George Beltran

Albert Ramirez

Kayleen Ponce

CS4780 Project 1

**SDES**

In order to run the SDES a run method was made and with the given rawykeys, plaintext, and ciphertext. Then a Project1Runner class is made, this class is to run the SDES and so that it doesn't compile the answer an infinite amount of times.

Raw Key Plaintext Ciphertext DecipheredText

00000 00000 1010 1010 0001 0001 1010 1010

11100 01110 1010 1010 1100 1010 1010 1010

11100 01110 0101 0101 0111 0000 0101 0101

11111 11111 1010 1010 0000 0100 1010 1010

00000 00000 0000 0000 1111 0000 0000 0000

11111 11111 1111 1111 0000 1111 1111 1111

00000 11111 0000 0000 0100 0011 0000 0000

00000 11111 1111 1111 1110 0001 1111 1111

10001 01110 0011 1000 0001 1100

10001 01110 0000 1100 1100 0010

00100 11111 1111 1100 1001 1101

00100 11111 1010 0101 1001 0000

**Triple SDES**

In order to run the TripleSDES a run method was made and with the given rawykeys, plaintext, and ciphertext. Then a Project1Runner class is made, this class is to run the TripleSDES and so that it doesn't compile the answer an infinite amount of times.

Raw Key1 Raw Key2 Plaintext CipherText

00000 00000 00000 00000 0000 0000 1111 0000

10001 01110 01101 01110 1101 0111 1011 1001

10001 01110 01101 01110 1010 1010 1110 0100

11111 11111 11111 11111 1010 1010 0000 0100

10001 01110 01101 01110 1111 1101 1110 0110

10111 01111 01101 01110 0100 1111 0101 0000

00000 00000 00000 00000 0101 0010 1000 0000

11111 11111 11111 11111 0010 0101 1001 0010

**Cracking SDES and TripleSDES**

In order to run the Cracking SDES and Cracking TripleSDES a run method was made and with the given rawykeys, plaintext, and ciphertext. Then a Project1Runner class is made, this class is to run the Cracking SDES and Cracking TripleSDES and so that it doesn't compile the answer an infinite amount of times.

For the second question and third question you will be asked to type “all”, “section”, or “answer”. This is for you to chose if you want to see “all” of the values that are in the CASCII string and to see the answer too. Or if you chose “section” you’ll only see the section of the values that are being looked for and you'll see a couple other values, you'll also see the answer. If “answer” is chosen then you'll only see the answer, no other values.

Question # 3.1

The plaintext in CASCII.

CRYPTOGRAPHY

The byte array of the plain text.

1100 0010 0110 0110 0001 0010 1111 1011

1000 1001 1000 0000 0100 0101 0011 0000

The byte array of the cipher text.

0110 0001 1100 1010 1011 0110 1111 0100

1100 0101 0111 0110 1111 1100 0111 0111

The cipher text in CASCII.

F?TZVWLTN,O?

Question # 3.2

756. key = { 1,0,1,1,1,1,0,1,0,0 } -> WHOEVER THINKS HIS PROBLEM CAN BE SOLVED USING CRYPTOGRAPHY, DOESN'T UNDERSTAND HIS PROBLEM AND DOESN'T UNDERSTAND CRYPTOGRAPHY. ATTRIBUTED BY ROGER NEEDHAM AND BUTLER LAMPSON TO EACH OTHER

Question # 3.3

922979. key 1 = { 1,1,1,0,0,0,0,1,0,1 } key 2 = { 0,1,0,1,1,0,0,0,1,1 } -> THERE ARE NO SECRETS BETTER KEPT THAN THE SECRETS THAT EVERYBODY GUESSES.







