Mangal
Date / /20

Cryptography

Terminologies

Plaintext : Original message
Ciphertext : Coded message
Encryption : Plaintext to ciphertext
Decryption : Ciphertext to plaintext
Cryptography : Schemes for enciphering
Cryptanalysis : Trying to decipher without the knowledge of enciphering
Cryptology : Cryptography + cryptanalysis.

Encryption Mechanisms

Symmetric cipher : Use of single key for enciphering and deciphering as well.
Public key encryption : Use of different keys for encryption & decryption

Two requirements for secure encryption mechanism

* Opponent must not be able to decipher / find out the key
* Secret key must be exchanged between sender and receiver in secure way.

1800 103 5525

Mangal
Date / /20

Plaintext $X = [x_1\ x_2 \ldots x_M]$

Key $K = [k_1\ k_2 \ldots k_J]$

Encryption:
Input: Key & Plaintext
Output: Ciphertext

$Y = E_K(X)$

Decryption:
Input: key, Ciphertext
Output: Plaintext

$X = D_K(Y)$

Cryptography

* Types of operations used for transforming plaintext to ciphertext
  - Transposition: Rearrangement in plaintext
  - Substitution: Substituting for every character in plaintext
* No of keys used
  - Symmetric: Single key
  - Public key: Public + Private keys
* Way in which plaintext is processed
  - Block cipher: One block of elements at a time
  - Stream cipher: Inputs processed continuously

Mangal
Date / /20

Cryptanalysis

General cryptanalysis : Deduce plaintext/key from plaintext-ciphertext pairs

Brute force attack : Try all possible keys.

Types of attack on encrypted messages

Apart from encryption algorithm & ciphertext to be decoded;

Ciphertext only	Plaintext ciphertext pairs
Known plaintext	One plaintext ciphertext
Chosen plaintext	One ciphertext plaintext
Chosen ciphertext	Both plaintext ciphertext & ciphertext-plaintext
Chosen text	

Unconditionally secure encryption algorithm : Scheme does not contain enough information to determine uniquely the corresponding plaintext

Computationally secure encryption algorithm

Two criteria.

* Cost of breaking the cipher exceeds the value of encrypted information
* Time reqd to break the cipher exceeds the useful lifetime of information

Mangal
Date / /20

Substitution Techniques

Caesar Cipher

Encryption :- $C = E(p) = (p+k) \bmod 26$

Decryption :- $p = D(C) = (C-k) \bmod 26$

Easily the key can be recognised using brute force. because

* encryption & decryption are known
* Only 25 keys.
* language is well known.

Attack at one
↓
K = 4
↓
Exxego exsrgi

We are captured
↓
K = 4
↓
aievi get xyvith

Monoalphabetic Cipher

Based on frequency of occurence of letters in ciphertext and based upon language. the original message can be found.

We are discoverd save yourself
ug rmk csx thmuf kmt bxog evmtaluiv

Playfair Cipher

key → Playfair
hide the gold in the tree stump
hide the gold in the tree

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

* Repeating letters are separated using a filler letter x
* Plain text falling in same row are replaced with letters to its right
* Plaintext falling in same column are replaced with letters to its beneath.
* If not, every plaintext letter is replaced by letter that lies in its own row & column of the adjacent letter.

lom od zb xd na be ku dm ui xm no wif

Eg: ... ug rmk cSxhmyfent krog cvmiaMiv

Hill Cipher

Mangal
Date / /20

* Replaces m successive plaintext letters with m successive ciphertext letters

* $m = 3$

$$C_1 = (k_{11}P_1 + k_{12}P_2 + k_{13}P_3) \bmod 26$$
$$C_2 = (k_{21}P_1 + k_{22}P_2 + k_{23}P_3) \bmod 26$$
$$C_3 = (k_{31}P_1 + k_{32}P_2 + k_{33}P_3) \bmod 26.$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod 26.$$

$$C = KP \bmod 26.$$

Take $K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$

Plaintext : Pay more money $\Rightarrow$ (15,0,24) (12,14,17) (4,12,14) (13,4,24)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$C = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} \bmod 26 = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} \bmod 26 = \begin{pmatrix} 527 \\ 861 \\ 375 \end{pmatrix} \bmod 26 = \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 \\ 12 \\ 14 \end{pmatrix} \bmod 26 = \begin{pmatrix} 342 \\ 594 \\ 298 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 22 \\ 12 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 13 \\ 4 \\ 24 \end{pmatrix} \bmod 26 = \begin{pmatrix} 409 \\ 849 \\ 920 \end{pmatrix} \bmod 26 = \begin{pmatrix} 19 \\ 17 \\ 2 \end{pmatrix}$$

Mondal
Date / /20

$$\begin{pmatrix} 11 & 13 & 18 \\ L & N & S \end{pmatrix} \quad \begin{pmatrix} 9 & 1 & 3 \\ J & B & C \\ H & D & L \end{pmatrix} \quad \begin{pmatrix} 4 & 22 & 12 \\ E & W & M \end{pmatrix} \quad \begin{pmatrix} 19 & 17 & 22 \\ T & R & W \end{pmatrix}$$

Decryption

$$P = K^{-1} C \bmod 26$$

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}^{-1} = \begin{pmatrix} 300 & -357 & 6 \\ -313 & 313 & -0 \\ 267 & -252 & -5 \end{pmatrix}$$

$$\begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} =$$

$$17(300) - 17(357) + 5(6)$$

$$5100 - 6069 + 30$$

$$-939$$

$$17 \times 18 - 17 \times 21$$
$$17(18 - 21)$$
$$17(-3)$$

3

$$P = K^{-1} C \bmod 26$$

$$= \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} \bmod 26 = \begin{pmatrix} 431 \\ 494 \\ 570 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} P \\ A \\ Y \end{pmatrix}$$

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} 220 \\ 222 \\ 355 \end{pmatrix} \bmod 26 = \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix}$$

$$= \begin{pmatrix} M \\ O \\ R \end{pmatrix}$$

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 4 \\ 22 \\ 12 \end{pmatrix} = \begin{pmatrix} 394 \\ 506 \\ 300 \end{pmatrix} \bmod 26$$

Mangal
Date / /20

$$= \begin{pmatrix} 4 \\ 12 \\ 14 \end{pmatrix} = \begin{pmatrix} E \\ M \\ O \end{pmatrix}$$

$$\begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 19 \\ 17 \\ 22 \end{pmatrix} = \begin{pmatrix} 559 \\ 706 \\ 830 \end{pmatrix} \bmod 26 = \begin{pmatrix} 13 \\ 4 \\ 24 \end{pmatrix} = \begin{pmatrix} N \\ E \\ Y \end{pmatrix}$$

* Hides single letter frequencies
* Strong against ciphertext only attack
* Can be broken with plaintext attack

Polyalphabetic Ciphers

Similarities between monoalphabetic and polyalphabetic ciphers

- Use of related monoalphabetic substitution rules.
- Key determines which particular rule is chosen for a given transformation

Vigenere Cipher

Plaintext → / Key ↓	a	b	c	d	...	z
a	a	b	c	d	...	z
b	b	c	d	e	...	a
...						
z	z	a	b	c	...	y

Date / /20

Key: deceptive deceptive
Plaintext: we are discovered

ZICVTWQNGRZVTW

Encryption $c_i = p_i \oplus k_i$
Decryption $p_i = c_i \oplus k_i$
} Vernam cipher

One time pad

* Use a key as long as the message with no repetitions.
* Produces random output

Limitations

* Problem of making large quantities of random keys
* Problem of key distribution & protection

Transposition Techniques

Rail fence

Plaintext: Meet me after the toga party

M e m a t r h t g
e t e f e t e o a
a t

Ciphertext:
Mematrhtg pr y etefeteoaat

Single transposition

Mangal
Date / /20

Plaintext : Attack postponed until two am

key : 4 3 1 2 5 6 7

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

Ciphertext : ~~ttaa~~ ttnaaptmtsuoaodwcoixknlypetz

Double transposition

4	3	1	2	5	6	7
t	t	n	a	a	p	t
m	t	s	u	o	a	o
d	w	c	o	i	x	k
n	l	y	p	e	t	z

Ciphertext : nscyauoptwltmdnaoiepaxtbokz

Rotor Machines

Single cylinder with 26 input & 26 output pins with internal wiring between one-to one i/p - o/p pins. Internal wiring changes during operation (Monoalphabetic substitution)
When output pin of one cylinder is connected to input pin of another cylinder, cryptanalysis becomes difficult

Steganography

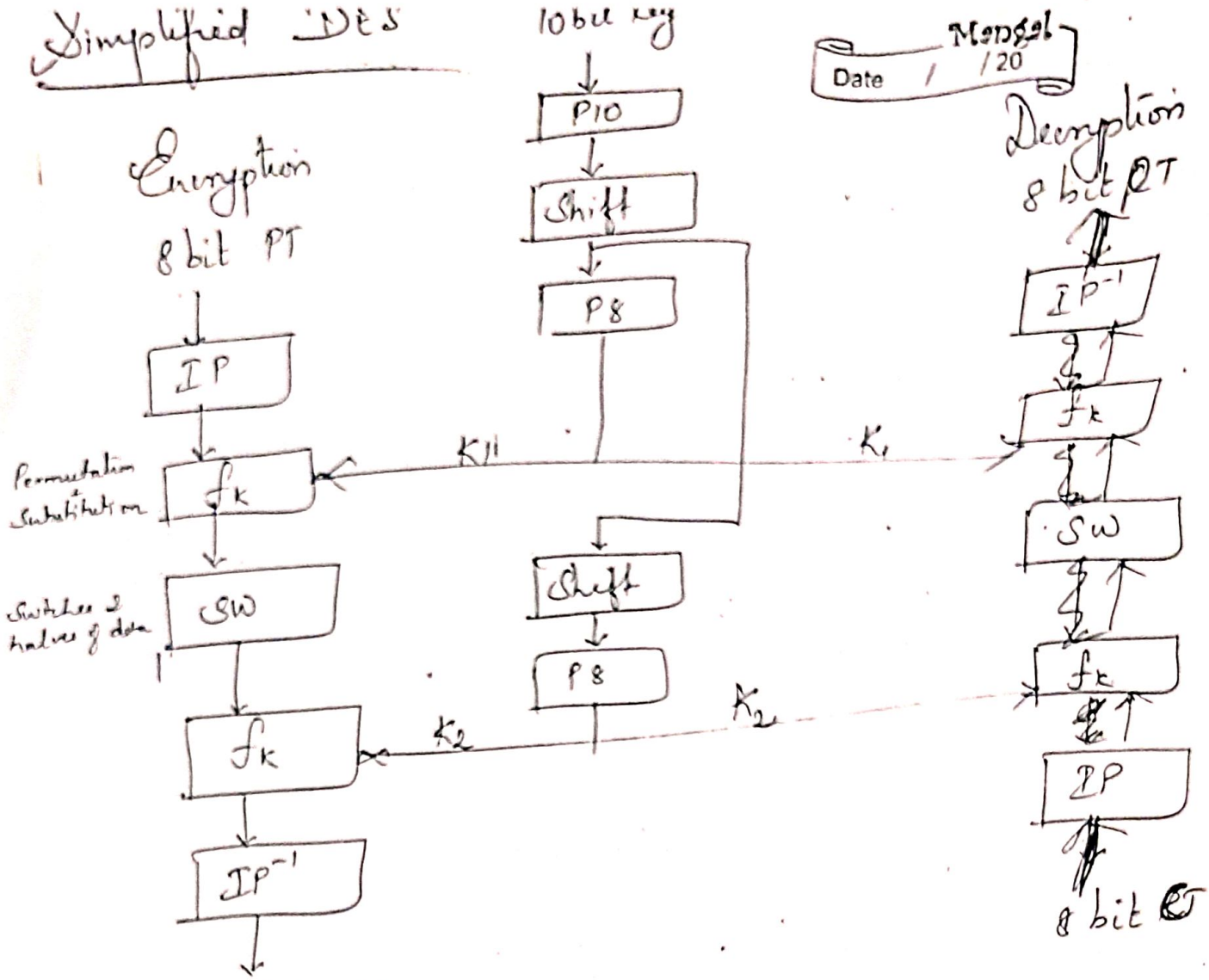
Mangal
Date / /20

* Method of concealing the message.

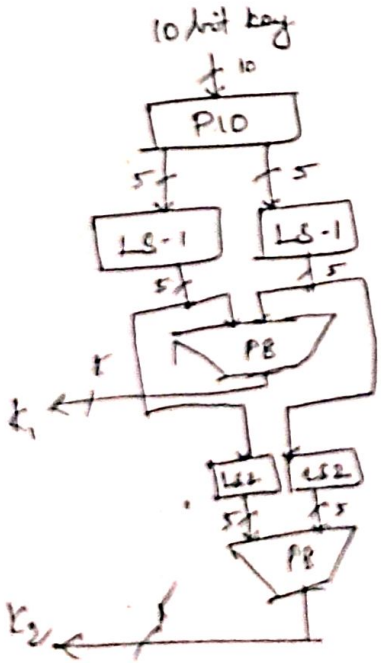
Techniques used historically

* Character marking : Marks are visible when held at certain angle to bright light
* Invisible ink : Message is visible only when chemical/heat is applied
* Pin punctures : Small pin punctures on selected letters
* Typewriter correction ribbon :

Simplified DES



S-DES Key Generation



P10 => 3, 5, 2, 7, 4, 10, 1, 9, 8, 6

Example => 10 bit key 10100 00010

P_{10} => 10000 01100

LS1 => 00001 11000

P_8 => 6, 3, 7, 4, 8, 5, 10, 9

K_1 10100100

LS_2 => 00010 10001

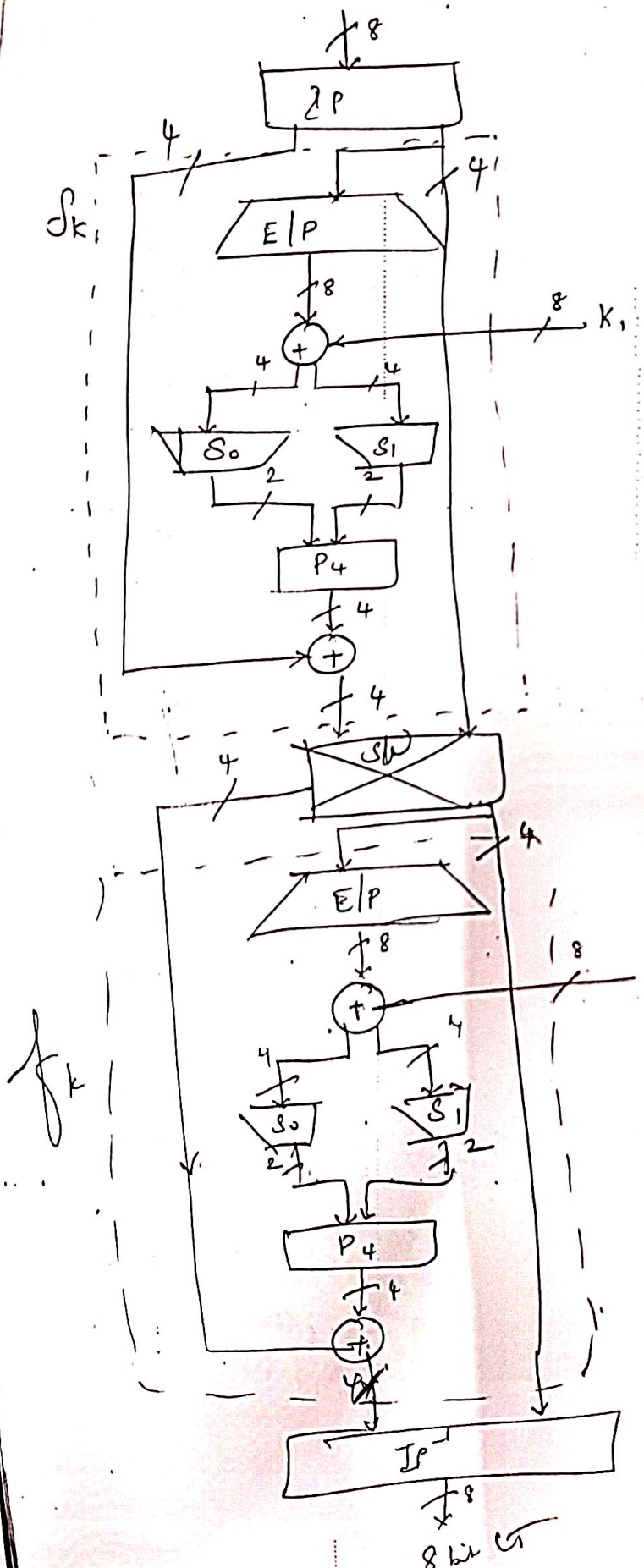
00100 00011

P_8 => ~~10010010~~ (01000011)

S-DES Encryption

Mondal
Date / /20

8 bit PT



IP

2	6	3	1	4	8	5	7

IP^{-1}

4	1	3	5	7	2	8	6

$f_k(L,R) = (L \oplus F(R, SK), R)$

E/P

4	1	2	3	2	3	4	1

n_4	n_1 n_2		n_3
n_2	n_3 n_4		n_1

EXOR with K_1

$n_4 + k_{11}$	$n_1 + k_{12}$	$n_2 + k_{13}$	$n_3 + k_{14}$
$n_2 + k_5$	$n_3 + k_{16}$	$n_4 + k_{17}$	$n_1 + k_{18}$

$P_{0,0}$	$P_{0,1}$	$P_{0,2}$	$P_{0,3}$
$P_{1,0}$	$P_{1,1}$	$P_{1,2}$	$P_{1,3}$

Output of S box

S_0 — P_{00} P_{03}

S_1 — P_{01} P_{02}

2	4	3	1

D1

Mangal
Date / /20

Key Generation

10 bit key => 11000 11110

P10
3, 5, 2, 7, 4, 10, 1, 9, 8, 6 => 0011100111

=> 01100 11110

LS1

=> 1110 1001 → K1

P8
6, 3, 7, 4, 8, 5, 10, 9

=> 10001 11011

LS2

=> 1010 0111 → K2

P8
6, 3, 7, 4, 8, 5, 10, 9

SDES Encryption

Plaintext - 0010 1000

IP → 0010 0010

E|P → 0 0 0 1 / 0 1 0 0 => 0001 0100

E|P ⊕ K1 =>

0⊕1	0⊕1	0⊕1 | 1⊕0
0⊕1	1⊕0	0⊕0 | 0⊕1

=>

1	1	1	1
1	1	0	1

=> 1111 1101

	C0	C1	C2	C3
S0 R0	1	0	3	2
R1	3	2	1	0
R2	0	2	1	3
R3	3	1	3	2

	C0	C1	C2	C3
S1 R0	0	1	2	3
R1	2	0	1	3
R2	3	0	1	0
R3	2	1	0	3

S0 => 1st => Row 3 Col 3 => 2 => 10

S1 => 1st Row 3 Col 2 => 0 => 00

1000

P4 ⇒ 0001

Mondal
Date / /20

SDES
8 bit

L ⊕ P4 0010 ⊕ 0001 ⇒ 0011

R 0010

SW ⇒ 0010 0011

E/P ⇒ 1 0 0 1
0 1 1 0 ⇒ 1001 0110

E/P ⊕ K_2 ⇒ 1 0 0 1 0 1 1 0
1 0 1 0 0 1 1 1
0 0 1 1 0 0 0 1

0	0 1 1
0	0 0 1

S_0 ⇒ Row 01 Col 01 ⇒ Row 1, Col 1 ⇒ 2 ⇒ 10

S_1 ⇒ Row 01 Col 00 ⇒ Row 1, Col 0 ⇒ 2 ⇒ 10

Sbox ⇒ 1010

P4 ⇒ 0011

P4 ⊕ SW ⇒ 0 0 1 0 ⊕
0 0 1 1
0 0 0 1

P^{-1} = 4 1 3 5 7 2 8 6

0 0 0 1 | 0 0 1 1
P4⊕SW | R

Ans: 1000 1010

SDES Decryption:

Mangal
Date / /20

8 bit CT :- 1000 1010

0001 0011

IP :-
2, 6, 3, 1, 4, 8, 5, 7

EP of R :- 1 0 0 1 ⇒ 1001 0110
0 1 1 0

EP of R ⊕ K_1 :- 1001 0110 ⊕
1110 1001
0111 1111

S_0 : 01 Row, 11 Col ⇒ 1 Row, 3 Col = 00 (0)
11 Row, 11 Col ⇒ 3 Row, 3 Col = 11 (3) } 0011

S_1 :

P_4 : 0110

2 4 3 1

L ⊕ P_4 ⇒ 0001 ⊕
0110
0111
0010 ⇒ 0011 0111
~~1010~~

SW :- 0111 0010

EP of R ⇒ 1011 ⇒ 1011 1110
1110

EP(R) ⊕ K_2 = 1011 1110 ⊕
1010 0111
0001 1001

S_0 - 01 Row 00 Col = 1 Row, 0 Col = 3 (11) } 1110
S_1 = 11 Row, 00 Col ⇒ 3 Row, 0 Col = 2 (10)

P_4 = 1011

L ⊕ P_4 = ~~1010~~ 0011 ⊕
~~1011~~ 1011
~~0001~~ 1000

IP⁻¹ (1000 0111) ⇒
~~0000 1011~~
~~1000 1011~~
9 1 3 5 7 2 8 6
0100 1011

Block Cipher Principles

Date / / Mangal 120

Motivation for Feistel Cipher structure.

Plaintext (n bits) → Block Cipher → Ciphertext (n bits)

There are 2^n possible different PT blocks and for encryption to be reversible, each must produce unique CT block. Only then the transformation is reversible.

Reversible Mapping

PT	CT
00	11
01	10
10	00
11	01

Irreversible Mapping

PT	CT
00	11
01	10
10	01
11	01

Eg: 4 bit I/P — 16 possible I/P states must be mapped to unique 16 possible O/P states.
But n should be large and reversible substitution between CT and PT, cryptanalysis becomes infeasible.

Feistel Cipher

Diffusion & Confusion

The cryptanalyst can deduce the keys if the statistical nature of plaintext can be found even in the ciphertext.

Diffusion: Statistical structure of PT is dissipated into long range statistics of CT.

Mangal
Date / /20

So, each PT digit affects the value of many CT digits and each CT digit is affected by many PT digits.

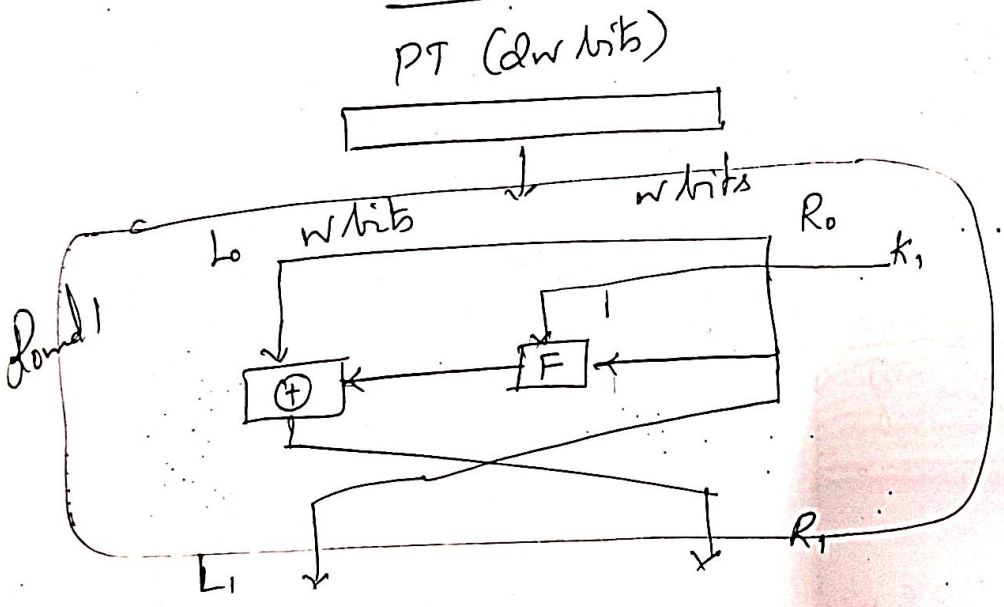
$$y_n = \sum_{i=1}^{k} m_{n+i} \bmod 26$$

adding k successive letters to CT y_n.

Msg $M = m_1 m_2 \ldots m_n$

While diffusion makes statistical relationship between CT and PT complex, confusion makes statistical relationship between CT and key as complex as possible. Confusion is achieved using complex substitution algorithm.

Classical Feistel Network



PT is divided into two halves L_0 and R_0. Round function F is applied to R. This is ⊕ with L. The resultant L and R are swapped

CT (2w bits)

Design features of Feistel network.

Mandal
Date / /20

Block size: Larger block size preferred. with reduced encryption/decryption speed. (64 bits)

Key size: Larger key size (64 bits)

No of rounds: Multiple instead of single rounds (16)

Subkey generation algorithm:

Round fn: Greater resistance to cryptanalysis

Fast software encryption/decryption.

Ease of analysis: DES does not have easily analyzed functionality.

Feistel Decryption Algorithm

Decryption is done in the same way like encryption but keys are used in ~~different~~ reverse order

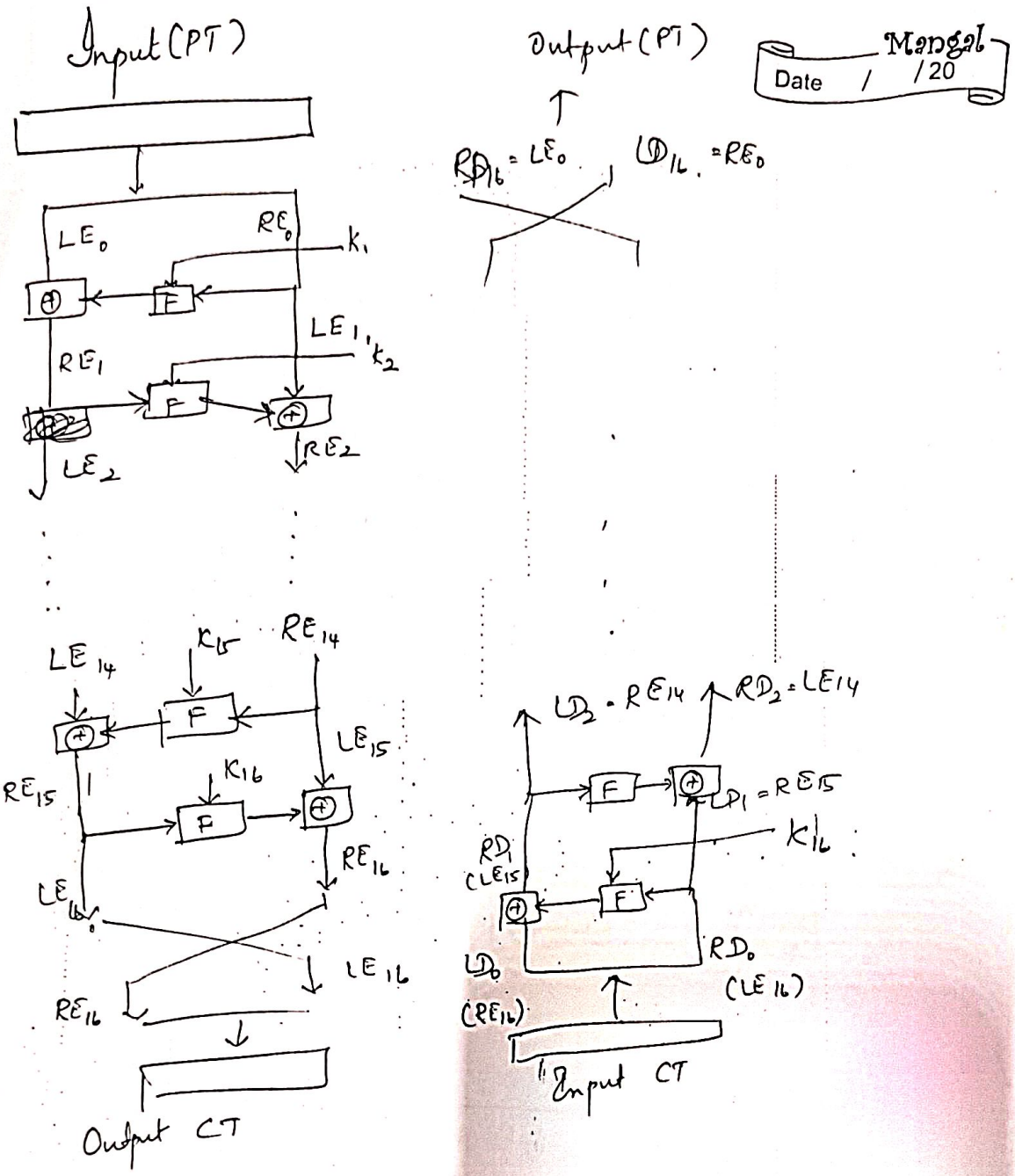
The intermediate value of decryption is equal to the corresponding value of encryption with left and right halves swapped.

Encryption

$$LE_{16} = RE_{15}$$
$$RE_{16} = LE_{15} \oplus F(K_{16}, RE_{15})$$

Decryption

$$LD_1 = RD_0 = LE_{16} = RE_{15}$$
$$RD_1 = LD_0 \oplus F(K_{16}, RD_0) \quad [\because LD_0 = RE_{16}]$$
$$= RE_{16} \oplus F(K_{16}, RE_{15})$$
$$= [LE_{15} \oplus F(K_{16}, RE_{15})] \oplus F(K_{16}, RD_0)$$
$$= LE_{15}$$


Input (PT)
Output (PT)
Mangal
Date / /20
$RD_{16} = LE_0$
$LD_{16} = RE_0$
LE_0
RE_0
K_1
F
LE_1
K_2
RE_1
RE_2
LE_2
LE_{14}
K_{15}
RE_{14}
LE_{15}
RE_{15}
K_{16}
RE_{16}
LE_{16}
RE_{16}
Output CT
$LD_2 = RE_{14}$
$RD_2 = LE_{14}$
$LD_1 = RE_{15}$
K_{16}
RD_1 (LE_{15})
RD_0 (LE_{16})
LD_0 (RE_{16})
Input CT

SDES Decryption

Date / /20 Mangal

8bit CT: 1000 1010

IP (2 6 3 1 4 8 5 7) = 0001 0011

EIP(R) = 1001 0110 (1 0 0 1 / 0 1 1 0)

EIP(R) ⊕ K_2 = 1001 0110 ⊕ 1010 0111 = 0011 0001

S_0 : 01 Row, 01 Col ⇒ Row 1, Col 3 ⇒ 2 (10)

S_1 : 00 Row, 00 Col ⇒ Row 0, Col 0 ⇒ 2 (10) → 1010

P_4 (2 4 3 1) : 0011

L ⊕ P_4 = 0001 ⊕ 0011 = 0010 (L of IP)

SW : 0010 0011 ⇒ 0011 0010

EIP of R ⇒ 0 0 1 0 / 0 0 0 0 ⇒ 0010 0000

EIP(R) ⊕ K_1 = 0010 0000 ⊕ 1110 1001 = 1100 0001

S_0 = 11 Row, 00 Col = Row 3, Col 0 = 3 (11)

S_1 = 00 Row, 01 Col = Row 0, Col 1 = 1 (01) → 1101

P_4 (2 4 3 1) = 1101

Mangal
Date / /20

$L \oplus P_4 =$ 1101 / 0100

$\mathcal{E}P^{-1}$ (0100 0100)

4135 7286

$E[P(R) = 0001 0100 = 0001 0100$

$E[P(R) \oplus K_1 =$ 1001 0110 / 1110 1001 / 0111 1111 = 0001 0100 / 1110 1001 / 1111 0101

$S_0 =$ 01 Row, 11 Col = Row 1, Col 3 = 0 (00)
$S_1 =$ 11 Row, 11 Col = Row 3, Col 3 = 3 (11) } 0011

$P_4 (2431) =$ 0110

$L \oplus P_4 =$ 0011 / 0110 / 0101

IP^{-1} (0101 0010)

$S_0 =$ Row 3 Col 3 = 2 (10)
$S_1 =$ Row 3 Col 2 = 0 (00) } 1000

$P_4 (2431) =$ 0001

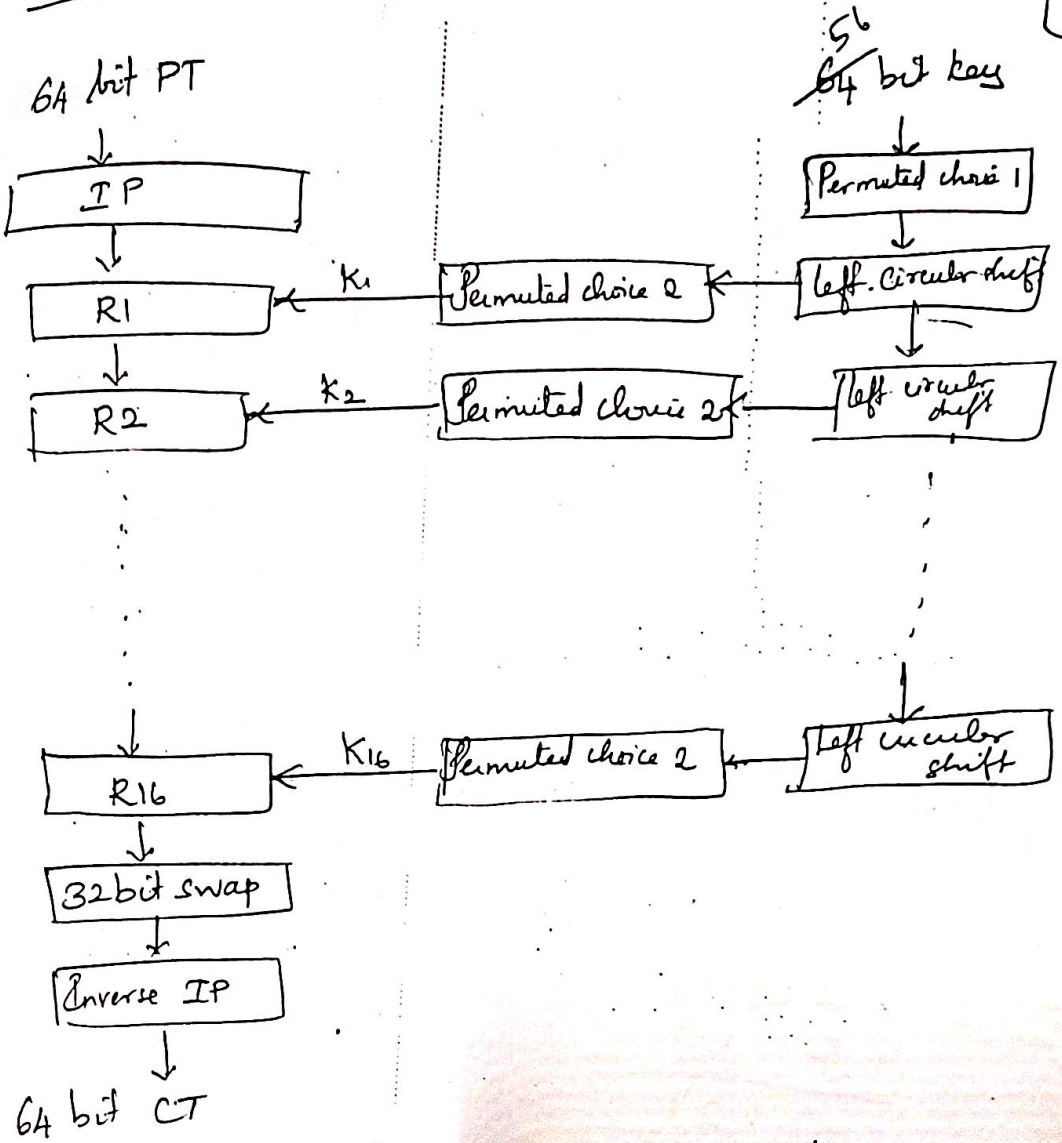
$L \oplus P_4 =$ 0011 / 0001 / 0010

IP^{-1} (0010 0010) = 0010 1000

4135 7286

Plaintext

DES

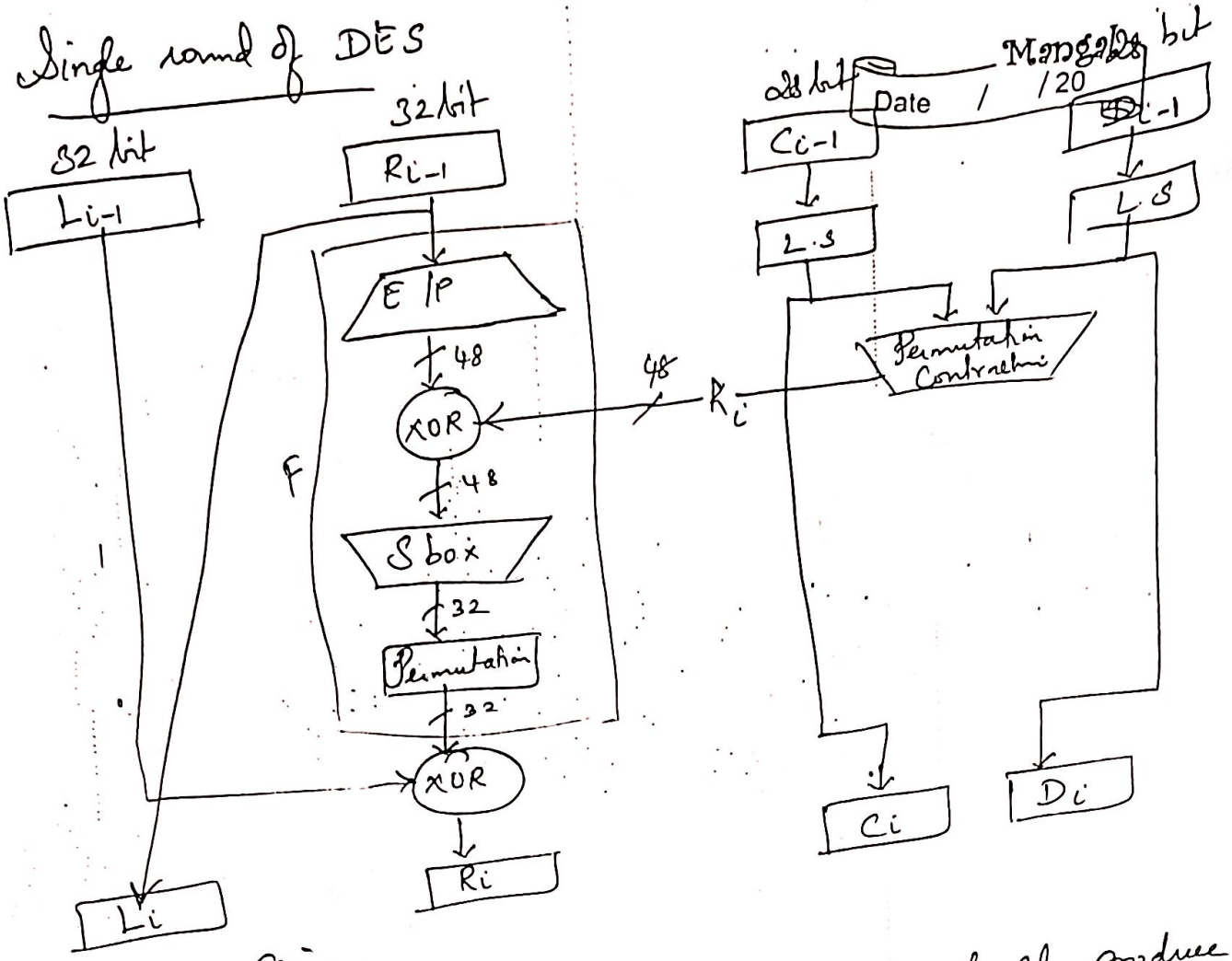


IP(M)

M_{58} M_{50} M_{42} M_{34}

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Single round of DES



Avalanche Effect:

Small change in plaintext or key should produce significant change in ciphertext.

Strength of DES

* Can't be broken by brute force approach.
* Fairly resistant to timing attack.

Differential and Linear Cryptanalysis.

Mandal
Date / /20

Original PT block m is split into 2 halves - m_0 and m_1.
At each round of DES, right hand and left hand outputs are swapped. & right hand output is function of left hand output & subkey.

$$m_{i+1} = m_{i-1} \oplus f(m_i, k_i) \qquad i = 1, 2, \ldots, 16.$$

In differential cryptanalysis, two messages m and m' their XOR difference $\Delta m = m \oplus m'$
Consider difference between intermediate message halves

$$\Delta m_{i+1} = m_{i+1} \oplus m'_{i+1}$$
$$= \left[m_{i-1} \oplus f(m_i, k_i)\right] \oplus \left[m'_{i-1} \oplus f(m'_i, k_i)\right]$$
$$= \Delta m_{i-1} \oplus \left[f(m_i, k_i) \oplus f(m'_i, k_i)\right]$$

Linear Cryptanalysis.

Mangal
Date / /20

Objective of linear cryptanalysis is to find an effective linear equation of the form

$$P[\alpha_1 \alpha_2 \ldots \alpha_a] \oplus C[\beta_1 \beta_2 \ldots \beta_b] = k[\gamma_1, \gamma_2 \ldots \gamma_c)$$

that holds with probability $p \neq 0.5$

Block Cipher Design Principles

DES Design Criteria

* No o/p bit of any S box should be a linear function of i/p bits
* Each row of S box should include all 16 possible output bit combinations.
* If two i/ps to S box differ in exactly 1 bit, outputs must differ in at least 2 bits
* If two i/ps to S box differ in two middle bits, outputs must differ in at least 2 bits
* If two i/ps to S box differ in first 2 bits but not same in last two bits, the two outputs must not be same
* for 6 bit difference b/w i/p's no more than 8/32 pairs of i/ps may result in same o/p difference

Number of rounds

By making cryptanalytic attacks only slightly less efficient than brute-force, DES algorithm stands secure against such attack. 15/16 rounds will make differential cryptanalysis better than brute force

Design of function F

Mangal
Date / /20

Design criteria for F

If F is more nonlinear, it will be difficult to break using cryptanalysis.

Strict avalanche criterion (SAC) states that any output bit j of S box should change with probability 0.5 when any single input bit i is inverted for all i, j.

Bit independence criterion (BIC) – Output bits j and k should change independently when any single bit i is inverted for all i, j and k.

SAC + BIC strengthens the confusion function.

S-box design

The characteristic of S box is its size. Larger S boxes are more resistant to cryptanalysis and more difficult to design. Limit on S box input is imposed as 8–10.

S boxes should satisfy SAC + BIC. All linear combinations of S box columns should be bent (special class of Boolean functions that are highly nonlinear)

Guaranteed avalanche criterion

S box satisfies GA of order 2 if for 1 bit input change, at least 2 output bits change.

$2 \leq 2 \leq 5$

S box design must be done using the following approaches.

Date / /20

* Random :- Pseudorandom number generation from some table of random digits to generate entries in S box
* Random with testing :- S box entries chosen randomly and tested
* Human-made :- Technique used in DES design & difficult to carry through for large S boxes.
* Math-made : Based on mathematics.

Key Schedule Algorithm

Subkeys are selected to maximize the difficulty of deducing individual subkeys and difficulty of working back to main key.

Block Cipher Modes of operation

1. Electronic Codebook Mode

Plaintext is handled 64 bits at a time and they are encrypted using same key. There is an unique cipher text for each block of plaintext. If message is longer than 64 bits break the message into 64 bit blocks and pad the last block if necessary. Decryption is also done using the same key on 64 bit block.

* Ideal for small amount of data
* Same 64 bit block plaintext when it gets repeated, it produces same 64 bit ciphertext
* Insecure for lengthy messages.
* Easy to cryptanalyse when there are regularities in the message.

2. Cipher Block Chaining Mode

Mandal
Date / / 20

The input to encryption algorithm is XOR of PT and preceding CT. Same key is used for processing all the blocks. Repeating patterns of 64 bits are not exposed.

For decryption, ciphertext block is XORed with previous cipher block. The encryption and dyrption process is modeled as:

$$C_j = E_k[C_{j-1} \oplus P_j]$$

$$D_k[C_j] = D_k\left[E_k[C_{j-1} \oplus P_j]\right]$$

$$= C_{j-1} \oplus P_j$$

$$C_{j-1} \oplus D_k[C_j] = C_{j-1} \oplus C_{j-1} \oplus P_j = 0 \oplus P_j = P_j$$

IV must be known to both sender and receiver. IV must be protected like the key and hence it is sent using ECB encryption.

$$C_1 = E_k(IV \oplus P_1)$$

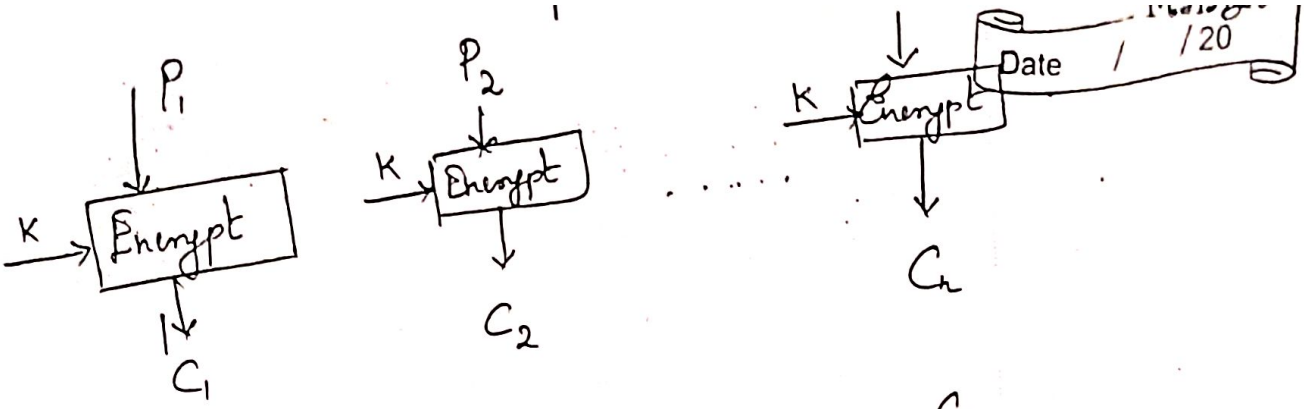
$$P_1 = IV \oplus D_k(C_1)$$

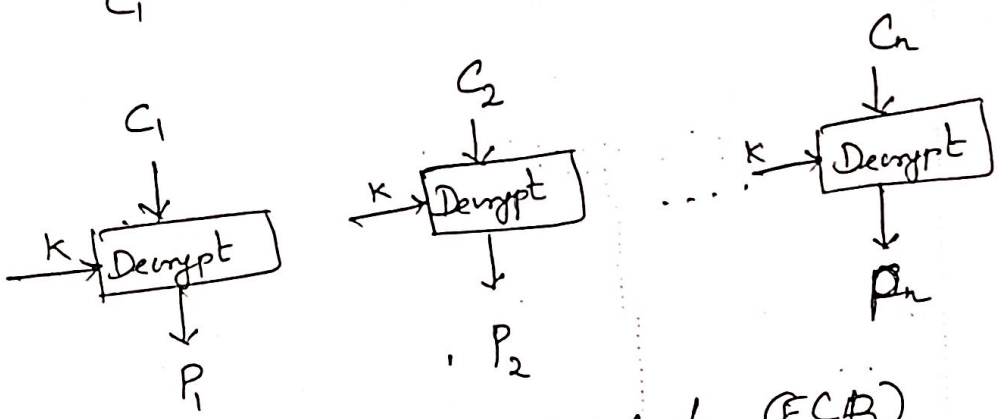
Consider X[i] to be ith bit of 64 bit quantity X.

$$P_1[i] = IV[i] \oplus D_k(C_1)[i]$$

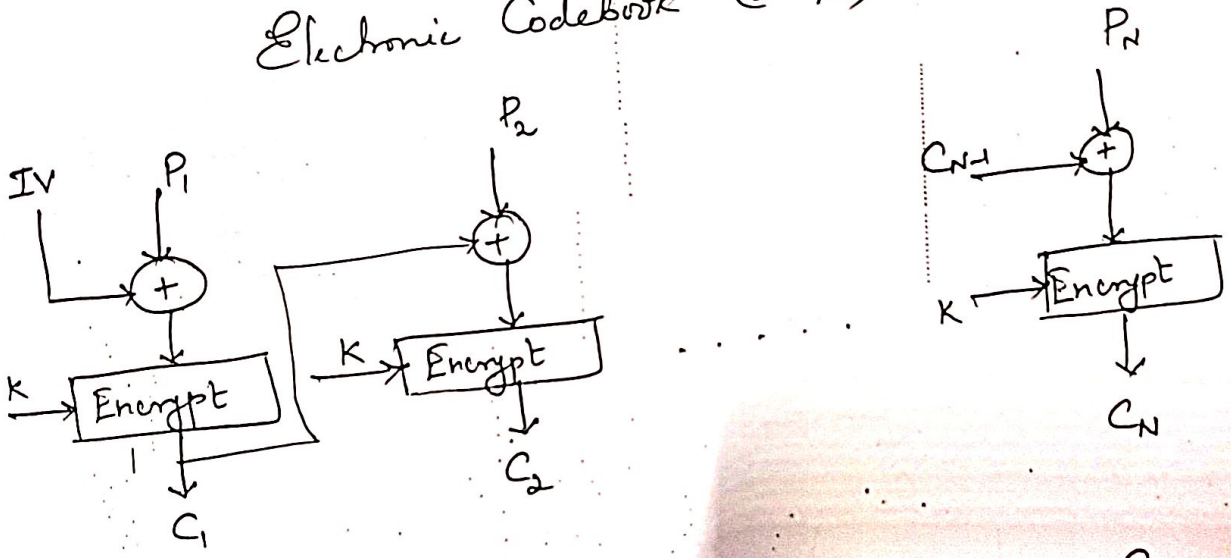
If opponent inverts the bit

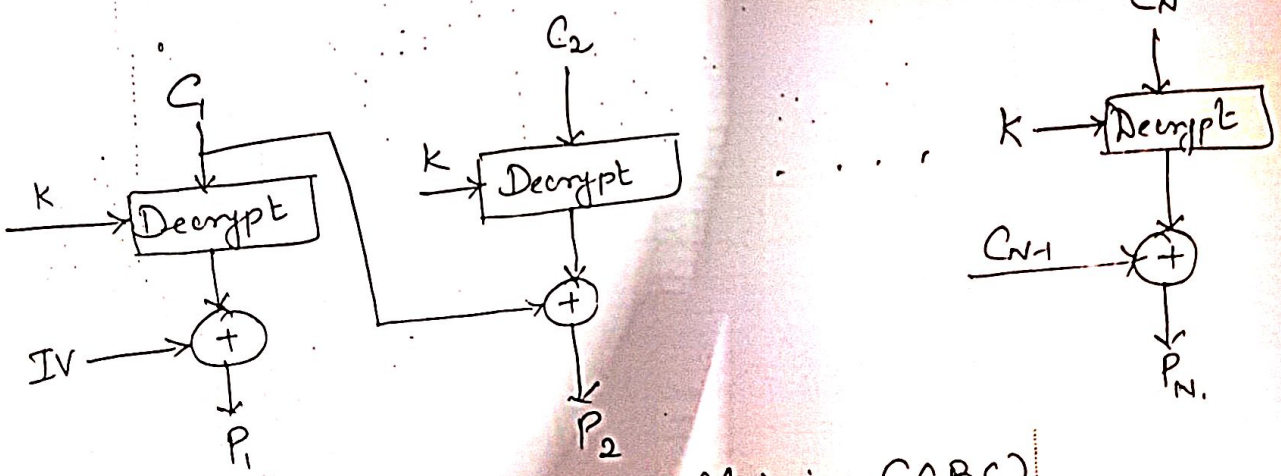
$$P_1[i]' = IV[i]' \oplus D_k(C_1)[i]$$





Electronic Codebook (ECB)





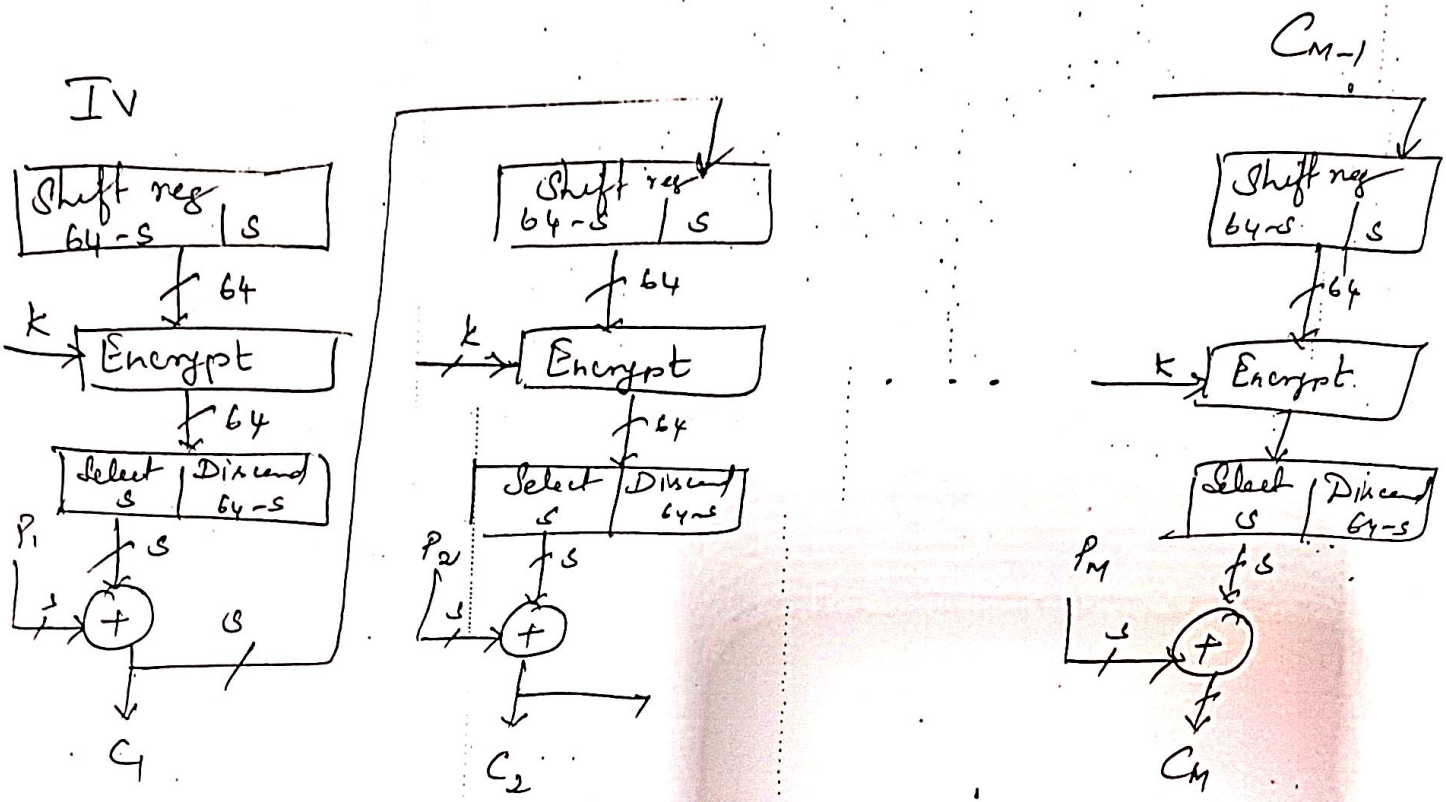
Cipher Block Chaining (CBC)

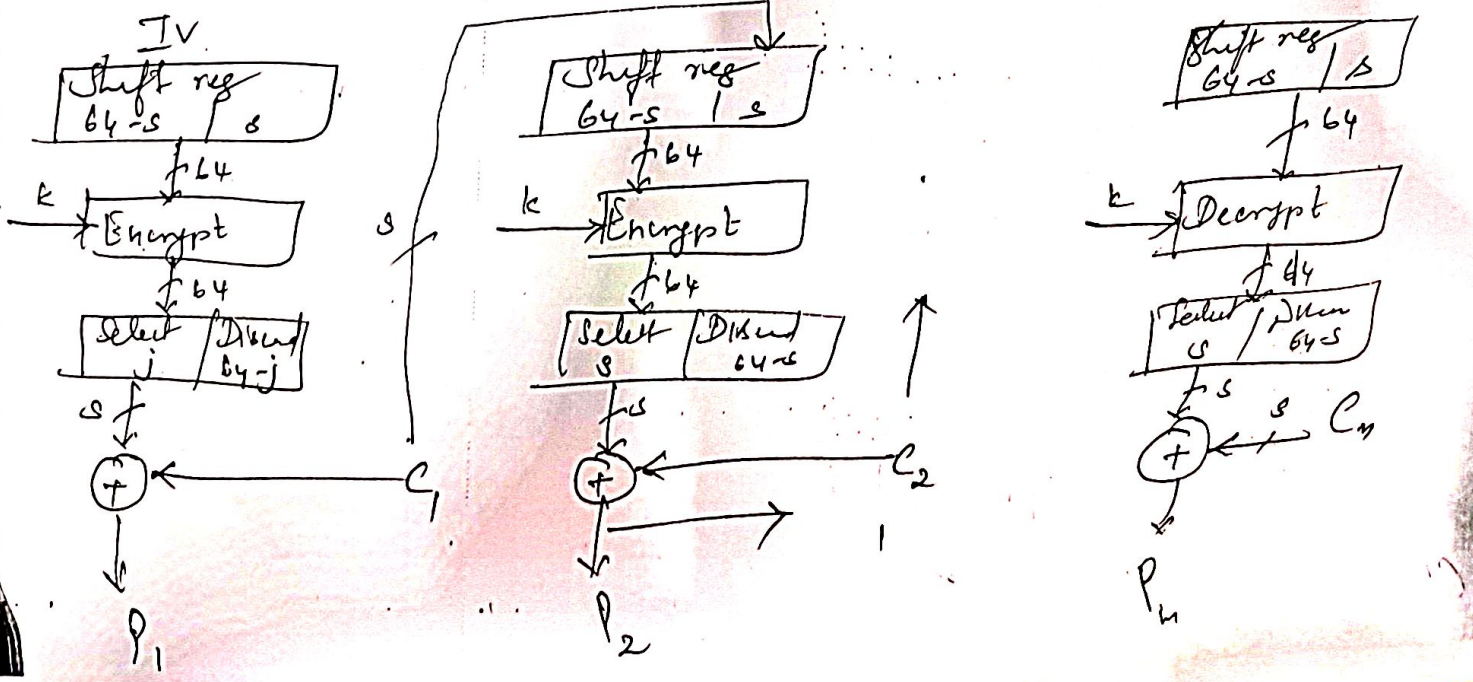
CBC is appropriate for handling message longer than 64 bits.

3. Cipher Feedback Mode.

Mangal
Date / / 20

Cipher feedback and output feedback tend to convert block cipher into stream cipher. Stream cipher has the advantage of not padding a message to make it integral number of blocks. It has ciphertext of length same as that of plaintext.





$C_1 = P_1 \oplus S_s\ (E_k(IV))$

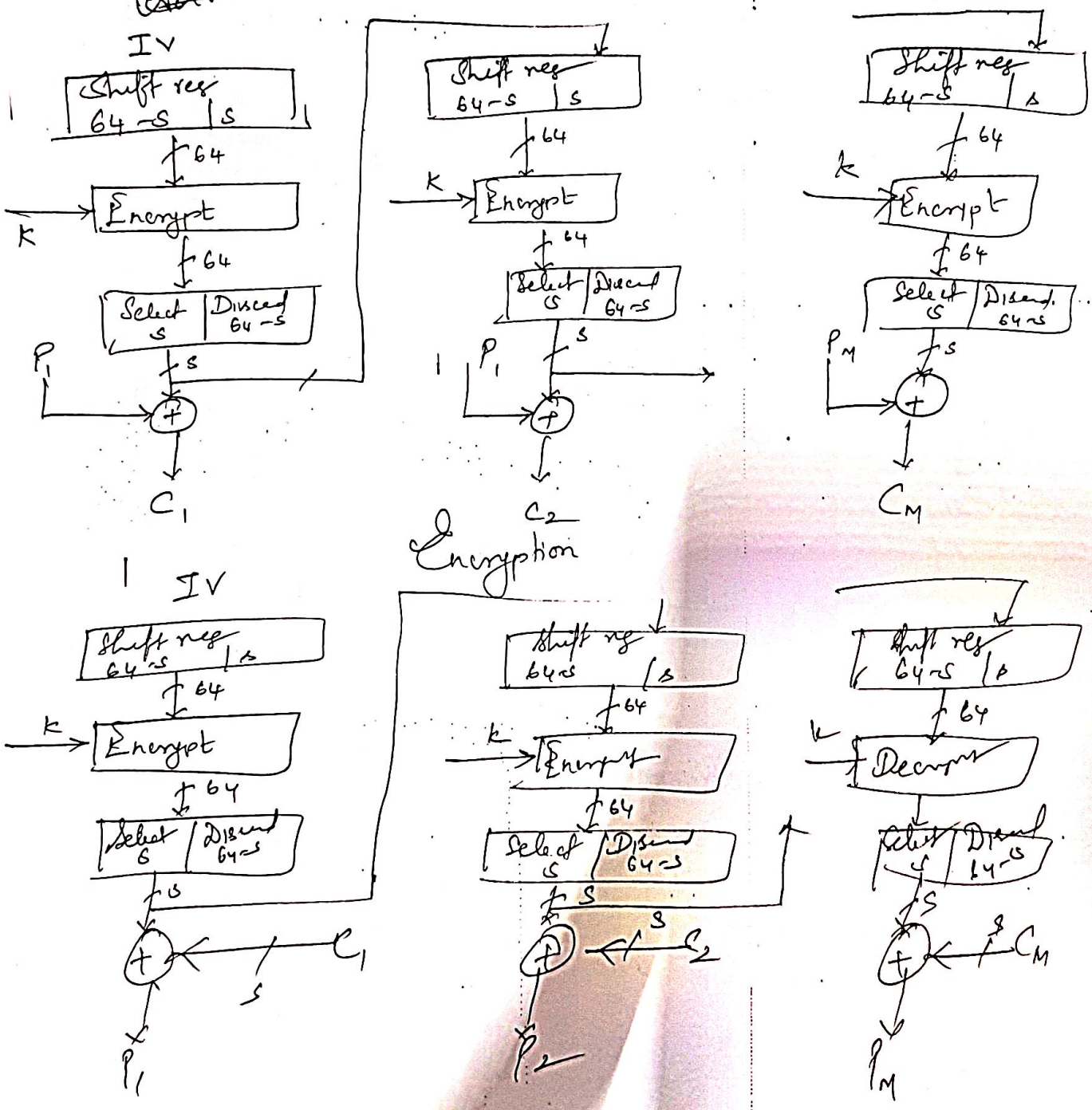
$P_1 = C_1 \oplus S_s\ (E_k(IV))$

S_s – MSB s-bits

Mangal
Date / /20

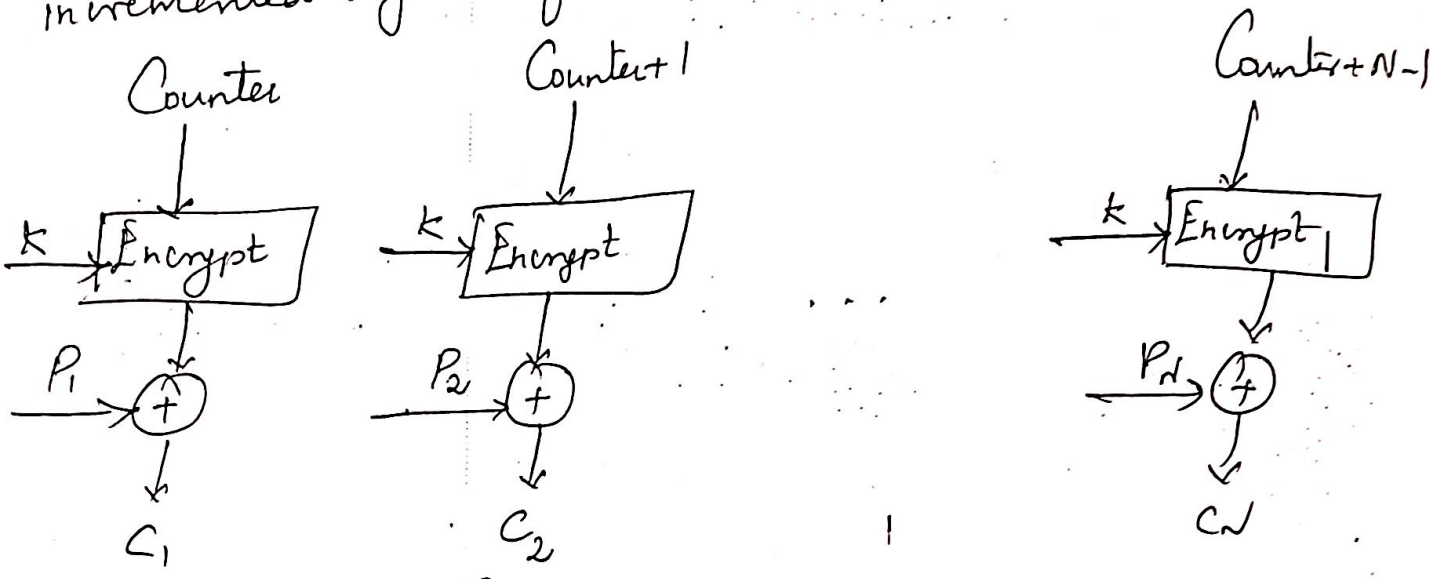
4. Output Feedback Mode

Output of encryption function is fed back to shift register. ~~in of~~ Bit errors in transmission are not propagated. But it is more vulnerable to message stream modification attack.

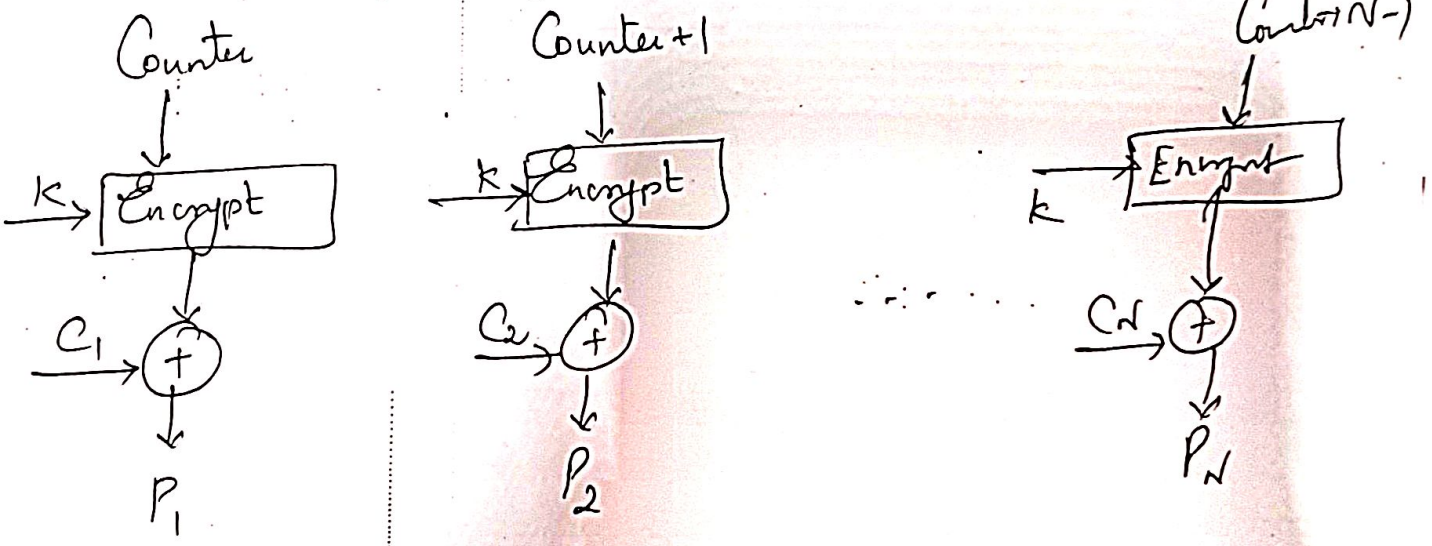


5. Counter Mode

A counter is set to plaintext block size. For every plaintext block, counter value must be different. Counter is initialized to some value and incremented by 1 for each subsequent block.



Encryption.



Decryption

Advantages.

Hardware efficiency: Encryption is done in parallel on multiple blocks. Throughput is based on parallelism achieved.

2b54c7b8

Mangal
Date / /20

Software efficiency: Processors that support parallel features can be effectively utilised.

Preprocessing: Incase sufficient memory and security is maintained, preprocessing can be used to prepare output of encryption boxes that are fed into XOR functions.

Random acces: ith block of PT of CT can be accessed in a random fashion

Provable security: At least as secure as other modes

Simplicity: Requires only implementation of encryption algorithm