Lab4 DES Block Cipher Internals & Modes of Use

Team member

- 20171847118 金正旭
- 20171847121 李昊淼
- 20171847127 刘思颖

Lab Environment

DES block cipher calculator

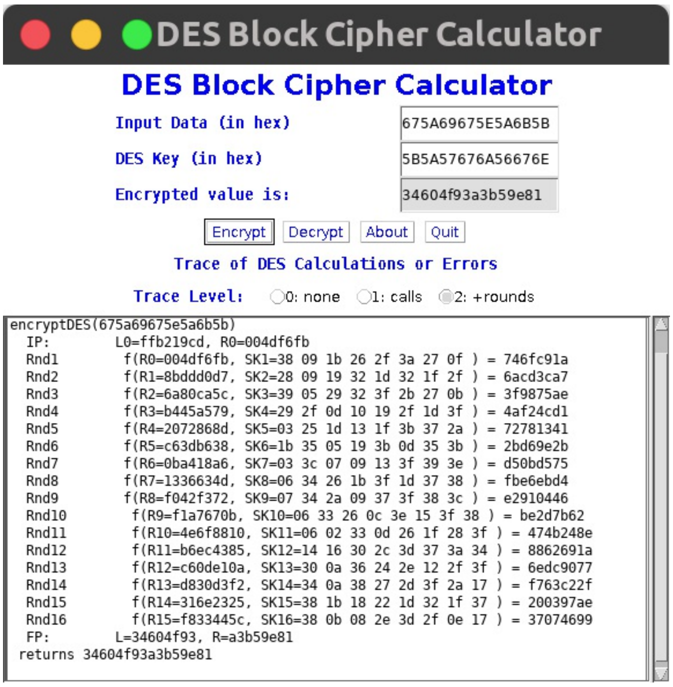
Archivment

1. understand the internal of the DES encryption
2. understand the process of CBC and CTR encryption

1. Proof of DES(Data Encryption Standard) Reversibility & Diffusion

```
Key:5B5A57676A56676E
Plaintext:675A69675E5A6B5B
Ciphertext:974AFFBF86022D1F
```

a. Input key and plaintext, press encrypt button to get ciphertext



DES Block Cipher Calculator
DES Block Cipher Calculator
Encrypt
Decrypt
About
Quit
Trace of DES Calculations or Errors

Input Data (in hex) 675A69675E5A6B5B

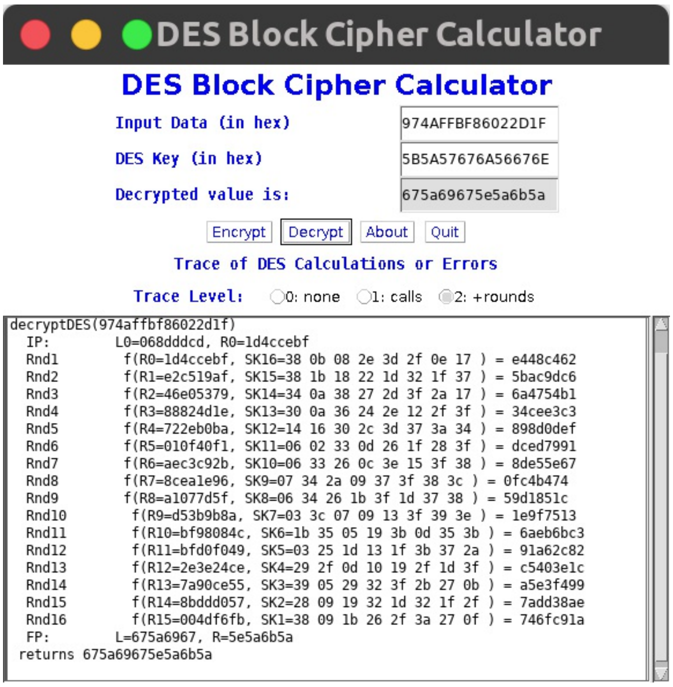
DES Key (in hex) 5B5A57676A56676E

Encrypted value is: 34604f93a3b59e81

Trace Level: ○0: none ○1: calls ●2: +rounds

```
encryptDES(675a69675e5a6b5b)
  IP:        L0=ffb219cd, R0=004df6fb
  Rnd1        f(R0=004df6fb, SK1=38 09 1b 26 2f 3a 27 0f ) = 746fc91a
  Rnd2        f(R1=8bddd0d7, SK2=28 09 19 32 1d 32 1f 2f ) = 6acd3ca7
  Rnd3        f(R2=6a80ca5c, SK3=39 05 29 32 3f 2b 27 0b ) = 3f9875ae
  Rnd4        f(R3=b445a579, SK4=29 2f 0d 10 19 2f 1d 3f ) = 4af24cd1
  Rnd5        f(R4=2072868d, SK5=03 25 1d 13 1f 3b 37 2a ) = 72781341
  Rnd6        f(R5=c63db638, SK6=1b 35 05 19 3b 0d 35 3b ) = 2bd69e2b
  Rnd7        f(R6=0ba418a6, SK7=03 3c 07 09 13 3f 39 3e ) = d50bd575
  Rnd8        f(R7=1336634d, SK8=06 34 26 1b 3f 1d 37 38 ) = fbe6ebd4
  Rnd9        f(R8=f042f372, SK9=07 34 2a 09 37 3f 38 3c ) = e2910446
  Rnd10        f(R9=f1a7670b, SK10=06 33 26 0c 3e 15 3f 38 ) = be2d7b62
  Rnd11        f(R10=4e6f8810, SK11=06 02 33 0d 26 1f 28 3f ) = 474b248e
  Rnd12        f(R11=b6ec4385, SK12=14 16 30 2c 3d 37 3a 34 ) = 8862691a
  Rnd13        f(R12=c60de10a, SK13=30 0a 36 24 2e 12 2f 3f ) = 6edc9077
  Rnd14        f(R13=d830d3f2, SK14=34 0a 38 27 2d 3f 2a 17 ) = f763c22f
  Rnd15        f(R14=316e2325, SK15=38 1b 18 22 1d 32 1f 37 ) = 200397ae
  Rnd16        f(R15=f833445c, SK16=38 0b 08 2e 3d 2f 0e 17 ) = 37074699
  FP:        L=34604f93, R=a3b59e81
 returns 34604f93a3b59e81
```

b. Input key and ciphertext, press decrypt button to get plaintext



DES Block Cipher Calculator

Input Data (in hex) 974AFFBF86022D1F

DES Key (in hex) 5B5A57676A56676E

Decrypted value is: 675a69675e5a6b5a

Trace of DES Calculations or Errors

Trace Level: ○0: none ○1: calls ●2: +rounds

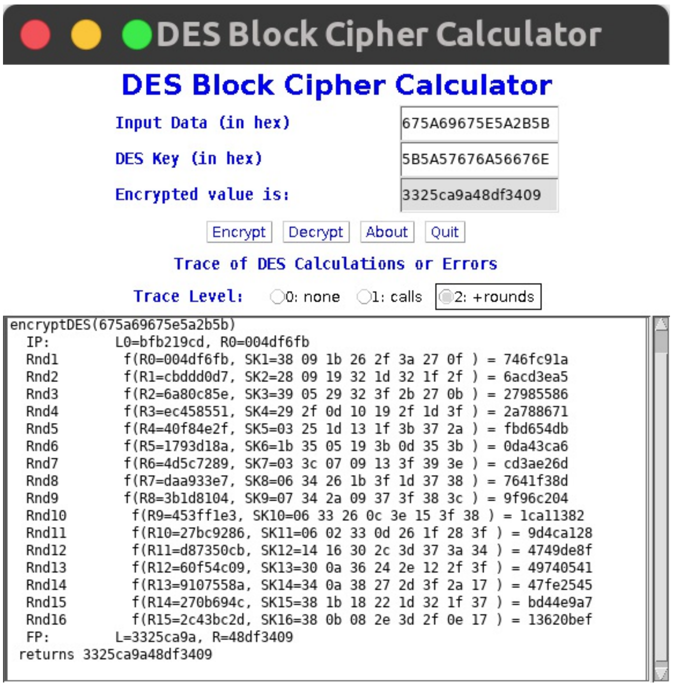
```
decryptDES(974affbf86022d1f)
  IP:        L0=068dddcd, R0=1d4ccebf
  Rnd1        f(R0=1d4ccebf, SK16=38 0b 08 2e 3d 2f 0e 17 ) = e448c462
  Rnd2        f(R1=e2c519af, SK15=38 1b 18 22 1d 32 1f 37 ) = 5bac9dc6
  Rnd3        f(R2=46e05379, SK14=34 0a 38 27 2d 3f 2a 17 ) = 6a4754b1
  Rnd4        f(R3=88824d1e, SK13=30 0a 36 24 2e 12 2f 3f ) = 34cee3c3
  Rnd5        f(R4=722eb0ba, SK12=14 16 30 2c 3d 37 3a 34 ) = 898d0def
  Rnd6        f(R5=010f40f1, SK11=06 02 33 0d 26 1f 28 3f ) = dced7991
  Rnd7        f(R6=aec3c92b, SK10=06 33 26 0c 3e 15 3f 38 ) = 8de55e67
  Rnd8        f(R7=8cea1e96, SK9=07 34 2a 09 37 3f 38 3c ) = 0fc4b474
  Rnd9        f(R8=a1077d5f, SK8=06 34 26 1b 3f 1d 37 38 ) = 59d1851c
  Rnd10        f(R9=d53b9b8a, SK7=03 3c 07 09 13 3f 39 3e ) = 1e9f7513
  Rnd11        f(R10=bf98084c, SK6=1b 35 05 19 3b 0d 35 3b ) = 6aeb6bc3
  Rnd12        f(R11=bfd0f049, SK5=03 25 1d 13 1f 3b 37 2a ) = 91a62c82
  Rnd13        f(R12=2e3e24ce, SK4=29 2f 0d 10 19 2f 1d 3f ) = c5403e1c
  Rnd14        f(R13=7a90ce55, SK3=39 05 29 32 3f 2b 27 0b ) = a5e3f499
  Rnd15        f(R14=8bddd057, SK2=28 09 19 32 1d 32 1f 2f ) = 7add38ae
  Rnd16        f(R15=004df6fb, SK1=38 09 1b 26 2f 3a 27 0f ) = 746fc91a
  FP:        L=675a6967, R=5e5a6b5a
 returns 675a69675e5a6b5a
```

c. Reverse one bit in plaintext(last)

We got the palintext 675A69675E5A6B5B, and convert it to binary code:

```
|  #  |  Raw  |       Binary       |
|:---:|:-----:|:-----------------:|
|  0  | 67 5A | 0110011101011010 |
|  2  | 69 67 | 0110100101100111 |
|  4  | 5E 5A | 0101111001011010 |
|  6  | 6B 5B | 0110101101011011 | <=== convert it to 0010101101011011
```

Then get a new hex code 675A69675E5A `2` B5B.



DES Block Cipher Calculator

Input Data (in hex) 675A69675E5A2B5B

DES Key (in hex) 5B5A57676A56676E

Encrypted value is: 3325ca9a48df3409

Trace of DES Calculations or Errors

Trace Level: ○0: none ○1: calls ●2: +rounds

```
encryptDES(675a69675e5a2b5b)
  IP:        L0=bfb219cd, R0=004df6fb
  Rnd1        f(R0=004df6fb, SK1=38 09 1b 26 2f 3a 27 0f ) = 746fc91a
  Rnd2        f(R1=cbddd0d7, SK2=28 09 19 32 1d 32 1f 2f ) = 6acd3ea5
  Rnd3        f(R2=6a80c85e, SK3=39 05 29 32 3f 2b 27 0b ) = 27985586
  Rnd4        f(R3=ec458551, SK4=29 2f 0d 10 19 2f 1d 3f ) = 2a788671
  Rnd5        f(R4=40f84e2f, SK5=03 25 1d 13 1f 3b 37 2a ) = fbd654db
  Rnd6        f(R5=1793d18a, SK6=1b 35 05 19 3b 0d 35 3b ) = 0da43ca6
  Rnd7        f(R6=4d5c7289, SK7=03 3c 07 09 13 3f 39 3e ) = cd3ae26d
  Rnd8        f(R7=daa933e7, SK8=06 34 26 1b 3f 1d 37 38 ) = 7641f38d
  Rnd9        f(R8=3b1d8104, SK9=07 34 2a 09 37 3f 38 3c ) = 9f96c204
  Rnd10        f(R9=453ff1e3, SK10=06 33 26 0c 3e 15 3f 38 ) = 1ca11382
  Rnd11        f(R10=27bc9286, SK11=06 02 33 0d 26 1f 28 3f ) = 9d4ca128
  Rnd12        f(R11=d87350cb, SK12=14 16 30 2c 3d 37 3a 34 ) = 4749de8f
  Rnd13        f(R12=60f54c09, SK13=30 0a 36 24 2e 12 2f 3f ) = 49740541
  Rnd14        f(R13=9107558a, SK14=34 0a 38 27 2d 3f 2a 17 ) = 47fe2545
  Rnd15        f(R14=270b694c, SK15=38 1b 18 22 1d 32 1f 37 ) = bd44e9a7
  Rnd16        f(R15=2c43bc2d, SK16=38 0b 08 2e 3d 2f 0e 17 ) = 13620bef
  FP:        L=3325ca9a, R=48df3409
 returns 3325ca9a48df3409
```

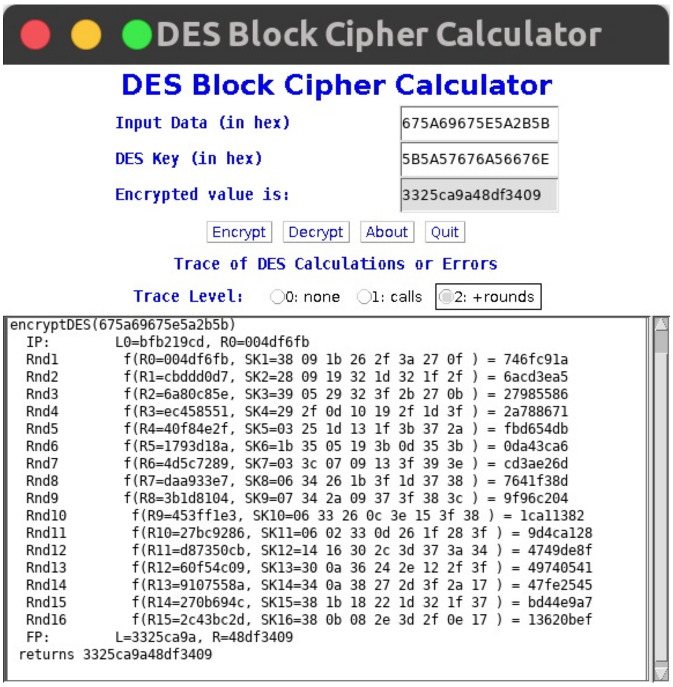
Notice code totally diiffernet than original code since Rnd2

d. Reverse one bit in ciphertext(last)

We got the ciphertext 974AFFBF86022D1F, and convert it to binary code:

```
| #  |  Raw  |      Binary      |
|:---:|:-----:|:----------------:|
| 0  | 97 4A | 1001011101001010 |
| 2  | FF BF | 1111111110111111 |
| 4  | 86 02 | 1000011000000010 |
| 6  | 2D 1F | 0010110100011111 | <=== convert it to 0110110100011111
```

Then get a new hex code 974AFFBF8602`6`D1F.


DES Block Cipher Calculator
DES Block Cipher Calculator
Encrypt
Decrypt
About
Quit
Trace of DES Calculations or Errors

Input Data (in hex) 675A69675E5A2B5B

DES Key (in hex) 5B5A57676A56676E

Encrypted value is: 3325ca9a48df3409

Trace Level: ○0: none ○1: calls ●2: +rounds

```
encryptDES(675a69675e5a2b5b)
  IP:        L0=bfb219cd, R0=004df6fb
  Rnd1        f(R0=004df6fb, SK1=38 09 1b 26 2f 3a 27 0f ) = 746fc91a
  Rnd2        f(R1=cbddd0d7, SK2=28 09 19 32 1d 32 1f 2f ) = 6acd3ea5
  Rnd3        f(R2=6a80c85e, SK3=39 05 29 32 3f 2b 27 0b ) = 27985586
  Rnd4        f(R3=ec458551, SK4=29 2f 0d 10 19 2f 1d 3f ) = 2a788671
  Rnd5        f(R4=40f84e2f, SK5=03 25 1d 13 1f 3b 37 2a ) = fbd654db
  Rnd6        f(R5=1793d18a, SK6=1b 35 05 19 3b 0d 35 3b ) = 0da43ca6
  Rnd7        f(R6=4d5c7289, SK7=03 3c 07 09 13 3f 39 3e ) = cd3ae26d
  Rnd8        f(R7=daa933e7, SK8=06 34 26 1b 3f 1d 37 38 ) = 7641f38d
  Rnd9        f(R8=3b1d8104, SK9=07 34 2a 09 37 3f 38 3c ) = 9f96c204
  Rnd10        f(R9=453ff1e3, SK10=06 33 26 0c 3e 15 3f 38 ) = 1ca11382
  Rnd11        f(R10=27bc9286, SK11=06 02 33 0d 26 1f 28 3f ) = 9d4ca128
  Rnd12        f(R11=d87350cb, SK12=14 16 30 2c 3d 37 3a 34 ) = 4749de8f
  Rnd13        f(R12=60f54c09, SK13=30 0a 36 24 2e 12 2f 3f ) = 49740541
  Rnd14        f(R13=9107558a, SK14=34 0a 38 27 2d 3f 2a 17 ) = 47fe2545
  Rnd15        f(R14=270b694c, SK15=38 1b 18 22 1d 32 1f 37 ) = bd44e9a7
  Rnd16        f(R15=2c43bc2d, SK16=38 0b 08 2e 3d 2f 0e 17 ) = 13620bef
  FP:        L=3325ca9a, R=48df3409
 returns 3325ca9a48df3409
```

2. Understanding of DES interal encryption

```
Key:5B5A57676A56676E
Plaintext:675A69675E5A6B5A
```

DES Block Cipher Calcuator return:

```
IP:     L0=ffb2194d, R0=004df6fb
Rnd1    f(R0=004df6fb, SK1=38 09 1b 26 2f 3a 27 0f ) = 746fc91a
Rnd2    f(R1=8bddd057, SK2=28 09 19 32 1d 32 1f 2f ) = 7add38ae
Rnd3    f(R2=7a90ce55, SK3=39 05 29 32 3f 2b 27 0b ) = a5e3f499
Rnd4    f(R3=2e3e24ce, SK4=29 2f 0d 10 19 2f 1d 3f ) = c5403e1c
Rnd5    f(R4=bfd0f049, SK5=03 25 1d 13 1f 3b 37 2a ) = 91a62c82
Rnd6    f(R5=bf98084c, SK6=1b 35 05 19 3b 0d 35 3b ) = 6aeb6bc3
Rnd7    f(R6=d53b9b8a, SK7=03 3c 07 09 13 3f 39 3e ) = 1e9f7513
Rnd8    f(R7=a1077d5f, SK8=06 34 26 1b 3f 1d 37 38 ) = 59d1851c
Rnd9    f(R8=8cea1e96, SK9=07 34 2a 09 37 3f 38 3c ) = 0fc4b474
Rnd10   f(R9=aec3c92b, SK10=06 33 26 0c 3e 15 3f 38 ) = 8de55e67
Rnd11   f(R10=010f40f1, SK11=06 02 33 0d 26 1f 28 3f ) = dced7991
Rnd12   f(R11=722eb0ba, SK12=14 16 30 2c 3d 37 3a 34 ) = 898d0def
Rnd13   f(R12=88824d1e, SK13=30 0a 36 24 2e 12 2f 3f ) = 34cee3c3
```

```
Rnd14   f(R13=46e05379, SK14=34 0a 38 27 2d 3f 2a 17 ) = 6a4754b1
Rnd15   f(R14=e2c519af, SK15=38 1b 18 22 1d 32 1f 37 ) = 5bac9dc6
Rnd16   f(R15=1d4ccebf, SK16=38 0b 08 2e 3d 2f 0e 17 ) = e448c462
FP:     L=974affbf, R=86022d1f
returns 974affbf86022d1f
```

Process:

1. We get Rnd1's answer 746fc91 , and then the HalfBlock will input in E-box to extend to 48 bits.
2. Use Subkey XOR the 48 bits message.
3. Convert the message to 8group and 6 bits peer group.
4. These groups will be input in S-box
5. Combine those answers and execute process P to get R0

```
SubKey:
hex: 5B5A57676A56676E
bin: 111000 001001 011011 100110 101111 111010 100111 001111
R0：
hex: 004df6fb
bin: 0000 0000 0100 1101 1111 0110 1111 1011
```

Input in E box:

```
100000 000000 001001 011001 011011 111110 101101 011111 110110
```

L0 XOR SK:

```
011000 001001 010010 111101 010001 010111 111000 111001
```

Input in S-box:

```
0101 1111 1101 0010 0101 1110 0000 0011
```

Input in P-box:

```
0111 0100 0110 1111 1100 1001 0001 1010
==> convert to hex: 746fc91a
```

3. Understanding of CBC and CTR

1. CBC

create a 24 bits message, assume IV=0, Key:5B5A57676A56676E

a. Use CBC encrpt message to get ciphertext.

```
message: JasonJin
=> hex: 6a61736f6e6a696e
=> bin: 0110101001100001
        0111001101101111
        0110111001101010
        0110100101101110
Key: 5B5A57676A56676E
C0: 113ad45eff4da8be
=> bin: 0001000100111010
        1101010001011110
        1111111101001101
        1010100010111110
M1: 69 6a 6b 6c 6d 6e 6f 70
=> bin: 0110100101101010
        0110101101101100
        0110110101101110
        0110111101110000

M1 ⊕C0: 0111100001010000
        1011111100110010
        1001001000100011
        1100011111001110  ==> hex: 7850bf329223c7ce

C1: 77e2cbe920e547db
=> bin: 0111011111100010
        1100101111101001
        0010000011100101
        0100011111011011

M2: 7172737475767778
=> bin: 0111000101110010
        0111001101110100
        0111010101110110
        0111011101111000

C1⊕M2 : 0000011010010000
        1011100010011101
        0101010110010011
        0011000010100011=> hex:0690b89d559330a3

C2 = d164732ce0638948

Ciphertext: 0113ad45eff4da8be 77e2cbe920e547db d164732ce0638948
```

b. Use CBC decrypt message to get plaintext.

```
D(k,C0)=6a61736f6e6a696e= M0
D(k,C1)=7850bf329223c7ce ⊕ C0 = M1=696a6b6c6d6e6f70
D(k,C2)=0690b89d559330a3 ⊕ C1 = M2=7172737475767778

plaintext: 6162636465666768 696a6b6c6d6e6f70 7172737475767778
```

2. CTR

create a 24 bits message, assume IV=0, Key:5B5A57676A56676E

c. Use CTR encrpt message to get ciphertext.

```
E (K,iv) : 7655744b71089ca2
E (K,iv+1) : fa56c2feb1750103
E (K,iv+2) : 4d4f18c5b58ab3de

对应二进制为
01110110  01010101  01110100  01001011  01110001  00001000  10011100  10100010

11111010  01010110  11000010  11111110  10110001  01110101  00000001  00000011

01001101  01001111  00011000  11000101  10110101  10001010  10110011  11011110


E (K,iv)     7655744b71089ca2  ⊕  M0
E (K,iv+1)   fa56c2feb1750103   ⊕  M1
E (K,iv+2)   4d4f18c5b58ab3de  ⊕  M2

==> C0:1737172f146efbca
    C1:8be445f9146efbca
    C2:3c3d6bb1c0fcc4a6

==> Ciphertext: 01737172f146efbca 8be445f9146efbca 3c3d6bb1c0fcc4a6
```

d. Use CTR encrpt message to get ciphertext.

```
C0⊕E (K,iv)  : 6162636465666768 = M0
C1⊕E (K,iv+1): 696a6b6c6d6e6f70 = M1
C2⊕E (K,iv+2): 7172737475767778 = M2
```