09/06/22 Data Encryption Standard (DES):- (contains 64-bits)

Feistel Cipher:- (based on DES)

↳ In Every Round of DES, it uses a 56-bit key.

09/08/22 How Secure is 2DES? (very Insecure)

Encryption	Decryption (It's matching & hence Insecure.)
$E_{K_1}(M) \rightarrow C'$	$D_{K_2}(C) \rightarrow C'$.
$E_{K_2}(C') \rightarrow C$	$D_{K_1}(C') \rightarrow M$.

→ The Adversary should have message (M) and ciphertext (C) to build the above table to break the 2DES.

3DES:-

How does it work?

3DES: $E_{K_3}(D_{K_2}(E_{K_1}(M))) = C$; where E = DES

Different Security Types of 3DES:

1) If, $K_1 = K_2 = K_3$ → Bad. vanilla 3DES, 56-bit security.

2) If, $K_1 = K_3$ → 112-bit security (secure and efficient)

3) If, $K_1 \neq K_2 \neq K_3$ → 168-bit security (very secure)

3DES with Two Keys :-

- Discovered by Tuchman.

I^st - way : $C = E_{K_1}(D_{K_2}(E_{K_1}(M)))$

$M = D_{K_1}(E_{K_2}(D_{K_1}(C)))$

II^nd - way : $C \leftarrow D_{K_3}(E_{K_2}(D_{K_1}(M)))$

$M \leftarrow E_{K_1}(D_{K_2}(E_{K_3}(C)))$

Generalizing Fiestel cipher Round :-

$LE_{i+1} \leftarrow RE_i$

$RE_{i+1} \leftarrow LE_i \oplus F(RE_i, K)$.