SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity Including BCT)

COURSE NAME : FUNDAMENTALS OF CRYPTOGRAPHY 19CS301

II YEAR / III SEMESTER

Unit II-

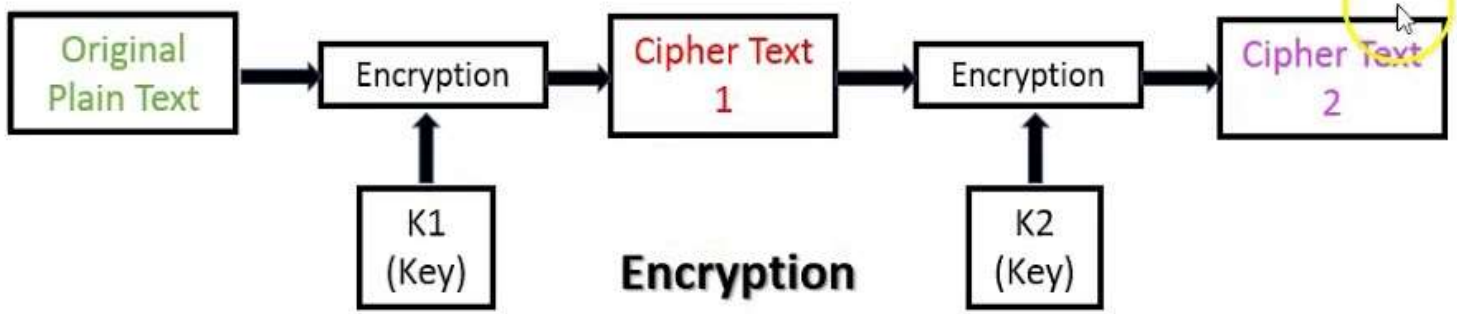
Topic :Double & Triple DES

Double DES (Encryption Process)

- Double DES performs the same operations as DES only difference is that double DES use two keys K1 & K2.

- First it performs encryption on plain text P, which is encrypted using K1 and obtains first cipher text C1.

- Again cipher text C1 is encrypted by using another key K2 & generate final cipher text C2.



Mathematically double DES encryption is represented as,

1. **C1 = E (K1, P)**
2. **C2 = E (K2, C1)**

   C2 = E (K2, E (K1, P))

Where, P = Plain text,

K1 = Key – 1,

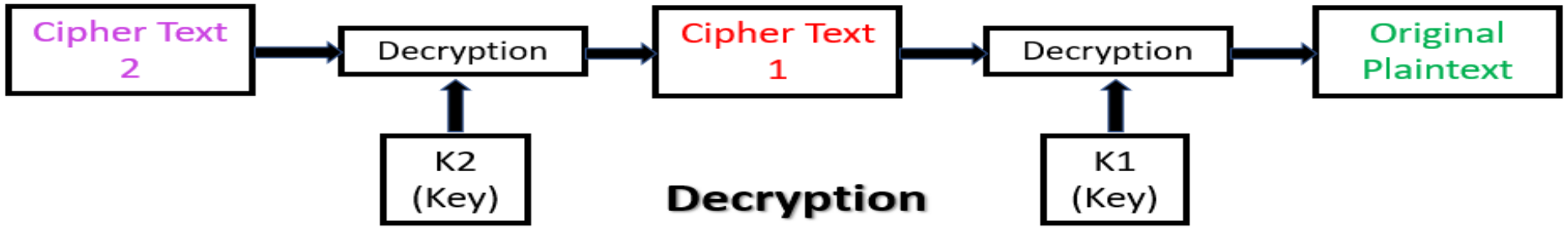
K2 = Key – 2,

C1 = first cipher text,

C2 = Final cipher text

E = Encryption Process

Decryption of double DES is reverse of encryption.



Mathematically double DES decryption is represented as,

1. **C1 = D (K2, C2)**
2. **P = D (K1, C1)**
   P = D (K1, D (K2,C2))

Where, P = Plain text,
K1 = Key – 1,
K2 = Key – 2,
C1 = first cipher text,
C2 = Final cipher text
D = Decryption Process

Triple DES(Encryption Process)

DES is a symmetric block cipher (shared secret key), it uses a key length of 56-bits.

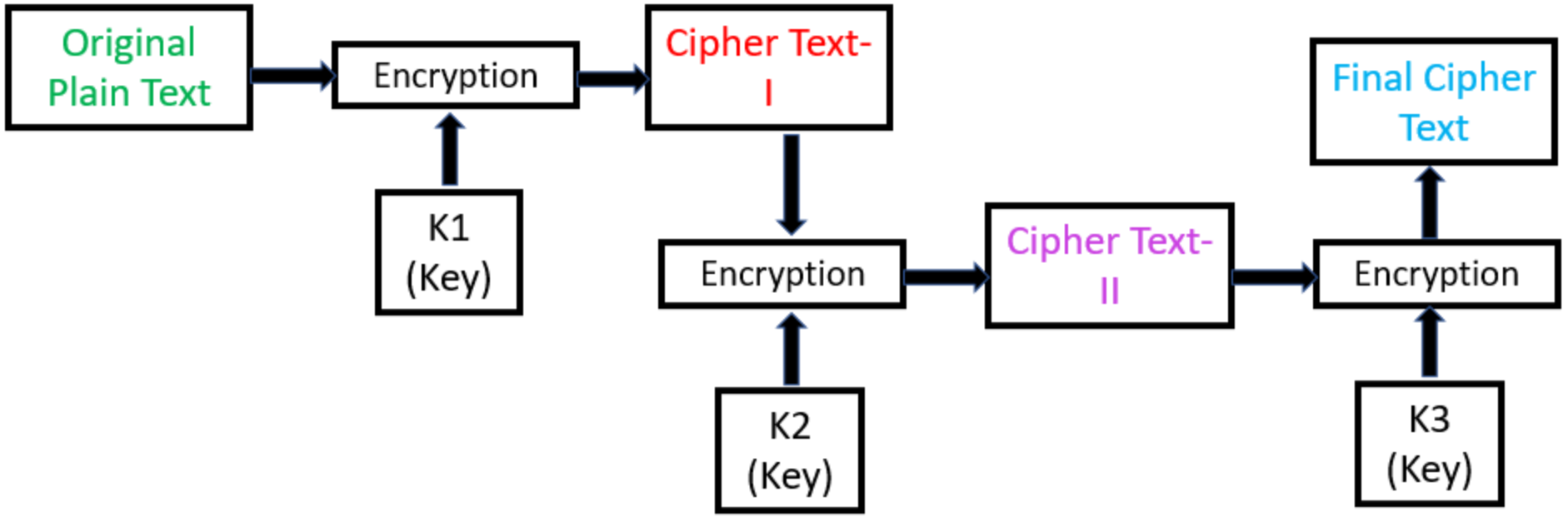
In Triple DES, each of the three rounds can be performed either encryption or decryption process using DES algorithm. It generates eight different possible modes for Triple DES. Triple DES is stronger than single DES because it performs more rounds of encryption.

Triple DES encrypts input data three times. The three keys are referred to as K1, K2 and K.

Triple DES with 3 keys

Encryption

- Triple DES performs the same operation as double DES. Triple DES using three keys K1, K2 & K3 while encrypting plain text
- First it performs encryption on plaintext P, which is encrypted using ***K1*** and obtains first cipher text ***C1***. Again, this cipher text is encrypted using key ***K2*** which obtain the second cipher text ***C2***.
- Which is again encrypted using ***K3*** & generate final cipher text ***C3***



Mathematically triple DES (with 3 keys) encryption is represented as,

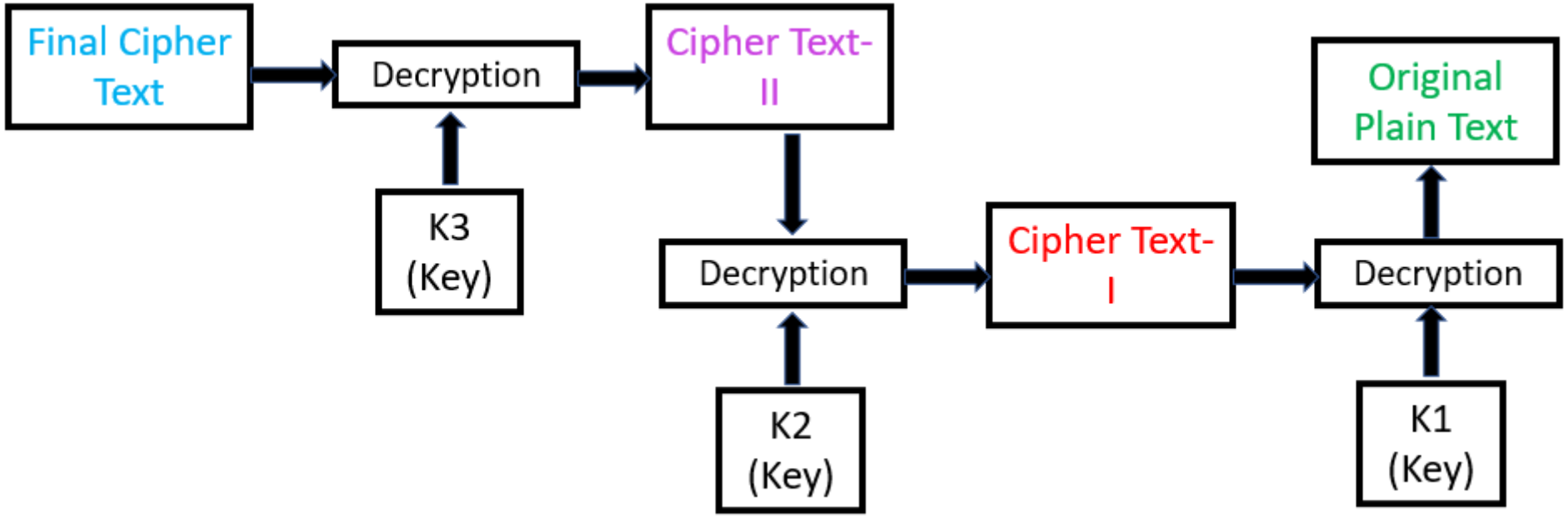
1. **C1 = E (K1, P)**
2. **C2 = E (K2, C1)**
   C2 = E (K2, E (K1, P))
3. **C3 = E (K3, C2)**
   C3 = E (K3, E (K2, C1))
   C3 = E (K3, E (K2, E (K1, P)))

Where, P = Plain text, K1 = Key – 1, K2 = Key – 2, K3 = Key – 3, C1 = first cipher text, C2 = second cipher text, C3 = Final cipher text, E = Encryption Process

Triple DES with 3 keys

Decryption

- Decryption of Triple DES is reverse of encryption.
- In triple DES decryption process final cipher text ***C3*** decrypt using ***K3***, result is cipher text ***C2***.
- ***C2*** will be decrypt with ***K2*** and get ***C1*** cipher text.
- Then ***C1*** cipher text decrypt with ***K1*** key and get original plain text ***P***.



Mathematically triple DES (with 3 keys) decryption is represented as,

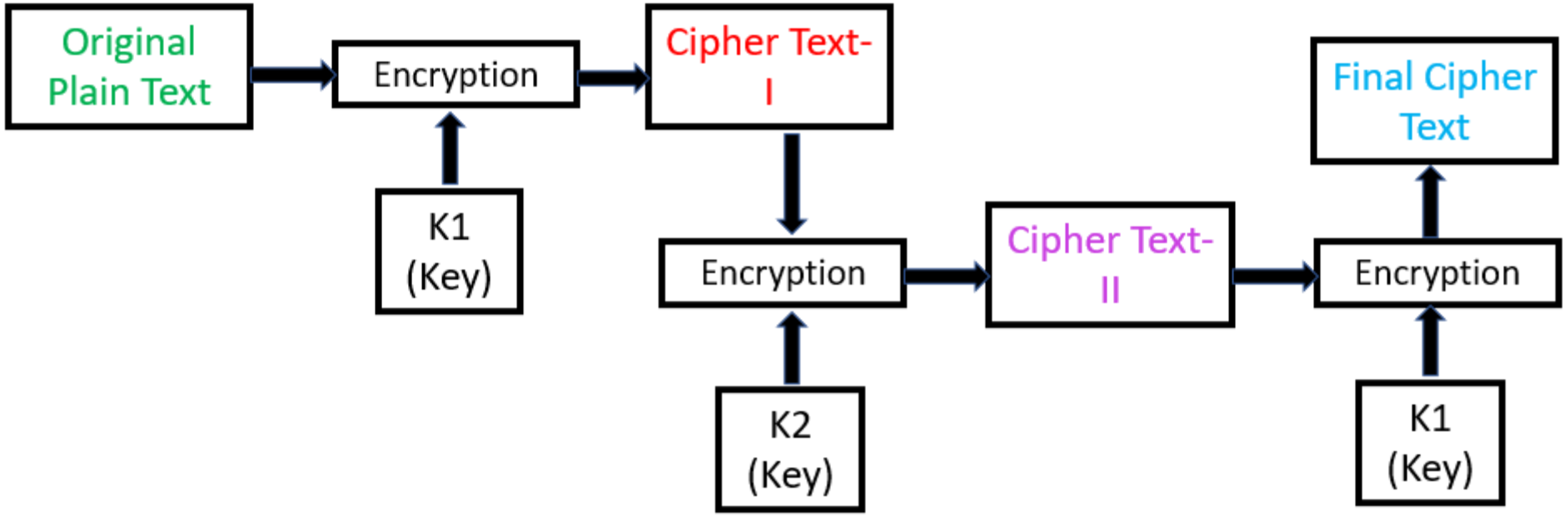
1. **C2 = D (K3, C3)**
2. **C1 = D (K2, C2)**
   C1 = D (K2, D (K3, C3))
3. **P = D (K1, C1)**
   P = D (K1, D (K2, C2))
   P = D (K1, D (K2, D (K3, C3)))

Where, P = Plain text, K1 = Key – 1, K2 = Key – 2, K3 = Key – 3, C1 = first cipher text, C2 = second cipher text, C3 = Final cipher text, D = Decryption Process

Triple DES with 2 keys

Encryption

- Triple DES performs the same operation as double DES.
- Triple DES using two keys K1 & K2 while encrypting plain text.
- First it performs encryption on plaintext ***P***, which is encrypted using ***K1*** obtains first cipher text ***C1***.
- Again, this cipher text is encrypted using key ***K2*** which obtain the second cipher text ***C2***.
- Which is again encrypted using ***K1*** & generate final cipher text ***C3***



Mathematically triple DES (with 2 keys) encryption is represented as,

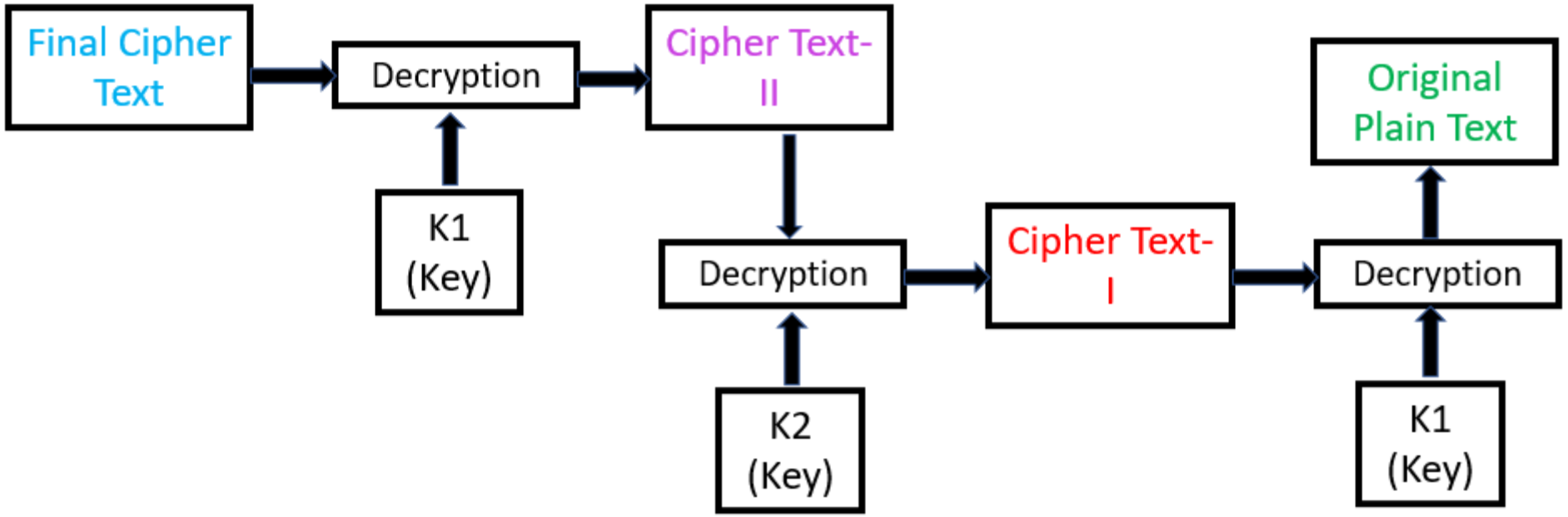
1. **C1 = E (K1, P)**
2. **C2 = E (K2, C1)**
   C2 = E (K2, E (K1, P))
3. **C3 = E (K1, C2)**
   C3 = E (K1, E (K2, C1))
   C3 = E (K1, E (K2, E (K1, P)))

Where, P = Plain text, K1 = Key – 1, K2 = Key – 2, C1 = first cipher text, C2 = second cipher text, C3 = Final cipher text, E = Encryption Process

Triple DES with 2 keys

Decryption

- Decryption of Triple DES is reverse of encryption
- In triple DES decryption process final cipher text ***C3*** decrypt using ***K1***, result is cipher text ***C2***.
- ***C2*** will be decrypt with ***K2*** and get ***C1*** cipher text.
- Then ***C1*** cipher text decrypt with ***K1*** key and get original plain text ***P***.



Mathematically triple DES (with 2 keys) decryption is represented as,

1. **C2 = D (K1, C3)**
2. **C1 = D (K2, C2)**
   C1 = D (K2, D (K1, C3))
3. **P = D (K1, C1)**
   P = D (K1, D (K2, C2))
   P = D (K1, D (K2, D (K1, C3)))

Where, P = Plain text, K1 = Key – 1, K2 = Key – 2, C1 = first cipher text, C2 = second cipher text, C3 = Final cipher text, D = Decryption Process