Project Name: Simulate DES

Designer: Junyan Dai

Instructor: Dr. Pinata Winoto

Course: MATH 3815

Date: 2018/6/10

**Introduction:**

This program purposes on simulating The Data Encryption Standard(DES), which is the most popular cryptographical algorithm in 1980s. Although DES now is replaced by other algorithms like AES, it becomes a relatively worthwhile study topic in learning cryptography.

**Flowchart:**

**Encryption**

String binary Ciphertext

IP-1(plaintext)

key\_schedule(String key, long[] k)

48-bit k[1] k[2] k[3] …… k[16]

16-round function

64 bit key

IP(plaintext)

StrToAscii(plaintext)

String Binary plaintext

String plaintext

**Decryption**

String binary Ciphertext

key\_schedule(String key, long[] k)

64 bit key

String plaintext

IP-1(String binary Ciphertext)

IP(String binary Ciphertext)

AsciiToStr()

48-bit k[1] k[2] k[3] …… k[16]

16-round function

**Functions:**

1) Encryption/decryption

2) key\_schedule

--including PC-1 and Transforms

3) f()

--including Expansion and substitutions

4) transform()

--here we split the key, rotate both left and right one, produce subkeys

5) permutation()

-- there are a few permutations in DES. We create one function to apply all permutations in DES

6) addzero()

-- put zero in the front of the string to enough length.

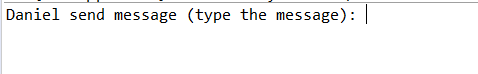
--e.g. when converting an integer num 2 to a 32-bit binary string. Using Integer.toBinaryString(num), we’ll get a string “10” in length 2 not 32. Thus, we create this function to put 30 more bits in the left of the string.

7) StrToAscii()

8) AsciiToStr()

**Output:**

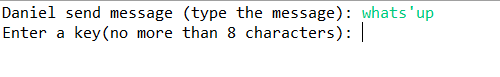
First, run this program. It requires to type some messages.



For example I entered: whats’up

Click ENTER

It asks me to enter a key. No more than 8 characters means no more than 64bits



Set a key and click ENTER

