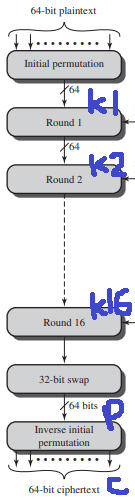
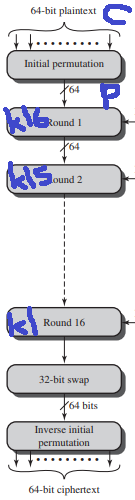
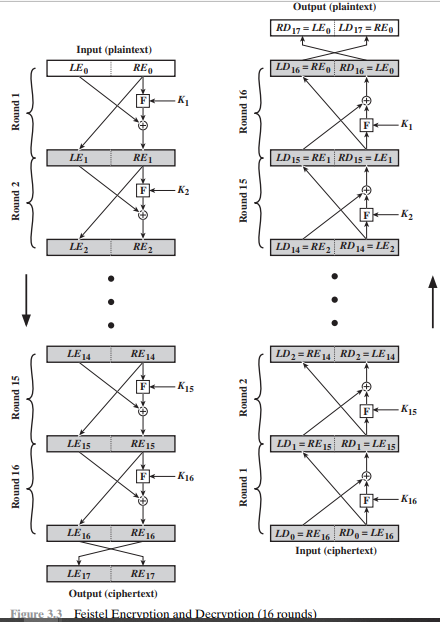
DES is based on the Feistel Cipher, which is a reversible cipher that uses the exact same algorithm to encrypt and decrypt, only with the round keys reversed. Because each round of the Feistel cipher can be reversed, it is its own inverse, and DES carries these properties as well. The only addition that DES adds onto the Feistel Cipher is an initial permutation at the beginning and an inverse initial permutation at the end. Ultimately, to prove that DES is its own inverse, the two steps are to show how the IP and inverse IP work and to show that the Feistel Cipher is its own inverse.

Encryption on left, Decryption on right

In the encryption, after the 32-bit swap, the algorithm produces something called the preoutput, which is denoted with *p.* Then, the inverse initial permutation is applied on *p,* producing ciphertext *c.* Because DES is its own inverse, the decryption structure will be the same as the encryption. During decryption, *c* is passed through the initial permutation. Since the inverse initial permutation from encryption is the inverse of the current initial permutation, they effectively cancel out. Thus, after the initial permutation, *c* becomes equivalent to *p* from the encryption. Likewise, the first initial permutation from encryption and last inverse initial permutation from decryption will also cancel each other out.



Feistel Cipher Encryption and Decryption

The next step is to show that the remainder of DES, the Feistel cipher, is its own inverse. In the previous picture, *p* represents LE17||RE17 in this picture. LE17||RE17 is equivalent to RE16||LE16, which is used as the input to the decryption. In the encryption process on the left, the following can be seen:

LE16 = RE15

RE16 = LE15 XOR F(RE15, K16)

For decryption, the following can be seen:

LD1 = RD0 = LE16 = RE15

RD1 = LD0 XOR F(RD0, K16)

RD1 = RE16 XOR F(RE15, K16)

RD1 = LE15 XOR F(RE15, K16) XOR F(RE15, K16)

Due to properties of XOR, RD1 can be simplified to just LE15. Thus, in decryption, LD1 equaled RE15 and RD1 equaled LE15. In other words, in encryption round 16, the input produced an output. Then, for decryption, that output was used as the first input to produce the same an output that was the same as the encryption’s input. This property works for all rounds, showing that the Feistel cipher is an inverse of itself.

Ultimately, DES decryption is an inverse of encryption because of the initial permutations between inverses and the Feistel cipher being its own inverse.