Omkar Gurav
BE IT
8048

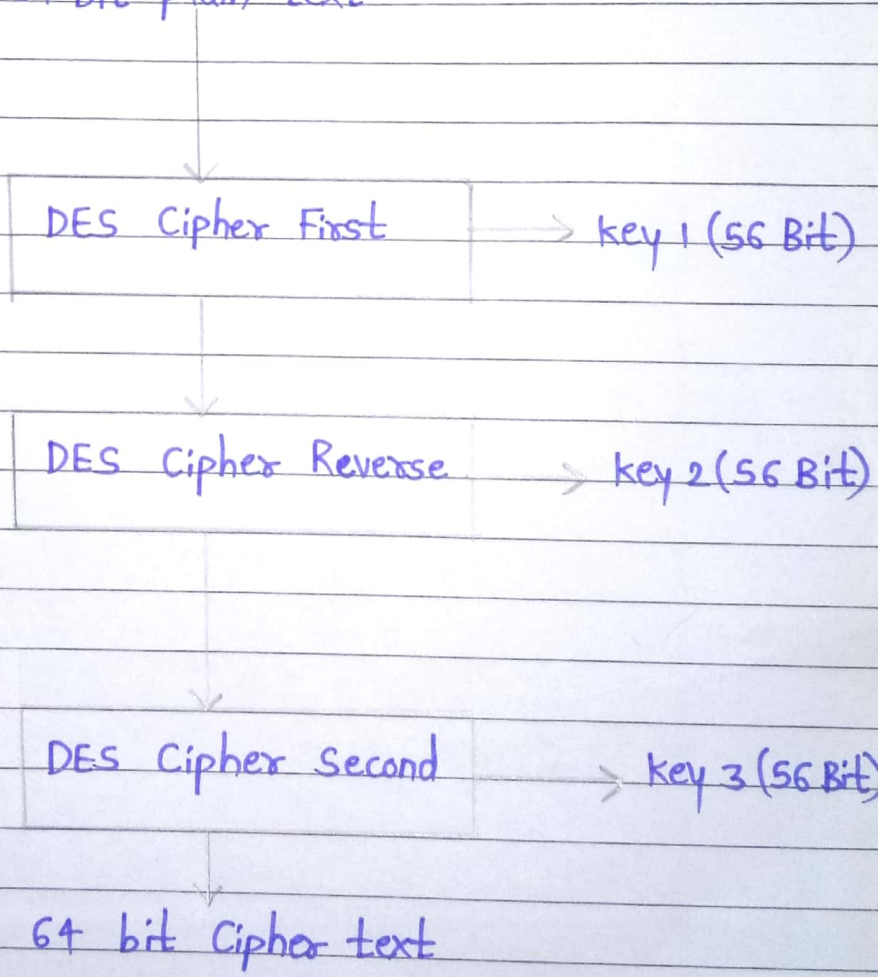
Rajdhani
DATE / /

ICS class Assignment 2 (Mapping CO1)

Describe Triple DES or 3DES in detail.

→

Triple DES or 3DES is an encryption technique which uses three instances of Data Encryption Standard (DES) on the same plaintext. It uses three different types of key choosing technique in First all used keys are different & in second two keys are same & one is different & in third all keys are same.



Triple DES is also vulnerable to meet in the middle attack because of which it gives total security level of 2^{112} instead of using 168 bit key. The block collision attack can also be done because of short block size & using same key to encrypt large size of the text. It is also vulnerable to the sweet32 attack.