

Features of cryptography

- Confidentiality ← message disclosed \rightarrow (Encryption) (Decryption)
- Integrity ← content modification \rightarrow (hash generation and verification)
- Availability ← data available \rightarrow (retrieval)

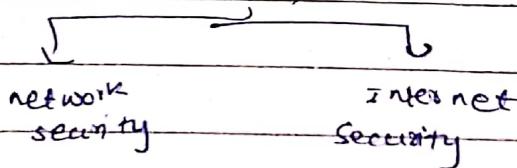
Non Repudiation

• sender can't deny his act, because message was sent but sender can't withdraw it
 digital signature uses \rightarrow (private key), can't withdraw
 Non Repudiation

⇒ Cryptography : Science of hiding a message.

Security

⇒ for all confidentiality, integrity etc., cryptography \rightarrow , security

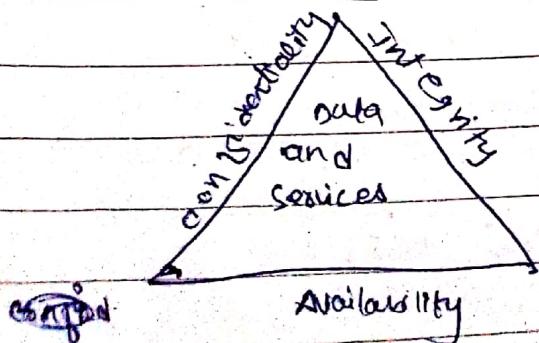


* The field of network internet security consists:

- detect (\rightarrow attempt to detect)
- prevent (\rightarrow attempt to prevent)
- correct detect (\rightarrow if attempt not detect \rightarrow correct)
- correct security violation

N.V. Imp \swarrow CIA Triad

- Confidentiality
- Integrity
- Availability



Ex: If you have computer security knowledge then you can work as a security officer.

Date _____
Page _____

Levels of Impact

- Low system bridge \rightarrow no systematic information flow
 - Moderate system bridge \rightarrow plus system control
 - High system bridge \rightarrow plus system control

Goals of computer security:

- To protect computer assets from:
 - human errors, natural disasters, physical and electronic malice

~~Conf~~ CIA

Confidentiality

message disease डाये बायोन।

privacy bridge କେବଳ ଶାଖା,

Integrity

Data integrity

-correctness of data

- specified person / authorized person or ~~not~~
change ~~in form~~)

System integrity

System P3CT intention of शास्त्रीय, अस्ति, System of
शास्त्रीय नियम, or, अस्ति system of
integrity maintenance

~~integrity maintained by 4th field, which
delete 1st 2nd 3rd field,~~

purpose लाई कर्तव्य दौड़ी गई थी।

Availability

authorized users of info access हाल अवॉर्ड्स वाइपन्यो

authorization

- users के को हाल पाइत, को के permission ही रखते।
- what he or she is allowed to do.

authentication

- user verify हो
- exact same person हो नहीं verify हो;

other goals

non repudiation

- can't deny हो सकता।
- can't deny that exchange took place.

legitimate use

- जुहाले use हो सकते हैं मात्र use हो सकती।

~~Threats~~

Vulnerability / loopholes

जुहाले software की weak point vulnerability.
ex- दूसरे में कोई threat use हो सकता, vulnerability
आति, constant threat हो सकता buggloss की,
आति, attack की, vulnerability use हो सकती,

Threat

- a potential for violation of security
- physical threats - weather, natural disaster, bombs, power, etc.
- Human threats - stealing, mockery

Network Security

Normal flow

sender to receiver normally (उसका नियम)

→ Impersonation

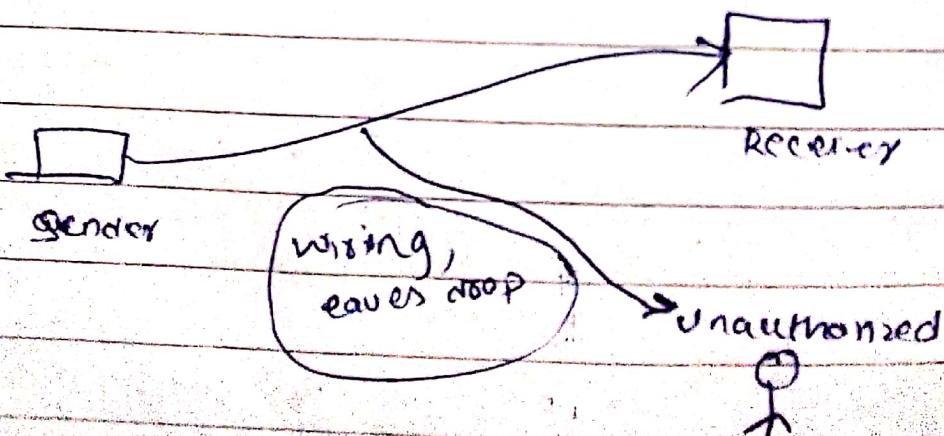
Four types of possible attacks are:

1) Interruption

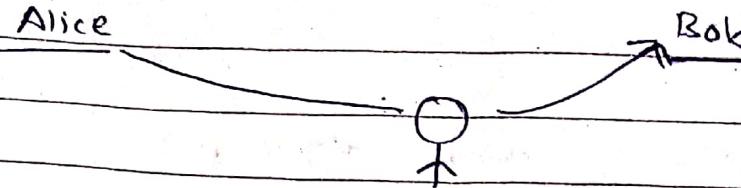
- stop service from working or disrupt message
- active attack

2) Interception

- normal flow interrupted by unauthorized or filtering message content
- active attack



3. Modification
• Active attack



Darth
(Unauthorized)
(message from modified आदि
sender)

4. Fabrication (Impersonation) (Masquerade)
• Alice & Bob के बीच ट्रैफ़िक वाला व्यक्ति ने,
Darth को जैसे Alice के रूप में communicate.
• Active

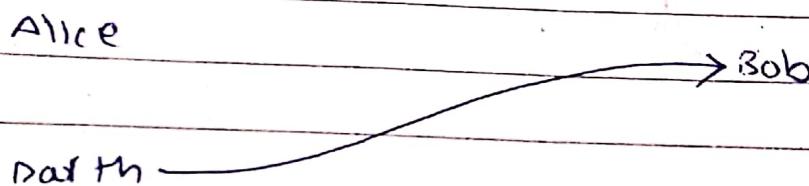
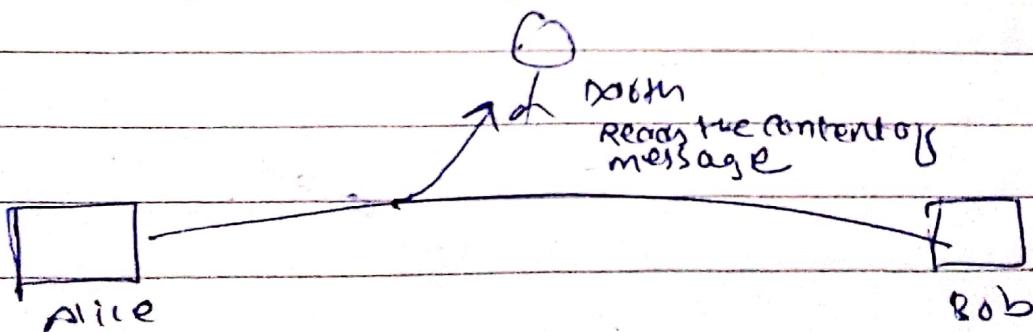


fig: Impersonation

Aspects

Passive attack

- frequency of message transmission, इसके द्वारा passive attack
- Replay, (path change सिद्धि)



Types:

- Release of message content
- Traffic analysis.

Aspects of Security

- Security attack
- Security Mechanism
- Security Service, (collection of mechanism ~~with~~ service)

Security Service

multiple mechanism user ~~for~~; mechanism ~~right~~, authorization, authentication, ~~to~~ ~~log~~

Standards:

X.800:

~ 193 CT document ~~for~~, ~~many~~ different services define ~~method~~,
- data transfer ~~related~~)

RFC 4946:

Request for

- internet ~~in~~ use ~~for~~ diff? technology (HTTP, FTP, UDP, ...)
- protocols ~~with~~ network related ~~and~~, ~~standards~~ ~~in~~, ~~etc~~
document ~~for~~,

Security service X-800

Authentication

- user verification पात्र, अन्तर्गत authentication
 - Peer entity authentication
Peer शक्ति त group of
 - Data origin authentication
• आवश्यक data specified organization of विभाग की

service:

- Data confidentiality
 - Data integrity
 - Non Repudiation.

Security mechanisms:

specific

- encipherment, digital signatures, access controls, data integrity, and

persuasive see

- trusted functionality, security labels,

→ word party et am
connection algorithm et
key generate str
key transmission str

Model

for network security

client or sender, receiver has got it, must do right

so, refresher T T T . RSA, HES,
in case failed third party et will be available most

जाति वा प्रोटोकॉल्सः

PKI, kerberos

node strand id

→

Using the model requires us to

- design a suitable algorithm.
- select info (key) word by the algorithm
- key exchange, current state protocol LDAP with else in 1981

Cryptography

Date _____
Page _____

Encryption:

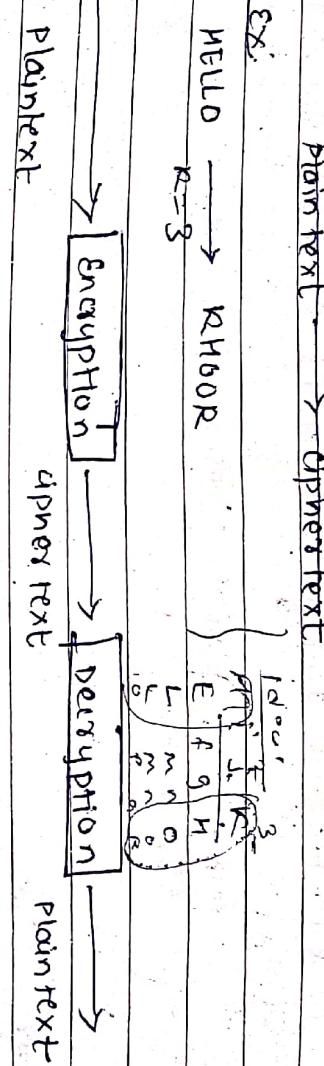


Fig. Encryption- Decryption

key

parameters or value ~~and~~ output. determine कि।

key की value public नहीं होती अतः इसका उपयोग डिस्क्रीप्ट करने में लाया जाता है।

cipher

algorithm used for encryption.

Decipher

algorithm used for decryption.

Crypto system

Crypto system : is a 5-tuple / quintuple (E, D, M, K, C) where M set of plaintexts, K set of keys, C set of ciphertexts, E set of encryption funs $e: M \times K \rightarrow C$ and D set of decryption funs $d: C \times K \rightarrow M$

↓
cipher text → key apply करके
plain text

Example: Ceased cipher

PLAIN TEXT

M = sequence of letters

$K \rightarrow k = 1, i$ is an integer $0 \leq i \leq 25$

$E \rightarrow E(k)$ and for all letters m , $E_k(m) = m + k \pmod{26}$

$D \rightarrow D(k)$ and for all letters c , $D_k(c) = (26 + c - k) \pmod{26}$

$c = M$

map sequence of letters, c is sequence of letters
 cipher text \rightarrow plain text \rightarrow cipher text

Ceaser Cipher

Cryptographic System characteristics

- Type of operations used for transforming Plain to cipher
- Number of keys used
- Symmetric: encryption & decryption \rightarrow same key
- Asymmetric
 - diff' n key
 - way in which plain text is processed

g) Stream cipher: character by character (often a lot of data)

(b) Block cipher:

Hindi में, आम ~~क्रिप्टोग्राफी~~ • यह 64 bit block \rightarrow

Hindi ASCII, 65 \rightarrow

E ग्राह्य अल्फॉड ७३, अर्थ $65 + 8 = 73$, जो आम अल्फॉड

bits का, intermix करने और फिर तो

— Highly secure

Substitution Ciphers

"Ceasar cipher" \rightarrow

$H \rightarrow E$ $L \rightarrow I$ $O \rightarrow O$
 $M \rightarrow V$ $J \rightarrow U$ $N \rightarrow P$
 $K \rightarrow H$ $I \rightarrow O$ $R \rightarrow R$

Encrypt .

"CRYPTOGRAPHY" using ceaser cipher by apply $k=4$

"gibcetesvetlc"

c	a	e	t	g
q	s	p	m	r
1	2	3	4	5
a	b	c	d	e

P Q R S T

$$E_K(C) = (2+4) \bmod 26 \quad E_K(t) = ((19+4) \bmod 26) + t \quad \text{in } \text{let } \text{DJ}$$

$$= 6 \bmod 26 \quad = 23 \bmod 26 \quad 0, \quad P \quad a \quad r \quad s$$

$$= 6 \quad = X \quad g \quad h \quad i \quad j \quad k$$

$$E_K(O) = 5$$

$$E_K(R) = (17+4) \bmod 26$$

$$E_K(g) = (6+4) \bmod 26 \quad P \quad Q \quad R \quad S$$

$$E_K(Y) = (24+4) \bmod 26$$

$$= 28 \bmod 26 \quad E_K(P) = (15+4) \bmod 26 \quad b \rightarrow 0 \quad m \rightarrow 12 \quad y \rightarrow 23$$

$$= 2$$

$$= t$$

$$E_K(P) = (15+4) \bmod 26$$

$$= t$$

$$\begin{array}{l} k^{-10} \\ k^{-11} \\ k^{-12} \end{array}$$

$$\Delta$$

Transposition ciphers

Substitution

Transposition

H E L L O → K I M O O R

H E L L O → O K H R O

"substitution cipher", but, location
of letters stay the same

actual positions of letters gets
changed making the text grabby

Rail-fence cipher

"Rail" की लाइनों पर लिखा जाता है।

Ex: "ATTACK TONIGHT"

Rail = 3

A T C N
T A K O I H T T Y
T K O I H T Y

A C N T A K O I H T T Y

Encrypt and Decrypt message

"BOB UNDER THE BRIDGE" using Rail=4

B	O	B			
O	N	E	R	E	
M	U	R	H	T	G
B	T	D			

④ cipher text:
"BOBONEREMURMI(BTD)"

Decrypt:

B	D	B		
O	N	E	E	
M	U	R	H	I
B	T	D		

Vertical wala in

"This is the planet", 3 rails

J. S. t p n
h i h l e
i s c e A t

The T set p n in h l e is ea t

1 2 3 4 5 6 7 8 9 10 " 12 13 14 15

Decrypt - T set p n in h l e is ea t
S a c t i o n s
A l g o r i t h m s

3. Vigenere cipher : substitution cipher (polyalphabetic)

if key = PRBN

Plain text A-Z

PRBN PRBN PRBN PRBN

Plain text A-Z, key, A-Z

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

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

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

Plain text: Examination

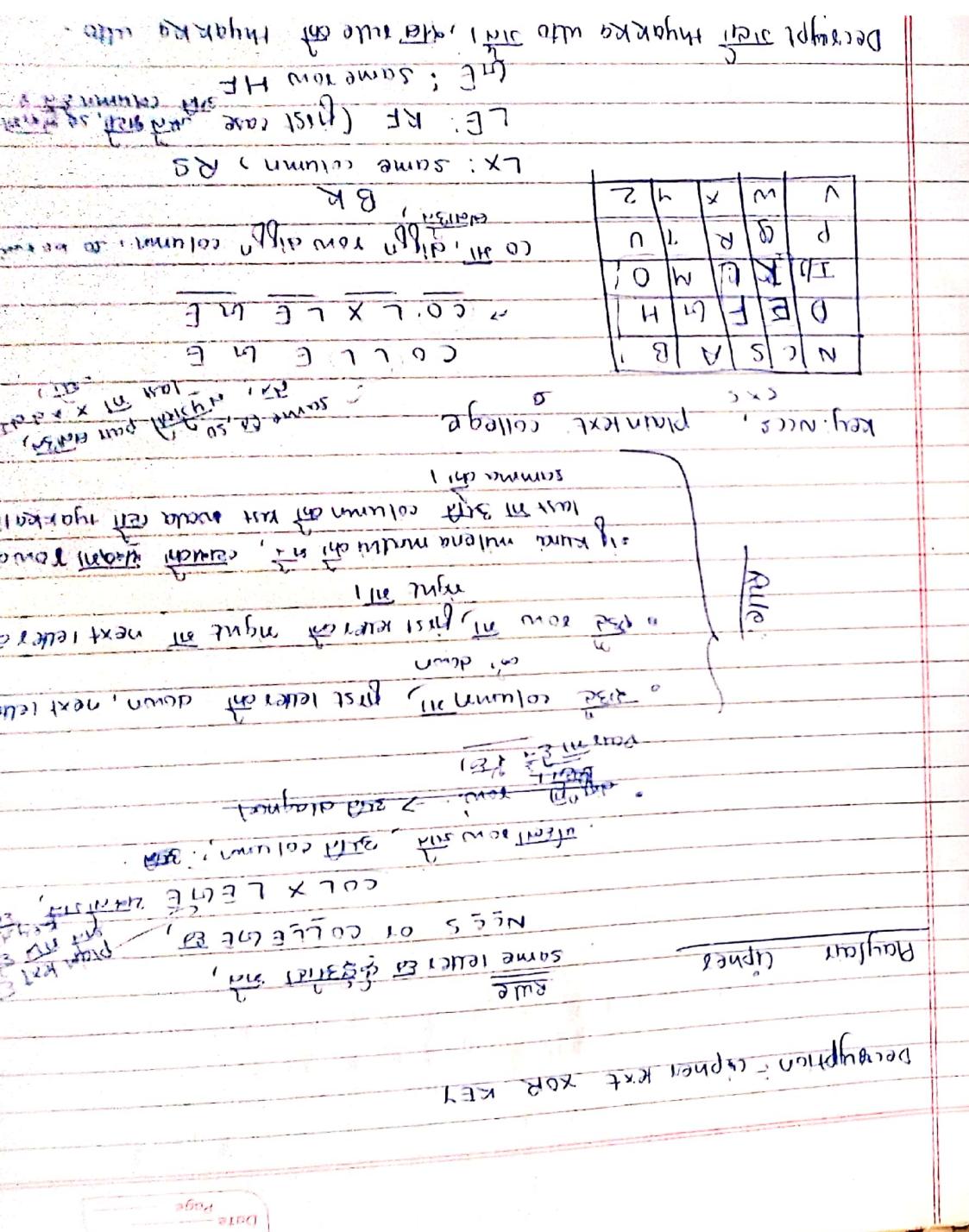
key: nccs

Plaintext: E X A M I N A T I O N
key: N C C S N C S N C C

Ciphertext: R Z C E V P C L V S P }

Decrypt করুন key N এর column টিন অক্ষর, যথে,

Date _____
Page _____



	7	15	8	10
01000100	01000100	01000100	01000100	01000100
01000011	01000011	01000011	01000011	01000011
00000011	00000011	00000011	00000011	00000011
00000101	00000101	00000101	00000101	00000101

One-time Pad (Simple XOR) (column cipher)

Message: HELLO

Key: 123456789

Decrypted Message: 7869347679

Date: 10/10/2023

Page: 1

Encryption

same column: element just below

same row: " " right

different row, column: element in its row and another element's column

Decryption

same column: Element just above

same row: Element just left

different row column: Element in its column and another

elements row.

Date _____

Page _____

alphabets 0123456789

$$\begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{bmatrix}$$

Hill cipher

- Hill cipher uses many matrix for encryption / decryption process.

Example:

$$\text{Key matrix } K = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \quad \left\{ \begin{array}{l} \text{determinant of key matrix should be } 1 \\ \text{relative prime to 26} \end{array} \right.$$

message : WELCOME

Encryption: M X R

(Given) message and divide with 26 ~~mod 26~~, if pair remain \times else

$$E(WE) = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 22 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} 108 \\ 86 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 6 \end{bmatrix} = EI$$

$$E(LL) = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 2 \end{bmatrix}$$
$$= \begin{bmatrix} 54 \\ 43 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 20 \end{bmatrix} = CU$$

$$E(SOW) = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 14 \\ 12 \end{bmatrix}$$

$$= \begin{bmatrix} 116 \\ 102 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 24 \end{bmatrix} =$$

$$E(TEX) = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 9 \\ 23 \end{bmatrix} = \begin{bmatrix} 139 \\ 127 \end{bmatrix} \bmod 26 = \begin{bmatrix} 17 \\ 23 \end{bmatrix} =$$

$a \equiv b \pmod{c}$
 $a - b$ should be exactly divided by c , then we can say, $a \equiv b \pmod{c}$

Decryption

Inverse of key matrix $4 \times 4 - 3 \times 3$ $\begin{bmatrix} 5 & -5 \\ -3 & 4 \end{bmatrix}$

$$\begin{aligned} &= \frac{1}{5} \begin{bmatrix} 5 & -5 \\ -3 & 4 \end{bmatrix} \\ &= (5^{-1}) \begin{bmatrix} 5 & -5 \\ -3 & 4 \end{bmatrix} \end{aligned}$$

$$a \equiv b \pmod{c}$$

or

$$(5x5^{-1}) \equiv 1 \pmod{26}$$

5^{-1} का अर्थात्, $5 \times 5^{-1} \equiv 1 \pmod{26}$,

अतः, 5^{-1} ,

5^{-1} का अर्थात् निम्न,

$$\begin{aligned} 5x - 1 &\equiv 0 \pmod{26}, \text{ exact value} \\ 26 & \\ = 21 & \end{aligned}$$

$$= 21 \begin{bmatrix} 5 & -5 \\ -3 & 4 \end{bmatrix}$$

$$= 21 \begin{bmatrix} 5 & 21 \\ 23 & 4 \end{bmatrix}$$

$$\equiv 5 \pmod{26}$$

$$= (5+21)/26 =$$

$$3 \times 5/26$$

$$= \begin{bmatrix} 105 & 44 \\ 483 & 84 \end{bmatrix} \pmod{26}$$

$$(3+23)/26$$

$$= \begin{bmatrix} 1 & 25 \\ 15 & 6 \end{bmatrix}$$

or, easy:

$$26 - 3 = 23$$

$$26 - 5 = 21$$

Note: Decrypt char prime $\frac{m}{d}$ is dominant, 26 \rightarrow relatively calculate $\frac{1}{d} \mod m$,

Date _____
Page _____

Dr(EI)

$$= \begin{bmatrix} 1 & 25 \\ 15 & 6 \end{bmatrix} \begin{bmatrix} 4 \\ 8 \end{bmatrix}$$

$$\begin{bmatrix} 204 \\ 108 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 22 \\ 4 \end{bmatrix} = \emptyset \text{ we } \subset$$

- Encrypt and decrypt Hill using key ematrix

$\begin{bmatrix} 3 & 3 \\ 5 & 6 \end{bmatrix}$ using Hill cipher.

HILL

$$E_R(HI) = \begin{bmatrix} 3 & 3 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 45 \\ 83 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 19 \\ 5 \end{bmatrix} = tf$$

$$E_R(1L) = \begin{bmatrix} 3 & 3 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 11 \\ 11 \end{bmatrix} = \begin{bmatrix} 66 \\ 121 \end{bmatrix} \bmod 26 = \begin{bmatrix} 14 \\ 17 \end{bmatrix} = OR$$

Decryption:

Determinant = 3

$$\gcd(3, 26) = 1 \quad \leftarrow$$

$$= \frac{1}{3} \begin{bmatrix} 6 & -3 \\ -5 & 3 \end{bmatrix}$$

$$\therefore 3^{-1} \begin{bmatrix} 6 & -3 \\ -5 & 3 \end{bmatrix} = 9 \begin{bmatrix} 6 & -3 \\ -5 & 3 \end{bmatrix}$$

$$\frac{2x^2 - 1}{2x} \quad \text{remainder}$$

$$= 9 \begin{bmatrix} 6 & 23 \\ 21 & 3 \end{bmatrix}$$

$$\therefore \text{D} = \begin{bmatrix} 54 & 207 \\ 189 & 27 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 2 & 25 \\ 7 & 1 \end{bmatrix}$$

$$\text{DR(7F)} = \begin{bmatrix} 2 & 25 \\ 7 & 1 \end{bmatrix} \begin{bmatrix} 19 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} 163 \\ 138 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 7 \\ 8 \end{bmatrix}$$

= MI

$$\text{DR(OR)} = \begin{bmatrix} 2 & 25 \\ 7 & 1 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix}$$

$$= \begin{bmatrix} 453 \\ 115 \end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} 11 \\ 11 \end{bmatrix}$$

= LL

~~CRYPTANALYSIS~~ (Cryptanalytic)

Cryptanalytic Attacks

- Key findout method (Encryption IT'S use ~~which~~ key)
Digital types of attack:

ciphertext only - ~~जो~~ algorithm में e cipher text जापा देते हैं, तो each bit, Water ~~पर्याप्त~~ check करते हैं।
(possible key नहीं पर्याप्त)

known plaintext :- plaintext का जापा है, cipher text लिया जाता है, (जो कोड
only. key जापा दिया, आपके text का प्रकार ज्ञात करते हैं)

chosen plaintext : intruder has access to encryption mechanism

- plain text देते हैं, choose ~~जोड़ी~~ plain text की ciphertext
generate ~~जोड़ी~~ संख्या, (machine जैसा है), 3 ग्री, (यह)
⇒ texts द्वारा key लिया,

chosen ciphertext: intruder has access to decryption mechanism.

- cipher text वाले plaintext दिये जाते, जो ज्ञात करते हैं
key ~~जोड़ी~~ नहीं।

chosen text:- combination of both

- known encryption and decryption mechanism.
- best one

~~Brute force attack~~ - Repeating the same process until the
match is found.
most used.

Symmetric Cryptography

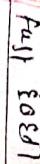
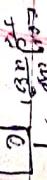
- same key used for encryption, decryption
- secret key shared by sender and receiver

Encryption, decryption algorithm is identical for,

main problems:

key transmission ~~and~~, out of band channel (diff' frequency
well channel so in need of key access ~~problem~~)

key generate \Rightarrow $\binom{n(n-1)}{2}$ key pairs.



~~Asymmetric key~~ confidentiality

public key

authentication

Encryption जैसे public part, इनहीं (sender के पास हो) public key use होते हैं। सत्र receiver के पास private key होते हैं।

जैसे decrypt होते हैं। (अब, यहीं key दर्शाया दिया रखा गया, तो secure)

जैसे entry के public key, private key जैसे दिया गया है।
entry का third word private provided होता है।

Stream and Block ciphers

message text को character process करते हैं जो बास में,

stream : one character at a time
example: caesar, vernam, vigenere cipher

block : one block at a time
(multiple characters)



Alice का जौही Bob के public key का encrypt
Bob के message का जौही private key का decrypt

Digital signature (जैसे public key use होता है)
public key use होता है (Asymmetric)

authentication एवं user ID, private key generate करता है।

Date
Page

Explain the round key generation process for DES.
Explain the DES algorithm.

卷之三

卷之三

- مکانیزم میگیرد که این را در این شرایط میتوان بازخواست کرد.

卷之三

الله يحيى العرش بروحه العطرة

•
KELLY
—> END

卷之三

August 20, 1900 - 2 Rock Upper.

-Indicates to insertion of symbols.
Given numbers of bills - to

Slow Food

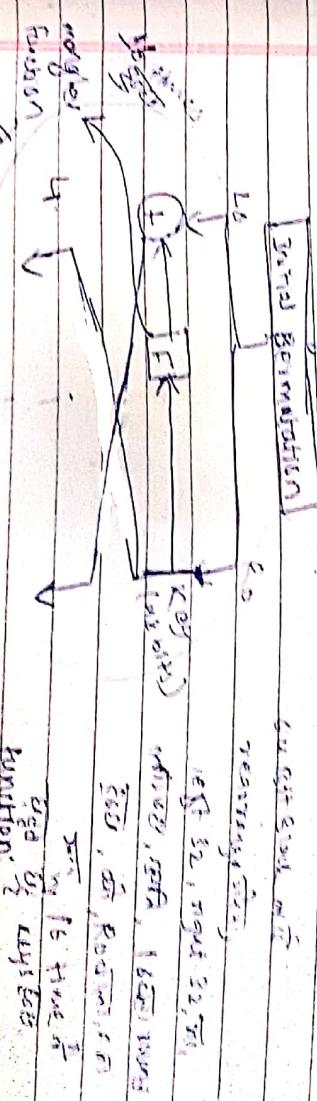
letter propagation (the streaks single bit of random noise next to which are randomize offset)

1991 Round

$$R_{n+1} = \ln(\oplus) f(R_{n+1}, R_n)$$

DES A.D.H.P.

- Block cipher algorithm based on Feistel structure
→ By bit block



we can't do much, and it
isn't very effective.

expansion of culture, which
is growing, spreading rapidly,
etc., etc., etc.

Permutation by Selection

15

9 (29) 0.0000

卷之三

100

卷之三

8
1
1

八

64



permuted

choice



56 bits

bit selection
8, 16, 24, 32, 40, 48, 56

28

8

C₀

arbitrary number of leftshift 16 times

Key generation process

K₁ = f(C₁, P₁ and D_{8,5})
K₂ = f(C₂, P₂ and D_{8,6})

C₁

D₁ 2

permutation table
ΣΦ_{i,j}, result will be
remaining 16 bits

C₁₆

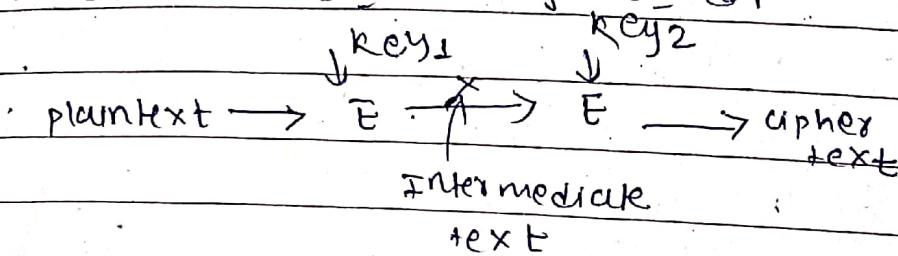
D₁₆

~~8~~ \rightarrow SP

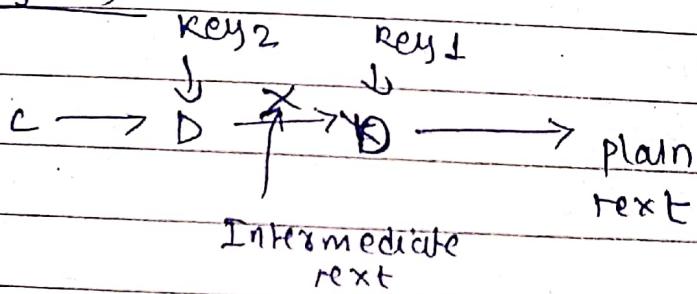
~~2~~ 32
Sironi Side 6 2/16 1

Double DES & Triple DES

- Double DES मा दो प्रत्येक 56 बिट के key use होते।



Deryn Hyn



more vulnerable, (not less strong than single DES)

~~group~~ meet in the middle attack

(Hackers in Brute force attack use ~~more~~, ~~64 bit~~ key ~~set~~,
~~64 bit~~ ~~key~~ ~~set~~ ~~for~~ ~~attack~~).

If plain text की cipher text नहीं हो पड़े, key का नियन्त्रण
 Encryption के 64 bit की तरफ से पड़े
 Decryption के 64 bit को प्राप्ति करने के लिए, k_1, k_2 चुनें।

AES example Encyption standard

384 bit block keys (128, 192, 256)

128 bit key - 10 rounds

192 bit key - 12 rounds

256 bit key - 14 rounds

(C-1) Identical round and 1 half round last 8 different round keys:

Each identical round contains:

- i) Substitution box
- ii) Mix column
- iii) Shift rows
- iv) Add round key

Last round doesn't have mix column step.

Each round use 128bit subkey

Block generation

128 bit key

W[4] to W[3]

W[5] to W[6]

W[6] to W[7]

W[7] to W[8]

W[8] to W[9]

W[9] to W[10]

W[10] to W[11]

$N[1] = W[10] \oplus W[7]$

W[11] to W[12]

128 bit

128 bit key

W[3] to W[5]

W[6] to W[8]

W[9] to W[11]

W[10] to W[12]

W[11] to W[13]

W[12] to W[14]

W[13] to W[15]

W[14] to W[17]

W[15] to W[18]

W[16] to W[21]

W[17] to W[22]

W[18] to W[23]

W[19] to W[24]

W[20] to W[25]

W[21] to W[26]

W[22] to W[27]

W[23] to W[28]

W[24] to W[29]

W[25] to W[30]

W[26] to W[31]

W[27] to W[32]

W[28] to W[33]

W[29] to W[34]

W[30] to W[35]

W[31] to W[36]

W[32] to W[37]

W[33] to W[38]

W[34] to W[39]

W[35] to W[40]

W[36] to W[41]

W[37] to W[42]

W[38] to W[43]

W[39] to W[44]

W[40] to W[45]

W[41] to W[46]

W[42] to W[47]

W[43] to W[48]

W[44] to W[49]

W[45] to W[50]

W[46] to W[51]

W[47] to W[52]

W[48] to W[53]

W[49] to W[54]

W[50] to W[55]

W[51] to W[56]

W[52] to W[57]

W[53] to W[58]

W[54] to W[59]

W[55] to W[60]

W[56] to W[61]

W[57] to W[62]

W[58] to W[63]

W[59] to W[64]

W[60] to W[65]

W[61] to W[66]

W[62] to W[67]

W[63] to W[68]

W[64] to W[69]

W[65] to W[70]

W[66] to W[71]

W[67] to W[72]

W[68] to W[73]

W[69] to W[74]

W[70] to W[75]

W[71] to W[76]

W[72] to W[77]

W[73] to W[78]

W[74] to W[79]

W[75] to W[80]

W[76] to W[81]

W[77] to W[82]

W[78] to W[83]

W[79] to W[84]

W[80] to W[85]

W[81] to W[86]

W[82] to W[87]

W[83] to W[88]

W[84] to W[89]

W[85] to W[90]

W[86] to W[91]

W[87] to W[92]

W[88] to W[93]

W[89] to W[94]

W[90] to W[95]

W[91] to W[96]

W[92] to W[97]

W[93] to W[98]

W[94] to W[99]

W[95] to W[100]

W[96] to W[101]

W[97] to W[102]

W[98] to W[103]

W[99] to W[104]

W[100] to W[105]

W[101] to W[106]

W[102] to W[107]

W[103] to W[108]

W[104] to W[109]

W[105] to W[110]

W[106] to W[111]

W[107] to W[112]

W[108] to W[113]

W[109] to W[114]

W[110] to W[115]

W[111] to W[116]

W[112] to W[117]

W[113] to W[118]

W[114] to W[119]

W[115] to W[120]

W[116] to W[121]

W[117] to W[122]

W[118] to W[123]

W[119] to W[124]

W[120] to W[125]

W[121] to W[126]

W[122] to W[127]

W[123] to W[128]

W[124] to W[129]

W[125] to W[130]

W[126] to W[131]

W[127] to W[132]

W[128] to W[133]

W[129] to W[134]

W[130] to W[135]

W[131] to W[136]

W[132] to W[137]

W[133] to W[138]

W[134] to W[139]

W[135] to W[140]

W[136] to W[141]

W[137] to W[142]

W[138] to W[143]

W[139] to W[144]

W[140] to W[145]

W[141] to W[146]

W[142] to W[147]

W[143] to W[148]

W[144] to W[149]

W[145] to W[150]

W[146] to W[151]

W[147] to W[152]

W[148] to W[153]

W[149] to W[154]

W[150] to W[155]

W[151] to W[156]

W[152] to W[157]

W[153] to W[158]

W[154] to W[159]

W[155] to W[160]

W[156] to W[161]

W[157] to W[162]

W[158] to W[163]

W[159] to W[164]

W[160] to W[165]

W[161] to W[166]

W[162] to W[167]

W[163] to W[168]

W[164] to W[169]

W[165] to W[170]

W[166] to W[171]

W[167] to W[172]

W[168] to W[173]

W[169] to W[174]

W[170] to W[175]

W[171] to W[176]

W[172] to W[177]

W[173] to W[178]

W[174] to W[179]

W[175] to W[180]

W[176] to W[181]

W[177] to W[182]

W[178] to W[183]

W[179] to W[184]

W[180] to W[185]

W[181] to W[186]

W[182] to W[187]

W[183] to W[188]

W[184] to W[189]

W[185] to W[190]

W[186] to W[191]

W[187] to W[192]

W[188] to W[193]

W[189] to W[194]

W[190] to W[195]

W[191] to W[196]

W[192] to W[197]

W[193] to W[198]

W[194] to W[199]

W[195] to W[200]

W[196] to W[201]

W[197] to W[202]

W[198] to W[203]

W[199] to W[204]

W[200] to W[205]

W[201] to W[206]

W[202] to W[207]

W[203] to W[208]

W[204] to W[209]

W[205] to W[210]

W[206] to W[211]

W[207] to W[212]

W[208] to W[213]

W[209] to W[214]

W[210] to W[215]

W[211] to W[216]

W[212] to W[217]

W[213] to W[218]

W[214] to W[219]

W[215] to W[220]

W[216] to W[221]

W[217] to W[222]

W[218] to W[223]

W[219] to W[224]

W[220] to W[225]

W[221] to W[226]

W[222] to W[227]

W[223] to W[228]

W[224] to W[229]

W[225] to W[230]

W[226] to W[231]

W[227] to W[232]

W[228] to W[233]

W[229] to W[234]

W[230] to W[235]

W[231] to W[236]

W[232] to W[237]

W[233] to W[238]

W[234] to W[239]

W[235] to W[240]

W[236] to W[241]

W[237] to W[242]

W[238] to W[243]

W[239] to W[244]

W[240] to W[245]

W[241] to W[246]

W[242] to W[247]

W[243] to W[248]

W[244] to W[249]

W[245] to W[250]

W[246] to W[251]

W[247] to W[252]

W[248] to W[253]

W[249] to W[254]

W[250] to W[255]

W[251] to W[256]

W[252] to W[257]

W[253] to W[258]

W[254] to W[259]

W[255] to W[260]

W[256] to W[261]

W[257] to W[262]

W[258] to W[263]

W[259] to W[264]

W[260] to W[265]

W[261] to W[266]

W[262] to W[267]

W[263] to W[268]

W[264] to W[269]

W[265] to W[270]

W[266] to W[271]

W[267] to W[272]

W[268] to W[273]

W[269] to W[274]

W[270] to W[275]

W[271] to W[276]

W[272] to W[277]

W[273] to W[278]

W[274] to W[279]

W[275] to W[280]

W[276] to W[281]

W[277] to W[282]

W[278] to W[283]

W[279] to W[284]

W[280] to W[285]

W[281] to W[286]

W[282] to W[287]

W[283] to W[288]

W[284] to W[289]

W[285] to W[290]

W[286] to W[291]

W[287] to W[292]

W[288] to W[293]

W[289] to W[294]

W[290] to W[295]

W[291] to W[296]

W[292] to W[297]

W[293] to W[298]

W[294] to W[299]

W[295] to W[300]

W[296] to W[301]

W[297] to W[302]

W[298] to W[303]

W[299] to W[304]

W[300] to W[305]

W[301] to W[306]

W[302] to W[307]

W[303] to W[308]

W[304] to W[309]

W[305] to W[310]

W[306] to W[311]

W[307] to W[312]

W[308] to W[313]

W[309] to W[314]

W[310] to W[315]

W[311] to W[316]

W[312] to W[317]

W[313] to W[318]

W[314] to W[319]

W[315] to W[320]

W[316] to W[321]

W[317] to W[322]

W[318] to W[323]

W[319] to W[324]

W[320] to W[325]

W[321] to W[326]

W[322] to W[327]

W[323] to W[328]

W[324] to W[329]

W[325] to W[330]

W[326] to W[331]

W[327] to W[332]

W[328] to W[333]

W[329] to W[334]

W[330] to W[335]

W[331] to W[336]

W[332] to W[337]

W[333] to W[338]

W[334] to W[339]

W[335] to W[340]

W[336] to W[341]

W[337] to W[342]

W[338] to W[343]

W[339] to W[344]

W[340] to W[345]

W[341] to W[346]

W[342] to W[347]

W[343] to W[348]

W[344] to W[349]

W[345] to W[350]

W[346] to W[351]

W[347] to W[352]

W[348] to W[353]

W[349] to W[354]

W[350] to W[355]

W[351] to W[356]

W[352] to W[357]

W[353] to W[358]

W[354] to W[359]

W[355] to W[360]

W[356] to W[361]

W[357] to W[362]

W[358] to W[363]

W[359] to W[364]

W[360] to W[365]

W[361] to W[366]

W[362] to W[367]

W[363] to W[368]

W[364] to W[369]

W[365] to W[370]

W[366] to W[371]

W[367] to W[372]

W[368] to W[373]

W[369] to W[374]

W[370] to W[375]

W[371] to W[376]

W[372] to W[377]

W[373] to W[378]

W[374] to W[379]

W[375] to W[380]

W[376] to W[381]

W[377] to W[382]

W[378] to W[383]

W[379] to W[384]

W[380] to W[385]

W[381] to W[386]

W[382] to W[387]

W[383] to W[388]

W[384] to W[389]

W[385] to W[390]

W[386] to W[391]

W[387] to W[392]

W[388] to W[393]

W[389] to W[394]

W[390] to W[395]

W[391] to W[396]

W[392] to W[397]

W[393] to W[398]

W[394] to W[399]

W[395] to W[400]

W[396] to W[401]

W[397] to W[402]

W[398] to W[403]

W[399] to W[404]

W[400] to W[405]

W[391] to W[406]

W[392] to W[407]

W[393] to W[408]

W[394] to W[409]

W[395] to W[410]

W[396] to W[411]

W[397] to W[412]

W[398] to W[413]

W[399] to W[414]

W[400] to W[415]

W[401] to W[416]

W[402] to W[417]

W[403] to W[418]

W[404] to W[419]

W[405] to W[420]

W[406] to W[421]

W[407] to W[422]

W[408] to W[423]

W[409] to W[424]

W[410] to W[425]

W[411] to W[426]

W[412] to W[427]

W[413] to W[428]

W[414] to W[429]

W[415] to W[430]

W[416] to W[431]

W[417] to W[432]

W[418] to W[433]

W[419] to W[434]

W[420] to W[435]

W[421] to W[436]

W[422] to W[437]

W[423] to W[438]

W[424] to W[439]

W[425] to W[440]

W[426] to W[441]

W[427] to W[442]

W[428] to W[443]

W[429] to W[444]

W[430] to W[445]

W[431] to W[446]

W[432] to W[447]

W[433] to W[448]

W[434] to W[449]

W[435] to W[450]

W[436] to W[451]

W[437] to W[452]

W[438] to W[453]

W[439] to W[454]

W[440] to W[455]

W[441] to W[456]

W[442] to W[457]

W[443] to W[458]

W[444] to W[459]

W[445] to W[460]

W[446] to W[461]

W[447] to W[462]

W[448] to W[463]

W[449] to W[464]

W[450] to W[465]

W[451] to W[466]

W[452] to W[467]

W[453] to W[468]

W[454] to W[469]

W[455] to W[470]

W[456] to W[471]

W[457] to W[472]

W[458] to W[473]

W[459] to W[474]

W[460] to W[475]

W[461] to W[476]

W[462] to W[477]

W[463] to W[478]

W[464] to W[479]

W[465] to W[480]

W[466] to W[481]

W[467] to W[482]

W[468] to W[483]

W[469] to W[484]

W[470] to W[485]

W[471] to W[486]

W[472] to W[487]

W[473] to W[488]

W[474] to W[489]

W[475] to W[490]

W[476] to W[491]

W[477] to W[492]

W[478] to W[493]

W[479] to W[494]

W[480] to W[495]

W[481] to W[496]

W[482] to W[497]

W[483] to W[498]

W[484] to W[499]

W[485] to W[500]

W[486] to W[501]

W[487] to W[502]

W[488] to W[503]

W[489] to W[504]

W[490] to W[505]

W[491] to W[506]

W[492] to W[507]

W[493] to W[508]

W[494] to W[509]

W[495] to W[510]

W[496] to W[511]

W[497] to W[512]

W[498] to W[513]

W[499] to W[514]

W[500] to W[515]

W[501] to W[516]

W[502] to W[517]

W[503] to W[518]

W[504] to W[519]

W[505] to W[520]

W[506] to W[521]

W[507] to W[522]

W[508] to W[523]

W[509] to W[524]

W[510] to W[525]

W[511] to W[526]

W[512] to W[527]

W[513] to W[528]

W[514] to W[529]

W[515] to W[530]

W[516] to W[531]

W[517] to W[532]

W[518] to W[533]

W[519] to W[534]

W[520] to W[535]

W[521] to W[536]

W[522] to W[537]

W[523] to W[538]

W[524] to W[539]

W[525] to W[540]

W[526] to W[541]

W[527] to W[542]

W[528] to W[543]

W[529] to W[544]

W[530] to W[545]

W[531] to W[546]

W[532] to W[547]

W[533] to W[548]

W[534] to W[549]

W[535] to W[550]

W[536] to W[551]

W[537] to W[552]

W[538] to W[553]

W[539] to W[554]

W[540] to W[555]

W[541] to W[556]

W[542] to W[557]

W[543] to W[558]

W[544] to W[559]

W[545] to W[560]

W[546] to W[561]

W[547] to W[562]

W[548] to W[563]

W[549] to W[564]

W[550] to W[565]

W[551] to W[566]

W[552] to W[567]

W[553] to W[568]

W[554] to W[569]

W[555] to W[570]

W[556] to W[571]

W[557] to W[572]

W[558] to W[573]

W[559] to W[574]

W[560] to W[575]

W[561] to W[576]

W[562] to W[577]

W[563] to W[578]

W[564] to W[579]

W[565] to W[580]

W[566] to W[581]

W[567] to W[582]

W[568] to W[583]

W[569] to W[584]

W[570] to W[585]

W[571] to W[586]

W[572] to W[587]

W[573] to W[588]

W[574] to W[589]

W[575] to W[590]

W[576] to W[591]

W[577] to W[592]

W[578] to W[593]

W[579] to W[594]

W[580] to W[595]

W[581] to W[596]

W[582] to W[597]

W[583] to W[598]

W[584] to W[599]

W[585] to W[600]

W[586] to W[601]

W[587] to W[602]

W[588] to W[603]

W[589] to W[604]

W[590] to W[605]

W[591] to W[606]

W[592] to W[607]

W[593] to W[608]

W[594] to W[609]

W[595] to W[610]

W[596] to W[611]

W[597] to W[612]

W[598] to W[613]

W[599] to W[614]

W[600] to W[615]

W[601] to W[616]

W[602] to W[617]

W[603] to W[618]

W[604] to W[619]

W[605] to W[620]

W[606] to W[621]

W[607] to W[622]

W[608] to W[623]

W[609] to W[624]

W[610] to W[625]

W[611] to W[626]

W[612] to W[627]

W[613] to W[628]

W[614] to W[629]

W[615] to W[630]

W[616] to W[631]

W[617] to W[632]

W[618] to W[633]

W[619] to W[634]

W[620] to W[635]

W[621] to W[636]

W[622] to W[637]

W[623] to W[638]

W[624] to W[639]

W[625] to W[640]

W[626] to W[641]

W[627] to W[642]

W[628] to W[643]

W[629] to W[644]

W[630] to W[645]

W[631] to W[646]

W[632] to W[647]

W[633] to W[648]

W[634] to W[649]

W[635] to W[650]

W[636] to W[651]

W[637] to W[652]

W[638] to W[653]

W[639] to W[654]

W[640] to W[655]

W[641] to W[656]

W[642] to W[657]

W[643] to W[658]

W[644] to W[659]

W[645] to W[660]

W[646] to W[661]

W[647] to W[662]

W[648] to W[663]

W[649] to W[664]

W[650] to W[665]

W[651] to W[666]

W[652] to W[667]

W[653] to W[668]

W[654] to W[669]

W[655] to W[670]

W[656] to W[671]

W[657] to W[672]

W[658] to W[673]

W[659] to W[674]

W[660] to W[675]

W[661] to W[676]

W[662] to W[677]

W[663] to W[678]

W[664] to W[679]

W[665] to W[680]

W[666] to W[681]

W[667] to W[682]

W[668] to W[683]

W[669] to W[684]

W[670] to W[685]

W[671] to W[686]

W[672] to W[687]

W[673] to W[688]

W[674] to W[689]

W[675] to W[690]

W[676] to W[691]

W[677] to W[692]

W[678] to W[693]

W[679] to W[694]

W[680] to W[695]

W[681] to W[696]

W[682] to W[697]

W[683] to W[698]

W[684] to W[699]

W[685] to W[700]

W[686] to W[701]

W[687] to W[702]

W[688] to W[703]

W[689] to W[704]

W[690] to W[705]

W[691] to W[706]

W[692] to W[707]

W[693] to W[708]

W[694] to W[709]

W[695] to W[710]

W[696] to W[711]

W[697] to W[712]

W[698] to W[713]

W[699] to W[714]

W[700] to W[715]

W[701] to W[716]

W[702] to W[717]

W[703] to W[718]

W[704] to W[719]

W[705] to W[720]

W[706] to W[721]

W[707] to W[722]

W[708] to W[723]

W[709] to W[724]

W[710] to W[725]

W[711] to W[726]

W[712] to W[727]

W[713] to W[728

Date: _____
Page: _____

more stronger since encryption decryption is twice as
Triple DES with 3 key

Decryption

```

graph LR
    P[P] --> E1[box E]
    E1 --> A1[box A]
    A1 --> B1[box B]
    B1 --> D1[box D]
    D1 --> C[C]
    K1[K1] --> E1
    K2[K2] --> A1
    K3[K3] --> B1
    K3 --> D1
  
```

Encryption

```

graph LR
    P[P] --> D1[box D]
    D1 --> B1[box B]
    B1 --> A1[box A]
    A1 --> E1[box E]
    K1[K1] --> D1
    K2[K2] --> B1
    K3[K3] --> A1
    K3 --> E1
  
```

Triple DES with 3 key

Decryption

```

graph LR
    P[P] --> E1[box E]
    E1 --> A1[box A]
    A1 --> B1[box B]
    B1 --> D1[box D]
    D1 --> C[C]
    K1[K1] --> E1
    K2[K2] --> A1
    K3[K3] --> B1
    K3 --> D1
  
```

Encryption

```

graph LR
    P[P] --> D1[box D]
    D1 --> B1[box B]
    B1 --> A1[box A]
    A1 --> E1[box E]
    K1[K1] --> D1
    K2[K2] --> B1
    K3[K3] --> A1
    K3 --> E1
  
```

Decryption

```

graph LR
    P[P] --> E1[box E]
    E1 --> A1[box A]
    A1 --> B1[box B]
    B1 --> D1[box D]
    D1 --> C[C]
    K1[K1] --> E1
    K2[K2] --> A1
    K3[K3] --> B1
    K3 --> D1
  
```

Encryption

```

graph LR
    P[P] --> D1[box D]
    D1 --> B1[box B]
    B1 --> A1[box A]
    A1 --> E1[box E]
    K1[K1] --> D1
    K2[K2] --> B1
    K3[K3] --> A1
    K3 --> E1
  
```

Decryption

```

graph LR
    P[P] --> E1[box E]
    E1 --> A1[box A]
    A1 --> B1[box B]
    B1 --> D1[box D]
    D1 --> C[C]
    K1[K1] --> E1
    K2[K2] --> A1
    K3[K3] --> B1
    K3 --> D1
  
```

Encryption

```

graph LR
    P[P] --> D1[box D]
    D1 --> B1[box B]
    B1 --> A1[box A]
    A1 --> E1[box E]
    K1[K1] --> D1
    K2[K2] --> B1
    K3[K3] --> A1
    K3 --> E1
  
```

text

Date _____
Page _____

1. Rotation of word $\overline{w_0 w_1 w_2 w_3}$: 1 byte left circular shift
[$w_0 w_1 w_2 w_3$] is transformed into [$w_1 w_2 w_3 w_0$]
2. Sub round performs a byte Substitution network
3. ADD round constant
(round 1 mod 13, 2nd mod 226, 3rd mod 1)

1st byte w_0 ,

4th byte w_3 after 3rd shift,

$w_0 \leftarrow w_0 \oplus w_3$

$w_1 \leftarrow w_1 \oplus w_2$

$w_2 \leftarrow$

$w_3 \leftarrow$

$w_0 \leftarrow$

$w_1 = g(w_3)$

2nd, circular shift,

$w_0 \leftarrow 20, 46, 75$

67, 20, 46, 75

byte substitution net use substitution box, II

for 20, 2 row in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$, column in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$

for 46, 5 row in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$, column in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$

for 75, 6 row in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$, column in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$

for 67, 7 row in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$, column in $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$

for 20, 90, 15

for 46, 90, 15

for 75, 90, 15

for 67, 90, 15

first round so, result A

first round so, (0, 0, 0, 0)

modular addition 2, right 2
sum and modulo 2 are given here
not left subtraction
one bit left 256

IDEA (International Data Encryption Algorithm)

6 bits



P_1 to P_4

60 bits

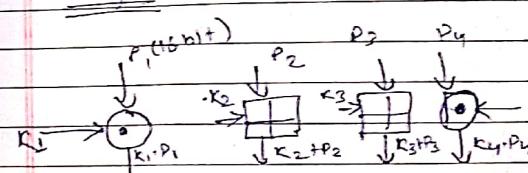
16 byte key

selected

Total rounds are one half round (3 rounds)

(initial round)

diagram



other rounds
R2

R1 - R4 (Data)

R5, R6 (even)

odd but even round

R7

description next

2. Cipher Block chaining mode (CBC)

Initialization vector (IV)
first block P_1 XOR, then encrypt, get 1st block cipher text, second block XOR next, c_2 etc (3...n)

More secure than ECB mode

Decrypt msg for given IV, c_1 , ..., cipher text c_1, c_2, \dots
plain text p_1, p_2, \dots (decrypt message text)

1. P_2 & c_2 are decrypted first then c_1 & c_1 are XOR
XOR c_1 & c_1

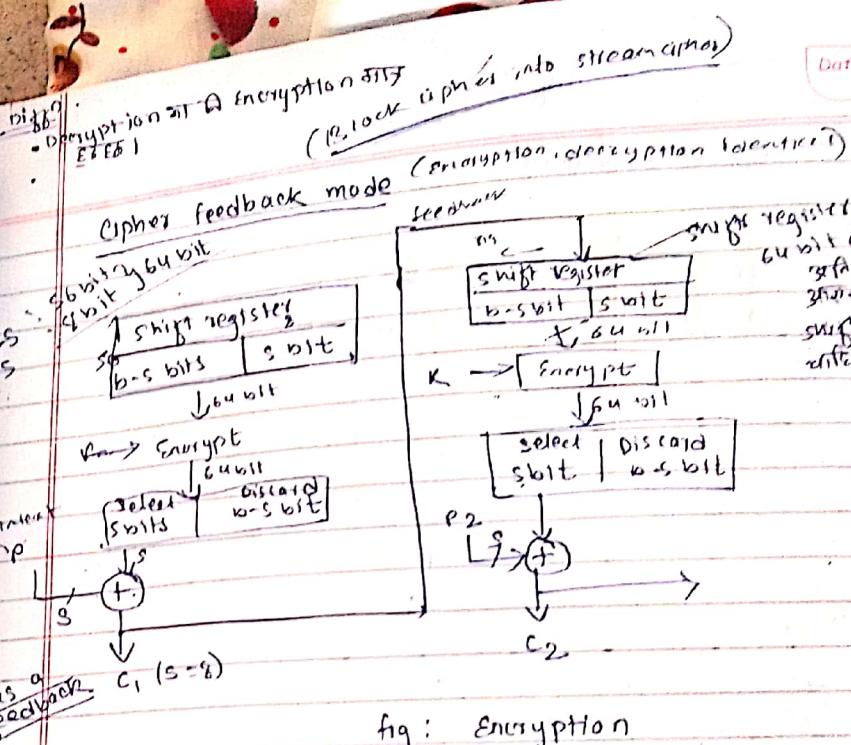
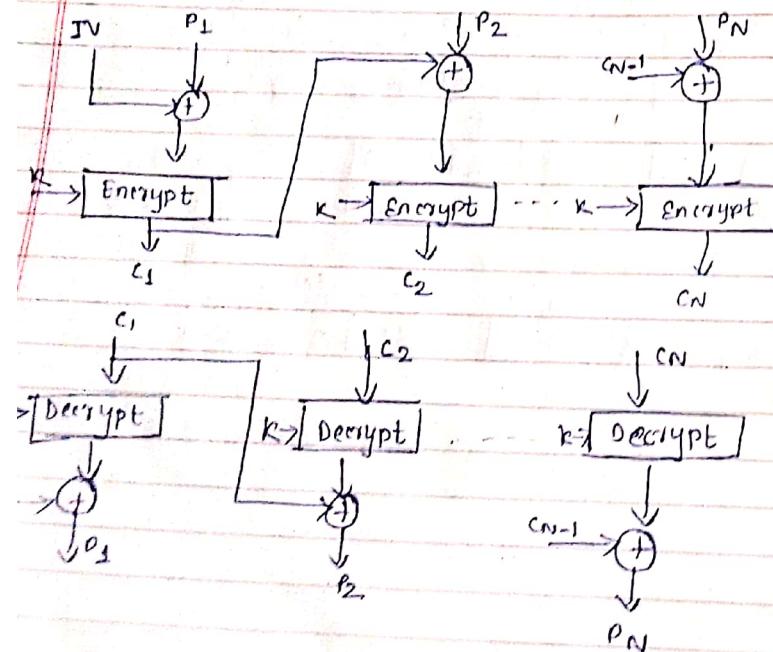


fig: Encryption

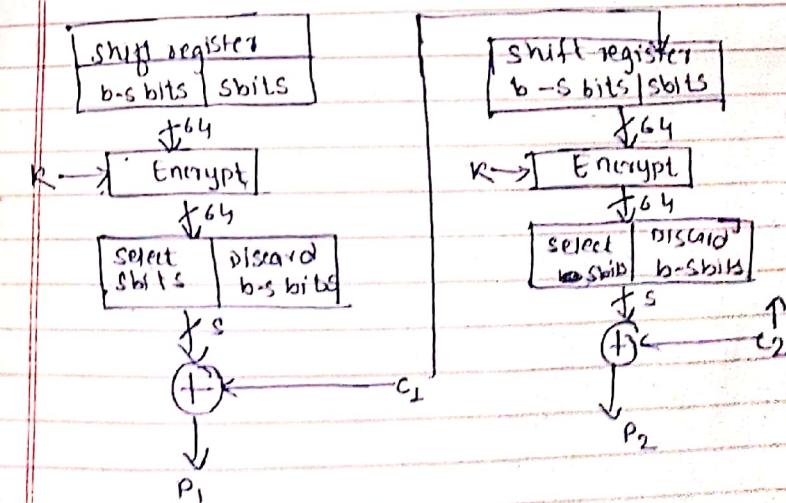


fig: Decryption

*(Date _____
Page _____)*

dig^n : shift feedback over counter

output feedback mode

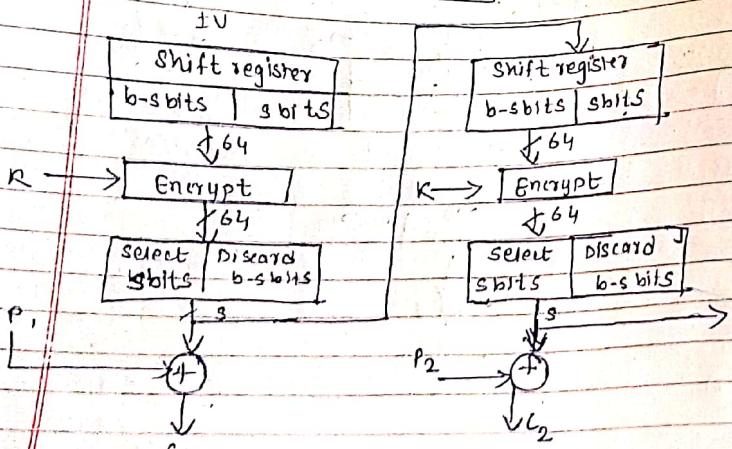
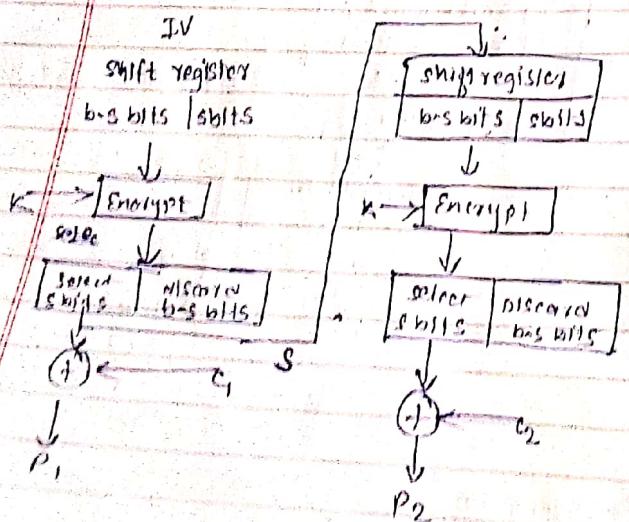


fig: Encryption



*(Date _____
Page _____)*

format for decryption at encrypt mode

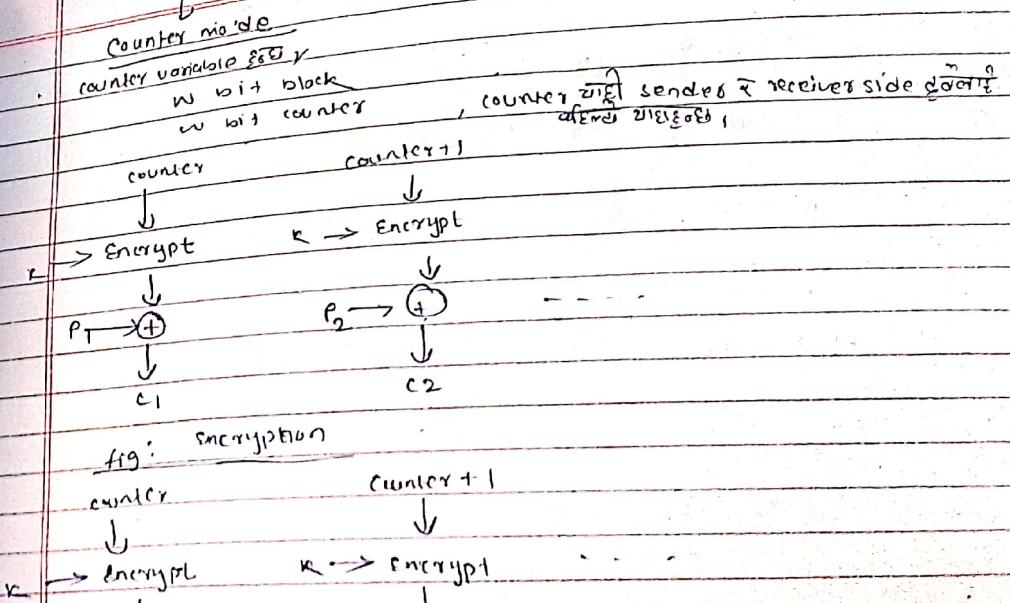


fig: Encryption

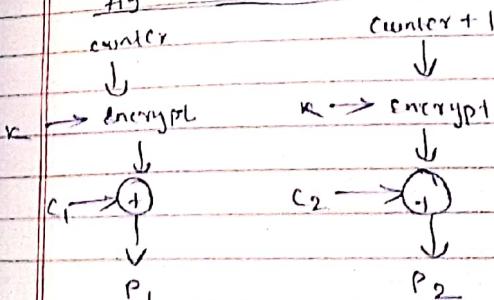


fig: Decryption

Chapter - 4

Public key cryptography
prime numbers sanga related [2]

• Euclidean group होता, अन्त ग्रूप में basically addition.

$$(Z, +) \subset (-\infty, +\infty)$$

set of integers under addition is a group

Group होता & यह cond'n satisfy इसके.
closure:

$$Z = \{-3, -2, -1, 0, 1, 2, 3, \dots\}$$

$$-3+1 = -2 \in Z,$$

Associative

$$1 + (2+3) = (1+2) + 3$$

Identity element:

Element in $\{Y\}$ such that,
 $a + e = e + a = a$

$$0 = 0 + 2 = 2$$

Element

Date _____
Page _____

Int. defn of Ring, field, group?

Date _____
Page _____

finite group

Set of integer's ⁽²⁾ infinite group. [set में infinite elements]
 Z_8 is finite group. [8 जीवने elements]

Abelian group:
-commutative groups

Ring

Rational number $\rightarrow \frac{p}{q}$

Real number \rightarrow

Complex number \rightarrow Real & imaginary parts,

Two operations:-

↳ addition, multiplication only.

$\{R, +, \times\}$ is a set of elements, with two binary operation called addition and multiplication. where R is, the set of Rational num, Real num and complex number.

A₅

M₁

M₂

M₃

Commutative

Closure under multiplication

Associative of multiplication

Distributive : $a(b+c) = ab+ac$ for all $a, b, c \in R$

Integral domain

additional two property: (i) Multiplicative identity: $a \cdot 1 = 1 \cdot a = a$
(ii) No zero divisor, if $ab=0$, then either
 $a=0$ or $b=0$.

Fields

Algebraic structures

M1 - M5

Multiplicative inverse

$$a \cdot a^{-1} = a^{-1} \cdot a = 1$$

Ex:-
5. $\frac{1}{5} \in \mathbb{Z}$ & $\frac{1}{5} \notin \mathbb{Z}$, so set of integers under multiplication is not a group.

But, set of rational numbers under addition and multiplication is field.

Condition	Result	Conclusion	Group	Properties
Integers domain	\mathbb{Z}	closed	Abelian group	(A1) Closure under addition (A2) Associativity of addition (A3) Additive identity (A4) Additive inverse (A5) Commutativity of addition
Integers domain	\mathbb{Q}	closed	Abelian group	(M1) Closure under multiplication (M2) Associativity of multiplication (M3) Distributive laws
Rational numbers domain	\mathbb{Q}	closed	Field	(M4) Commutativity of multiplication (M5) Multiplicative identity (M6) No zero divisors (M7) Multiplicative inverse

Modular Arithmetic

$$a = qn + r$$

q = quotient
 r = remainder

$$\text{Ex: } a = 21, n = 4$$

$$21 = 5 \times 4 + 1$$

$a \equiv b \pmod{n}$ This means, $a - b$ is exactly divisible by n .

Ex:

$$21 \equiv 1 \pmod{4}$$

2. $(a \bmod n) - (b \bmod n) \bmod n = (a - b) \bmod n$

3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

$$7^{11} \bmod 4$$

$$7^1 \equiv 3 \bmod 4$$

$$7^2 \equiv 3^2 \equiv 9 \equiv 1 \bmod 4$$

$$7^4 \equiv 1^2 \equiv 1 \bmod 4$$

$$7^8 \equiv 1^2 \equiv 1 \bmod 4$$

$$\therefore 7^{11} \bmod 4 = (1 \times 1 \times 3) \bmod 4 = 3$$

$$5^{12} \bmod 3$$

$\bmod 3$

$$5^1 \equiv 5 \equiv 2 \bmod 3$$

$$5^2 \equiv 2^2 \equiv 4 \bmod 3$$

$$5^4 \equiv 1^2 \equiv 1 \bmod 3$$

$$5^8 \equiv 1^2 \equiv 1 \bmod 3$$

$$5^{12} \equiv 1 \cdot 1 \cdot 1 \equiv 1 \bmod 3$$

$$\therefore (1 \times 1) \bmod 3 = 1$$

$$T \bmod 3 = 1$$

Modular arithmetic

$$28 \equiv 40, 11, 2, 3, 4, 5, 6, 7 \pmod{3}$$

\mathbb{Z}_n = set of integers less than n .

Aithmetic modulo 8.

\times	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

$$(1+2) \pmod{8} = 3$$

$$(1+7) \pmod{8} = 0$$

relative prime तो कठीन मात्र
inverse exist नहीं,

Additive and multiplicative inverse modulo 8.

(P.D) mod = 0 remainders

$\text{N} \rightarrow \text{W}$ (additive inverse) $\text{W} \rightarrow \text{N}$ (multiplicative inverse)

$$\text{cod} \equiv 1 \pmod{m}$$

$$I \times I^{-1} \equiv 1 \pmod{0}$$

since, relative prime doesn't

$$\gcd(2, 8) \neq 1$$

$$\frac{3 \times 3 - 1}{8} = 0 \quad [3 \times 3 \equiv 1 \pmod{8}]$$

$$2 \cdot 1 \equiv 2 \not\equiv 1$$

Note that 2_8 is commutative w.r.t. \oplus & \otimes last two most

property list out just commutative result हो, अर्थात् सत्य नहीं होता।

Associativity:

$$+ (2+3) \text{ mod } 8 : 1 + 5 \text{ mod } 8$$

$$1 + 5$$

$$1+2+3 \text{ mod } 8 : 6$$

$$3+3$$