Date ______
Page ______

features of cryptography

→ Confidentiality ← message disclose हुन नदिने (Encryption गर्न सक्ने) (Decryption)
→ Integrity ← (कुनै पनि content modification हुन नदिने, hash function use गर्ने।)
→ Availability ← (चाहिएको बेलामा data available हुन पर्ने।)
→ Non Repudiation
कसैले कहीं message पठायो but sender ले मैले पठाको हैन भनेर deny गर्न सक्छ, त्यो नगराउन भनेर digital signature use गरिन्छ, त्यो चाहिँ Non Repudiation भनिन्छ।

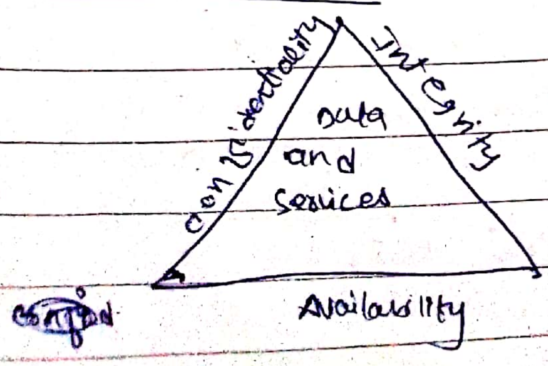
→ cryptography :- Science of hiding a message.

security
यही भित्र पर्छ confidentiality, integrity सब, त्यो cryptography पनि,

security
- network security
- Internet Security

* The field of network internet security consists:
- deter (आउन नै नदिने।)
- prevent (attempt गर्यो भने रोक्ने।)
- ~~attack~~ ~~correct~~ detect (if भइहाल्यो भने detect गर्ने।)
- correct security violation

N.V. Imp **CIA Triad** ← • confidentiality • Integrity • Availability



Ex: if कसैले computer मा केही काम गरिराख्दा कोहिन गयो भने, अर्कैले केही गर्दियो भने, security bridge भयो।

~~Security bridge भयो भने/कसलाई थाहा भएको छ~~ भने, measures गर्ने,

Levels of Impact

- low
- Moderate — system bridge गर्ने प्रति system बाट informations लिने,
- High — system bridge गर्ने plus system control गर्ने

Goals of computer security:

- To protect computer assets from:
  - Human errors, natural disasters, physical and electronic maliciousness
- ~~Long~~ CIA

Confidentiality

message disclose गर्न नहुने।

privacy bridge हुन नहुने,

Integrity

- Data integrity
  - correctness of data
  - Specified person/authorized person ले मात्र change गर्न मिल्ने।

System integrity

- system प्रति intention ले बनाइएको, अनि, system ले अरूको काम गर्दैन भने, or, जुन system ले integrity maintain गर्छ भने पनि दिएको, बाहिरने delete गर्न चाहिँ नहुने।
- जुन purpose लाई बनेको हो त्यही गर्न पर्यो।

Availability

- authorized users ले info access गर्न ~~सक्ने~~ खोजेका पाउनुपर्छ

  - authorization
    - users ले के के गर्न पाउने, के के permission दिने सक्ने।
    - what he/or she is allowed to do.
  - authentication
    - user verify गर्ने
    - Exactly same person हो कि होइन verify गर्ने।

Other goals

- Non repudiation
  - कसैले deny गर्न सक्दैन।
  - can't deny that exchange took place.

- Legitimate use
  - जसले use गर्न पर्ने त्यसले मात्र use गर्न पर्छ।

~~Threats~~

- Vulnerability / loop holes

  कुनै पनि software को weakpoint vulnerability.

  Ex:- घरको मूल ढोकाको चुकुल use बिग्रायाछ, त्यो vulnerability हुने भयो burglars को, constant threat अति, attack गर्छन्, त्यही vulnerability use गरेर गर्ने हो।

Scanned with CamScanner

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 पठाउन पाइने।

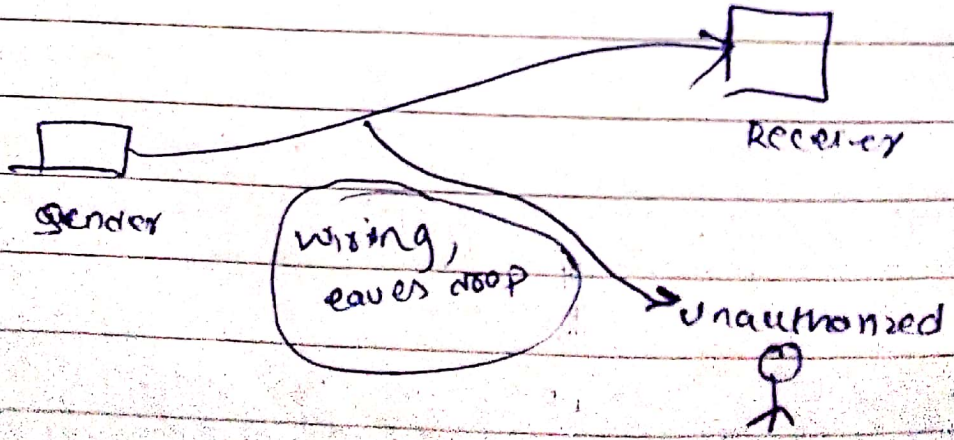
VV.IMP

Four types of possible attacks are:

- Active
  - Interruption
  - Interception
  - Modification
  - Fabrication
- Passive

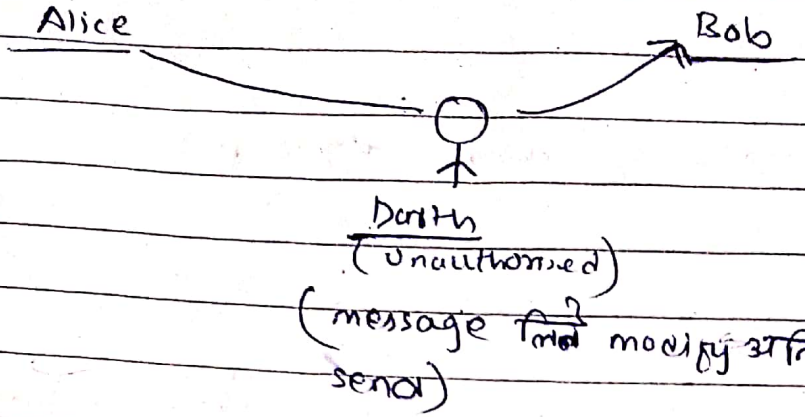
1. Interruption
   - जुन service लिन खोज्दैछ, त्यो disrupt गरिदिने।
   - active attack

2. Interception
   - normal flow मध्यमबाटै unauthorized ले नै information content पाइहाल्ने
   - active attack



3. Modification

- Active attack



(message लिने modify गरि send)

4. Fabrication (Impersonation) (Masquerade)

- Alice र Bob बिचमा हुनपर्ने नर, Darth आफि Alice भएर communicate.
- Active

fig: Impersonation

5. Denial of service

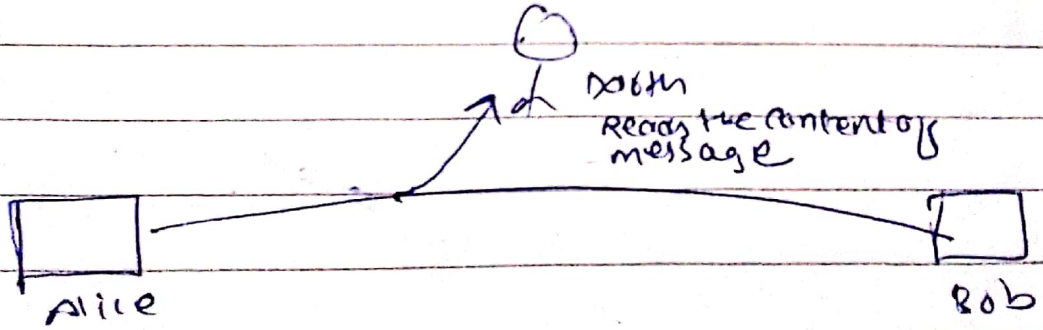
- authorized user ले चाहेको बेलामा user use गर्न नपाउने।

~~Aspects~~

Passive attack

- frequency of message transmission, number of message कति बेला transfer हुन्छ rate मा हुन्छ info collect गर्न चाहि attack हुन्छ passive attack.

or, Replay, (path change गर्दिने।)



Types:

- Release of message content
- Traffic analysis.

Aspects of Security

- Security attack
- Security Mechanism
- Security Service (collection of mechanism वाँहि service)

- **Securityservice**

multiple mechanism use गर्ने, mechanism कुनको, authorization, authentication हेर्ने हुन्छ।

Standards :

X-800:

- यसले document हो, जसमा different services define गरेको हुन्छ,
- data transfers related हुन्छ।

RFC4949:

- Request for
- internet मा use हुने diff^n technology (HTTP, FTP, UDP ...) यसले गर्दा, protocols आदि network related गर्छ, यसलेहुने के, यो document मा।

Date
Page

Security service X-800

Authentication

- user verification गर्ने, धेरैको धेरैको authentication.

- Peer entity authentication

  peer धेरैको र group of .

- Data origin authentication

  - आएको data specified organization को हो कि होइन, यसको लागी

service:

- Access control
- Data confidentiality
- Data integrity
- Non Repudiation.

Security Mechanisms:

specific .

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

persuasive sec

- Trusted functionality, security labels, .

Trusted third party को काम :

→ connection algorithm create गर्ने
key generate गर्ने
~~key transmission गर्ने~~

Model for network security

कहिले काहीं sender, receiver एक अर्कालाई trust नगर्न सक्छन्,

so, त्यतिबेला T T P लिएर आइन्छ,

यो यदि trusted third party हो भने सबैलाई available हुनुपर्छ

यसमा use हुने protocols:

PKI, kerberus

Model सर को बाट हेर्ने।

Using this model requires us to

- design a suitable algorithm.
- secret info (keys) used by the algorithm
- key transmit गर्ने।, (यसमा अर्को protocol LDAP जस्तो use हुन सक्छ।)

Trusted third party → message transmission को mechanism तयार गर्छ।

Date ____ Page ____

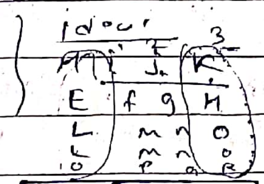
Cryptography

Encryption:

Plain text ——→ cipher text

Ex:

HELLO ——→ KHOOR (K=3)



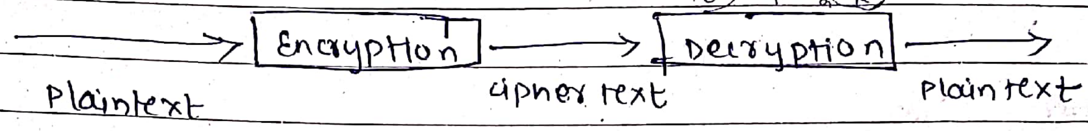


fig. Encryption- Decryption

Key

- parameter or value जसले output determine गर्छ।
  key को value public भयो भने जसले नि decrypt गर्न सक्छ।

cipher

- algorithm used for encryption.

Decipher

algorithm used for decryption.

Crypto system

Crypto system : is a 5-typle/quintuple (E, D, M, K, C) where M set of plaintexts, K set of keys, C set of cipher texts, E set of encryption fxn's e: M x K → C and D set of decryption fxn's d: C x K → M

- $e: M \times K \to C$ — M: plaintext, K: key } plain text र key बाट cipher text बन्छ।
- $d: C \times K \to M$ — cipher text मा key apply गर्दा plain text

- Example: Ceaser Cipher

Date ____ Page ____

← plain text

M = {sequence of letters}

key → K = {i | i is an integer 0 ≤ i ≤ 25}

E = {E_k | k ∈ K and for all letters m, $E_k(m)$ = (m+k) mod 26}

D = {D_k | k ∈ K and for all letters c, $D_k(c)$ = (26+c−k) mod 26}

C = M,
cipher text — M नि sequence of letters, C नि sequence of letters
मात्र रहन्छ।

Ceaser Cipher

- **Cryptographic System characterstics**

  - Type of operations used for transforming plain to cipher
  - Number of keys used
    - symmetric: encryption र decryption मा same key
    - asymmetric " " diffⁿ key
  - way in which plain text is processed

a) stream cipher: character by character (पहिला H अनि E, - - -)

b) Block cipher:
- HELLO छ, अनि ~~~~ ~~~~. अब 64 bit block हो भने, त्यसलाई लिन्छ, अनि transmit गर्छ
H को ascii 65 हो, अनि 65+8=73, त्यो अनि अब, E पनि अलग्ग भने, त्यो block मा त्यो नि लिन्छ।
- bits को intermix गरेर आउँछ।
- Highly secure)

Date ____ Page ____

Substitution Cipher

(यही) ceaser cipher है,

H E LL O → map करो, (यहाँ)

K H O O R

Encrypt

(25+4) mod 26
= 29 mod 26
= 3 r ; j r

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

"g v c t s k v e t l c"

$E_k(C) = (2+4) \bmod 26$
$= 6 \bmod 26$
$= 6$
$= g$

$E_k(R) = (17+4) \bmod 26$
$= 21$
$= v$

$E_k(Y) = (24+4) \bmod 26$
$= 28 \bmod 26$
$= 2$
$= c$

$E_k(P) = (15+4) \bmod 26$
$= t$

$E_k(t) = (19+4) \bmod 26$
$= 23 \bmod 26$
$= x$

$E_k(O) = s$

$E_k(g) = (6+4) \bmod 26$
$= 10 \bmod 26$
$= k$

$E_k(p) = (15+4) \bmod 26$
$= t$

c d e f g
r s t u v
y z a b c
p q r s t
t u v w x
o p q r s
g h i j k
r s t u v
a b c d e
p q r s t
h i j k
y z a b

a-0, b-1, c-2, d-3, e-4, f-5, g-6, h-7, i-8, j-9, k-10, l-11, m-12, n-13, o-14, p-15, q-16, r-17, s-18, t-19, u-20, v-21, w-22, x-23, y-24, z-25

Date
Page

~~Transposition cipher~~

Substitution

HELLO → KHOOR

substitute गरिन्छ ।

Transposition

HELLO → OKHRO

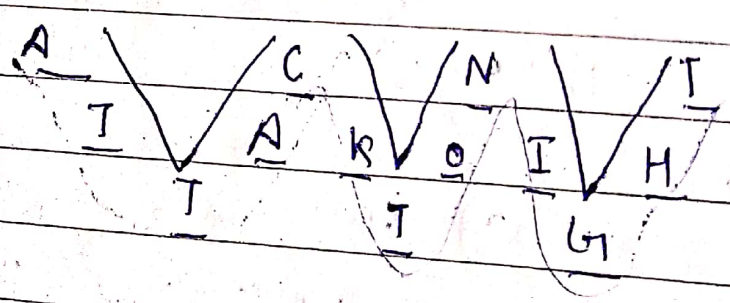
- substitute त हुन्छ, but, location फेरा पुर्ति जस्तो हुन्छ ।
- actual position of letter gets changed making the text garble.

Rail-fence cipher

एक कोर्ने वेला line मा लेख्न हुने भनेर हो ।

Ex: "ATTACK TONIGHT"

Rail = 3



ACNTAKOIHTTG

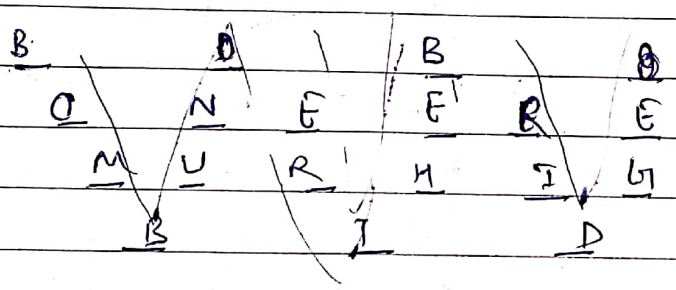
Encrypt and Decrypt message

"BOMB UNDER THE BRIDGE" using Rail=4,

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

Cipher text:
"BOBONEEREMURHIGBTD"

Decrypt:



Vertical wala ni

"This is the planet", 3 rails

T S t p n
h i h l e
i s e a t

T S t p n h i h l e i s e a t
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Decrypt- T h i

3. Vigenere Cipher : substitution cipher (Polyalphabetic)

if key = PKG

NCCS COLLEGE CS IT

PKGPKGPKGPKGPKG

सूत्रण plain text A-Z, key A-Z ले कर H से ले , H, H अंतर्गत

key

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

Plaintext: Examination
Key: Nccs

plaintext	E	X	A	M	I	N	A	T	I	O	N
key	N	C	C	S	N	C	C	S	N	C	C
ciphertext	R	Z	C	E	V	P	C	L	V	Q	P

Decrypt करते key N को column हैं समझना, अति,

One-Time Pad (Simple XOR) (vernam cipher)

→ message: HELLO
72 69 76 76 79

message र key को length बराबर लिने।
message मा 5 वटा छ, so, key पनि 5 वटा छ।

72 : 01001000
69 : 01000101
76 : 01001100
76 : 01001100
79 : 01001111

Key: ABCDE

A : 01000001
B : 01000010
C : ~~01000100~~ 01000011 (67)
D : 01000100
E : 01000101

01001000 01000101 01001100 01001100 01001111
01000001 01000010 01000011 01000100 01000101
00001001 00000111 00001111 00001000 00001010

9 7 15 8 10

(यतिहरुको corresponding ASCII हेर्न मिल्छ, so यस्तो राख्ने।)

cipher text: (9 7 15 8 10)

Decryption = cipher text XOR KEY

Playfair Cipher

Rule
same letter छ छुट्याउन मिल्छ, NCCS or COLLEGE छ, COL X LEGE बनाउने, plain text मा पनि key मा।

- पहिला row भरे, अनि column: अनि
- ~~diagonal row~~ → उल्टो diagonal pair मा हुन्छ।

Rule
- एउटै column मा, first letter को down, next letter को down
- एउटै row मा, first letter को right मा next letter को right मा।
- if kunai milena matrix को भने, त्यसको आफ्नो row को last मा अनि column को first wala लिने tyarka l samma को।

key: NCCS, plaintext: college

same छ, so पहिलो pair बनाउने, last मा x राख्ने।

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

C O L L E G E
→ CO LX LE GE

CO मा, diff row diff column, so BK बनाउने।

LX: same column, RS

LE: RF (first case भनेको, so अनि column हेर्ने)

GE: same row HF

Decrypt गर्दा thyakka ulto गर्ने, सबै rule को thyakka ulto.

Encryption

Same column: Element just below
Same row: " " right
different row, column: Element in its row and on 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.

alphabet की

a - 0
b - 1
⋮
z - 25

Hill Cipher

- Hill cipher use key matrix for encryption / decryption process.

Example:

Key matrix = $\begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix}$ {determinant of key matrix should be relative prime to 26}

message : ~~HI~~ WELCOME

Encryption: M × K

(सबसे) message लाई दुईदुई word मा छुट्याउने, अनि if pair पुग्दैन भने x थप्ने

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

$= \begin{bmatrix} 108 \\ 86 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 8 \end{bmatrix} =$ EI

$E_K(LC) = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 2 \end{bmatrix}$

$= \begin{bmatrix} 54 \\ 43 \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 \\ 20 \end{bmatrix} =$ CU

$E_K[OM] = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 14 \\ 12 \end{bmatrix}$

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

$E_K[EX] = \begin{bmatrix} 4 & 5 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} 4 \\ 23 \end{bmatrix} = \begin{bmatrix} 131 \\ 127 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 \\ 23 \end{bmatrix} =$

$a \equiv b \bmod c$
$a - b$ should be exactly divided by c, then only we can say $a \equiv b \bmod c$

Decryption

Inverse of key matrix $= \frac{1}{4\times5 - 3\times5}\begin{bmatrix} 5 & -5 \\ -3 & 4 \end{bmatrix}$

$= \frac{1}{5}\begin{bmatrix} 5 & -3 \\ -3 & 4 \end{bmatrix}$

$= 5^{-1}\begin{bmatrix} 5 & -5 \\ -3 & 4 \end{bmatrix}$

$a \equiv b \bmod c$.

or,

$5 \times 5^{-1} \equiv 1 \bmod 26$

5^{-1} काय यो 5 हुनछ, कसै, 5×5^{-1} लेख्दा,

अनि, छ,

5^{-1} यो कोशाख्या जाहि,.

$\frac{5 \times x - 1}{26}$ हुन्छ, exact value निकाल्दा,

$= 21$

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

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

$= \begin{bmatrix} 105 & 441 \\ 483 & 84 \end{bmatrix} \bmod 26$

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

$= 5 \bmod 26$

$= (5+21) \bmod 26 =$

$(3+23) \bmod 26$

or, easy:

$26 - 3 = 23$

$26 - 5 = 21$

Note:
Decrypt गर्दा determinant, 26 सँग relatively prime हुनु पर्छ calculate गर्न मिल्दैन।

Date
Page

Dk(EI)

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

$= \begin{bmatrix} 204 \\ 108 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 22 \\ 4 \end{bmatrix} = \text{WE}$

- Encrypt and decrypt HILL using key matrix $\begin{bmatrix} 3 & 3 \\ 5 & 6 \end{bmatrix}$ using Hill cipher.

→ HI LL

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

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

Decryption:

Determinant = 3

gcd(3, 26) = 1

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

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

$\frac{3x \cdot x - 1}{26}$ remain den हुन पर्छ।

26 भन्दा सानो calculate गर्ने

$= 9$

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

$= \begin{bmatrix} 54 & 207 \\ 189 & 27 \end{bmatrix} \bmod 26$

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

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

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

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

$= HI$

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

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

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

$= LL$

Date ______
Page ______

V.imp ~~(Cryptany)~~

Cryptanalytic Attacks

- Key findout गर्ने method (encryption गर्न use भाको key)

Diff^n types of attack:

ciphertext only - कुनै algorithm use भएर cipher text निकालेको छ। बाहा हुन्छ, अनि each bit, data राखेर check गर्छ। (possible key सबै राख्छ।)

known plaintext only. : plaintext नि थाहा छ, cipher text नि थाहा छ, (use भाको key थाहा पाएर, आफ्नो text चाहिं पढाउन मिल्ने भयो नि)

chosen plain text : intruder has access to encryption mechanism
- plain text हुन्छ, choose गरेको plain text को ciphertext generate गर्न सक्छ, (machine जस्तो हुन्छ), अनि, त्यही texts हरूबाट key निकाल्छ।

chosen ciphertext: intruder has access to decryption ~~mechanism~~ mechanism.
- ciphertext बाट plaintext आउँछ, अनि, त्यहीबाट key निकाल्न सजिलो।

chosen text:- combination of both
- known encryption and decryption mechanism.
- best one

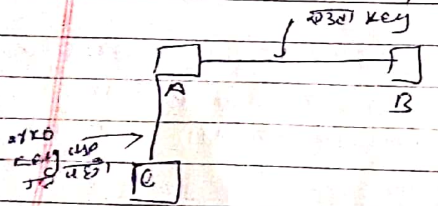
V.imp
Brute force attack - : Repeating the same process until the match is found.
- most used.

Symmetric ~~cipher~~ cryptography

- same key used for encryption, decryption
- Secret key shared by sender and receiver
- Encryption, decryption algorithm दुवै identical हुन्छ,

Main problems:

- key transmission गर्दा, out of band channel (diffⁿ frequency wala channel so intruder ले key access नपाओस्।)
- हरेक key generate हुन्छ, $\left(\frac{n(n-1)}{2}\right)$ key pairs.



- Fast हुन्छ।

Public key (Asymmetric key) → confidentiality → authentication

- Encryption गर्दा public part, use हुन्छ, (sender ले पठाउँदा public key use गर्छ।) अनि receiver ले आफ्नो private key use गरेर decrypt गर्छ।) (अब, त्यो key अरुलाई हुँदै हुँदैन, so, secure)

हरेक entity को public key, private key हुन्छ। अनि यो दुईवटा entity बाहेक third trusted party ले provide गर्छ।)

Diffⁿ betn symmetric, asymmetric key

Alice ले चाहे Bob को public key ले encrypt
Bob ले message चाहि आफ्नो private key ले decrypt (digital signature) (यसमा फेरि encrypt गर्दा private, decrypt गर्दा public key use हुन्छ।)

- यसले authentication लाई use हुन्छ, public key (Asymmetric) diffⁿ चाहे यसले use हुन्छ. secret key generate गर्न नि हो।
- Comparatively slow (10,000 times slower than symmetric cryptography)

Stream and Block ciphers

- message text लाई कसरी process गर्छ? को basis मा,

Stream : one character at a time
Example: ceaser, vernam, vigenere, cipher

Block : one block at a time (multiple characters)

Stream v/s Block cipher

Advantage of Stream cipher:
- Speed fast, negligible time
- Low error propagation (एक समय at a time [illegible] [illegible] [illegible] [illegible] [illegible])

Disadvantage:
- Low diffusion ([illegible]), Streamcipher [illegible]
HELLO $\xrightarrow{E3}$ KHOOR
- [illegible] [illegible] [illegible] detect [illegible] [illegible]।

HELLO → KXDOOR

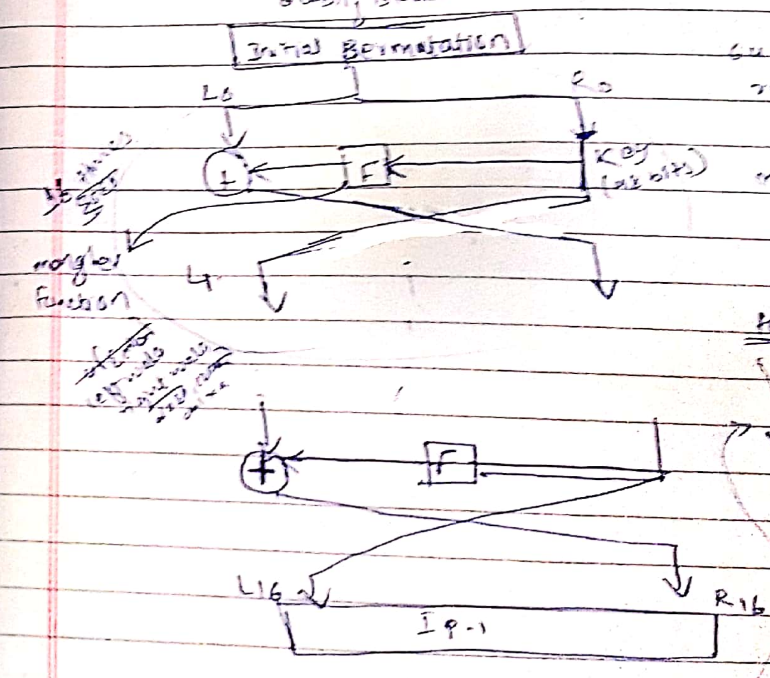
Advantage of Block cipher:
- High diffusion
- Immunity to insertion of symbols (fixed number of bits [illegible] [illegible] [illegible])

Disadvantage:
- Slow [illegible],
- Error propagation (एक block की single bit से, [illegible] cipher text में [illegible] [illegible] (Avalanche effect))

- Explain the Round key generation process for DES?
- SPN ([illegible]) SPN [illegible] (DES, Fistel algorithms) [illegible]

DES Algorithm

→ Block cipher Algorithm based on Feistel structure
→ 64 Bit Block
→ 64 Bit key initially, but only 56 bits are used
→ 16 identical rounds
→ 48 bit sub-key for each round (6×8 bit, Block)



64 bit Block [illegible], left 32, right 32, [illegible], 16 [illegible] round [illegible], [illegible] Round [illegible] 16 time [illegible] keys [illegible]

Function:
- Expansion: 32 bit [illegible] 48 [illegible]
- Keymixing: [illegible] expanded bit with key
- Substitution: 48 bit [illegible] 32 bit
- Permutation: [illegible]

DES Round

$L_n = R_{n-1}$

$R_{n-1} = L_n \oplus f(R_{n-1}, K_n)$

([illegible] [illegible] operation)

(1)

Date
Page

64

↓

permuted choice

↓

56 bits ← 8 bits ← 8, 16, 24, 32, 48, ...

↓ 28

C_0 D_0

arbitary number of leftshift 16 times

C_1 D_1

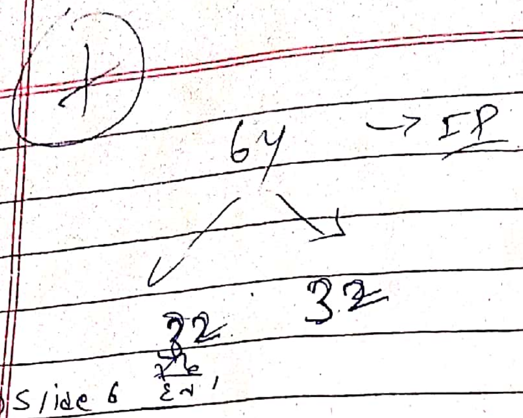
C_{16} D_{16}

permutation table

Key generation process

K_1 तयार C_1 D_1 नंतर

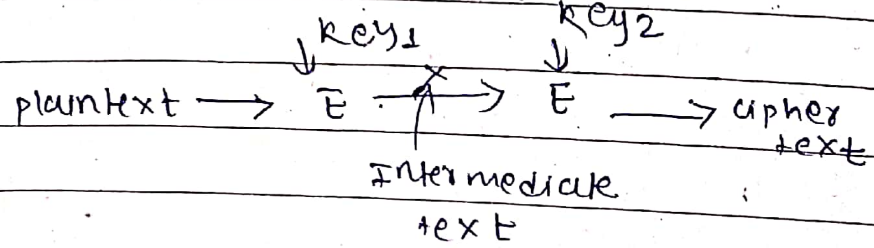
K_2 तयार C_2 D_2 नंतर



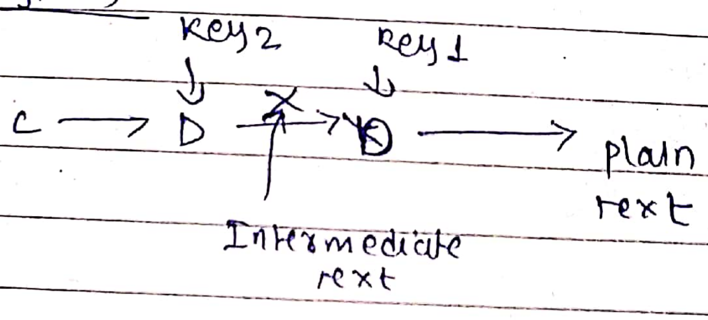
sir को slide 6 हेर्न।

Double DES & Triple DES

- Double DES मा चाँहि दुईवटा key use हुन्छ।



Decryption



- more vulnerable, (अझ less strong than single DES)

Imp // meet in the middle attack।

(Hackers ले Brute force attack use गरेर, ~~64 bit को key हुन्छ, 2^{64} ... निकाल्छ~~),

if plaintext र cipher text दुईवटै चाहिन्छ, key चाहिं निकाल्न पर्छ,

but 2^{64} ... नहुने

Encryption गर्दा 64 bit को

Decryption गर्दा नि 64 bit को आयो भने match गरेर, k1, k2 guess

finds

Triple DES with 2-key

$P \rightarrow [E] \xrightarrow{A} [D] \xrightarrow{B} [E] \rightarrow C$ (keys: K_1, K_2, K_1)

EDE — Encryption

$P \rightarrow [D] \xrightarrow{A} [E] \xrightarrow{B} [D] \rightarrow P$ (keys: K_1, K_2, K_1)

Decryption

- more stronger since encryption decryption is mixed

Triple DES with 3 key

$P \rightarrow E \xrightarrow{A} D \xrightarrow{B} E \rightarrow C$ (keys: K_1, K_2, K_3)

Encryption

$P \rightarrow D \xrightarrow{A} E \xrightarrow{B} D \rightarrow C$ (keys: K_1, K_2, K_3)

Imp AES का key generation

AES example
(Advance Encryption Standard)

- 128 bit block
- Keys (128, 192, 256)
  - 128 bit key – 10 rounds
  - 192 bit key – 12 rounds
  - 256 bit key – 14 rounds
- (n-1) identical round and 1 ~~half round~~ last different round (Ex: 14 मे 13 वटा identical, last वाला diff^n)
- Each identical round contains:
  1. substitute byte
  2. shift rows
  3. mix columns
  4. Add round key
- → last round doesn't have mix column step.
- → Each round use 128 bit subkey

Subkey generation

→ 128 bit key
= 4 words (w[0] to w[3])
w[4] to w[43]

$w_8 = g(w_7) \oplus w_4$
$w_9 = w_8 \oplus w_5$
$w_{10} = w_9 \oplus w_6$
$w_{11} = w_{10} \oplus w_7$

128 bit
↓ 16 byte छ,

K_0 K_4 K_8 K_{12}

generate गर्नु पर्छ, w_4 to w_{43}

K_3 K_7 K_{11} K_{15}
↓ ↓ ↓ ↓
w_0 w_1 w_2 w_3 → w_4

($w_0 \oplus$ → w_4 w_5 w_6 w_7)

w_4, w_8, w_{12} ... generate गर्दा, अरु previous बाट निकाल्ने
$w_4 = g(w_3) \oplus w_0$; $w_5 = w_4 \oplus w_1$; $w_6 = w_5 \oplus w_2$; $w_7 = w_6 \oplus w_3$

1. Rotation of word हो : 1 byte left circular shift
[b0, b1, b2, b3] is transformed into [b1 b2 b3 b0]
2. Sub word performs a byte substitution method
3. ADD round constant
(round 1 मा 1 add, 2 मा 2 add गर्ने)

Ex:

16 byte छ भने,
w0 w1 w2 w3 को matrix बन्छ,
w0 भन्दा 4 बाट
w1 next 4
w2
w3 67, 20, 46, 75

$w_4 = g(w_3)$

पहिला, circular shift,
= 20, 46, 75, 67

byte substitution मा use substitution box, 2 row मा, 0 देखि F, column मा 0-7
for 20, 2 row मा, 0 column मा, B7
for 46, 4 row मा छ, 6 column मा, 5A
75, 9D
67, 85

Adding round constant, (01, 00, 00, 00) (first round मा 01)

---

modular addition 1, भन्ने modulus prime number हुन्छ ... कति छ ...

IDEA (International Data Encryption Algorithm)

64 bit
↓
P1 to P4
16 byte

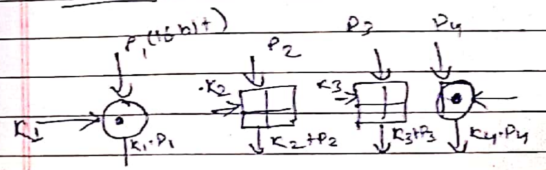
- 16 byte key
- Total 8 rounds and one half round (9 rounds) (output round)

f(x) = y

Ex:
1 mod 8

∴ 50 mod 8 ...

- diagram



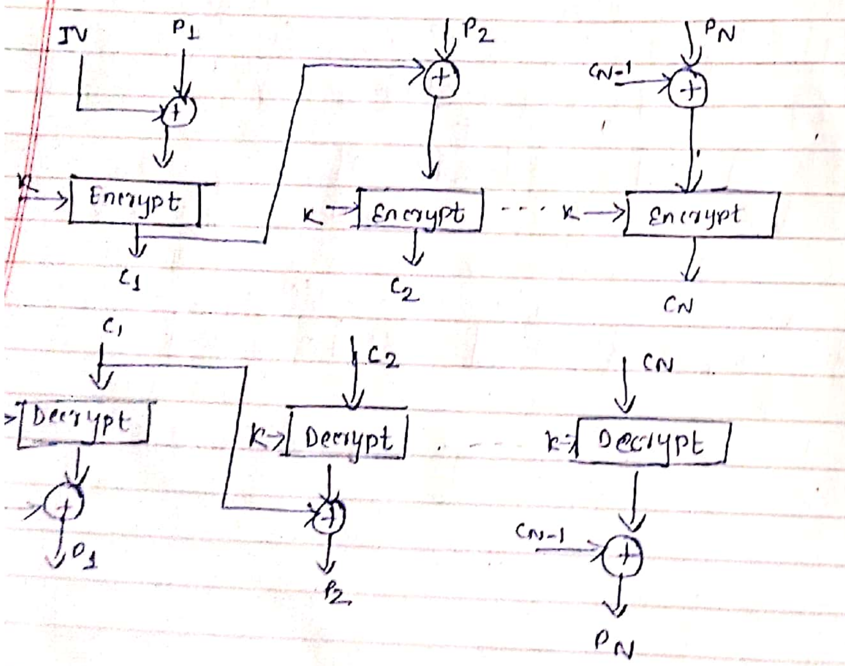
K1 – K4 (Odd)

K5 K7 (even)

अनि 17

2. Cipher Block chaining mode (CBC)

- Initialization vector (IV) (64 bit को fix message) लाई first block संग XOR, अनि encrypt, अनि आको cipher text, second block (plaintext) संग XOR गर्ने, C_2 अनि C_3 (सम्म)
- More secure than ECB mode.
- Decrypt गर्दा नि सुरुमा I.V. जोड्ने, cipher text मा, अनि plain text आउछ। (decrypt भाको cipher text)
- P_1, P_2 नि C_2 लाई decrypt गरेर आएको मा C_1 लाई XOR गरेपछि आउछ।



- Decryption मा नि Encryption मात्र हुन्छ। (Block cipher into stream cipher)

Cipher feedback mode (encryption, decryption identical)

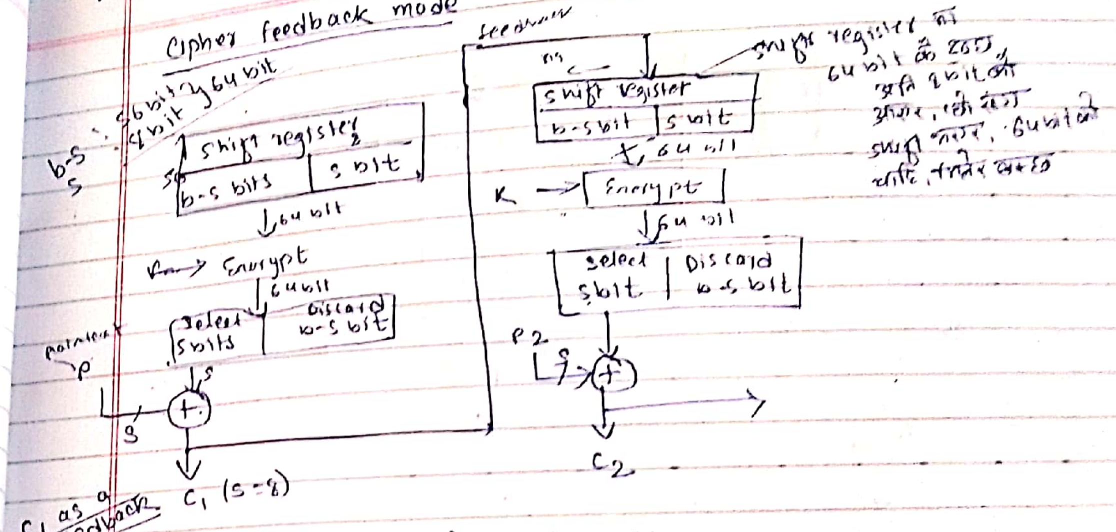


fig: Encryption

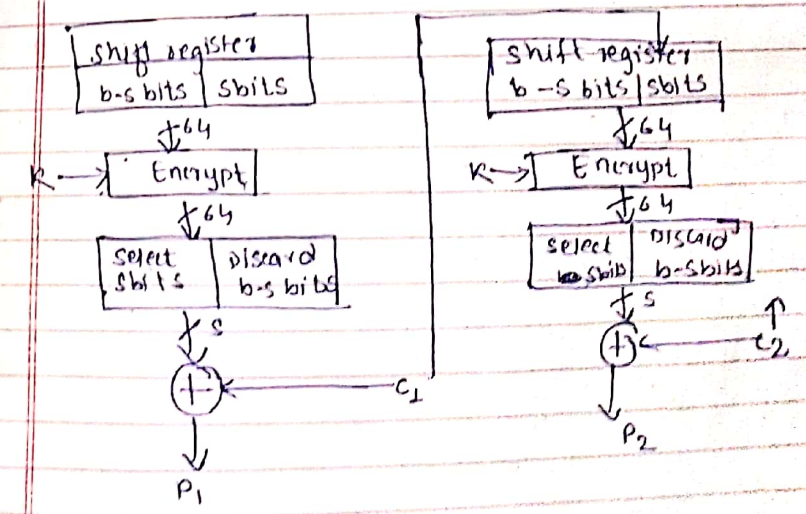


fig: Decryption

output feedback mode

digram: schai feedback જેવી જ છે।

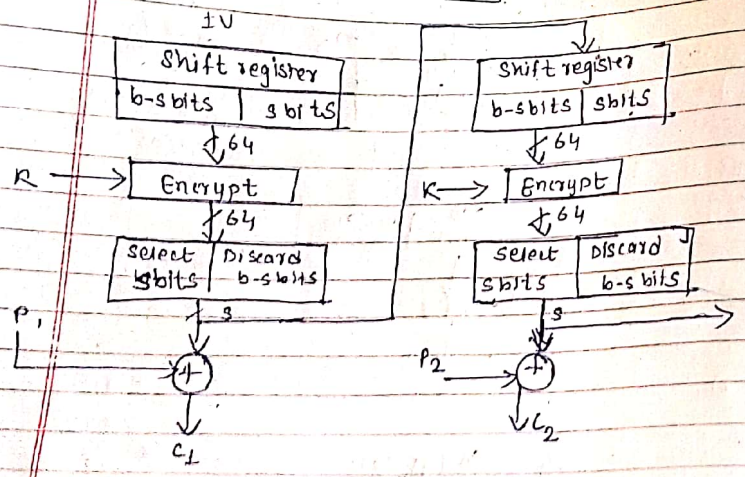
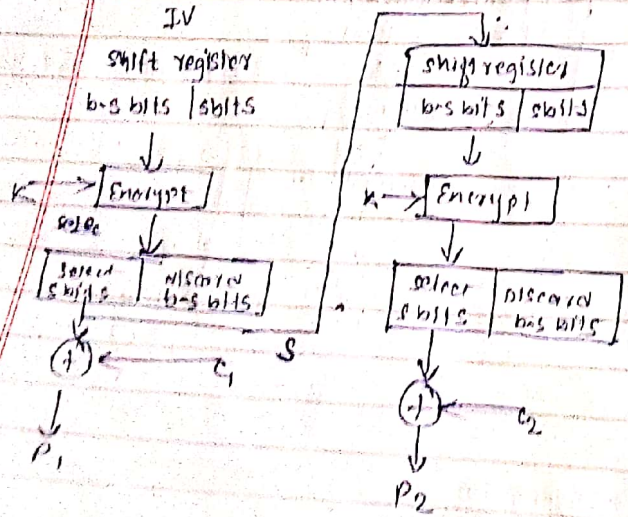


fig: Encryption



ધ્યાનમાં રાખો કે decryption પણ encrypt જ થાય છે।

Counter mode

counter variable હોય છે

w bit block

w bit counter

counter વાળી sender ને receiver side બંનેમાં એકસમાન રાખવામાં આવે છે।

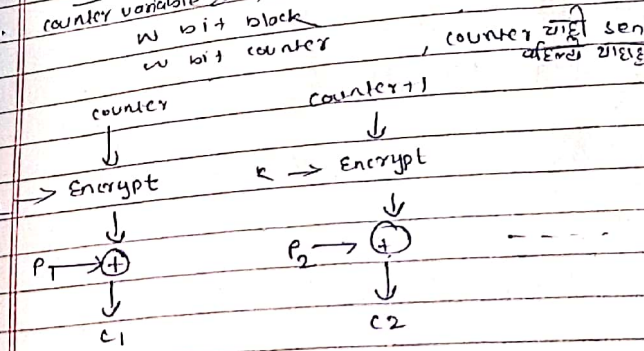


fig: Encryption

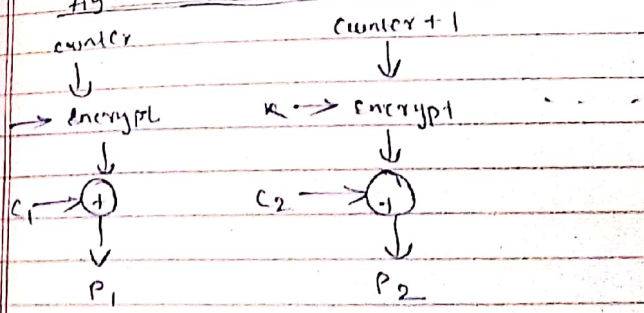


fig: Decryption

Chapter - 4

Public key cryptography

prime numbers sanga related हुन्छ।

- यसमाथि chai group हुन्छ, अनि group मा basically addition

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

- set of integers under addition is a group

Group हुनको लागि 4 वटा condn satisfy हुनपर्छ:-

closure:

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

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

Associative

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

Identity element:

element in G such that,

$a + e = e + a = a$

$0 = 0 + 2 = 2$

Element

2nd देखि of Ring, field, group?

Finite group

set of integer (Z) is infinite group. [set मा infinite element]

Z_8 is finite group. [8 ओटा elements]

Abelian group:

- commutative हुनपर्छ

Ring

Two operations:- Rational number → $\frac{p}{q}$
Real number →
Complex number → Real र imaginary हुन्छ नि।

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
M_0. Commutative
M_1. closure under multiplication
M_2. Associative of multiplication
M_3. Distributive : $a(b+c) = ab + ac$ for all a, b, c in R

Integral domain

additional two property: (M) Multiplicative identity: $a.1 = 1.a = a$

No zero divisor. यदि $ab = 0$, then either $a = 0, b = 0$.

Fields

A1 - A5

M1 - M5

Multiplicative inverse

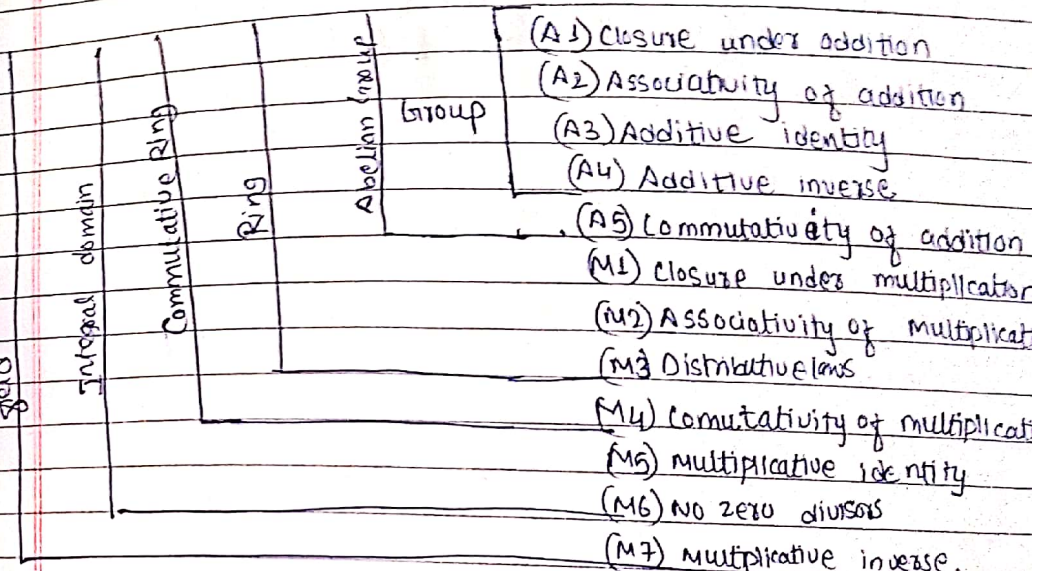
$a a^{-1} = a^{-1} a = 1$

Ex.

5. $\frac{1}{5} = 1$

$\frac{1}{5} \notin \mathbb{Z}$, so, set of integers under multiplication is not field.

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



(A1) Closure under addition
(A2) Associativity of addition
(A3) Additive identity
(A4) Additive inverse.
(A5) Commutativity of addition
(M1) Closure under multiplicatior
(M2) Associativity of Multiplicat
(M3) Distributive laws
(M4) Comutativity of multiplicat
(M5) multiplicative identity
(M6) No zero divisors
(M7) multiplicative inverse.

9 Modular Arithmetic

$a = qn + r$

q = quotient
r = remainder

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:

$21 \equiv 1 \bmod 4$

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

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

$7^{11} \bmod 4$

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

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

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

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

$8+2+1 = 11$

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

$5^{12} \bmod 3$

$5 \bmod 3$

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

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

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

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

$8+4 = 12$

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

Modular airthmetic

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Z_n = set of integers less than n.

Airthmetic modulo 8.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(12) mod 8

(1+7) mod 8 = 0

×	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

14 mod 8

21 mod 8

49 mod 8

relative prime हुने को मात्र multiplicative inverse exist गर्छ।

Additive and multiplicative inverse modulo 8.

(7+1) mod 8 = 0 (remainder)

w	(Additive inverse) $-w$	(Multiplicative inverse) w^{-1}
0	0	–
1	7	1
2	6	–
3	5	3
4	4	–
5	3	5
6	2	–
7	1	7

cond^n: $I \times I^{-1} \equiv 1 \bmod m$

$\frac{1 \times 1 - 1}{8}$ = remainder 0

since, relative prime doesn't satisfy,

gcd(2, 8) = 2 ≠ 1

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

∴ Multiplicative inverse of 3 is 3.

Prove that Z_8 is commutative ring:

हरेक को last मा mod8 गर्नु पर्छ result मा।

पहिला property list out गर्ने commutative ring को लागी, अनि satisfy गरेर देखाउने।

Associativity:

1 + (2+3) mod 8 = 1 + 5 mod 8

= 1 + 5

= 6

(1+2) + 3 mod 8 = 3 + 3 mod 8

= 3 + 3