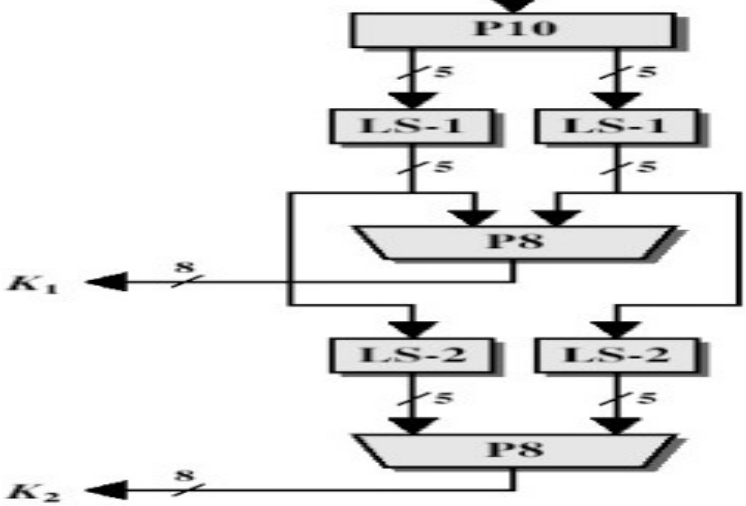
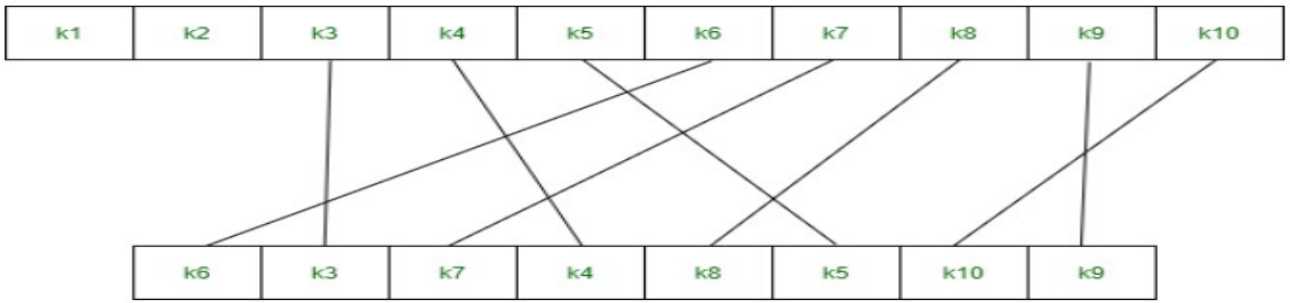

P10
5
5
LS-1
LS-1
5
5
P8
8
K_1
LS-2
LS-2
5
5
P8
8
K_2

2. Permutation P8



```
(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (1, 0, 1, 0, 0, 0, 0, 0, 1, 0)

P10 Permutation is: P10(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k3, k5,
k2, k7, k4, k10, k1, k9, k8, k6)
After P10, we get 1 0 0 0 0 0 1 1 0 0
```

Step 2: We divide the key into 2 halves of 5-bit each.

```
l=1 0 0 0 0, r=0 1 1 0 0
```

Step 3: Now we apply one bit left-shift on each key.

```
l = 0 0 0 0 1, r = 1 1 0 0 0
```

Step 6: Combine the 2 halves obtained from step 5 and permute them by putting them in the P8 table. The output of the given table is the second key K2.

```
After LS-2 combined = 0 0 1 0 0 0 0 0 1 1
P8 permutation is: P8(k1, k2, k3, k4, k5, k6, k7, k8, k9, k10) = (k6, k3, k7,
k4, k8, k5, k10, k9)
After P8, we get Key-2 : 0 1 0 0 0 0 1 1
```

Final Output:

```
Key-1 is: 1 0 1 0 0 1 0 0
Key-2 is: 0 1 0 0 0 0 1 1
```

first block and the key to ensure all subsequent blocks result in ciphertext that does not match that of the first encryption block.

What are the different modes of operation in block cipher?

Block ciphers only encrypt messages that are the same size as their block length, so each block of plaintext with more or less blocks needs to be encrypted separately.

- **Electronic codebook (ECB) mode.**
- **Cipher block chaining (CBC) mode.**
- **Ciphertext feedback (CFB) mode.**
- **Output feedback (OFB) mode.**
- **Counter (CTR) mode.**

previous blocks. Each plaintext block is XORed (exclusive OR) with the previous ciphertext block before being encrypted with the cipher algorithm. CBC mode is used in a variety of security applications.

Ciphertext feedback (CFB) mode. In contrast to CBC mode, which encrypts a set number of bits of plaintext at a time, it is sometimes necessary to encrypt and transfer plaintext values instantly, one at a time.

Output feedback (OFB) mode. OFB mode can be used with any block cipher and is similar in some respects to CBC mode. It uses a feedback mechanism, but instead of XORing the previous block of ciphertext with the plaintext before encryption, in OFB mode, the previous block of ciphertext is XORed with the plaintext after it is encrypted.

The DES encryption algorithm uses symmetric keys, which means that the same key is used for encrypting and decrypting the data.

DES Algorithm Steps

Let us take a look at the steps involved in the DES algorithm:

- The initial permutation (IP) function receives the 64-bit plaintext block.
- The IP is performed on plaintext.
- The IP then makes two halves of the block that has been permutated. The two halves are known as left plan text (LPT) and right text (RPT).
- All LPTs and RPTs are encrypted 16 times.
- The LPT and RPT are joined, and then the final permutation (FP) is performed on this block.
- The 64-bit ciphertext is now ready.

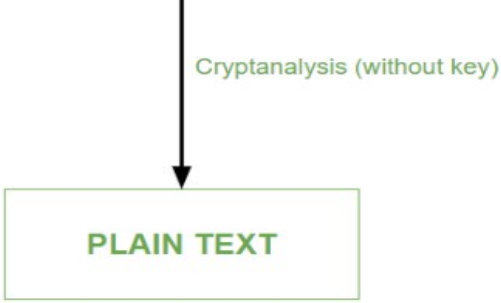
In the encryption process (step 4), there are five stages:

- Key transformation
- Expansion permutation
- S-Box permutation
- P-Box permutation
- XOR, and swap

- DES was designed for hardware; it is fast in hardware, but only relatively fast in software.

Disadvantages of DES Algorithm

- DES can be implemented quickly on hardware. But since it was not designed for software, it is relatively slow on it.
- It has become easier to break the encrypted code in DES as the technology is steadily improving. Nowadays, AES is preferred over DES.
- DES uses a single key for encryption as well as decryption as it is a type of symmetric encryption technique. In case that one key is lost, we will not be able to receive decipherable data at all.



Cryptanalysis is used to break cryptographic security systems and gain access to the contents of the encrypted messages, even if the cryptographic key is unknown.

2. The attacker tries to decrypt the messages using these two.
3. This type of attack is somewhat easy to implement.

Different Forms of Cryptanalysis:

1. Linear Cryptanalysis:

Linear cryptanalysis is a general type of cryptanalysis based on discovering affine approximations to a cipher's action in cryptography. Block and stream ciphers have both been subjected to attacks. Linear cryptanalysis is one of the two most common attacks against block ciphers, with differential cryptanalysis being the other.

S. No.	Linear Cryptanalysis	Differential Cryptanalysis
1.	Linear cryptanalysis was basically invented by Matsui and Yamagishi in the year 1992.	Differential cryptanalysis was first defined in the year 1990 by Eli Biham and Adi Shamir.
2.	Linear cryptanalysis always works on a single bit (one bit at a time).	Differential cryptanalysis can work on multiple bits at a time.
3.	In the case of Linear cryptanalysis, ciphertext attack is a very big disadvantage.	In the case of differential cryptanalysis plain text attack is a very big disadvantage.

8.	Plaintext is used one by one in linear Cryptanalysis.	Plaintext is used in pairs in Differential Cryptanalysis.
9.	Complexity of attack is low in linear Cryptanalysis.	Complexity of attack is High in Differential Cryptanalysis
10.	Mathematical relation between plaintexts used has Linear approximation (such as a series of XOR operations).	Mathematical relation between plaintexts used has Specific differences (such as XOR).
11.	Goal of the attack is to identify the linear relation between some bits of the plaintext, some bits of the cipher text and some bits of the unknown key.	Goal of the attack is to Identify some bits of the unknown key.