		<u></u>
09/06/22	Data Encryption Standard (DES): (Contains 64-bits)	
	Feistel Ciphon: - (based on DES)  Exery Round of DEC, it usef a 56-bit  (sey.	
	Feigle Ciphon: - (based on DES)	
	Expression of DEC, it uses a 56-bit	
	(cey ,	
20/20/22	How Sewe is 2DES? (very Instructe)  Encryption  Decryption  Decryption  To nothing &  Decryption  Decryption  There Instructe.	
0 (108) 120	How Sewel 4 WES!	I'm ratching &
	Encryption	Destruction hence Instante.
	_	200 31 200
	EK, (M) -> C1	1 K2 (c) -> c'.
	F	0 ( (1
	Ex2(c)->c	Dr. (c) -> M.
	The Advisor of 11 hours speed to Call a Collaboration	
	to built the above table to break the 2DES.	
	to great the way they	
	30ES:-	
	How does it work?	
	30ES: $E_{K_2}(D_{K_2}(E_{K_1}(M))) = C$ ; where $E = DES$	
	Dipperent Security Types of 3DES:	
	1) If, K,=Kz=Kz -> Dad . Vanilla3DES, 56-bit sewroty.	
	2) Ib, K,=K3 > 112-bit Sewrity (Sewre and)  3) Ib, K, 7527 K3 > 168-bit Sewrity (Vory  Sewre)	
	3) The K, I to I know 168-bit senditu ( vois )	
		( Seudre)

3DES with Two Keys: -

· Discouded by Tushman.

 $\frac{T^{st} way:}{C = E_{K_1}(D_{K_2}(E_{K_1}(n)))}$ 

 $M = D_{k_1} \left( E_{k_2} \left( D_{k_1} \left( c \right) \right) \right)$ 

 $\frac{\mathbb{Z}^{nd-way:}}{M \subset \mathbb{E}_{K_1}(\mathbb{E}_{K_2}(\mathbb{E}_{K_2}(\mathbb{E}_{K_3}(C)))}$ 

Generalizing Fiestel Cifher hound:

LEiH C- RE; REiH C-LE; F(REi, K).