Always make the answer figure in Juhi mam's subject (+1 | 2)

Saathi

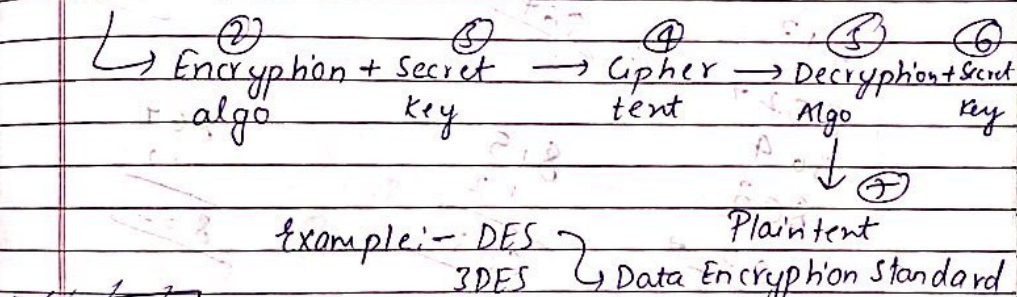
Date __/__/____

⇒ Suppose in a group of N people, everyone wants to communicate secretly with (n-1) other users using symmetric & assy. key. The communication b/w any two people should not be decodable by other users. find out number of keys required in both cases.

Symmetric (no. keys) = $\frac{n(n-1)}{2}$

Assymetric (no. keys) = $2 * n$.

* Symmetric cipher (DES, 3DES, AES)



Example:- DES → Data Encryption Standard
3DES
Advanced ← AES.
Encryption Standard.

DES → works of 56 bits → 2^{56} combination to crack DES

DES1 works at 192 bits

AES → works at 128, 192, 256 → 2^n combinat

Page No.

Date __/__/____

Suppose in a

Date __/__/____

Asymmetric :-

Plain text

↳ Encryption → Public key of receiver

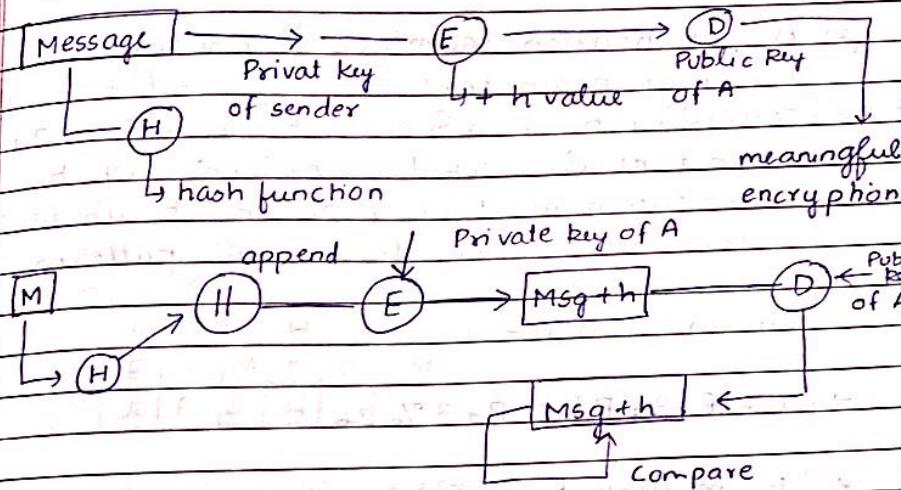
↳ Decryption → Private key of receiver

} ex. RSA algo

Saathi

Date __/__/____

Digital Signature:-



- Digital signature is used for message authentication, authencity, non-repudation but it is not used for confedentiality.
- Its asymmetric method.
- Importance of Digital signature:-

(*) authentication

Page No. ____

CS1x4Fs

Date

Root Unit-1

Saathi

Substitution technique:-

(*) A substitution technique is one in which the letter of plain text are replaced by other letters or by numbers or by symbols If the plain text is viewed as sequence of bits then substitution involves replacing plain text with pattern with cipher text with patterns

Caesar Cipher:-

→ $C = E(3, P) = P + 3 \% 26$

(*) Mono Alphabetic Substitution, Poly Alphabetic Substitution

Transposition Technique

Five UNIVESITIES = Plain Text

1	2	3	4	5
F	I	V	E	U
N	I	V	E	R
S	I	T	I	E
S				

Key: 43512

4 3 5 1 2

(EEI)(VVT)(URE)(FNSS)(III)

SQL

Date __/__/____

Saathi

Plain text:-

→ 'Kill Corona virus at twelve in tomorrow'

Matrix size → 7 x 5 (col) (row) Key → 4312567.

1	2	3	4	5	6	7
K	I	L	L	C	O	R
O	N	A	V	I	R	U
S	A	T	T	W	E	L
V	E	A	M	T	O	M
O	R	R	O	W		

(LVTNO) (LATAR) (KOSVO) (INAER) (CIWTW) (OREO) (RULM)

4 3 5 2 6 7

Stream Cipher

Plain text → 10110110

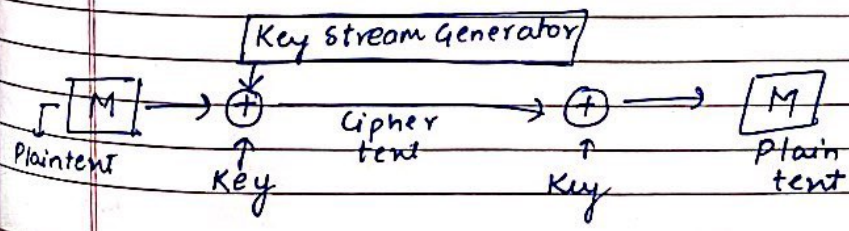
Key → ⊕ 01010101

Encrypted → 11100011 } Cipher = Plain text XOR Key

11100011 Cipher

⊕ 01010101 Key

Decrypted → 10110110 → Plain text



Page No.

Date __/__/____

Saathi

Row column ciphering:-

Msg → $M_1\ M_2\ M_3\ M_4 \ldots\ M_n$

Key → ⊕ $K_1\ K_2\ K_3\ K_4 \ldots\ K_n$

Cipher $C_1\ C_2\ C_3\ C_4 \ldots\ C_n$

Key ⊕ $K_1\ K_2\ K_3\ K_4 \ldots\ K_n$

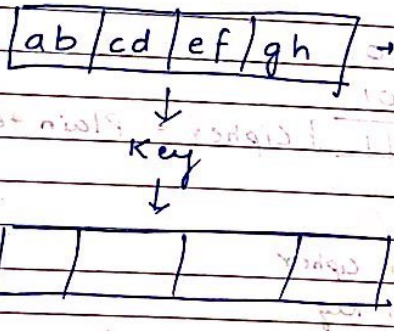
$M_1\ M_2\ M_3\ M_4 \ldots\ M_n$

→ Block cipher:- Plain text is divided into num of blocks.

(*) Block size: 40 bits, 56 bits, 64 bits, 128 bits, 256 bits

Plain text block size = Cipher Text Block size

example:- DES algo



Saathi

Date __/__/____

7 Block cipher vs stream ciphr

(*) complexity of block cipher is simple	(*) complexity of stream cipher is more.
(*) block cipher converts the plain text into cipher text by taking plain text block at a time	(*) stream cipher converts the plain text into cipher text by taking 1 bit of plain text at a time
(*) uses either 64 bits or more than 64 bits	(*) uses 8 bits.
(*) algorithm modes which are used in block cipher are ECB, CBC	(*) algorith modes which are used in stream cipher are CFB (Cipher Feedback), OFE Output Feedback)
(*) block cipher works on transposition techniques like railfence technique, row column transposition technique	(*) while stream cipher works on substitution technique like Caesar Cipher / Polygram Substh Cipher
(*) slow speed	(*) comparitively high speed

Page No.

Name: Ansh Gupta
SAP: 500075765
Roll: R177219035
Date ___/___/___

(Assignment - 1)

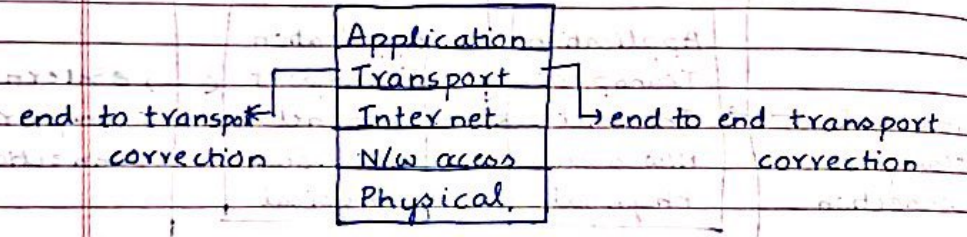
Saathi

A1. (a) Packet filtering firewall:- applies a set of rules to each incoming and outgoing ip packet and then forward/discard the packet. Rules of filtering are as follows:

(*) source and destination ip address
(*) source and destination transport layer address
(*) IP protocol field
(*) Interface

Two default policies are also there to take default action to determine whether to forward/discard the packet. → Default = discard
→ Default = forward

Some possible attacks on firewall:-
(*) IP address spoofing
(*) Source routing attack
(*) Tiny fragment attacks



(b) Application proxy firewall:- An application level gateway also called an application proxy acts as a rely of application-level traffic.

(*) user request ~~requies~~ service as proxy
(*) proxy validates request as legal

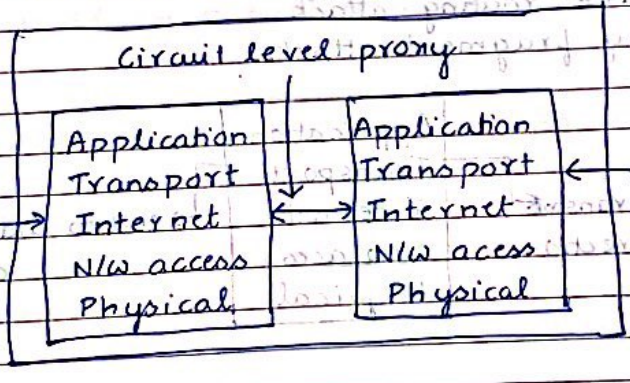
Page No.

Date __/__/____

(x) then action request and returns results to user
(x) can log/audit traffic at application level.

(c) Stateful Inspection Firewall:- It tightens up the rule for TCP traffic by creating a directory of outbond TCP connection. There is an entry for each currently establish connection. The packet is filter and now allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in this directory. It receives same packet information as a packet filtering firewall but also record information about TCP connection.

(d) Cirait level firewall



(x) this can be a stand alone system or it can be a specialized function perform by an application level gateway for certain application.

(x) does not permit end to end TCP connection, rather the gateway acts as two TCP connection

Page No.

Date __/__/____

Saathi

a typical use of circuit level gateway is a situation in which the system administrator trust the internal users

A2. Different type of security attacks in computer system :-

Cyber attacks are classified in two types :-

(a) Web based attack

→ Injection attack :- in this some data will be injected into a web application to manipulate the application and fetch the required info

→ DNS Spoofing :- is a type of computer security hacking where by data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address diverting traffic to attacker's computer

→ Session hijacking :- is a security attack on a user session over a protected network. In this hacker stoles cookies

(b) System based attack

→ Virus :- a type of malicious software program that spread throughout the computer files without the knowledge of the user. Its a self replicating program.

Page No.

Date __/__/____

Saathi

- Worm:- a type of malware whose primary function is to do replicate itself to spread to uninfected computer. It work same as computer virus

- Security Attack:- Any action that comprises the security of information owned by an organization.

- Security mechanism:- A mechanism designed to detect, prevent, recover form a security attack.

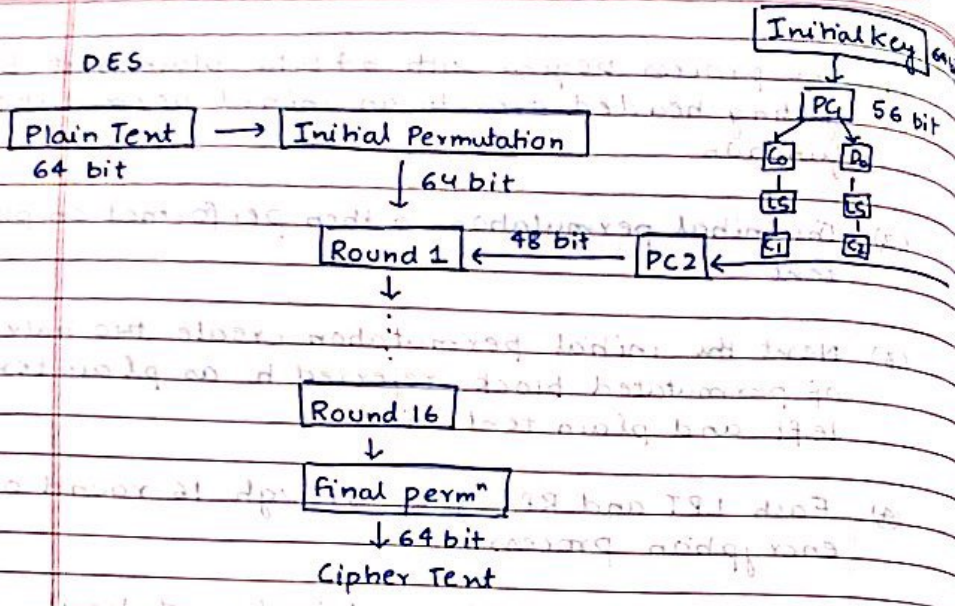
- Security service:- A service that enchances security of data processing system and the information transfer of an organization. The service are intended to counter security attack and they make use of one or more security mechanism to provide service.

A3. Public key cryptography:- an encryption method that need a paired public and private key algorithm for secure data communication. It is also called asymmetric cryptography. It is a form where pair of keys are used by the user.

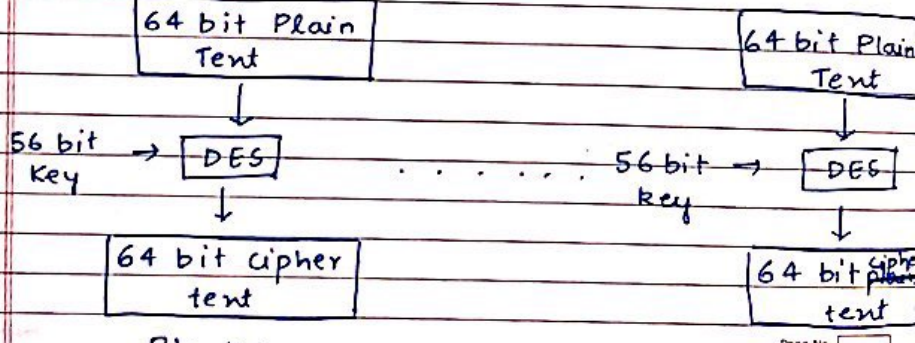
Role of session key → An encrypion and decryption key that is randomly generated to ensure the security of communication session between users and another computer. Also called symmetric keys because the same key is used for encryption and decryption.

Page No.

Date ___/___/___



Ans. DES stands for Data Encryption Standard is a block cipher and encrypts data in blocks of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of cipher text. The same algorithm is used for encryption and decryption with a key. The key length is 56 bits. The basic idea of DES:-



Page No.

Date __/__/____

Saathi

(1) The process begins with 64 bits plain text blocks getting headed over to an initial permutation function.

(2) The initial permutation is then performed on plain text.

(3) Next the initial permutation create two halves of permutated block referred to as plain text left and plain text right.

(4) Each LPT and RPT goes through 16 round of encryption process.

(5) Finally LPT and RPT are joined and final permutation is performed on newly combined block.

(6) The result of this process produces desire 64 bit cipher text.

Page No.