SIL-765: Networks and System Security
Assignment-1

By:
Mahima Manik (2017MCS2093)
Sruti Goyal (2017MCS2078)

User Input - Character string (min. 8 characters)
Input to DES function - Hexadecimal (equivalent of user input)
Output from DES function - Hexadecimal

Data Encryption Standard (DES):

DES is a symmetric key cryptographic system where the same key is used for both encryption and decryption.
It has a 16 round Feistel Structure.
The plaintext is 64 bits long.
The key is 64 bits long.

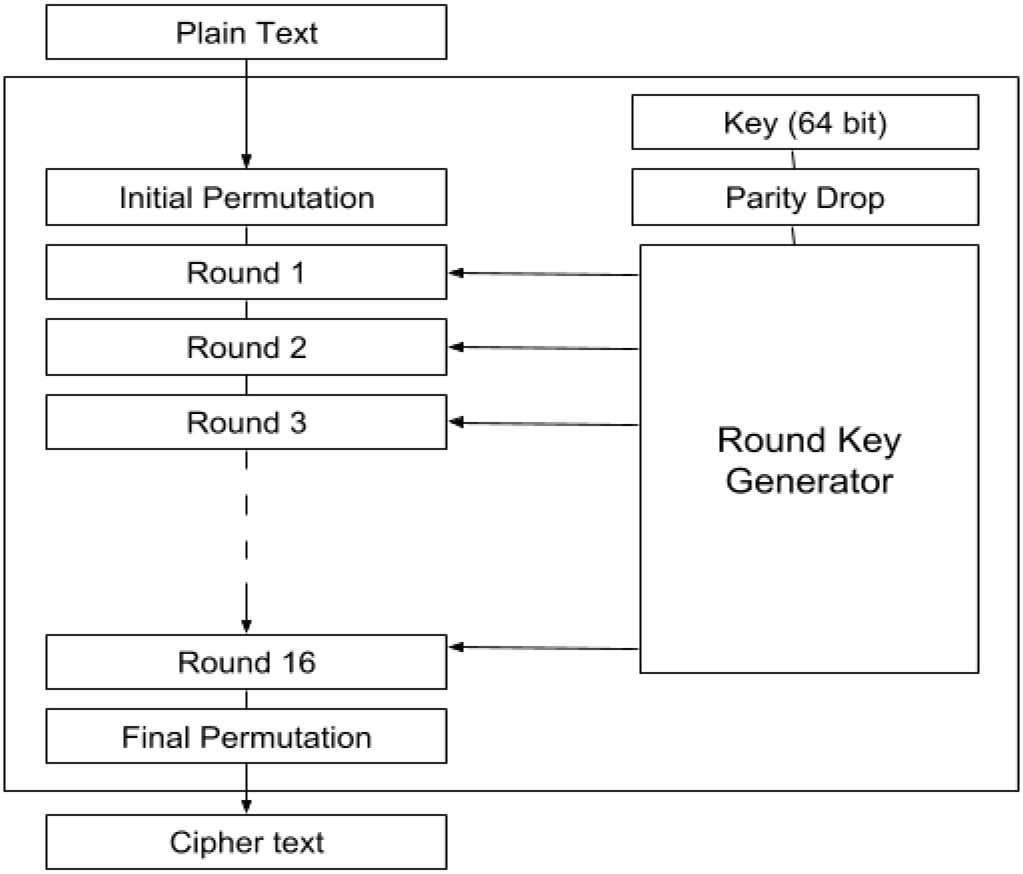

Fig. Basic Structure of DES

Key Generation

User enters a 64 bits / 8 characters long cipher key for the algorithm. If the key size is not sufficiently long, then the user is asked to enter the key again. For the key longer in length, the first 8 characters are only considered for the encryption and decryption.
Preprocessing of the cipher key has the following steps:

1. The key thus obtained is passed to a function called “convert2bit”, which takes the character string as the input and returns an array of the bits of size 64 bits.
2. 64 bit array is permuted according to a table and the bits at the 8, 16, 24, .. 64 positions are dropped. Thus 64 bit key reduces to 56 bits. This is a compression P-box.

After the preprocessing steps, 56 bits cipher key is obtained which is used in subsequent 16 rounds.

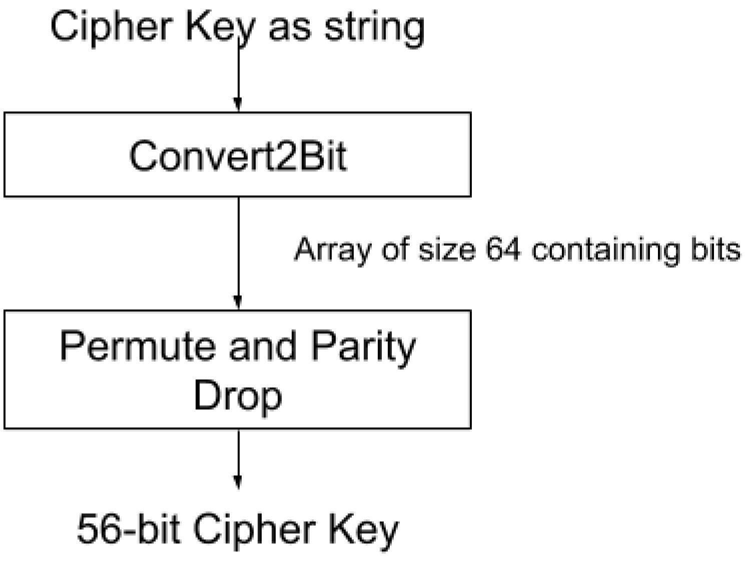

Fig. Preprocessing of key

For each of the 16 rounds of DES, different cipher keys are generated out of 56 bits cipher key. Also, partial output of the previous round key is taken as the input for the next round.

1. Round key generator function divides the key into two equal parts, left and right. Each part of the key is then passed to circular shift function where the bits of the keys are shifted by 1 or 2 positions to the left, depending on the round number.
   In rounds 1, 2, 9 and 16, 1 bit shift left takes place. In other rounds, shift_by_one function is simply called twice
   Decryption – Shift right operation takes place. In rounds 1, 8, 15 and 16, 1 bit shift right takes place. In other rounds, 2 bit shift right.

2. The result of round key generator is then passed into compression P- box, which permutes the bits according to a table and generates a 48 bit round key.
3. The result of round key generator is also passed as an input for the key generation for the next round.

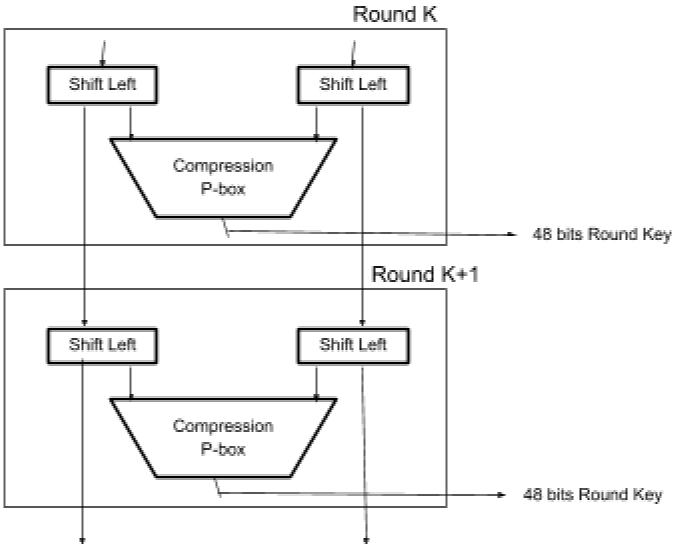

Fig. Round Key Generation for Encryption

For the purpose of Decryption, same steps are taken in the reverse order. The output of the shift lefts of the 16th round of encryption (56 bits) is passed as the input for the decryption. It is then passed to the Compression P-box, whose output is treated as the first decryption key.

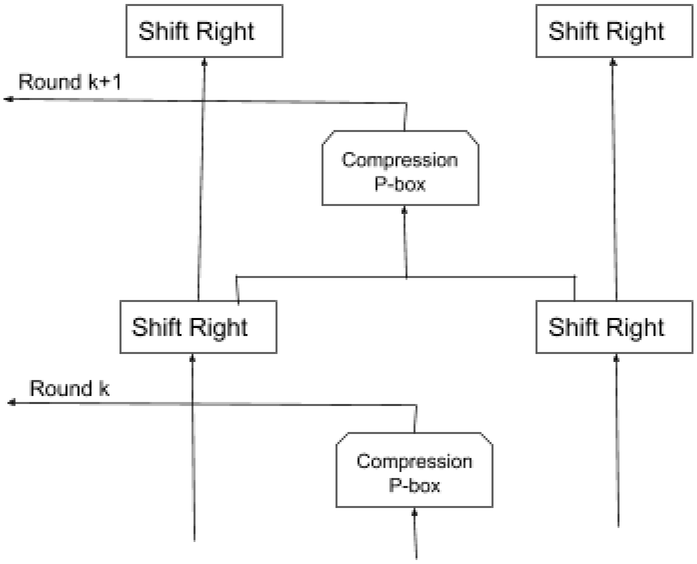

Fig. Round Key generation for Decryption

Rounds in DES

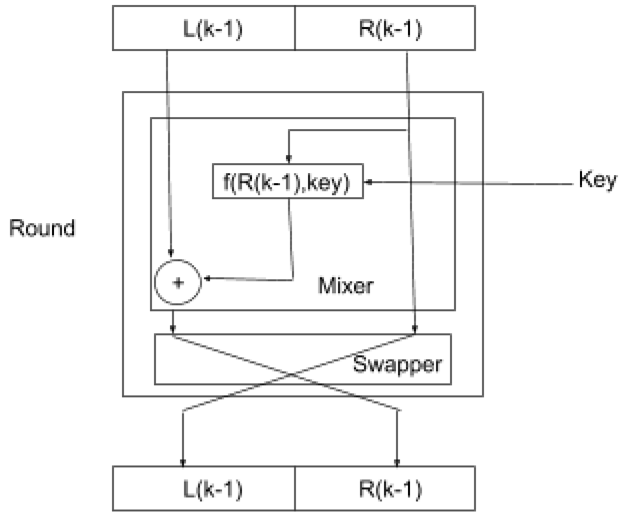

Fig. Round in DES

Before entering the DES rounds, plaintext goes through initial straight keyless permutation. The output of the initial permutation is the input to the first round of encryption. The final permutation takes place after 16 rounds and is exactly the inverse of the initial permutation.
Steps for DES round is as follows:

1. The ciphertext obtained from the each round is divided equally into two halves - left and right, 32 bits each.
2. Each round is a feistel cipher which takes output of the previous round as input and applies Mixer and swapper functions to it.
3. Mixer: The right part is passed into the f-box. f - box consists of the following operations - expansion P-box, XOR, 8 S-boxes and a straight P-Box.
   a. The right part is passed through the expansion P-box and its XOR is taken with the key for that round. Expansion P-box converts the 32 bits into 48 bits in a predetermined fashion. XOR operation also acts as the whitener in DES.
   b. The 48 bits output is passed through array of S-boxes of size 8. Each S-box converts 6 bits to 4 bits and thus 48 bits input to 32 bits output. Finally the output is passed through a straight P-box.
4. Swapper: The output of the F-box is XOR-ed with the left part of the previous round output and it forms the right-part of this round. The right-part of the previous round output becomes the left-part of this round.