classfellow

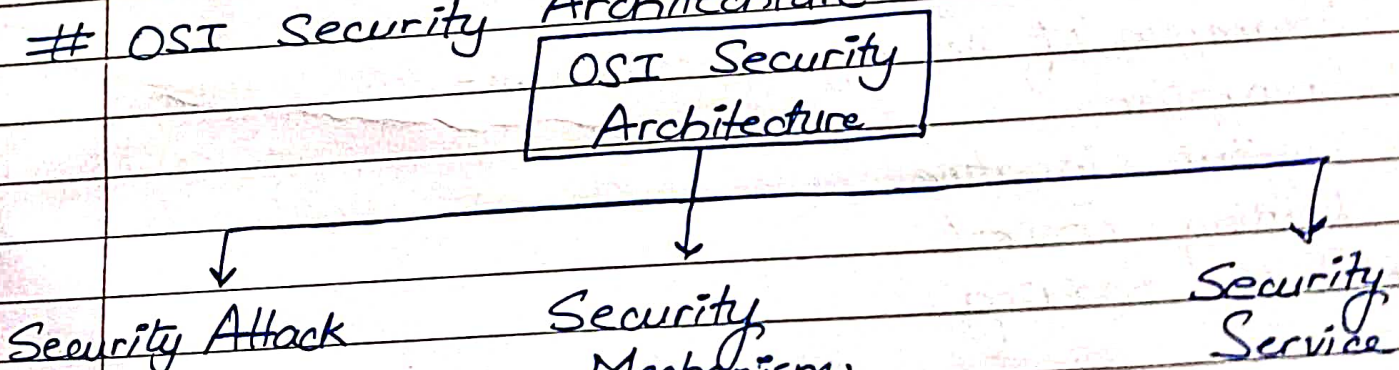
ISC

=> Computer Security → Collection of tools designed to protect data and to prevent from hackers.

=> CIA Triad
CIA triad is a well-known model that represents the three main goals or objectives of information security.

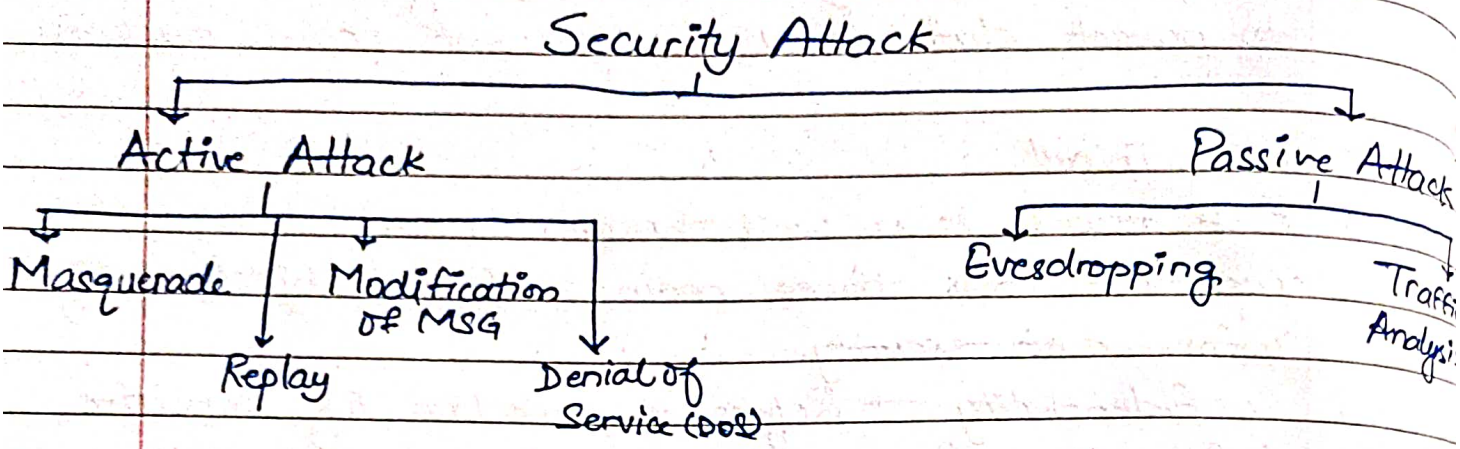
1. Confidentiality → Refers to protection of sensitive information from unauthorised access or disclosure.
2. Integrity → Refers to assurance that data is accurate and has not been altered with an unauthorised manner.
3. Availability → Refers to assurance that data and information systems are available to authorised user when needed.

OSI Security Architechture



Security Attack
A security attack is an attempt by a person or entity to gain unauthorised access to disrupt or compromise the security of a system, network or device.
There are two types of security attacks:
1. Passive Attack

2. Active Attack



Security Mechanism

Mechanism built to identify any breach of security or attack on the organisation is called a security mechanism.

They are responsible for protecting a system, network or device against unauthorised access or security threats.

Examples of security mechanism:-

1. Encryption
2. Digital signature
3. Routing control
4. Traffic Padding.

Security Services

Refers to different services available for maintaining the security and safety on an organisation. They help in preventing any potential risks to security.

Types of security service:-

1. Authentication
2. Access Control...

classfollow

3. Data Confidentiality
4. Data integrity
5. Non-repudiation

Benefits of OSI Architecture
* Providing security
* Organise tasks
* Meets international standards

=> Security Attacks

1. Passive Attack → Refers to types of attacks in which a third-party intruder tries to access/manage to steal the message/data shared b/w the sender and receiver by keeping a close watch on the transmission. Here the sender/receiver don't have the clue that the message/data is accessible to third party intruder.
Message/data remains in its usual form
One way to prevent passive attack is to encrypt the data shared.

Two types of passive attacks:-

1. Eavesdropping → In this the attacker listens to the conversions b/w two or more parties without their consent. For example, man in the middle attack.

2. Traffic Analysis → This involves attacker analysing network traffic pattern and metadata to gather information about

the network or device. Here ~~[illegible]~~ the attacker can't read message but identify the pattern and length of a encryption.

2. Active Attacks → Refers to attacks in which attacker actively disrupt the network. These attacks are focused on damaging rather than stealing the data.
Here, both sender and receiver dont have clue that data is modified.
Message & shared doesnot remain in its usual form.
Types of Active Attack:-
1. Masquerade → In this attacker pretends to be the original sender in order to gain access.

2. Replay → Attacker intercepts the transmitted msg through a passive channel and delays it at a later time.

3. Modification of Message → Original msg is modified and transmitted in order to look alike the original text.

4. DOS → Attacker Sends a large volume of traffic to a system so that it becomes unavailable for users.

classfellow

Date: / / 2022

Page No.

Security Mechanism

=> Encryption → Used to protect data transmitted over a network. Text is encrypted with the help of a key.

=> Digital signature → With the use of cryptography techniques, a verifiable identifier is created for the signature to check the authenticity.

=> Traffic padding → Adding network data to traffic stream to make it more difficult to analyze.

=> Routing control → Enables routing changes.

Security Services

* Authentication → Process of verifying the identity of user in order to grant access to the system.

* Access Control → Use of policies to determine who is allowed to access the system.

* Data confidentiality → for protection of data

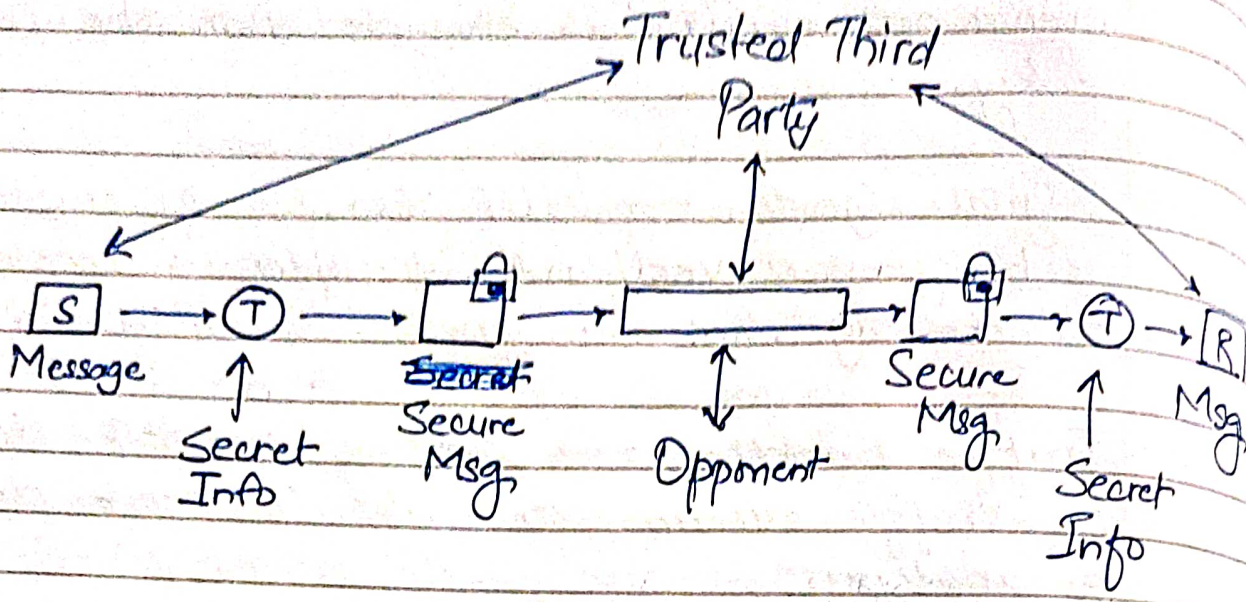
* Data integrity → to check whether data hasn't been modified.

* Non-repudiation → To create verifiable records.

Date : / / 2022

Page No.

Network Security Model



S → Sender
R → Receiver
T → Transformation

classfellow

Date: / / 2022

Page No.

Substitution Techniques

In a substitution technique, letters of plain text are replaced by other letters or numbers or symbol.

Caeser Cipher or Shift Cipher

→ Earliest known substitution cipher

→ It involves replacing of each letter of alphabet with the letter standing 3 places further, down.

$C = (p+k) \bmod 26$

$p = (c-k) \bmod 26$

Example:-

p = pay more money

C = sdb pruh prqbb

To decrypt, reverse the algorithm, move 3 steps up the alphabet.

Playfair Cipher

1. Create a 5×5 matrix
2. The matrix is made by inserting the value of key and then remaining alphabets in the matrix. Letter I and J will be together.
3) Convert the text into pair of alphabet

   Helloo → HE LL OO

   If any term is left add Z to that
4) If any letter is repeated in the pair seperate that and add X to previous letter.

   → HE LX LO OZ

ABBDEEJ → AB BD BX EX EJ

HEXXOE → HE XZ XO EZ

X was already there so we took Z.

4. Code will be formed using 3 rules:-

* If both letters are in same row, take the letter to the right
* If both letters are in same column, take the letter below
* If not in same row or column, replace them with same row but on opposite corners.

Example:-

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

Key — NAYANIKA

Plaintext — HELLO WORLD

HE LX LO WO RL DZ

Cipher text — MC MW MG WR FW

To decrypt, use rules as:-

* If both letters are in same row, & replae with left
* If both letters are in same column, replace with above.

classfellow

Date: / / 2022
Page No.

* If not in same row or column, replace with same row but on opposite corners.

Decrypted text - HE LX LO WO RL D2

=> HECLO WORLD

=> Strength of playfair
Since there are 26 letters, 26×26 = 676 diagrams are possible.
∴ Identification becomes more difficult.

Vigenere Cipher
Substitution rule changes continously from letter to letter according to key and plain text.

A matrix is made with repeating alphabets in this way:-

A	B	C	D	....	Z
B	C	D	E		A
C	D	E	F		B
:	:	:	:		:
:	:	:	:		:
:	:	:	:		:
Z	A	B	C	.....	Y

Key is written over the plain text.
Key is search in horizontal direction and PT in vertical.
Intersection of both gives Cipher Text.

Date: / / 2022

Page No.

classfellow

Strength:-

There are multiple ciphertext for plaintext letters so identification is difficult.

One Time Pad Cipher / Vernam Cipher

* Uses a random key of same length of message.
* Key is not repeated
* Sender is generating new key for every new msg while sending message to reciver so it is called one time pad.

Example:-

PT	H	O	W	A	R	E	Y	O	U
	7	14	22	0	17	4	24	14	20
Key	N	C	B	T	Z	Q	A	R	X
	13	2	1	19	25	16	0	17	23
Total	20	16	23	19	42	20	24	31	43
Sub 26 if >25	20	16	23	19	16	20	24	5	17
CT	U	Q	X	T	Q	U	Y	F	R

Advantage:-

* Unbreakable encryption for a cipher text attack.

Disadvantage:-

* Requires very long key.

Date : / / 2022
Page No.

classfellow

Transposition Techniques

1. Railfence Cipher

PT - GOOD MORNING

Depth = 2 → No. of rows to be made

G	O	M	R	I	G
O	D	O	N	N	X

Read it row wise

CT → GOMRIGODONNX

Decryption :-

Depth = 2

$PT = \frac{12}{2} = 6$

G	O	M	R	I	G
O	D	O	N	N	X

Read it column wise

PT = GOOD MORNING

2. Columnar Transposition Technique

PT - HELLO WORLD

Column 1	Column 2	Column 3	Column 4
H	E	L	L
O	W	O	R
L	D	X	X

Order → 4, 1, 3, 2

CT → LRXHOLLOXEWD

For IInd round.

1	2	3	4
L	R	X	H
O	L	L	O
X	E	W	D

Order → 4, 1, 3, 2

CT → HODLOXXLWRLE

Double encryption.

To decrypt, divide in 3-3 pairs. and write acc. to order.

1	2	3	4
L	R	X	H
O	L	L	O
X	E	W	D

Read it row-wise

CT → LRXHOLLOXEWD

1	2	3	4
H	E	L	L
O	W	O	R
L	D	X	X

PT → HELLO WORLD

classfellow

Date: / / 2022
Page No.

Row Transposition Cipher

Message is written row wise and read as columnwise. Order becomes the key.

PT = HELLO WORLD
Key = 4132

4	1	3	2
H	E	L	L
O	W	O	R
L	D		

CT = EWDLRLOHOL

Steganography

The technique of hiding secret data within an ordinary, non-secret file or message to avoid detection. The secret data is then extracted at its destination.
Most common method → Hiding info in digital images.
In jpeg files, there are pixels which leave a space for the message in which the attacker can add malware that starts to work once the image is downloaded.

Difference b/w original image and stonographic image is subtle and attackers can take advantage of this.

3 techniques used in Steganography.

1. Least Significant Bit
In this method attacker identifies the least significant bit of the information in the carrier image and replace that with malicious code which on downloading starts to work and the system gets hacked.

2. Palette Based Technique.
Digital images are used as malware carriers. Attacker encrypts the message and then add to the stretched palette of image. This can carry only limited amount of data.

3. Secure Cover Selection.
Attacker compares the blocks of image with blocks of malware. If the image has same blocks then malware is added to that and the image is identical to the original image.

classfellow

Date: / / 2022
Page No.

Group → A group G denoted by $\{G, \cdot\}$ is a set under some operations (.) if it satisfies CAIN properties.

C – Closure
A – Associative
I – Identity
N → iNverse

Abelian Group → A group is said to be Abelian if it already a group and commutative property is also satisfied, $(a.b) = (b.a)$ for all a, b in G.

Properties :-

Closure
$a, b \in G$ then $(a.b) \in G$

Associative
$a.(b.c) = (a.b).c$ for all $a, b, c \in G$

Identity
$(a.e) = (e.a) = a$ for all $a, e \in G$

Inverse
$(a.a') = (a'.a) = e$ for all $a, e \in G$

Commutative
$(a.b) = (b.a)$ for all $a, b \in G$

classfollow

Ques Is $(Z, +)$ a group?

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

Closure

$(a.b)$ for all $a, b \in G$

$a = 1, \quad b = 2$

$(a.b) = 3 \in G$

$\Rightarrow$ Satisfied

Associative

$a.(b.c) = (a.b).c$ for all $a, b, c \in G$

$a = 1, \quad b = 2, \quad c = 3$

~~$1 \times (2 \times 3)$~~ ~~$= 2$~~

$1.(2.3) = 6 = (1.2).3$

$6 \in G$

$\Rightarrow$ Satisfied

Identity

$(a.e) = (e.a) = a$ for all $a, e \in G$

$a = 5 \quad e = 0$

$(5.0) = (0.5) = 5 \in G$

$\Rightarrow$ Satisfied

Inverse

$(a.a') = (a'.a) = e$ for all $a, e \in G$

$a = 2 \quad e = 0$

$(2.-2) = (-2.2) = 0 \in G$

$\Rightarrow$ Satisfied

Group as well as Abelian Group.

Commutative

$(a.b) = (b.a) \quad a = 2 \quad b = 3$

$(2.3) = (3.2) = 5 \in G$

$\Rightarrow$ Satisfied.

classfollow

Date: / / 2022
Page No.

Rings
A ring R denoted by $\{R, +, *\}$ is a set of elements with two binary operations called addition, multiplication.

* It should be Group and Abelian Group.
* M1 – Closure under Multiplication
  $a, b \in R$ then $ab \in R$

* M2 – Associativity of Multiplication
  $a(bc) = (ab)c$ for all $a, b, c \in R$

* M3 – Distributive law
  $a(b+c) = ab + ac$
  $(a+b)c = ac + bc$
  ] for all $a, b, c \in R$

Commutative Rings
A ring is said to be commutative if it satisfies the following additional condition:-

M4 Commutativity of multiplication:
$ab = ba$ for all $a, b \in R$

Integral Domain
It is a commutative ring that follows:-

M5 * Multiplicative identity
There is an element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$.

M6 * No zero division
If $a, b \in R$ and $ab = 0$ then either $a = 0$ or $b = 0$

Field

A field F, sometimes denoted by $\{F, +, *\}$ is a set of elements with two binary operations called multiplication and addition such that for all $a, b, c \in F$ follows:-

A1 - A5 and M1 - M6

M7 Multiplicative Inverse

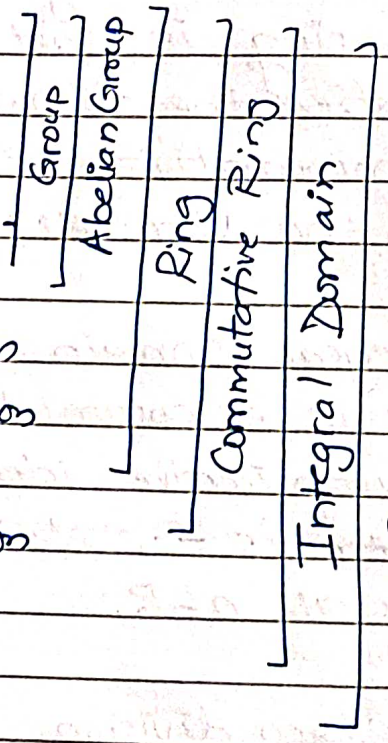
For each a in F except 0 there is an element a^{-1} in F such that

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

Examples of fields:-

* Rational Number
* Real Number
* Complex number

A1 - Closure
A2 - Associative
A3 - Identity
A4 - Inverse
A5 - Commutativity of Add
M1 - Closure under Multiplication
M2 - Associativity of Multiplication
M3 - Distributive
M4 - Commutativity of Multiplication
M5 - Multiplication Identity
M6 - No zero divisor
M7 - Multiplicative Inverse



classfollow

Finite Field

* A field with a finite set of elements that satisfies all the operations and properties.
* Finite set can be integers (mod p) where p is a prime number.

Euclid's Algorithm

Used to find GCD → greatest common divisor.

$gcd(a, b) = gcd(b, a \bmod b)$

$gcd(a, 0) = a$ Answer

Example:-

gcd(1025, 35)
⇒ gcd(35, 1025 % 35)
⇒ gcd(35, 10)
⇒ gcd(10, 35 % 10)
⇒ gcd(10, 5)
⇒ gcd(5, 10 % 5)
⇒ gcd(5, 0) = 5 Answer

gcd(11, 7)
⇒ gcd(7, 11 % 7)
⇒ gcd(7, 4)
⇒ gcd(4, 7 % 4)
⇒ gcd(4, 3)
⇒ gcd(3, 4 % 3)
⇒ gcd(3, 1)
⇒ gcd(1, 3 % 1)
⇒ gcd(1, 0) = 1 Answer

Fermat's Little Theorem

If p is a prime number and a is a positive integer not divisible by p then

$$a^{p-1} \equiv 1 \pmod{p}$$

Ques Does Fermat's Th hold true for p=5 and a=2?

Sol p=5 a=2

$a^{p-1} \equiv 1 \pmod{p}$

$2^{5-1} \equiv 1 \pmod{5}$

$2^4 \equiv 1 \pmod{5}$

$16 \equiv 1 \pmod{5}$

16%5=1 true

⇒ Fermat's theorem holds true

Ques p = 13 a=11

$a^{p-1} \equiv 1 \pmod{p}$

$11^{12} \equiv 1 \pmod{13}$

$-2^{12} \equiv 1 \pmod{13}$

$-2^{4\times3} \equiv 1 \pmod{13}$

$-2^4 \times 2^3 \equiv 1 \pmod{13}$

$3 \times -8 \equiv 1 \pmod{13}$ ~~$3^3 = 1 \pmod{13}$~~

~~$-24 \equiv 1 \pmod{13}$~~ ~~$27 = 1 \pmod{13}$~~

$-11 \equiv 1 \pmod{13}$ True

$2 \equiv 1 \pmod{13}$

~~Doesn't hold true~~

$23^3 \bmod 30$

$-7^3 \bmod 30$ [23-30]

$-7^2 \times -7 \bmod 30$

$49 \times -7 \bmod 30$

$-133 \bmod 30$

$-13 \bmod 30$

$17 \bmod 30 = 17$

classfellow

Ques $p=6 \quad a=2$

$a^{p-1} \equiv 1 \pmod{p}$

$2^5 \equiv 1 \pmod{6}$

$32 \equiv 1 \pmod{6}$

Not true

Euler's Theorem

For every positive integer 'a' & 'n' which are said to be

Euler's Totient Function

Denoted as $\Phi(n)$

$\Phi(n)$ = No. of positive integers less than 'n' that are relatively prime to n.

Ex. Find: $\Phi(5)$

Numbers less than 5 are 1, 2, 3, 4

GCD	Relatively prime
GCD(1,5)=1	〃
GCD(2,5)=1	〃
GCD(3,5)=1	〃
GCD(4,5)=1	

$\Phi(5) = 4$

Eg $\phi(11)$

No. = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

gcd(1, 11) = 1
gcd(2, 11) = 1
gcd(3, 11) = 1
gcd(4, 11) = 1
gcd(5, 11) = 1
gcd(6, 11) = 1
gcd(7, 11) = 1
gcd(8, 11) = 1
gcd(9, 11) = 1
gcd(10, 11) = 1

As all are relatively prime
$\Rightarrow \phi(11) = 10$

$\phi(8)$

gcd(1, 8) = 1
gcd(2, 8) = 2
gcd(3, 8) = 1
gcd(4, 8) = 4
gcd(5, 8) = 1
gcd(6, 8) = 2
gcd(7, 8) = 1

$\phi(8) = 4$

Date : / / 2022

Page No.

2
27
x3
81

Euler's Theorem

For every positive integer a & n which are said to be relatively prime then

$$a^{\phi(n)} \equiv 1 \bmod n$$

Ques $a=3 \quad n=10$

$a^{\phi(n)} \equiv 1 \bmod n$

$3^{\phi(n)} \equiv 1 \bmod 10$

$3^4 \equiv 1 \bmod 10$

$81 \equiv 1 \bmod 10$

True

Ques $a=2 \quad n=10$

$a^{\phi(n)} \equiv 1 \bmod n$

$2^{\phi(10)} \equiv 1 \bmod 10$

$2^4 \equiv 1 \bmod 10$

$16 \equiv 1 \bmod 10$

False Invalid congruence

Ques $a=10 \quad n=11$

$a^{\phi(n)} \equiv 1 \bmod n$

$10^{\phi(11)} \equiv 1 \bmod 11$

$10^{10} \equiv 1 \bmod 11$

$-1^{10} \equiv 1 \bmod 11$

$1 \equiv 1 \bmod 11$

True

CRT → Chinese Remainder Theorem

It is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below:

$X \equiv a_1 \pmod{m_1}$

$X \equiv a_2 \pmod{m_2}$

$\vdots$

$X \equiv a_n \pmod{m_n}$

CRT states that the above eqn have a unique solution of the moduli are relatively prime.

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}) \bmod M$$

Ques $X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$a_1 = 2 \quad m_1 = 3$

$a_2 = 3 \quad m_2 = 5$

$a_3 = 2 \quad m_3 = 7$

$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

classfollow

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_1 \times M_1^{-1} = 1 \mod m_1$

$35 \times M_1^{-1} = 1 \mod 3$

$35 \times 2 = 1 \mod 3$

$M_1^{-1} = 2$

$M_2 \times M_2^{-1} = 1 \mod m_2$

$21 \times M_2^{-1} = 1 \mod 5$

$21 \times 1 = 1 \mod 5$

$M_2^{-1} = 1$

$M_3 \times M_3^{-1} = 1 \mod m_3$

$15 \times M_3^{-1} = 1 \mod 7$

$M_3^{-1} = 1$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \mod M$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \mod 105$

$= (140 + 63 + 30) \mod 105$

$= 233 \mod 105$

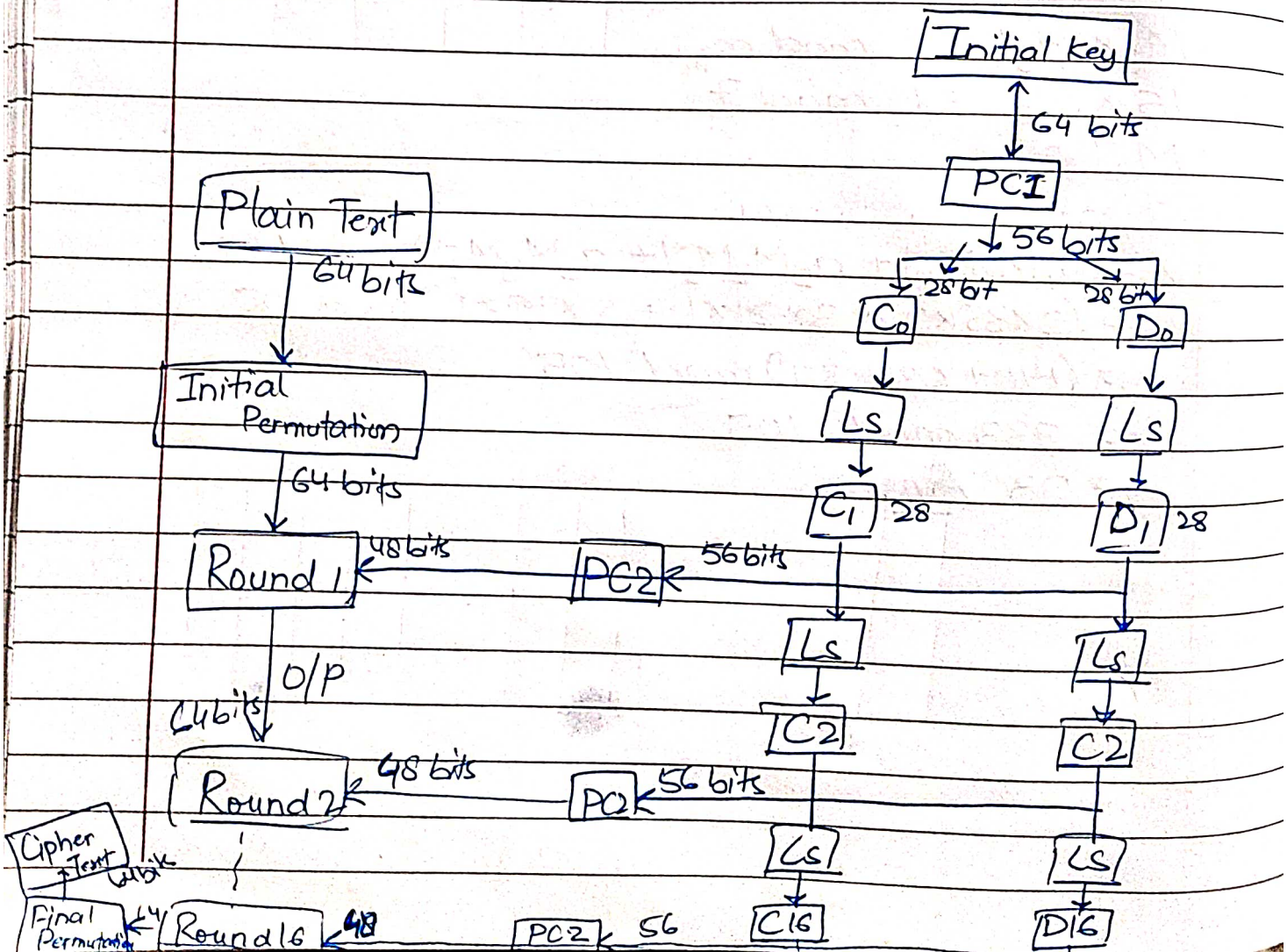
$= 23$ Ans

classfollow

DES Algorithm → Data Encryption Standard
- Block Cipher Algorithm
- Converts plain text to cipher text
- Has total of 16 rounds

Text size = 64 bits
Key size = 48 bits
- 8 bits for parity
- 8 bits for rearrangement

In each step, 4 steps:-
1. Divide bits in two parts 32 bits each
2. Bit shuffling
3. Non linear substitution
4. Exclusive OR operation



classfellow

Date : / / 2022

Page No.

In PC1,

- Initially 64 bits, 8 parity bits are to be removed from every 8th position.
  i.e. 56

- Then apply left circular shift after dividing 56 into 2 parts : C_0, D_0 each sharing 28 bits.

- D_1 and C_1 as result

Left circular shift → move bits based on round number.
⇒ shift by 1 in 1st round and 2 in 2nd round.

PC2,

- C_1 and D_1 are combined to form 56 bits again.
  Permuted choice 2 is applied.
  56 bits are rearranged, permuted and 48 bits are selected.
  Key for Round ①

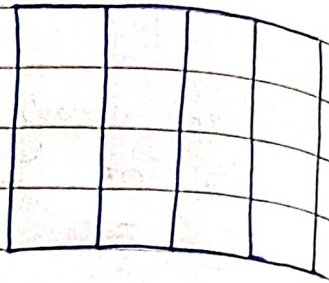
Round 1: I/P

Different key for each round
In order to make more secure, different keys are there

AES Algorithm → Advanced Encryption Standard

- Has I/P Array, State Array, Key Array

- Input Array — 4×4 matrix
  Each cell = 1 byte
  Total = 16 cells
  16×8 = 128 bits
  4 words (32 bits each)
  PT is represented in I/P Array.



- State Array — used to store intermediate states within array.

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

Total (4) words

- Key Array → 4 words are expanded into 44 words
  Each round = 4 words
  10 rounds × 4 words
  = 40 words + 4 (for add rounds)
  = 44 words

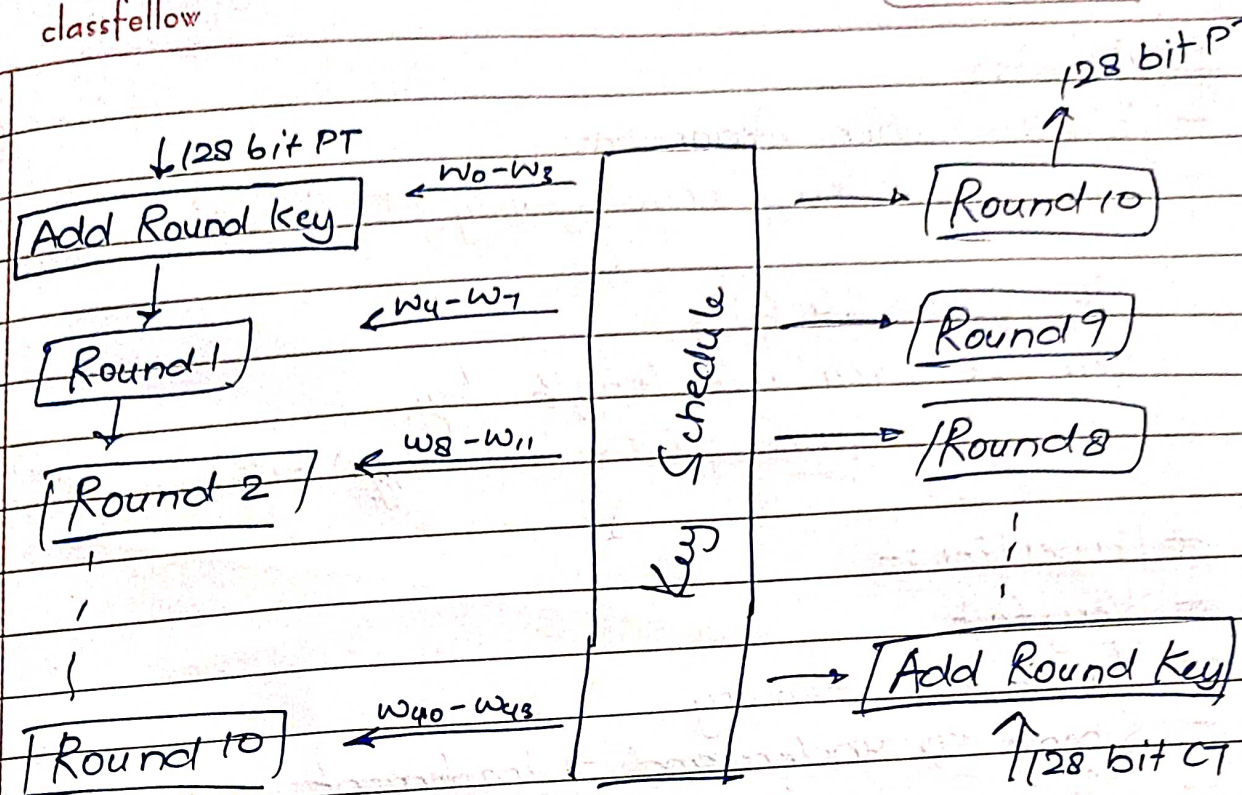
K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

→

W_0	W_1	------	W_{43}

Date: / / 2022

Page No.



Encryption

Decryption

No. of Rounds = 10

In each round, (4 steps)

1. Substitute Bytes
2. Shift rows (LCS)
3. Mix columns — Not in round (10)
4. Add round ~~key~~ key

↓

(XOR operation b/w PT and key)

Date: / / 2022
Page No.

Blowfish

- Block Cipher Algorithm
- Symmetric key cryptography → same key

I/P size = 64 bits
key size = variable length key
(from 32 to 448 bits)

* Properties :-
- Very fast
- Takes less memory
- Simple to understand + implement
- More secure (bcz of variable length key)

Blowfish Algo has (2) steps
- Key ~~Encryption~~ Generation
- Data Encryption

* Key Generation
1. Keys are stored in an array
$K_1, K_2 \dots K_n$ $[1 \le n \le 14]$
↓
length of each block = 32 bits
$32 \times 14 = 448$ bits

2. Initialise an array
$P_1, P_2 \dots P_{18}$
↓
length of each word = 32 bits

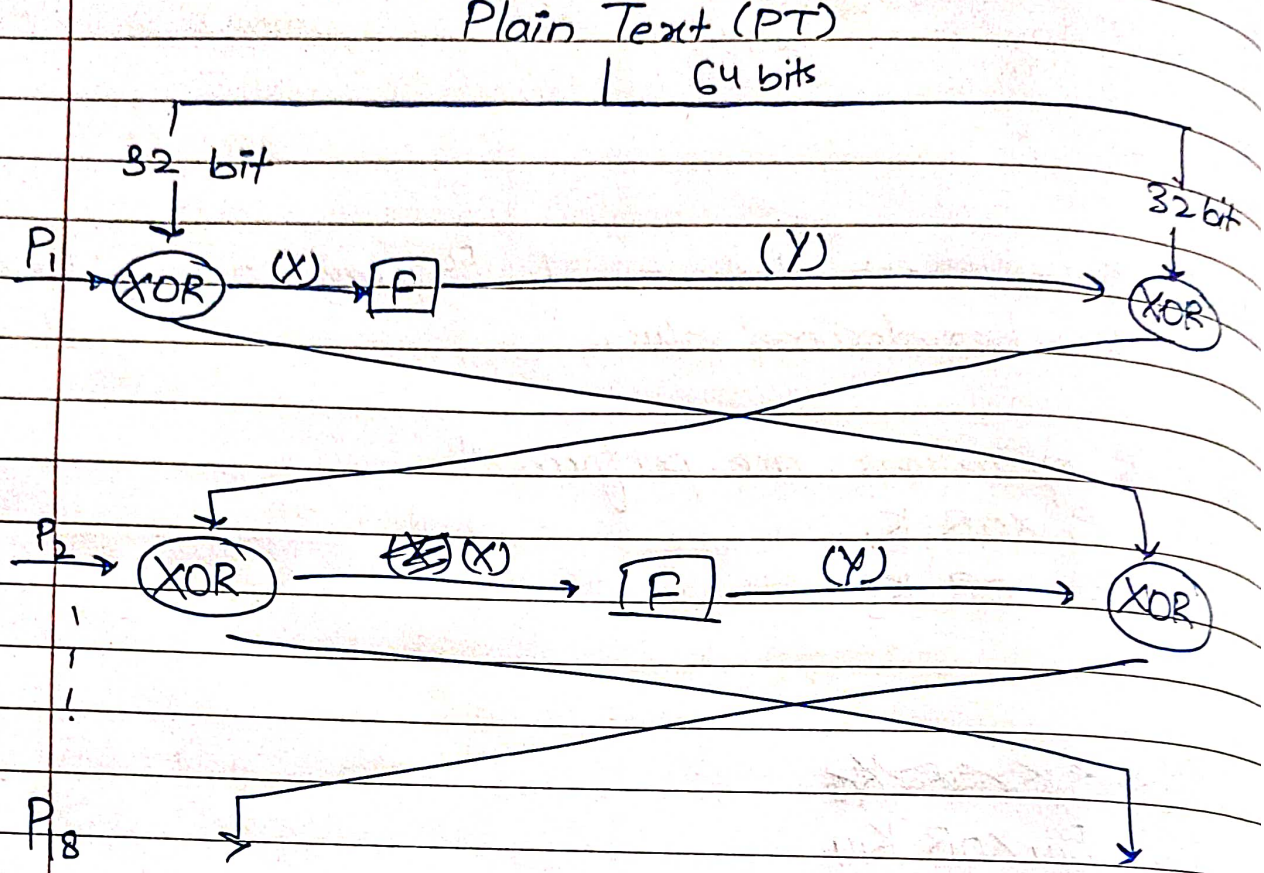
3. Initialise s-boxes (4)
$S_1 \Rightarrow S_0, S_1 \ldots S_{255}$ (Substitution boxes)
$S_2 \Rightarrow S_0, S_1 \ldots S_{255}$
$S_3 \Rightarrow$ "
$S_4 \Rightarrow$ "

4. Initialise each element of P-array and S-boxes with hexadecimal values.

5. XOR operations are performed.
$P_1 = P_1$ XOR K_1
$P_2 = P_2$ XOR K_2
⋮
~~$P_{18} = P_{18}$ XOR K_{18}~~
$P_{14} = P_{14}$ XOR K_{14}
$P_{15} = P_{15}$ XOR K_{15}
⋮
$P_{18} = P_{18}$ XOR K_4

6. Take 64 bits PT → (0,0, ..0)
Subkey is generated

Data Encryption



Upto P_{18}.

↓

CT is generated

classfellow