In [1]:
```
%run DES_sumbit.ipynb
```

In [15]:
```
print("processing DES algorithm")
import os,binascii
import random
import string

PRINT_FLAG = True

# time schedule
XOR_Operation_ = []
Int_2_bin_ = []
Permutation_table_ = []
Cycle_shift_left_ = []
Byte_2_Bit_ = []
Initial_Permutation_ = []
PC_1_Permutation_ = []
Ring_Shift_Left_ = []
PC_2_Permutation_ = []
Sub_key_creation_ = []
E_Expansion_ = []
S_Box_permutation_ = []
P_Expansion_ = []
Feistel_network_ = []
Cross_Iteration_Encryption_ = []
Cross_Iteration_Decryption_ = []
P_inverse_Permutation_ = []
DES_Encryption_ = []
DES_Decryption_ = []
Create_Secret_Key_ = []
To_Bit_String_ = []
To_Ascii_Char_ = []

#M="0000000100100011010001010110011110001001101010111100110111101111"#plaintext for testing
#K="0001001100110100010101110111100110011011101111001101111111110001"#Keys for testing
```

```
processing DES algorithm
```

In [16]:
```
letters = string.ascii_letters
M =  ''.join(random.choice(letters) for i in range(8))
```

```python
Key = createSecrteKey()
print("key is",Key)
K = ToBitString(Key)
print("plaintext is" , M)
coded_string = Encryption(ToBitString(M), K)
print("After encoding:" , ToAsciiChar(coded_string))
decipher_string = Decryption(coded_string, K)
print("After decoding" ,ToAsciiChar(decipher_string) )
```

```
key is aph@2s32
plaintext is ENDyxRIJ
> start Encrypt 64 bits plain text
> processing initial IP permutation
> processing cross iteration in cryption
> Createing 16 bits sub-key
> processing PC-1 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
```

```
                > processing P Expansion permutation
                > processing Feistel function
                > processing E Expansion permutation
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing P Expansion permutation
                > processing Feistel function
                > processing E Expansion permutation
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing P Expansion permutation
                > processing Feistel function
                > processing E Expansion permutation
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing P Expansion permutation
                > processing Feistel function
                > processing E Expansion permutation
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
                > processing P Expansion permutation
                > processing Feistel function
                > processing E Expansion permutation
                > processing S Box permutation with 6-4 transform
                > processing S Box permutation with 6-4 transform
```

```
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing P inverse Permutation
After encoding: (3I?`♂ë»
> start Decrypt 64 bits cipher text
> processing initial IP permutation
> processing the cross iteration in decryption
> Createing 16 bits sub-key
> processing PC-1 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing P inverse Permutation
After decoding ENDyxRIJ
```

In [17]:

```
decipher_string = Decryption(coded_string, K)
print("After decoding" ,ToAsciiChar(decipher_string) )
```

```
> start Decrypt 64 bits cipher text
> processing initial IP permutation
> processing the cross iteration in decryption
> Createing 16 bits sub-key
> processing PC-1 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing PC-2 permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing Feistel function
> processing E Expansion permutation
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing S Box permutation with 6-4 transform
> processing P Expansion permutation
> processing P inverse Permutation
After decoding ENDyxRIJ
```

In [18]:

```
PRINT_FLAG = False
```

In [41]:

```
from tqdm.notebook import tqdm
round_number = 5000
for i in tqdm(range(round_number)):
    letters = string.ascii_letters
    M =  ''.join(random.choice(letters) for i in range(8))

    Key = createSecrteKey()
    #print("key is",Key)
    K = ToBitString(Key)
    #print("明文是" , M)
    coded_string = Encryption(ToBitString(M), K)

    output_cipher = ToAsciiChar(coded_string)
    #print("加密后:" , ToAsciiChar(coded_string))

    decipher_string = Decryption(coded_string, K)
    output_decipher = ToAsciiChar(decipher_string)
    #print("解密后" ,ToAsciiChar(decipher_string) )
```

In [42]:

```
general_timestamp = {
    "To_Bit_String" : To_Bit_String_,
    "To_Ascii_Char" : To_Ascii_Char_,
    "Create_Secret_Key": Create_Secret_Key_,
}
```

In [43]:

```
encrpt_timestamp = {
    "XOR_Operation" :        XOR_Operation_,
    "Int_2_bin" :            Int_2_bin_,
    "Permutation_table" :    Permutation_table_,
    "Cycle_shift_left" :     Cycle_shift_left_,
    "Initial_Permutation" :  Initial_Permutation_,
    "PC_1_Permutation" :     PC_1_Permutation_,
    "PC_2_Permutation" :     PC_2_Permutation_,
    "Sub_key_creation" :     Sub_key_creation_,
    "E_Expansion" :          E_Expansion_,
    "S_Box_permutation" :    S_Box_permutation_,
    "P_Expansion" :          P_Expansion_,
    "Feistel_network" :      Feistel_network_,
    "Cross_Iteration_Encryption":Cross_Iteration_Encryption_,
    "P_inverse_permutation": P_inverse_Permutation_,
    "DES_Encryption" :       DES_Encryption_,
}
```

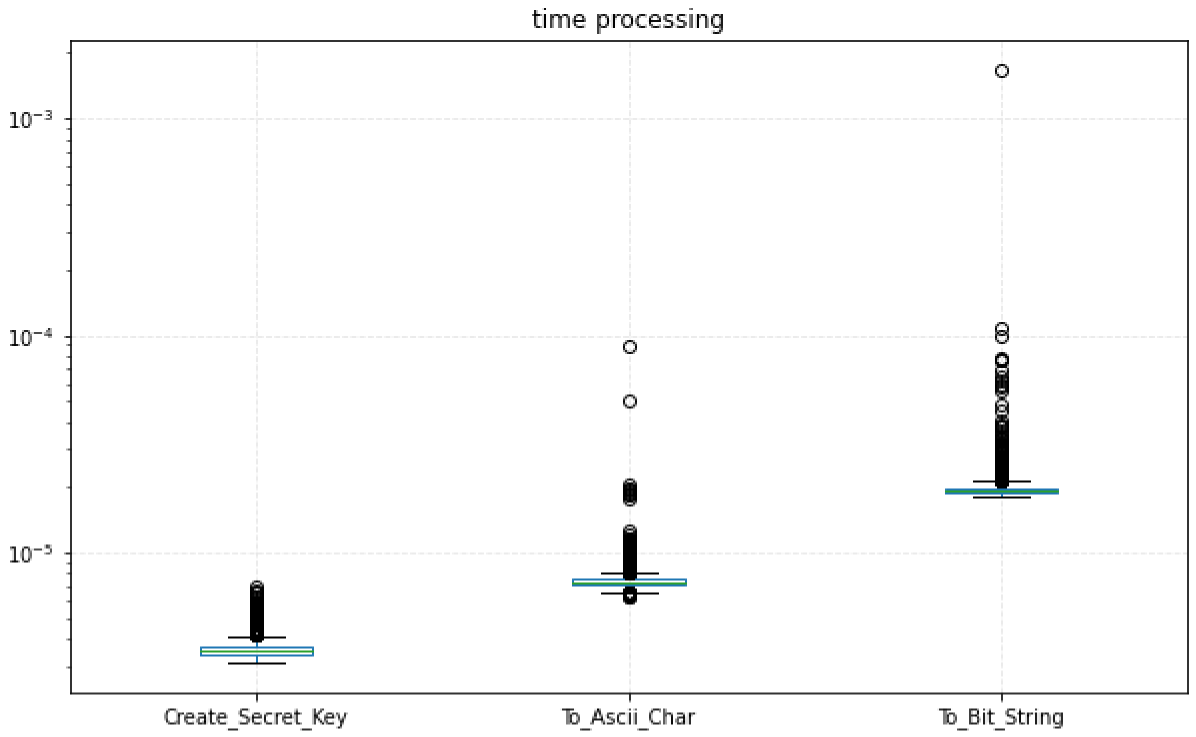
In [44]:

```
decrpt_timestamp = {
    "XOR_Operation" :        XOR_Operation_,
    "Int_2_bin" :            Int_2_bin_,
    "Permutation_table" :    Permutation_table_,
    "Cycle_shift_left" :     Cycle_shift_left_,
    "Initial_Permutation" :  Initial_Permutation_,
    "PC_1_Permutation" :     PC_1_Permutation_,
    "PC_2_Permutation" :     PC_2_Permutation_,
    "Sub_key_creation" :     Sub_key_creation_,
    "E_Expansion" :          E_Expansion_,
    "S_Box_permutation" :    S_Box_permutation_,
    "P_Expansion" :          P_Expansion_,
    "Feistel_network" :      Feistel_network_,
    "Cross_Iteration_Decryption":Cross_Iteration_Decryption_,
    "P_inverse_permutation": P_inverse_Permutation_,
    "DES_Decryption" :       DES_Decryption_,
}
```

In [45]:

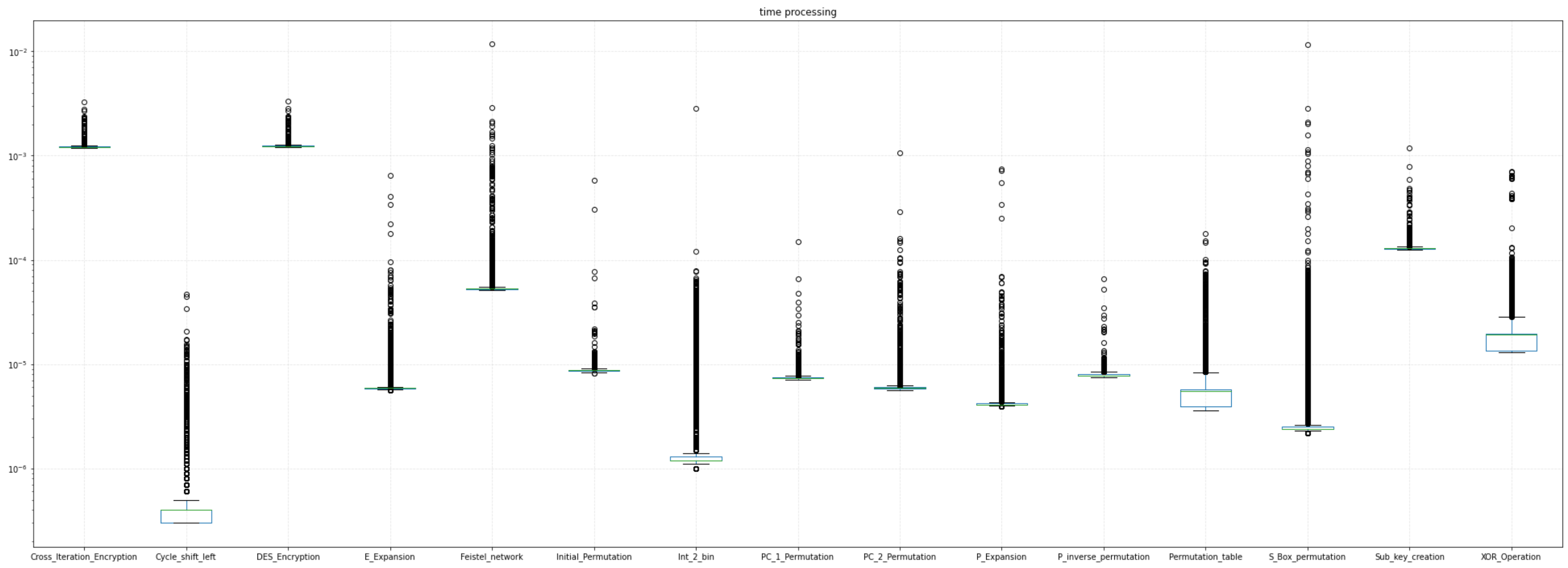
```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
from matplotlib.pyplot import figure


df = pd.DataFrame()
for item in general_timestamp.keys():
    df1 = pd.DataFrame(general_timestamp[item],columns=[item])
    df = pd.concat([df,df1],sort=True)
df.plot.box(title="time processing",logy=True,figsize=(10,6))
plt.grid(linestyle="--", alpha=0.3)
plt.show()
```



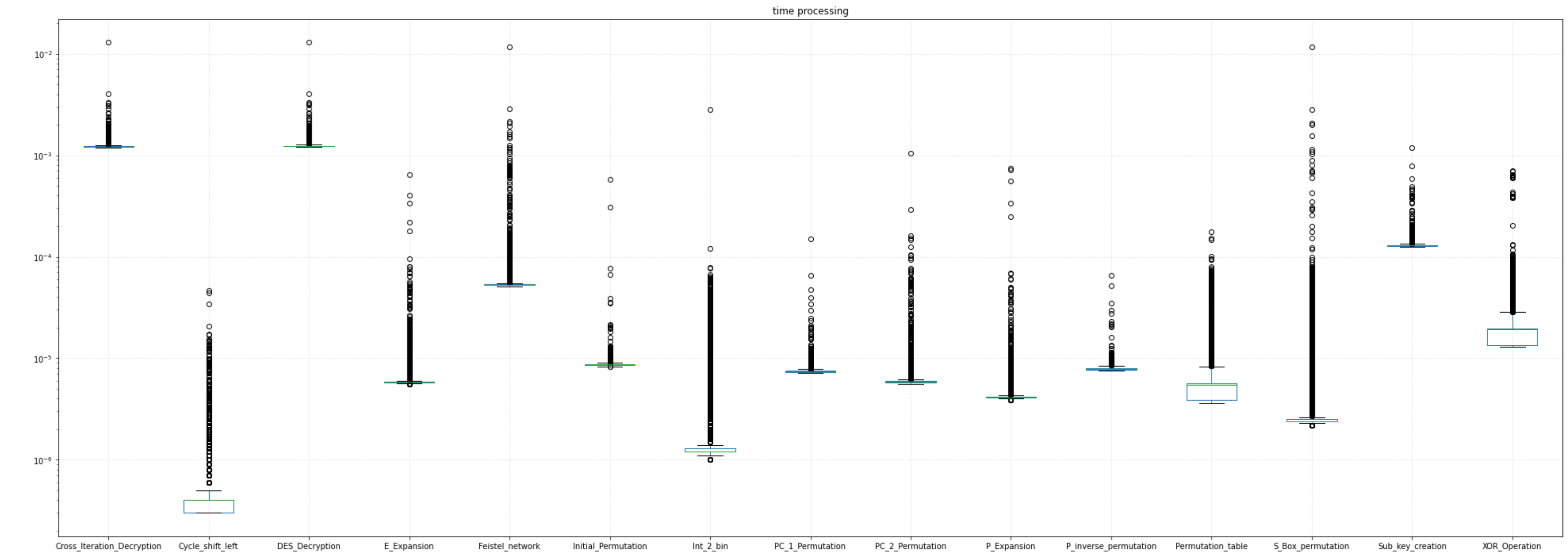
In [46]:

```
cipher_df = pd.DataFrame()
for item in encrpt_timestamp.keys():
    cipher_df1 = pd.DataFrame(encrpt_timestamp[item],columns=[item])
    cipher_df = pd.concat([cipher_df,cipher_df1],sort=True)
cipher_df.plot.box(title="time processing",logy=True,figsize=(34,12))
plt.grid(linestyle="--", alpha=0.3)
plt.show()
```



In [47]:

```
decipher_df = pd.DataFrame()
for item in decrpt_timestamp.keys():
    decipher_df1 = pd.DataFrame(decrpt_timestamp[item],columns=[item])
    decipher_df = pd.concat([decipher_df,decipher_df1],sort=True)
decipher_df.plot.box(title="time processing",logy=True,figsize=(34,12))
plt.grid(linestyle="--", alpha=0.3)
plt.show()
```



In [48]:
```
for items in general_timestamp.keys():
    print(df[items].describe())
```

```
count    10002.000000
mean         0.000020
std          0.000017
min          0.000018
25%          0.000019
50%          0.000019
75%          0.000020
max          0.001684
Name: To_Bit_String, dtype: float64
count    10002.000000
mean         0.000007
std          0.000001
min          0.000006
25%          0.000007
50%          0.000007
75%          0.000007
max          0.000088
Name: To_Ascii_Char, dtype: float64
count    5.001000e+03
mean     3.579704e-06
std      3.185749e-07
min      3.100000e-06
25%      3.400000e-06
```

```
50%      3.500000e-06
75%      3.700000e-06
max      7.000000e-06
Name: Create_Secret_Key, dtype: float64
```

In [49]:

```
for items in encrpt_timestamp.keys():
    print(cipher_df[items].describe())
```

```
count    320064.000000
mean          0.000017
std           0.000005
min           0.000013
25%           0.000014
50%           0.000019
75%           0.000020
max           0.000701
Name: XOR_Operation, dtype: float64
count    1.360272e+06
mean     1.289366e-06
std      2.497192e-06
min      9.999999e-07
25%      1.200000e-06
50%      1.200000e-06
75%      1.300000e-06
max      2.815400e-03
Name: Int_2_bin, dtype: float64
count    510102.000000
mean          0.000005
std           0.000001
min           0.000004
25%           0.000004
50%           0.000006
75%           0.000006
max           0.000178
Name: Permutation_table, dtype: float64
count    3.200640e+05
mean     3.769918e-07
std      2.174599e-07
min      2.999998e-07
25%      3.000000e-07
50%      3.999999e-07
75%      4.000001e-07
max      4.660000e-05
Name: Cycle_shift_left, dtype: float64
count    10002.000000
mean         0.000009
std          0.000007
min          0.000008
```

```
25%          0.000009
50%          0.000009
75%          0.000009
max          0.000582
Name: Initial_Permutation, dtype: float64
count    10002.000000
mean         0.000008
std          0.000002
min          0.000007
25%          0.000007
50%          0.000007
75%          0.000008
max          0.000149
Name: PC_1_Permutation, dtype: float64
count    160032.000000
mean          0.000006
std           0.000003
min           0.000006
25%           0.000006
50%           0.000006
75%           0.000006
max           0.001055
Name: PC_2_Permutation, dtype: float64
count    10002.000000
mean         0.000130
std          0.000018
min          0.000125
25%          0.000128
50%          0.000129
75%          0.000130
max          0.001179
Name: Sub_key_creation, dtype: float64
count    160032.000000
mean          0.000006
std           0.000002
min           0.000006
25%           0.000006
50%           0.000006
75%           0.000006
max           0.000647
Name: E_Expansion, dtype: float64
count    1.280256e+06
mean     2.503701e-06
std      1.133240e-05
min      2.200000e-06
25%      2.400000e-06
50%      2.400000e-06
75%      2.500000e-06
max      1.172090e-02
```

```
Name: S_Box_permutation, dtype: float64
count    160032.000000
mean          0.000004
std           0.000003
min           0.000004
25%           0.000004
50%           0.000004
75%           0.000004
max           0.000749
Name: P_Expansion, dtype: float64
count    160032.000000
mean          0.000054
std           0.000035
min           0.000051
25%           0.000053
50%           0.000053
75%           0.000054
max           0.011779
Name: Feistel_network, dtype: float64
count    5001.000000
mean        0.001222
std         0.000071
min         0.001190
25%         0.001204
50%         0.001213
75%         0.001223
max         0.003267
Name: Cross_Iteration_Encryption, dtype: float64
count    1.000200e+04
mean     7.913347e-06
std      9.378640e-07
min      7.500000e-06
25%      7.700000e-06
50%      7.800000e-06
75%      8.000000e-06
max      6.560000e-05
Name: P_inverse_permutation, dtype: float64
count    5001.000000
mean        0.001243
std         0.000072
min         0.001209
25%         0.001224
50%         0.001233
75%         0.001243
max         0.003330
Name: DES_Encryption, dtype: float64
```

In [50]:

```
for items in decrpt_timestamp.keys():
    print(decipher_df[items].describe())
```

```
count    320064.000000
mean          0.000017
std           0.000005
min           0.000013
25%           0.000014
50%           0.000019
75%           0.000020
max           0.000701
Name: XOR_Operation, dtype: float64
count    1.360272e+06
mean     1.289366e-06
std      2.497192e-06
min      9.999999e-07
25%      1.200000e-06
50%      1.200000e-06
75%      1.300000e-06
max      2.815400e-03
Name: Int_2_bin, dtype: float64
count    510102.000000
mean          0.000005
std           0.000001
min           0.000004
25%           0.000004
50%           0.000006
75%           0.000006
max           0.000178
Name: Permutation_table, dtype: float64
count    3.200640e+05
mean     3.769918e-07
std      2.174599e-07
min      2.999998e-07
25%      3.000000e-07
50%      3.999999e-07
75%      4.000001e-07
max      4.660000e-05
Name: Cycle_shift_left, dtype: float64
count    10002.000000
mean         0.000009
std          0.000007
min          0.000008
25%          0.000009
50%          0.000009
75%          0.000009
max          0.000582
Name: Initial_Permutation, dtype: float64
count    10002.000000
mean         0.000008
```

```
std          0.000002
min          0.000007
25%          0.000007
50%          0.000007
75%          0.000008
max          0.000149
Name: PC_1_Permutation, dtype: float64
count    160032.000000
mean          0.000006
std           0.000003
min           0.000006
25%           0.000006
50%           0.000006
75%           0.000006
max           0.001055
Name: PC_2_Permutation, dtype: float64
count    10002.000000
mean         0.000130
std          0.000018
min          0.000125
25%          0.000128
50%          0.000129
75%          0.000130
max          0.001179
Name: Sub_key_creation, dtype: float64
count    160032.000000
mean          0.000006
std           0.000002
min           0.000006
25%           0.000006
50%           0.000006
75%           0.000006
max           0.000647
Name: E_Expansion, dtype: float64
count    1.280256e+06
mean     2.503701e-06
std      1.133240e-05
min      2.200000e-06
25%      2.400000e-06
50%      2.400000e-06
75%      2.500000e-06
max      1.172090e-02
Name: S_Box_permutation, dtype: float64
count    160032.000000
mean          0.000004
std           0.000003
min           0.000004
25%           0.000004
50%           0.000004
```

```
75%           0.000004
max           0.000749
Name: P_Expansion, dtype: float64
count    160032.000000
mean          0.000054
std           0.000035
min           0.000051
25%           0.000053
50%           0.000053
75%           0.000054
max           0.011779
Name: Feistel_network, dtype: float64
count    5001.000000
mean        0.001226
std         0.000193
min         0.001187
25%         0.001203
50%         0.001212
75%         0.001222
max         0.012944
Name: Cross_Iteration_Decryption, dtype: float64
count    1.000200e+04
mean     7.913347e-06
std      9.378640e-07
min      7.500000e-06
25%      7.700000e-06
50%      7.800000e-06
75%      8.000000e-06
max      6.560000e-05
Name: P_inverse_permutation, dtype: float64
count    5001.000000
mean        0.001246
std         0.000193
min         0.001206
25%         0.001222
50%         0.001231
75%         0.001242
max         0.012965
Name: DES_Decryption, dtype: float64
```

```
In [ ]:
```