DES (Data Encryption Standard) uses a 64-bit packet length and 56-bit key length. It takes a 64-bit input through a series of transformations to get a 64-bit output. The decryption uses the same steps and the same key, the only difference is that the key sequence is opposite to the encryption process.

DES encryption:

​ The input of the algorithm includes the plain text that needs to be encrypted and the key used for encryption, both of which are 64 bits in length. The 8, 16, 24, 32, 40, 48, 56, 64 bits of the key are parity bits

1. Clear text processing
   1. Read the plaintext into the program and turn it into a binary string
   2. Perform IP permutation on the plaintext and divide it into two left and right substrings
2. Handling of keys
   1. Read the key into the program and store it in the form of a binary string  
      Perform PC-1 permutation on the key and divide it into two substrings
   2. It is necessary to perform permutation compression on the key before generating the key required for the iteration
   3. Generate the sub-keys required for each iteration of DES for direct use in encryption and decryption
3. F function

In each round of transformation, the entire process can be expressed by the following formula: L\_i = R\_{i-1}  
   
R\_i = L\_{i-1}\O F(R\_{i-1},K\_i)  
   
The round key K\_i is 48 bits long and R is 32 bits long. First, the $R$ replacement is expanded to 48 bits. These 48 bits are XORed with K\_i, and the result obtained is used as a substitute function to generate a 32-bit Output. The 32-bit output is XORed with L\_{i-1} after being replaced by P to get a new R\_i  
   
The replacement function is composed of 8 $S$ boxes, each $S$ box has 6 bits of input and 4 bits of output. For each S box, the first and last digits of the input form a 2-digit binary number, which is used to select one of the four-row replacement values ​​of the S box, and the middle 4 digits are used to select the 16-column A certain column.

1. Encryption process  
     
   DES encryption needs to go through 16 iterations, the first$15 iterations need to exchange L\_i and R\_i at the end of each iteration, and no exchange at the 16th time