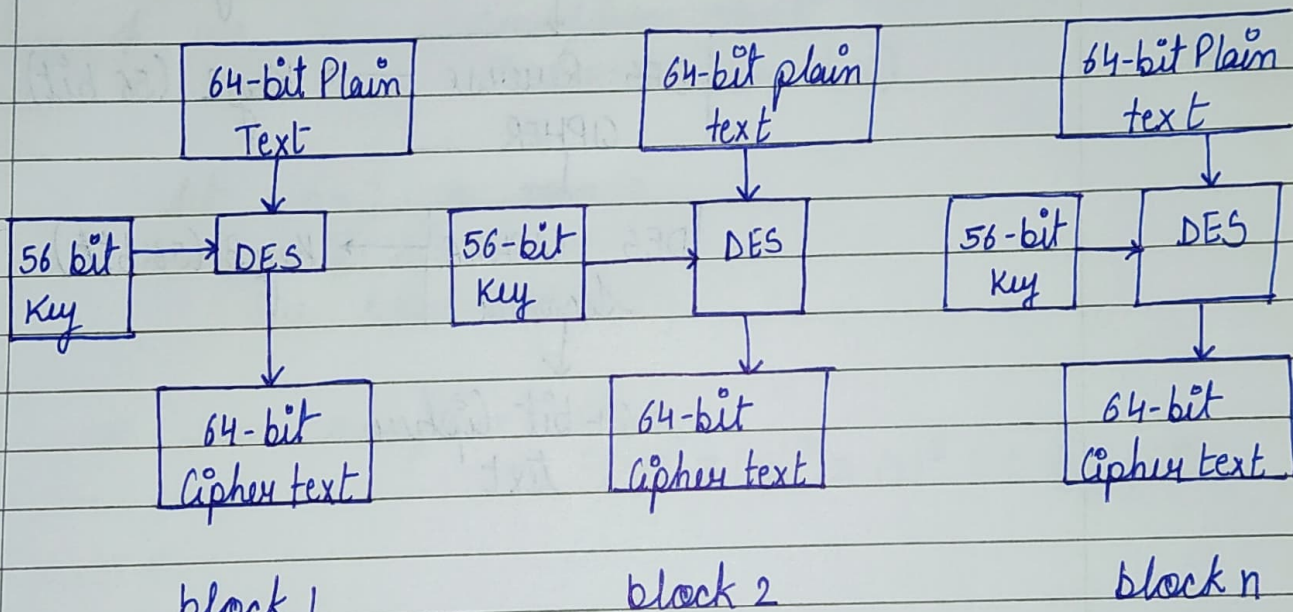
Date

ASSIGNMENT-1

① Explain DES.

Data encryption standard is a block cipher & encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm & key are used for encryption & decryption with minor differences. The key length is 56 bits.

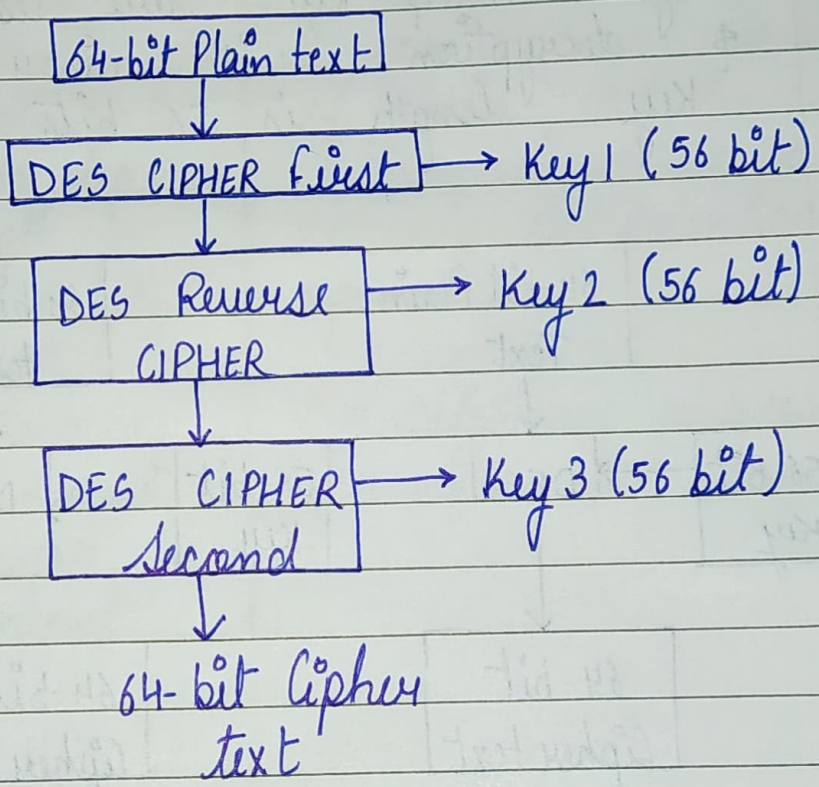


#

Date

(2) Explain Triple DES

Triple DES is an encryption technique which uses three instance of DES on same plain text. It uses there three different types of key choosing technique in first all used keys are different & in second two keys are same & one is different & in third all keys are same.



Date

③ Explain Euler's Theorem.

For 2 positive integers n & m which are relatively prime we have that

$$m^{\phi(n)} \equiv 1 \pmod{n}$$

where,

$\phi(n)$ is the Euler ϕ-function

Example –

let $n=10$, we saw earlier than $\phi(10) = 4$. Consider $m = 3$

we have that

$$\gcd(3, 10) = 1$$

& we can confirm that

$$3^4 \equiv 81 \equiv 1 \pmod{10}$$

let $n = 7$ & $m = 2$

then, $\phi(7) = 7 - 1 = 6$

we have $\gcd(2, 7) = 1$

we can confirm that,

$$2^6 \equiv (2^3)^2 \equiv (8)^2 \equiv (1)^2 \equiv 1 \pmod{7}$$

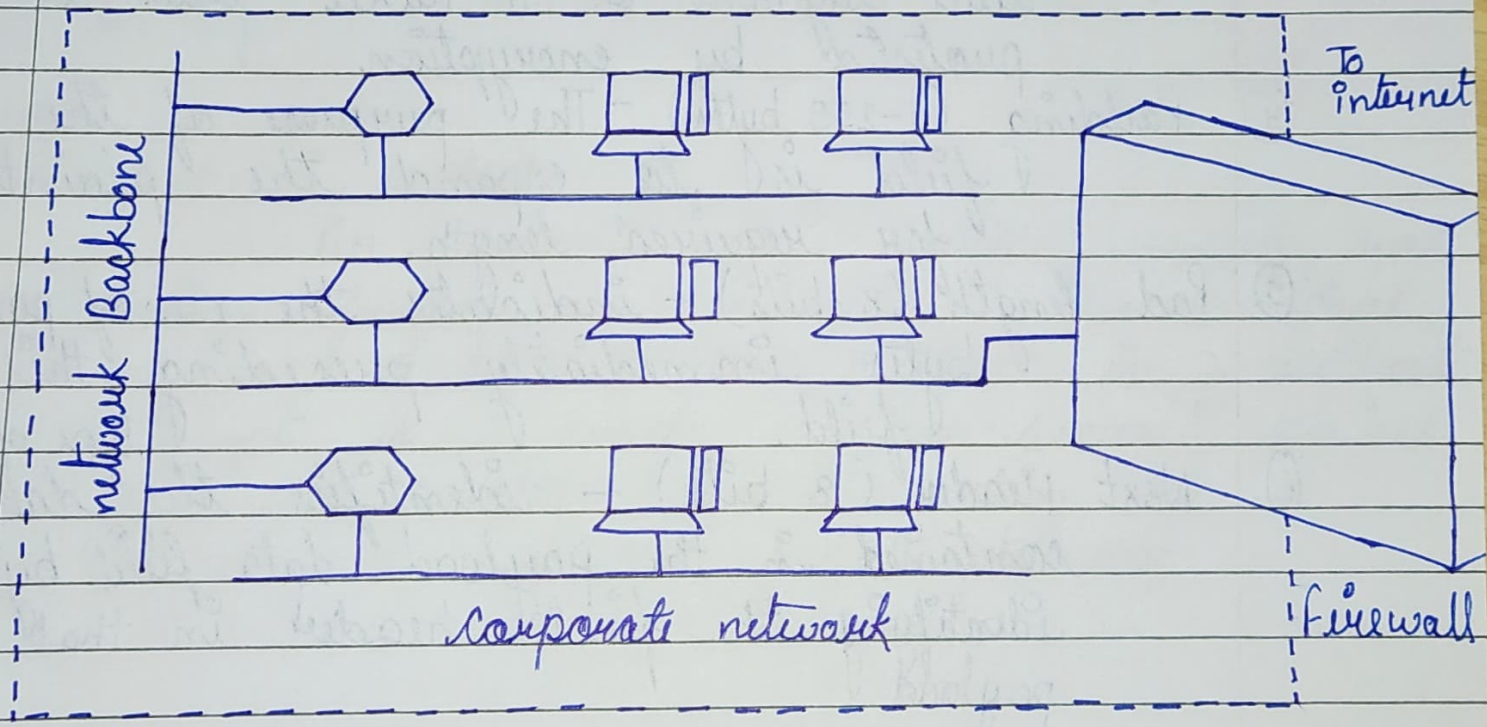
Date

ASSIGNMENT - 4

① What do you mean by firewall.

A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering & leaving the network & provides protection from various kinds of IP spoofing & routing attacks.

A firewall works just like sentry. The implementation of the firewall guards a corporate network by standing b/w the network & the outside world. All traffic b/w the network & the internet must pass through the firewall It depends on the firewall that the traffic should be allowed to flow or not.



#

Date

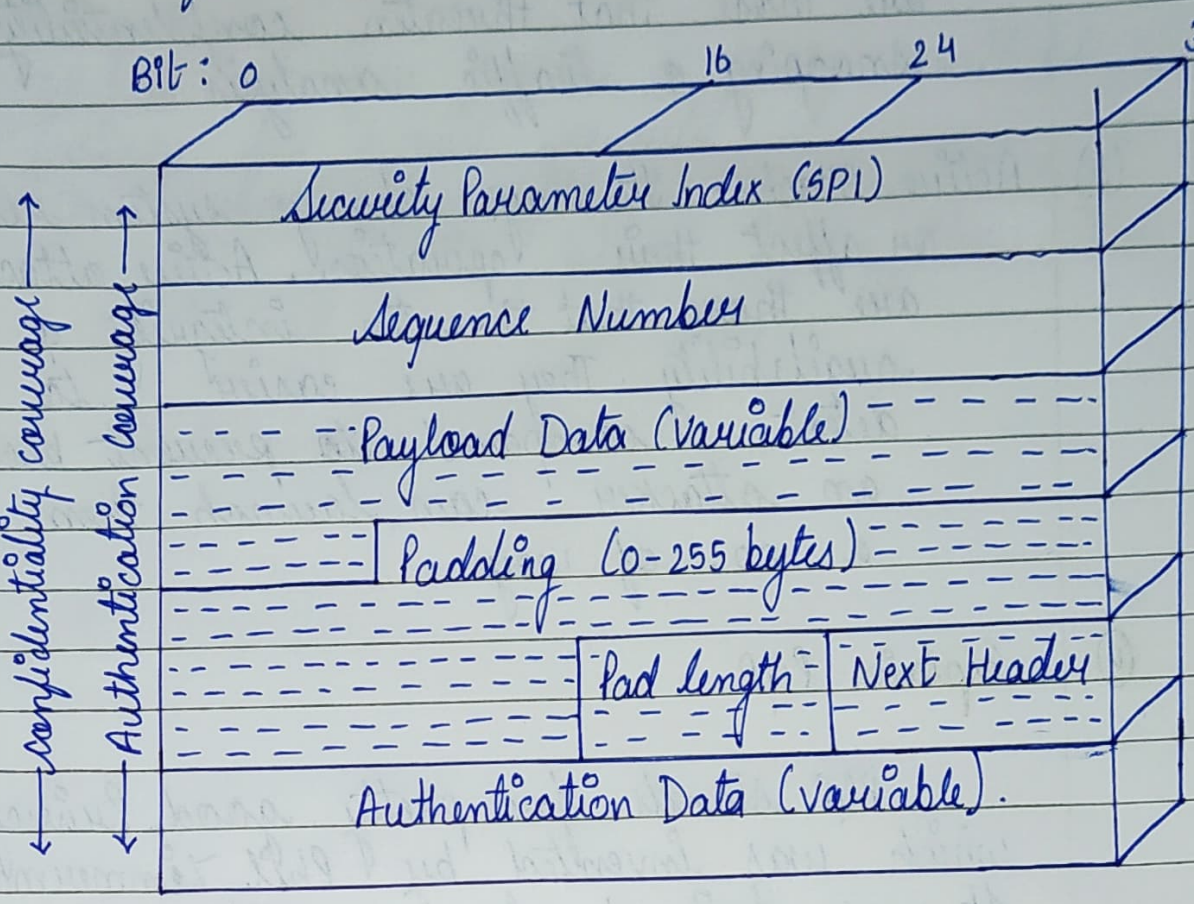
② write short note on ESP

The encapsulating security Payload Protocol provides confidentiality services, as well as confidentiality of message contents & limited traffic flow confidentiality. As an optional feature, ESP can also provide the same authentication service as AH
ESP packet contains the following fields -

① Security parameters Index (32 bits) - identifies a security association
② Sequence number (32 bits) - a monotonically increasing counter value. This provides an anti-replay function, as discussed for AH.
③ Payload Data (variable) - This is the transport level segment or IP Packet that is protected by encryption.
④ Padding (0-255 bytes) - The purpose of the field is to expand the plaintext for required length.
⑤ Pad length (8-bits) - indicates the no. of pad bytes immediately preceding this field.
⑥ Next Header (8 bits) - identifies the type of data contained in the payload data field by identifying the first header in that payload

Date

⑦ Authentication Data (variable) – a variable length field that contains the integrity check value computed over the ESP packet minus the authentication data field.



③ What is attack

An assault on system security that derives from an intelligent threat; that is an intelligent act that is a deliberate attempt to evade system security services & violate the security policy of a system. The two types of attempts are —

#

Date

(a) Passive Attacks - It attempts to learn or make use of info from the system but does not affects the system resources. It means that the goal of the opponent is to obtain info. Passive attacks are those that threaten confidentiality - snooping & traffic analysis

(b) Active Attacks - It may change system resources or affect their operation. Active attacks are those that threaten integrity & availability. They are easier to detect compared to prevent because an attacker can launch them in a no. of ways.

(4) Explain PGP.

PGP stands for pretty good Privacy which was invented by Phil Zimmermann It was designed to provide all aspects of security - privacy, integrity, authentication & non-repudiation in the sending of email.
It provides authentication through the use of digital signature. It uses digital signature to provide integrity, authentication & non-repudiation.

#

Date

PGP uses a combination of secret key encryption & public key encryption to provide privacy. Therefore, we can say that the digital signatures uses one hash function, one secret key & two private-public key pairs.

PGP is an open source & freely available s/w package for e-mail security.

It provides confidentiality through the use of symmetric block encryption.

Date

ASSIGNMENT-5

① What is information security.

Information security is a set of practices designed to carry private data secure from unauthorized access & alteration for the duration of storing or transmitting from one location to another.

Information security is ~~a set of~~ designed & carried out to protect the print, digital & other private, sensitive & private data from unauthorized persons. It can be used to secure data from being misused, acknowledgment, distruction, alteration & disruption.

There are various services of info security which are -

① Message confidentiality - It ~~me~~ defines that the sender & the reciever expect confidentiality. The transmitted message should make sense to only the predetermined reciever.

② Message integrity - It defines that the data should appear at the reciever accurately as they were sent.

#

Date

③ Message authentication – It is a service that furthers message integrity

④ Message non-repudiation – It defines that a sender should not be able to deny sending a message that they send

⑤ Entity Authentication – In this, the entity or user is documented previous to access to the system resources.

② Write short note on Dos attack

The common name employed for an attacker's interruption or disruption of the computing services of the victim is denial of service (DoS). A DoS attack attempts to prevent legitimate user to gain access to network resources. It can take the form of flooding a network or server with traffic so that legitimate messages cannot get through or it can bring down a server. DoS attack exhaust the computing power, memory capacity & communication bandwidth of their targets so they are rendered unavailable.

Date

At various times, the websites of high profile targets have been targetted. To prevent an alarm being raised, an advanced version of the DoS attack on a web server, for example, does not necessarily paralyze it. Instead, it slows down the web servers so that its response time to requests from the outside world is unacceptably high.

③ Describe Trojan Detection Tools.

① fport - command line tools for viewing open ports & connections

② tcpview - GUI tool for viewing open ports & connections

③ Process viewer - GUI tool for showing open processes including child processes.

④ Autoruns - lists all programs that will run on start up & where they are called from.

⑤ Hijack this - Displays a list of unusual registry entries & files on the drive.

⑥ Spybot S & D - Originally volunteer supported scanning & detection tool.

Date

(4) What is S-MIME.

A security service designed for e-mail is secure / multipurpose Internet mail Extension. It is a security enhancement to the MIME internet e-mail format standard, based on technology from RSA data security. Although both PGP & S/MIME will emerge as a industry standard for commercial & organizational use, while PGP will remain the choice for personal e-mail security for many years users. S/MIME adds some new content types to include security services to the MIME. All of these new types include the parameter "application/pkcs7-mime", in which "pkcs" defines public key cryptography specification.