Double DES and Triple DES
For IT 7th Sem Students

Developed and Presented By:

Dileep Kumar Yadav

Assistant professor

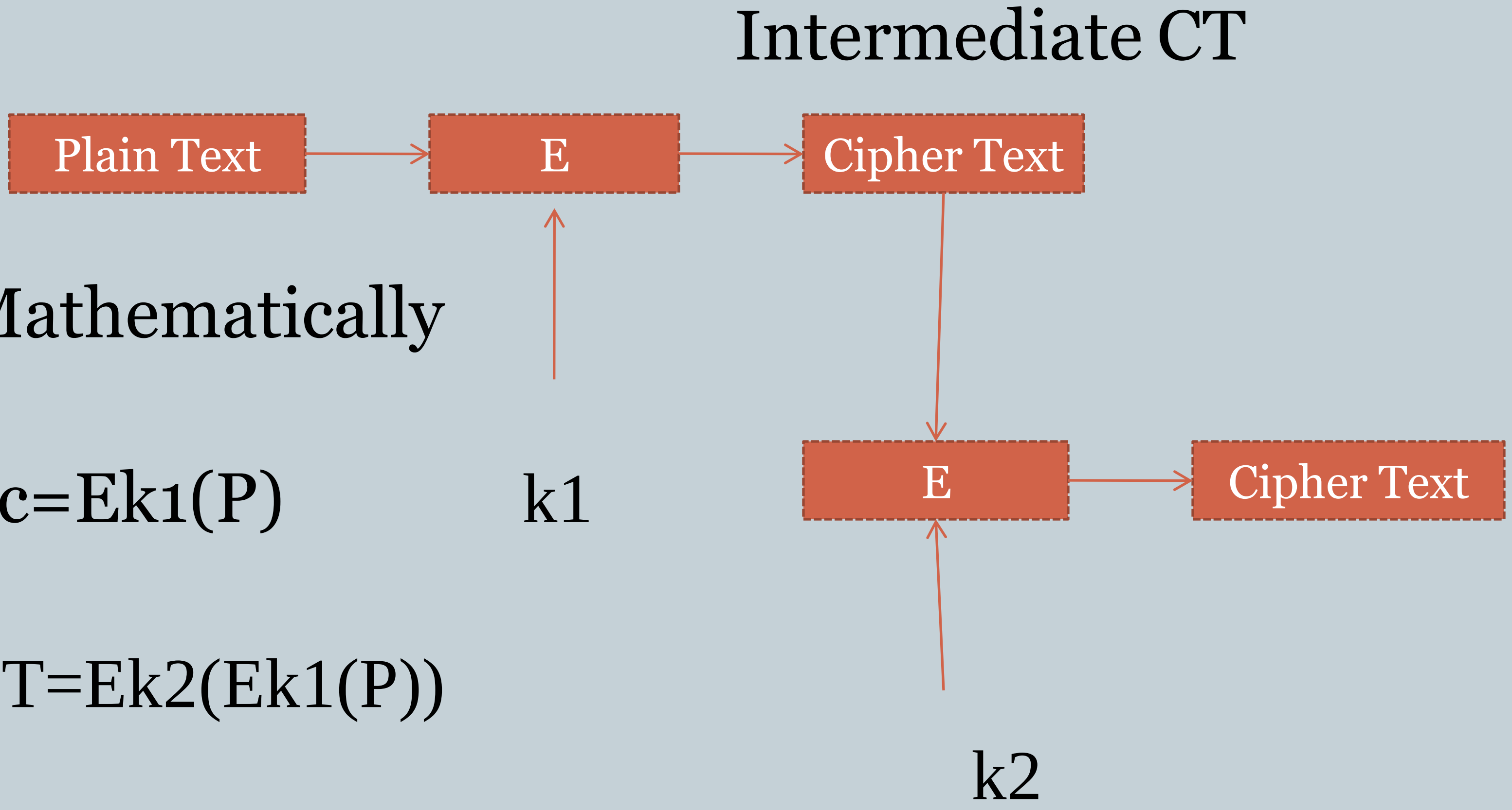
Dept. of CSE

V.B.S PU,Jaunpur

Mb. No.8726943272

Email-dileep1482@gmail.com

Double DES



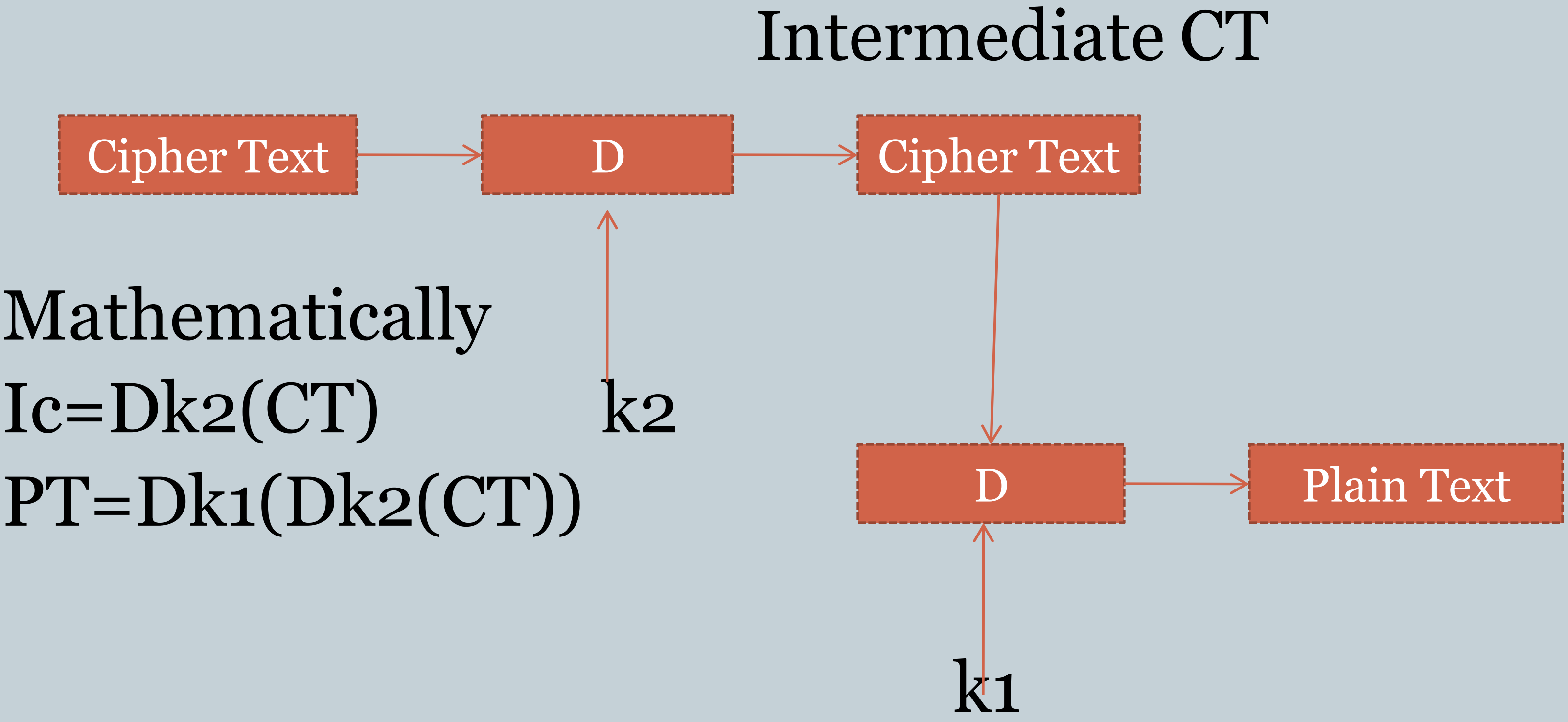
- Mathematically

$Ic=Ek1(P)$

$CT=Ek2(Ek1(P))$

Encryption Process

Cont…



Mathematically

Ic=Dk2(CT)

PT=Dk1(Dk2(CT))

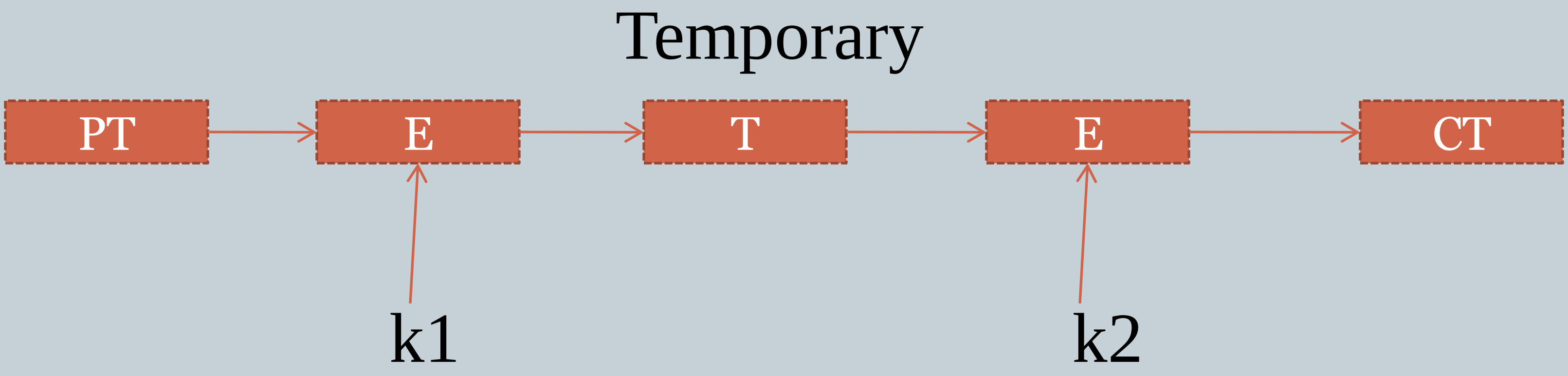
Decryption Process

Problem of Double DES

- Markel and Hellman introduced encryption from one end and decryption from other end and matching the results in the middle hence the name “**meet in the middle attack**”**.**

Meet in the Middle Attack

- Suppose that cryptanalysis knows two basic pieces of information P (a plain text block) and CT(corresponding the final cipher text block) for a message.



Ek1(P) T=Ek1(P) Ek2(Ek1(P))

CT=Ek2(Ek1(P))

Cont…

- The result of 1^{st} encryption is called as T and denoted

$$T=Ek1(P)$$

- After this encryption the encrypted block is encrypted with another key k2 then

$$CT=Ek2(Ek1(P))$$

- Now the aim of the cryptanalysis who is armed with the knowledge of P and C is to obtain the values of k1 and k2 the cryptanalysis do…

Cont…

- Step 1- for all possible values of 2^56 of k1 the cryptanalysis would use a large table in the memory of the computer and perform the following two points…
- 1-the cryptanalysis would encrypt the plain text block P by performing the 1st encryption operation.

  i.e. T=Ek1(P)
- 2-the cryptanalysis store the output of the operation Ek1(P) in temporary T and calculate
- CT=Ek2(Ek1(P))

Cont…

- Step 2- for decryption process

$$T=Dk2(CT)$$

$$PT=Dk1(Dk2(P))$$

- From above two steps

$$T=Ek1(P)=Dk2(CT)$$

- Now if the cryptanalysis creates a table of Ek1(P) for all possible values of k1 and then perform Dk2(CT) for all possible values of k2,so there is a chance that she or he gets the same T in both operation.

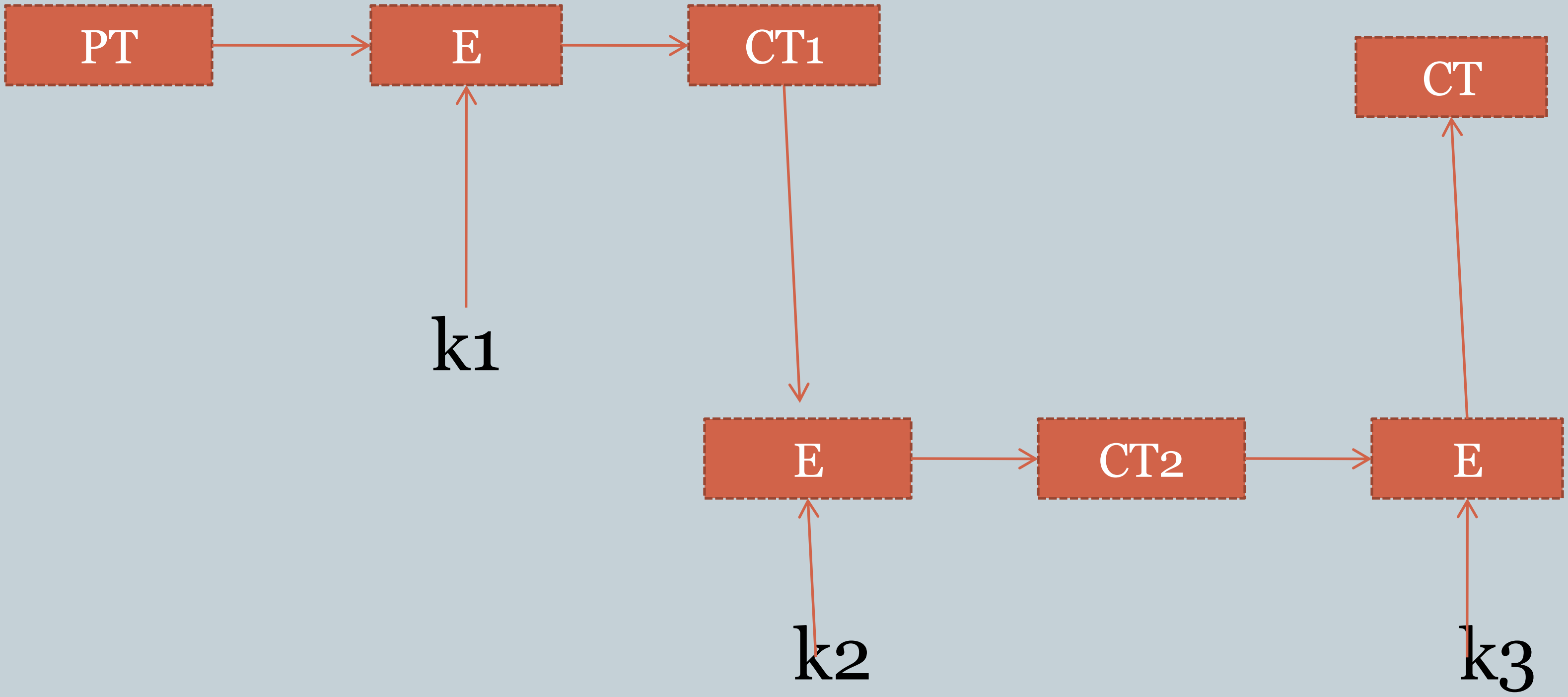
Cont…

- If the cryptanalysis is able to find the same T for both encryption with k1 and decryption with k2,its means that the cryptanalysis knows not only P and C but he has been also able to find out the possible values of k1 and k2.

Triple DES

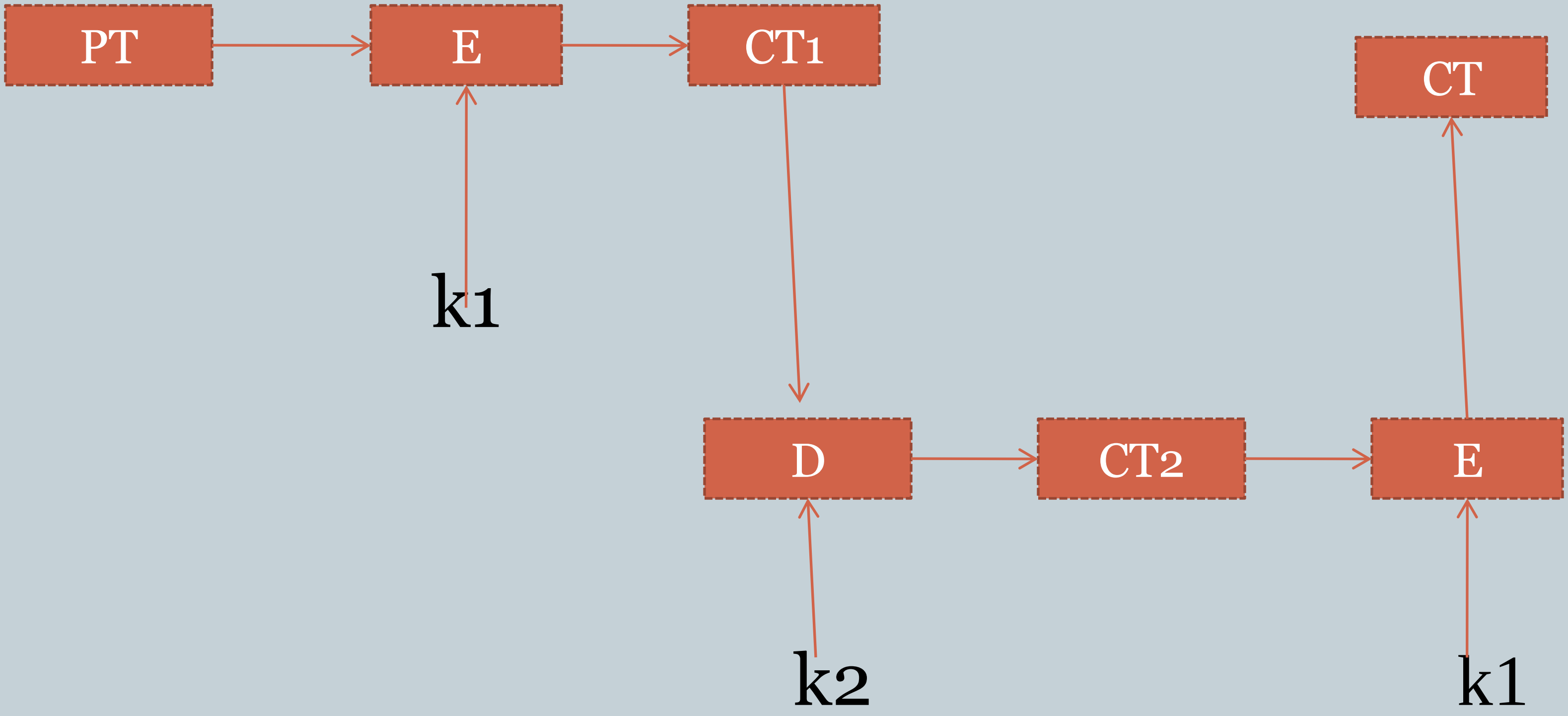
- Although the meet in the middle attack on double DES is not quite practical yet in cryptography, but it is always better to minimum chances.
- As we can imagine triple DES is DES three times. It comes in two variations like…
- Triple DES with Three keys.
- Triple DES with two keys.

Triple DES with Three Keys



- CT=Ek3(Ek2(Ek1(PT)))

Triple DES with Two Keys



PT E CT1

CT

k1

D CT2 E

k2 k1

- CT=Ek1(Dk2(Ek1(PT)))

Reference

- Cryptography and network security “Atul Kahate” 3e,Mc Graw hill education.