for k1 and k2
3. Write KeyGeneration() method for calculating K1 and K2
4. Initialise plaintext string variable and set equal to “ENIGMACODE”
5. Use for loop to read in each letter of plaintext
6. Encode the plain text letter into a binarystring
7. Implement InitialPermutation() method
8. Implement F(R,K1) function method
9. Implement fk1() method
10. Perform swap operation on fk1 output
11. Perform Mapping F(R,k2)
12. Implement fk2() method
13. Implement InversePermutation() method

Further Guidelines

To convert a plaintext character to a binary array use the following:

Use charAt() method to access character

Cast char to int

Use method toBinaryString from int class

Declare and initialise int array of size 8

Read binary string at position i using charAt()

Convert to char 1 or 0 by subtracting 48 and cast to int

Note 48 is the ASCII encoding for 0 and 49 is for 1.

To implement the permutations you will need a for loop to index the permutation arrays holding the ordering. Then use this to index the bit arrays you want to reorder.

For shift operations you will need a combination of for loop and if else.

Also to implement XOR between bytes use a for loop to iterate through each bit.