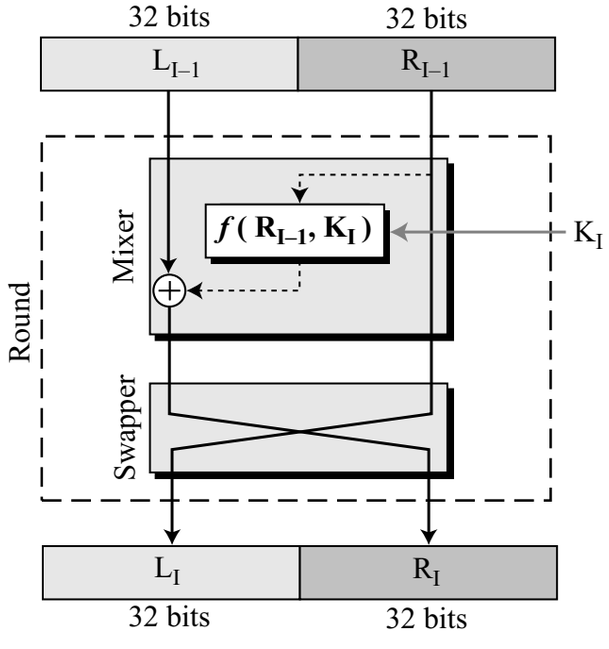
Differential Cryptanalysis, and some Encipherment Modes

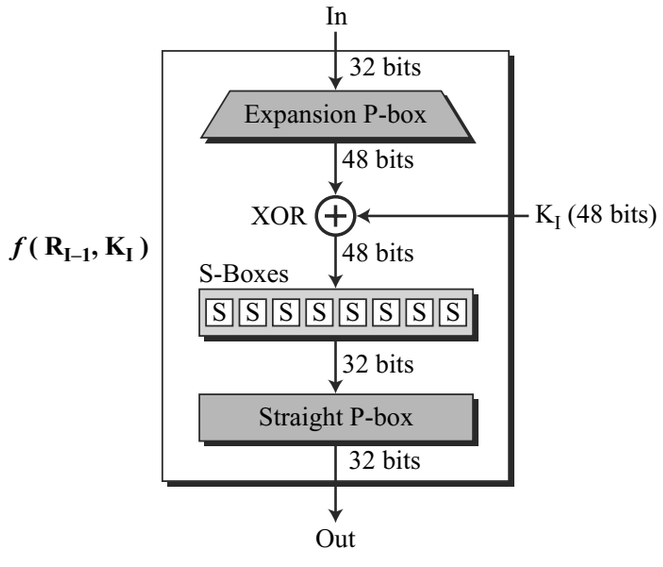
Part III: Attacks on Block-Ciphers, and use of Block Ciphers as Stream Ciphers

Priyank Kalla
Professor
Electrical & Computer Engineering

Differential Cryptanalysis Attack

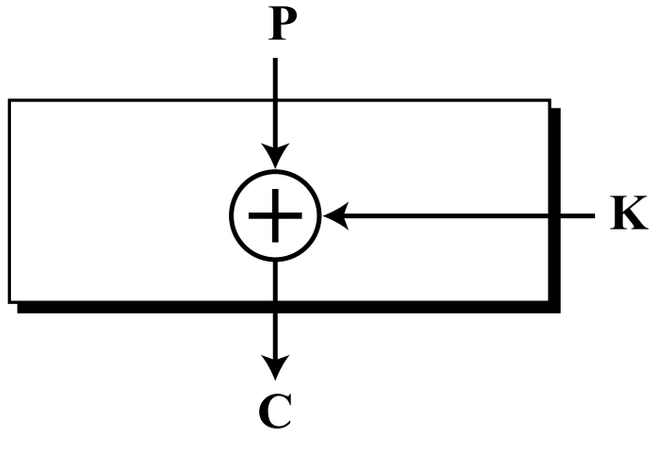
- While it is non-trivial to break DES, particularly, double- or triple DES, attacks on Block Ciphers have been studied
- One interesting attack on early block ciphers: Differential Cryptanalysis attack
- Belongs to the class of “Chosen Plain Text” Attacks
- Known/Published Cipher, Eve has access to Alice’s Computer
- Eve can generate (P_i, C_i) pairs. Objective: find out the key K





Differential Cryptanalysis Attack

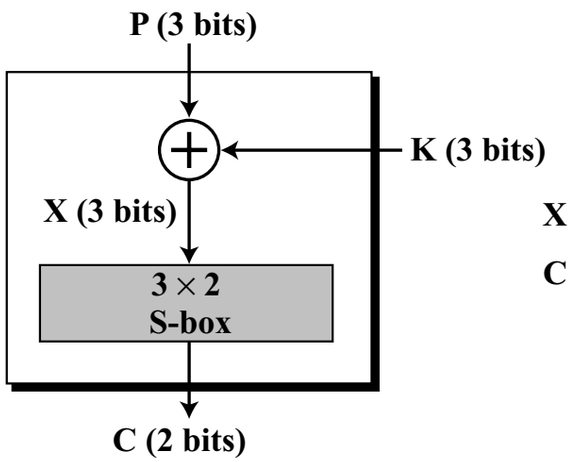
- First Step: Analyze the encryption, collect some information about (P_i, C_i) relationships
- Try to guess some bits of the key
- Use this information to try brute-force attacks on a smaller problem
- Differential Cryptanalysis: how do the “differences in plaintext” relate to the “differences in ciphertext”?



$$C_1 = P_1 \oplus K$$
$$C_2 = P_2 \oplus K$$
$$C_1 \oplus C_2 = P_1 \oplus P_2$$

Differential Cryptanalysis Attack

- Non-linearity is added by S-Boxes
- S-Box functions are known (published)
- Relationship between P & C = relationship between X & C
- Build a Differential Distribution Table (also called XOR profile)

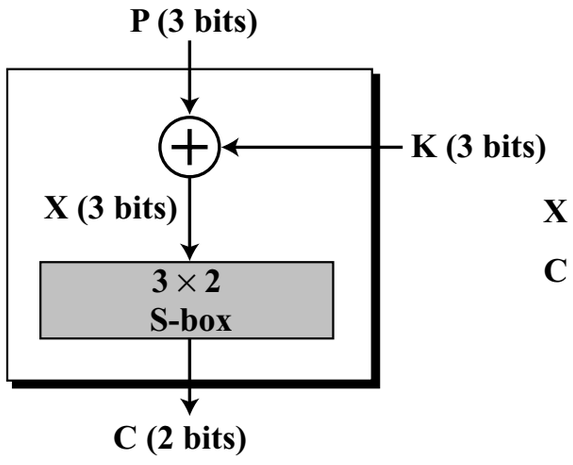


X	000	001	010	011	100	101	110	111
C	11	00	10	10	01	00	11	00

S-box table

$$X_1 \oplus X_2 = P_1 \oplus P_2$$
$$C_1 \oplus C_2 \neq P_1 \oplus P_2$$

Differential Distribution Table (DDT)



X	000	001	010	011	100	101	110	111
C	11	00	10	10	01	00	11	00

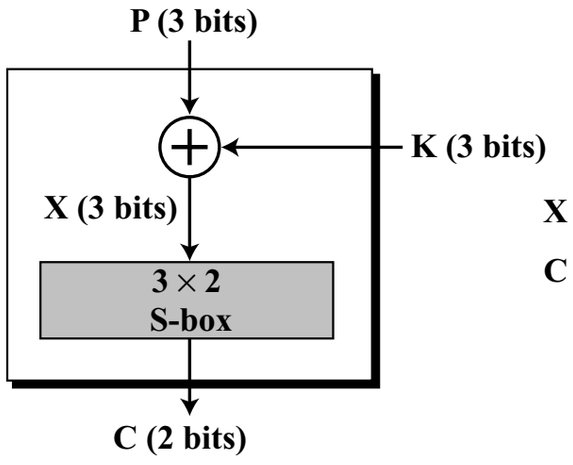
S-box table

$P_1 \oplus P_2$ \ $C_1 \oplus C_2$	*00*	*01*	*10*	*11*
000	**8**			
001	**2**	**2**		**4**
010	**2**	**2**	**4**	
011		**4**	**2**	**2**
100	**2**	**2**	**4**	
101		**4**	**2**	**2**
110	**4**		**2**	**2**
111			**2**	**6**

- $P_1 \oplus P_2 = (000) \implies C_1 \oplus C_2 = (00)$
- When $P_1 \oplus P_2 = 100$
  - Two cases $C_1 \oplus C_2 = 00$
  - Two cases 01 output diff
  - Four cases 10 output diff

- E.g.: Two cases for the 1st column
- P1 = 001, P2 = 101; C1=00, C2 = 00: Diff = 00
- P1 = 101, P2 = 001, C1 = 00, C2 = 00: Diff 00
- And so on….

Differential Distribution Table (DDT)



X	000	001	010	011	100	101	110	111
C	11	00	10	10	01	00	11	00

S-box table

$C_1 \oplus C_2$

$P_1 \oplus P_2$	*00*	*01*	*10*	*11*
000	**8**			
001	**2**	**2**		**4**
010	**2**	**2**	**4**	
011		**4**	**2**	**2**
100	**2**	**2**	**4**	
101		**4**	**2**	**2**
110	**4**		**2**	**2**
111			**2**	**6**

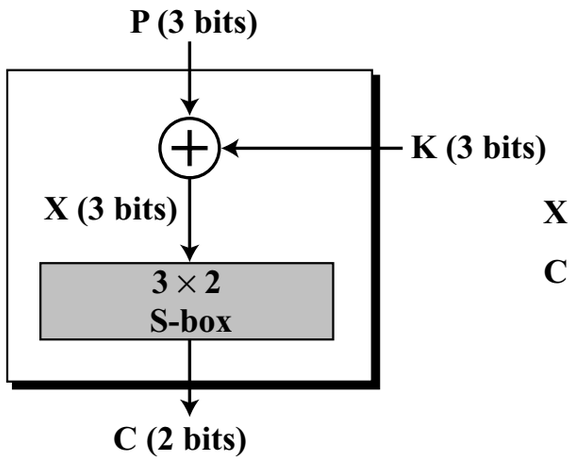
$C_1 \oplus C_2$

$P_1 \oplus P_2$	*00*	*01*	*10*	*11*
000	**1**	**0**	**0**	**0**
001	**0.25**	**0.25**	**0**	**0.50**
010	**0.25**	**0.25**	**0.50**	**0**
011	**0**	**0.50**	**0.25**	**0.25**
100	**0.25**	**0.25**	**0.50**	**0**
101	**0**	**0.50**	**0.25**	**0.25**
110	**0.50**	**0**	**0.25**	**0.25**
111	**0**	**0**	**0.25**	**0.75**

DDT

- First build a DDT
- Then launch a chosen plaintext attack…

Launch Chosen Plaintext Attack



X	000	001	010	011	100	101	110	111
C	11	00	10	10	01	00	11	00

S-box table

$P_1 \oplus P_2$ \ $C_1 \oplus C_2$

	00	*01*	*10*	*11*
000	**1**	**0**	**0**	**0**
001	**0.25**	**0.25**	**0**	**0.50**
010	**0.25**	**0.25**	**0.50**	**0**
011	**0**	**0.50**	**0.25**	**0.25**
100	**0.25**	**0.25**	**0.50**	**0**
101	**0**	**0.50**	**0.25**	**0.25**
110	**0.50**	**0**	**0.25**	**0.25**
111	**0**	**0**	**0.25**	**0.75**

- If P1 xor P2 = 001, then C1 xor C2 = 11 with 50% probability
- Choose C1 = 00, and suppose that the obtained P1 = 010
- X1 = 001, or 101, or 111

$$X \oplus P = K$$

- $001 \oplus 010 = 011$
- $101 \oplus 010 = 000$
- $111 \oplus 010 = 101$

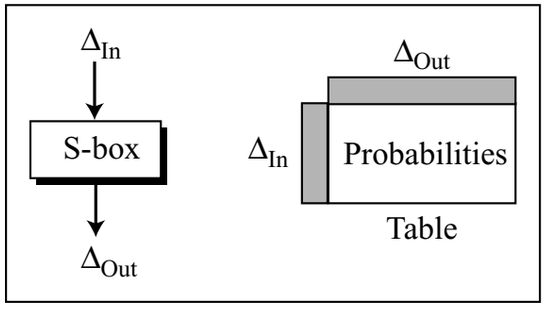
- Choose C2 = 11, and suppose the obtained P2 = 011
- X1 = 000, or 110,

$$X \oplus P = K$$

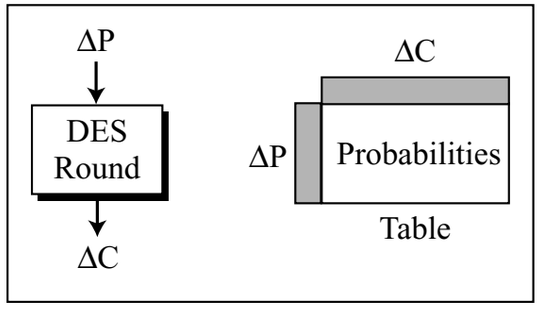
- $000 \oplus 011 = 011$
- $110 \oplus 011 = 101$
- Maybe K = 011 or 101
- Last bit of K = 1

Extending to Rounds

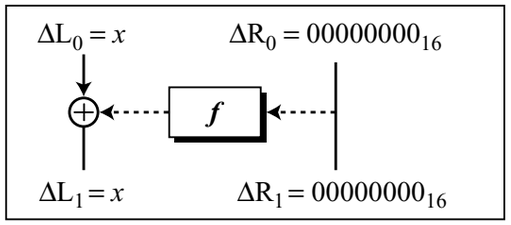
- DDT for multiple rounds of DES



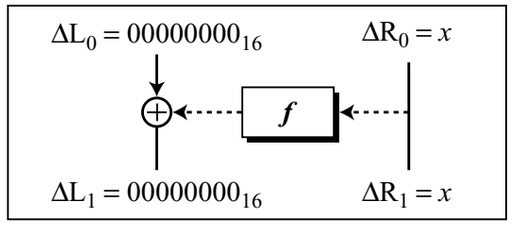
a. Differential Profile



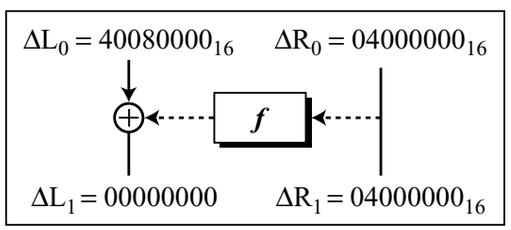
b. Round Characteristic



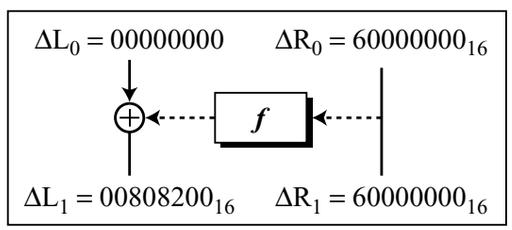
a. P = 1



b. P = 1/234



c. P = 1/4



d. P = 14/64

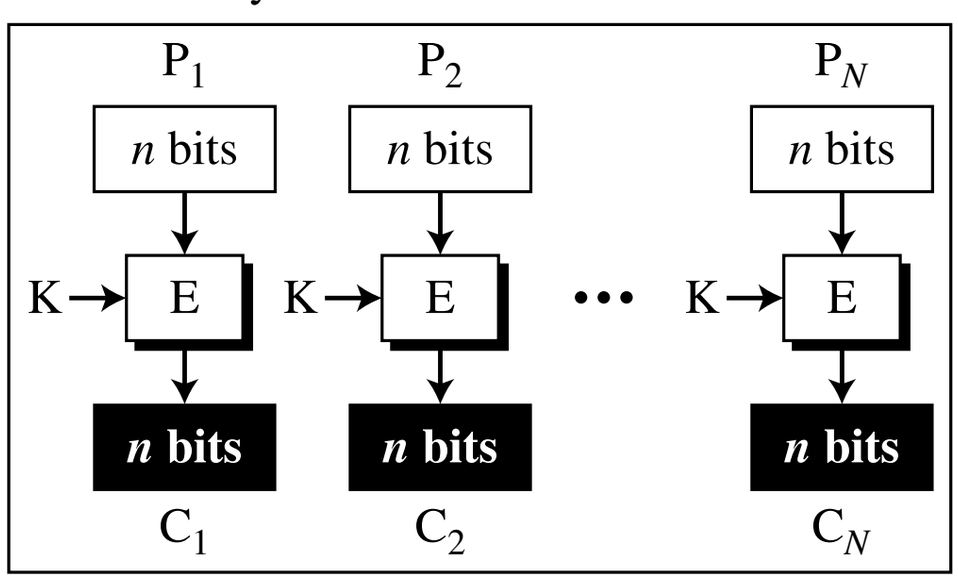
- Examples of chosen plaintext and DDTs for DES

- It has been shown using DDTs: $2^{47}(P_i, C_i)$ pairs needed to break 16-round DES using DDTs

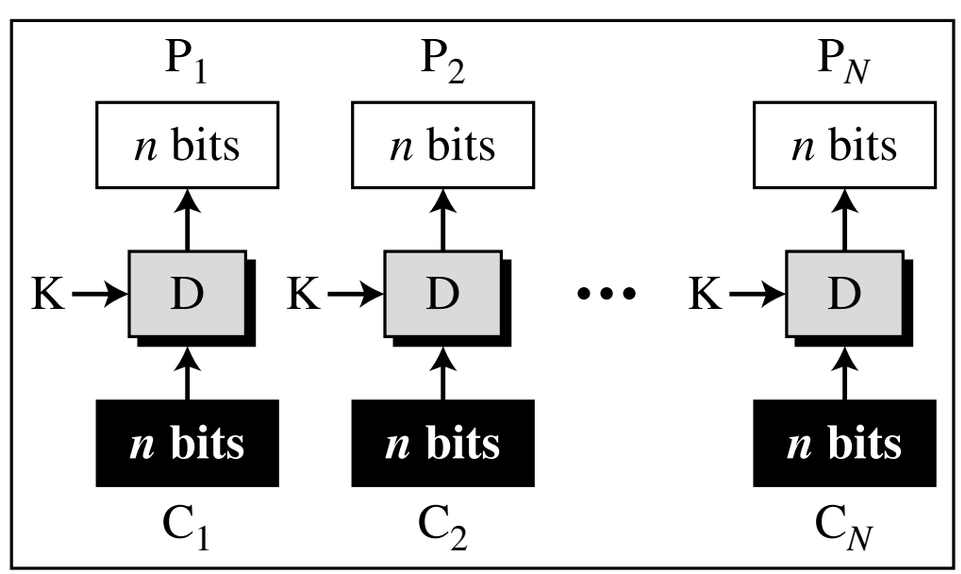
Modes of Encipherment

- When data is not 64-bits (DES) or 128 bits (AES):
- Instead of using just one Block Cipher, use different modes
- Simplest: Electronic CodeBook (ECB)

E: Encryption
D: Decryption
P_i: Plaintext block i
C_i: Ciphertext block i
K: Secret key



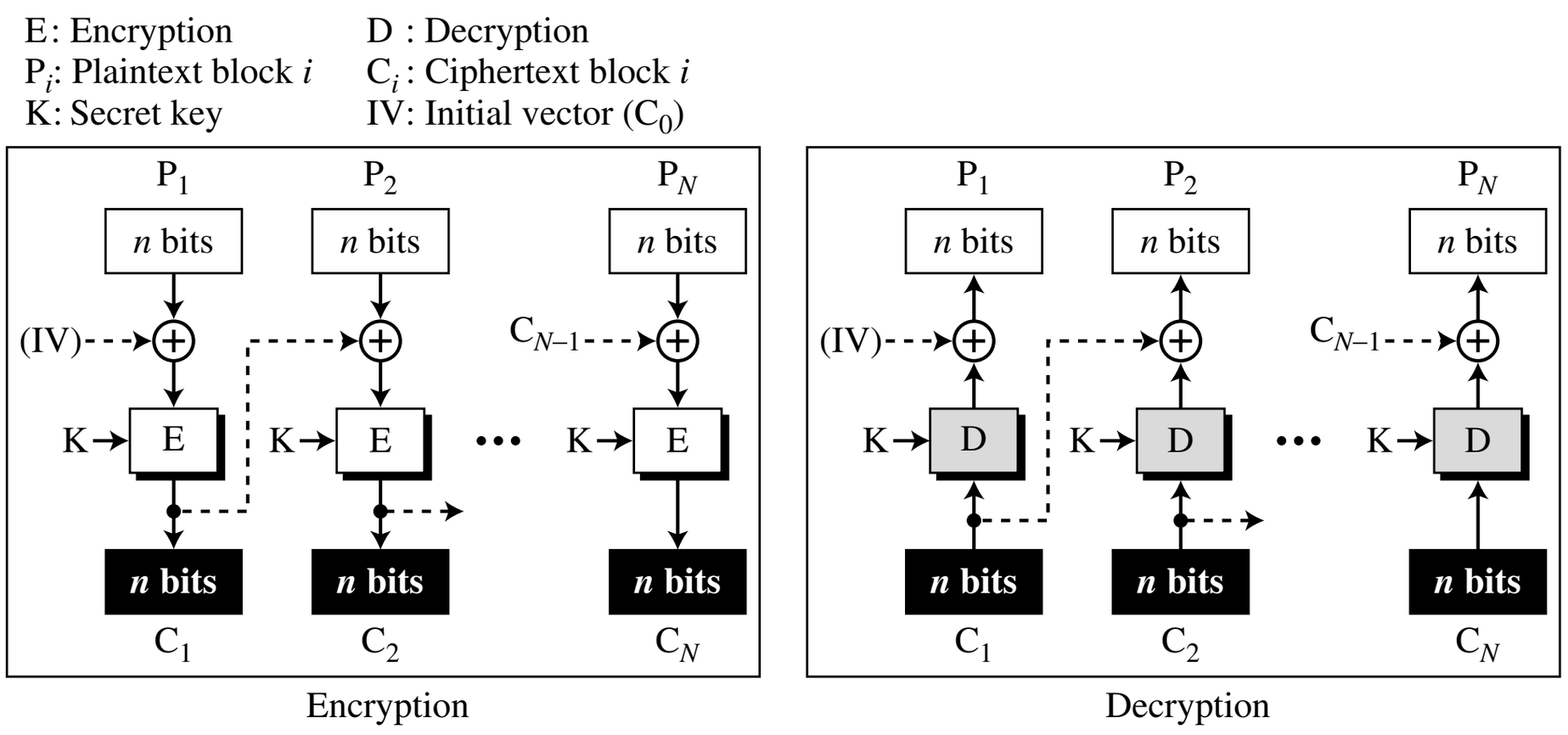
Encryption



Decryption

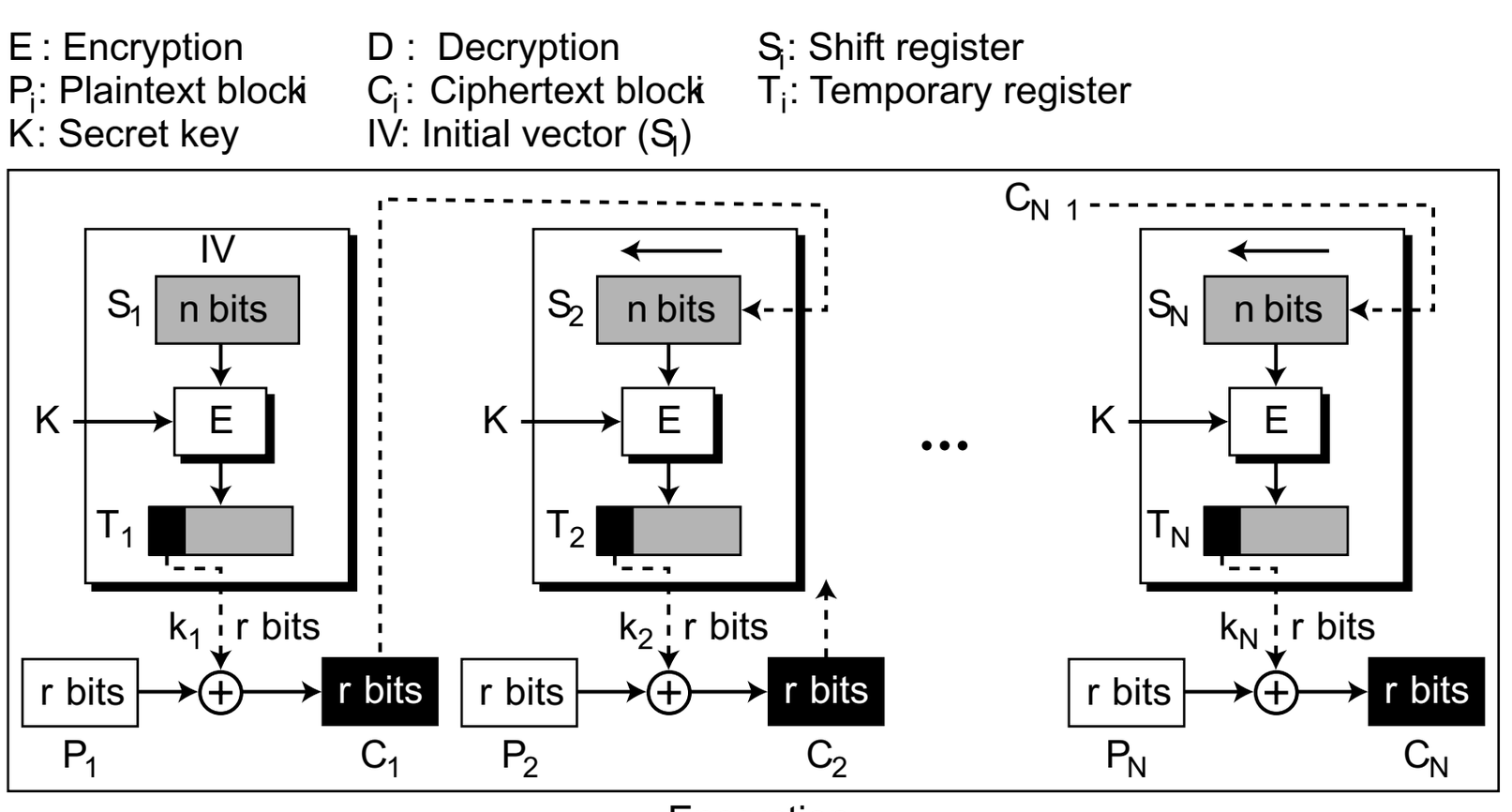
Modes of Encipherment

- Cipher Block Chain to enhance security
- Share IV, in addition to Key



Modes of Encipherment

- Cipher Feedback Mode
- When data r << 64 or 128 bits. E.g. ASCII code = r = 8 bits



Cipher Feedback Mode = Stream Cipher

E : Encryption
P_i: Plaintext block i
K: Secret key

D : Decryption
C_i : Ciphertext block i
IV: Initial vector (S_1)

S_i: Shift register
T_i: Temporary register