Project Name: Simulate DES

Designer: Junyan Dai

Instructor: Dr. Pinata Winoto

Course: MATH 3815

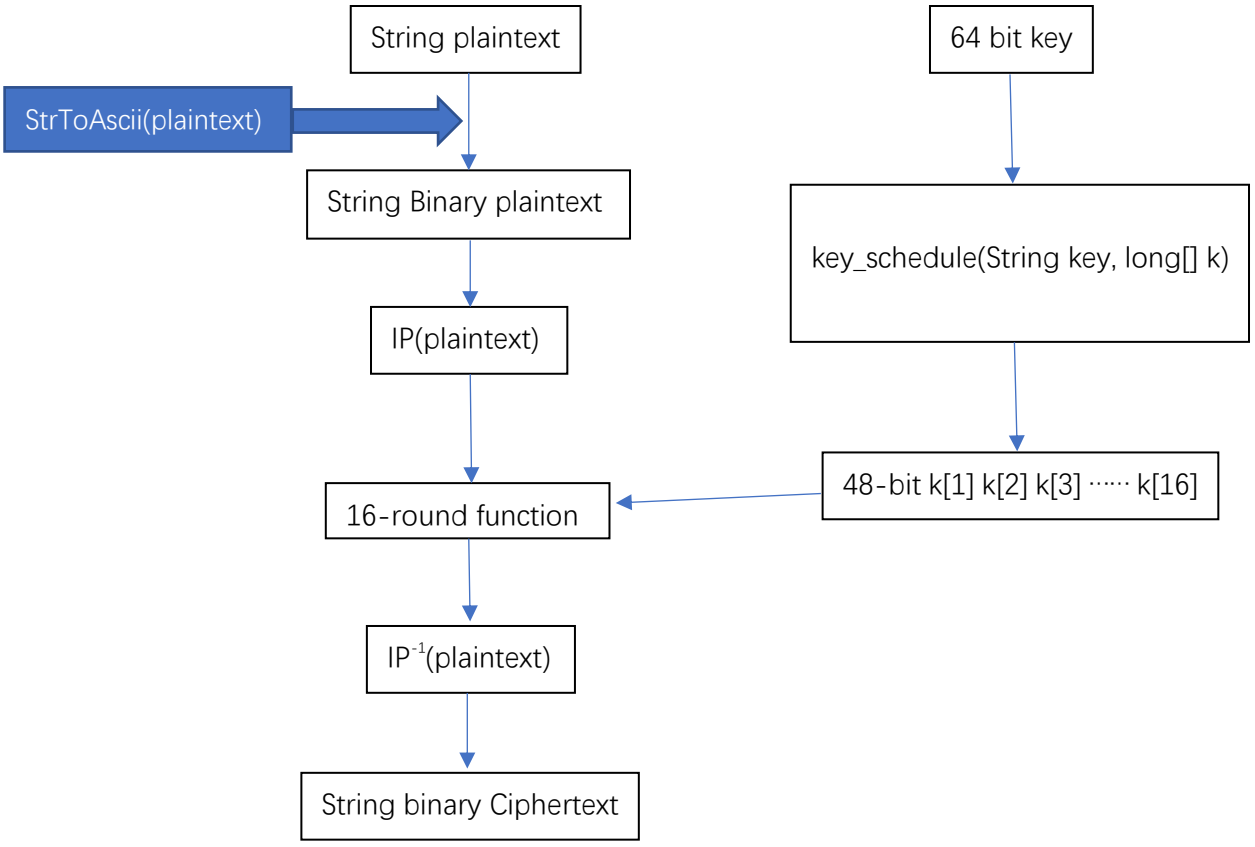
Date: 2018/6/10

Introduction:

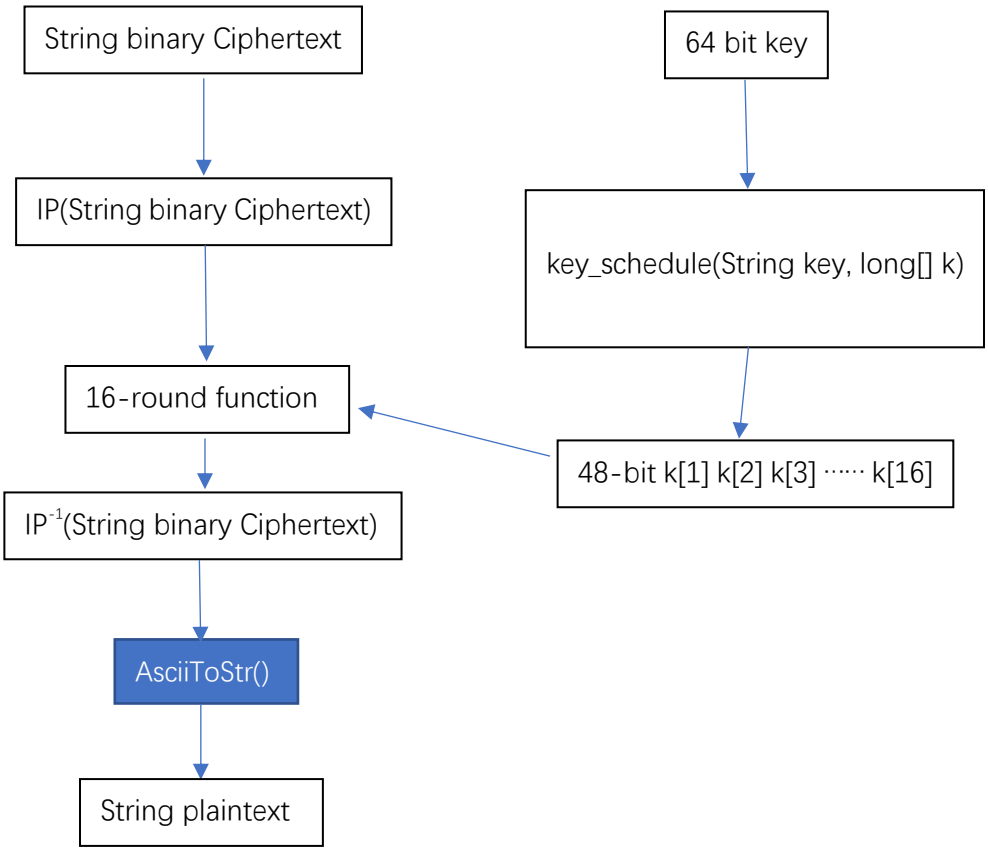
This program purposes on simulating The Data Encryption Standard(DES), which is the most popular cryptographical algorithm in 1980s. Although DES now is replaced by other algorithms like AES, it becomes a relatively worthwhile study topic in learning cryptography.

Flowchart:

Encryption



Decryption



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.

```
Daniel send message (type the message):
```

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

```
Daniel send message (type the message): whats'up
Enter a key(no more than 8 characters):
```

Set a key and click ENTER

```
Daniel send message (type the message): whats'up
Enter a key(no more than 8 characters): Dai123
Encrypting...
ciphertext:0111100000000010011110111111111110011111010010111110110001011100100110010000101000001001101000110100011111100000111101011001110101
Decrypting...
Wangyu recieve the message: whats'up
```