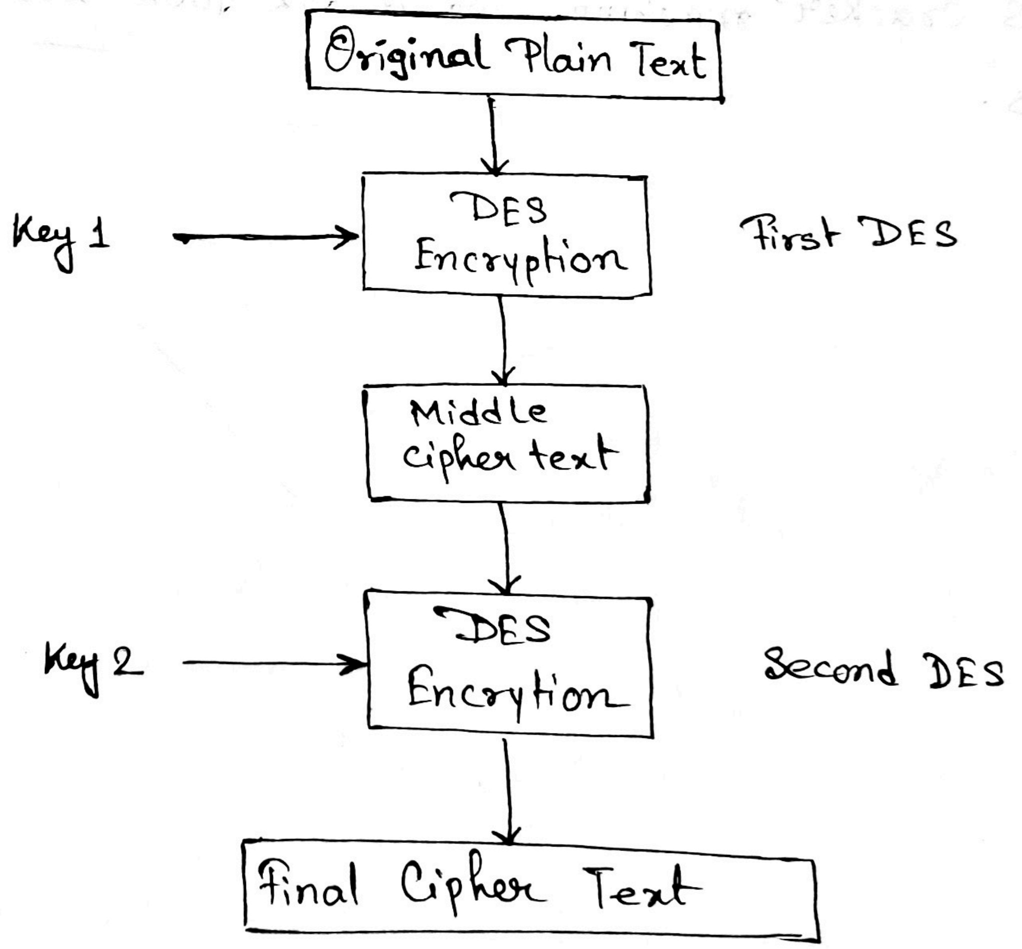
Double DES:

Double DES is an encrytion technique which uses two instances of DES on same plain text. In both the instances it uses different keys to encrypt the plaintext. Both keys are required at the time of decryption. The 64 bit plaintext goes into first DES instance which then converted into middle cypher text using the first key and then this middle cypher text goes to second DES instance ~~wich~~ which gives the final 64 bit cipher text using second key.



~~Encryption of~~

Decryption of Double DES: Decryption of double DES is the reverse process of the encryption. In Double DES the encrypted ~~text~~ cipher-text block is first decrypted using the second key (i.e key 2 or K2) to make the single encrypted cipher text (i.e middle cipher text). This cipher text block is then decrypted using ~~they~~ the first key (i.e key 1 or K1) to acquire the original plaintext block.

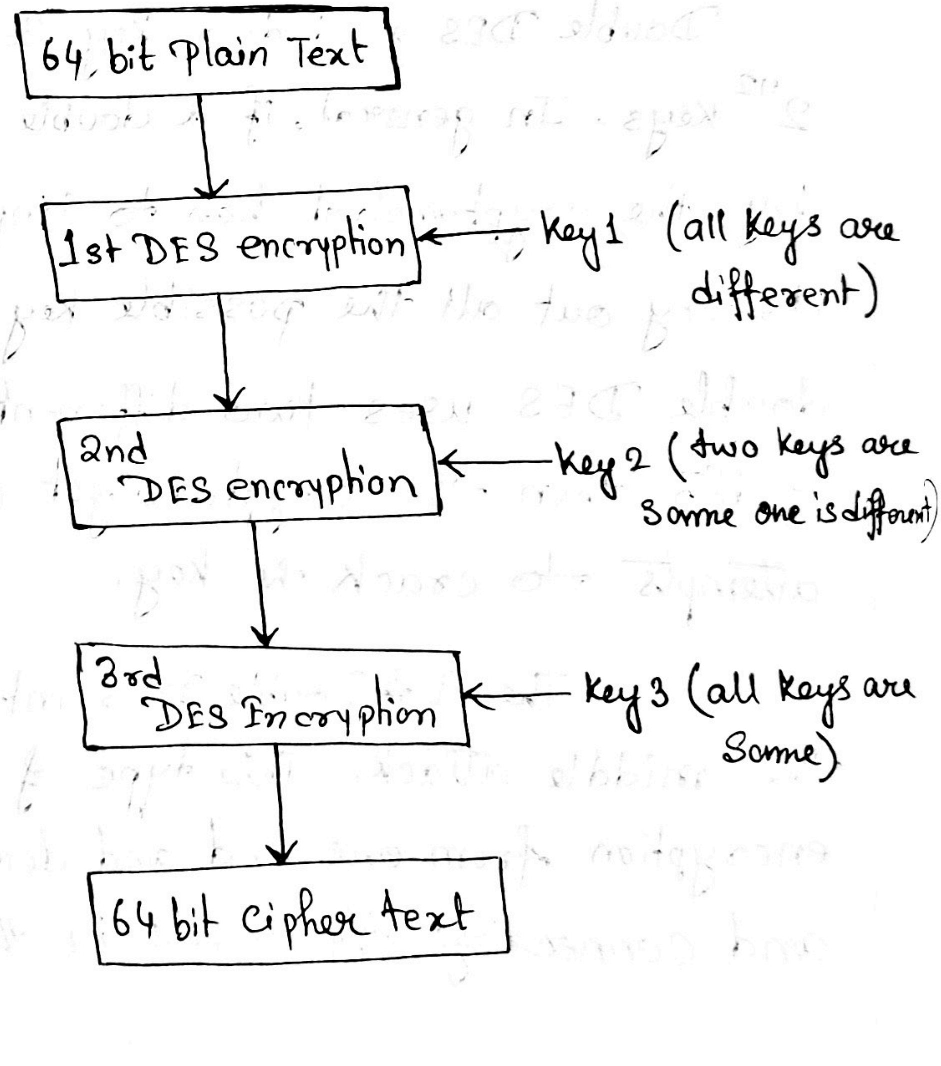
Strength of Double DES:

Double DES needed a key search of (2^{2*56}) i.e 2^{112} keys. In general, if a double DES use an n-bit key, the cryptanalyst has to implement 2^{n} operations to try out all the possible key combinations. As double DES uses two different keys, each including n bits, then the cryptanalyst would require 2^{2n} attempts to crack the key.

The ~~Dob~~ Double DES introduce the meet-in-the-middle attack. This type of attack contains encryption from one end and decryption from the other and connecting the result in the middle.

Triple DES:

Triple Data Encryption Algorithm (3DES/TDES) is the upgraded form of the famous DES standard algorithm. 3DES uses symmetric key block cipher. Triple DES is an encryption technique which uses three instance of DES on Same plain text. It uses three different types of key choosing techniques. In first all used key are different and in second two keys are Same and one is different and in the third again all keys are Same.


64 bit Plain Text
1st DES encryption
Key 1 (all Keys are different)
2nd DES encryption
Key 2 (two keys are Same one is different)
3rd DES Encryption
Key 3 (all Keys are Same)
64 bit Cipher text