Notes

Date :

INFORMATION SECURITY

NOTES (Things to mug)

UNIT - 1

① Simplified DES

~~→ Uses 64 bit Plain text~~

~~→ 56~~

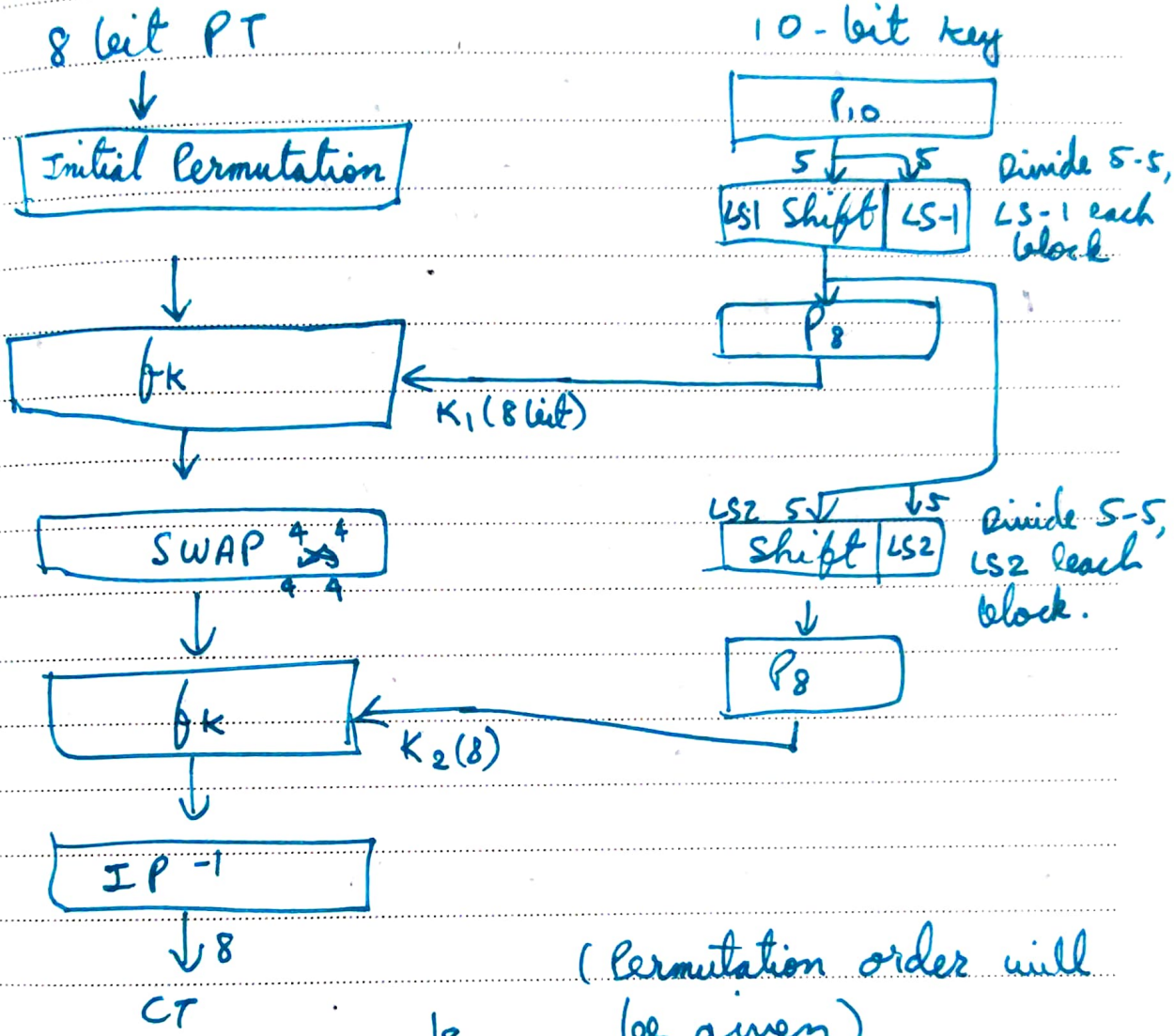
- 8 bit Plain text
- 10 bit key
- 8 bit cypher text

MUG VIMP Notes

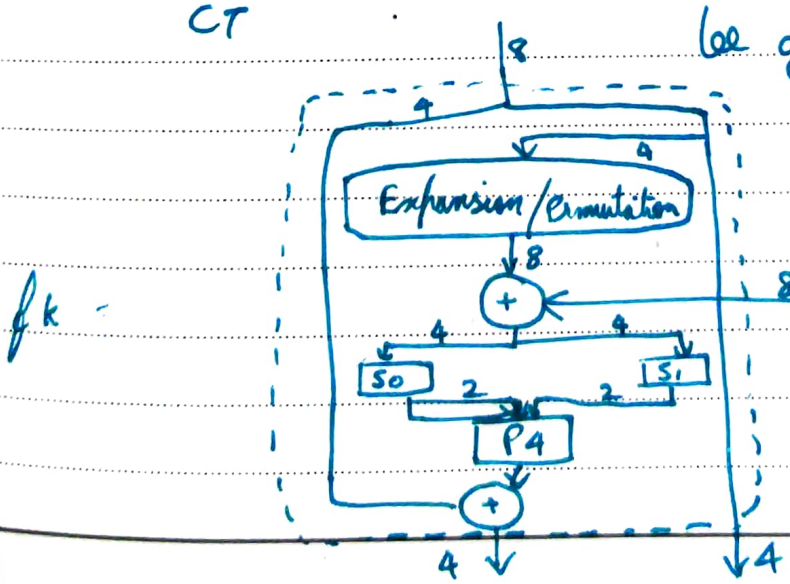
Date :

S-DES block diagram

Encryption



(Permutation order will be given)



Example

0100

S0 → Matrix

0100 row (0,3)

col

11

VIMP

Notes Date:

② Hill cypher

$$\text{key} = \begin{bmatrix} H & I \\ L & L \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

Indexing always from 0. ∴ A = 0, B = 1, Z = 25

PT should be colum vector of key matrix size.

SHORT EXAMPLE ⇒ $\begin{bmatrix} S \\ H \end{bmatrix}\begin{bmatrix} O \\ R \end{bmatrix}\begin{bmatrix} T \\ E \end{bmatrix}\begin{bmatrix} K \\ A \end{bmatrix}\begin{bmatrix} M \\ P \end{bmatrix}\begin{bmatrix} L \\ E \end{bmatrix}$

↓

$\begin{bmatrix} 18 \\ 7 \end{bmatrix}\begin{bmatrix} 14 \\ 17 \end{bmatrix}\begin{bmatrix} 19 \\ 4 \end{bmatrix}\begin{bmatrix} 23 \\ 0 \end{bmatrix}\begin{bmatrix} 12 \\ 15 \end{bmatrix}\begin{bmatrix} 11 \\ 4 \end{bmatrix}$

⇒ Use X when not fitting properly.

Formula: $C = KP \bmod 26$

$= \begin{bmatrix} 0 \\ 15 \end{bmatrix}\begin{bmatrix} 0 \\ 3 \end{bmatrix}\begin{bmatrix} 9 \\ 19 \end{bmatrix}\begin{bmatrix} 5 \\ 19 \end{bmatrix}\begin{bmatrix} 22 \\ 11 \end{bmatrix}\begin{bmatrix} 5 \\ 9 \end{bmatrix}$

$= \begin{bmatrix} A \\ P \end{bmatrix}\begin{bmatrix} A \\ D \end{bmatrix}\begin{bmatrix} J \\ T \end{bmatrix}\begin{bmatrix} F \\ T \end{bmatrix}\begin{bmatrix} W \\ L \end{bmatrix}\begin{bmatrix} F \\ J \end{bmatrix} = \underline{\underline{APADJTFTWLFJ}}$

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

Date:

V IMP

Notes

③ Types of attacks

- Passive
  - ↳ Release of message contents
  - ↳ Traffic analysis
- Active
  - ↳ Masquerade (pretends to be someone else)
  - ↳ Replay (Man in the middle)
  - ↳ Modification of messages (altering messages)
  - ↳ Denial of service

④ Playfair Cypher

Key = MSRIT

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

PT = "PROGRAMMING IS FUN"

↳ EPROGRA

← MX MI NG

Repeat (x)

IS FU NZ

↳ Extra (z)

→ Same row, replace with right.
→ Same col, replace with below.
→ Else, same row, other's col.

⑤ Security Services in X.800 (MUG)

i) Authentication
   a) Peer entity authentication
   b) Data origin authentication
ii) Access control
iii) Data confidentiality
   a) Connection confidentiality
   b) Connectionless confidentiality
   c) Selective-field confidentiality
   d) Traffic flow confidentiality
iv) Data Integrity
   a) Connection integrity with recovery
   b) Connection integrity without recovery
   c) Selective field connection integrity
   d) Connectionless integrity
   e) Selective-field connectionless integrity
v) Non repudiation : Protection against denial
   a) Non repudiation, origin
   b) Non-repudiation, destination

⑥ Strengths of DES (MUG)

① 56 bit key
② Nature of the algorithm
③ Resistant to timing attacks

VIMP

Date :

Notes

⑦ Block cypher modes of operation

i) Electronic Codebook (ECB) : Each 64 bit block is encoded with same key independently

ii) Cipher Block Chaining (CBC) : Input is XOR of next 64 bit PT with previous 64 bit CT.

iii) Cipher feedback (CFB) : Previous CT encrypted, XORed with PT to get new CT.

iv) Output feedback (OFB) : Similar to CFB, except input is previous DES output

v) Counter (CTR) : PT block is XORed with encrypted counter.

⑭ Basic functions of encryption algorithms

- Substitution
- Transposition

⑧ Security Mechanisms in X.800

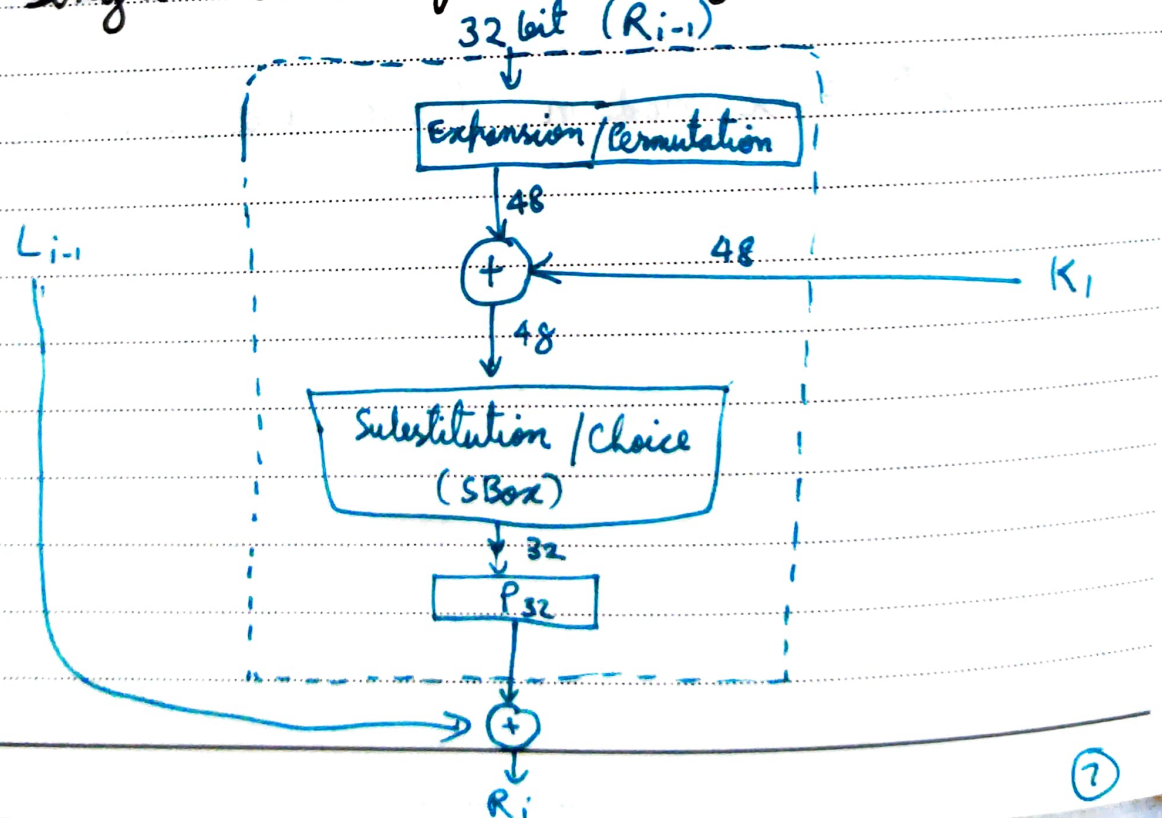
i) Encipherment
ii) Digital Signature
iii) Access control
iv) Data Integrity
v) Authentication Exchange
vi) Traffic Padding
vii) Routing Control
viii) Notarization

→ Specific Security Mechanisms

ix) Trusted Functionality
x) Security Label
xi) Event detection
xii) Security audit trial
xiii) Security recovery

→ Pervasive Security Mechanisms

⑨ Single Round of DES algorithm



(10) Differential and Linear Cryptanalysis

a) **Differential** : Observe the behaviour of PAIRS of text blocks evolving along each round of cipher and try to explain the difference

b) **Linear** : Finding linear approximations to describle the transformations performed in DES.

(11) Key discarding in DES : A 64 bit key is generated and every 8th bit is discarded to get 56 bit key.

(12) Diffusion and Confusion

- Diffusion seeks to make the statistical relationship between PT & CT as complex as possible.

- Confusion seeks to make the relationship between Statistics of CT and value of encryption key as complex as possible.

(13) Ingredients of Symmetric Cipher

- PT
- CT
- Encryption Algo
- Decryption algo
- Secret key