Code No.: 20-CS-PC-313 | R20 | H.T.No. | | | R | 0 | | | | | |

SET-2

CMR INSTITUTE OF TECHNOLOGY: HYDERABAD
UGC AUTONOMOUS
III–B.Tech–Semester-I - Mid Term Examinations – OCT– 2023
INFORMATION AND CYBER SECURITY
(CSE, CSE (AI&ML), CSE (DS), AI&ML, AI&DS)

[Time: 90 Minutes] **[Max. Marks: 25]**

MID Key

PART-A **5 x 2M=10M**

i) Define a security threat?

Ans: A security threat is a threat that has the potential to harm computer systems and organizations.

ii) Compare Active attacks and Passive Attacks.

Ans: An active attack is when an attacker **changes** or **modifies** the system or data, while a passive attack is when an attacker **monitors** or **eavesdrops** on the system or data without altering it[2]. Active attacks are more **aggressive** and can harm the **integrity** and **availability** of the system or network, while passive attacks are more **subtle** and can harm the **confidentiality** of the system or network

iii) What are the services in cloud computing?

Ans: The services of cloud computing are:

- Infrastructure as a service (IaaS), which offers compute and storage services
- Platform as a service (PaaS), which offers a develop-and-deploy environment to build cloud apps
- Software as a service (SaaS), which delivers apps as services
- Network as a service (NaaS), which offers network connectivity and security services
- Function as a service (FaaS), which offers serverless computing capabilities

iv) What is Message authentication code?

Ans: Message Authentication Code (MAC), also referred to as a tag, is used to authenticate the origin and nature of a message. MACs use authentication cryptography to verify the legitimacy of data sent through a network or transferred from one person to another.

In other words, MAC ensures that the message is coming from the correct sender, has not been changed, and that the data transferred over a network or stored in or outside a system is legitimate and does not contain harmful code.

v) Define Firewall and list out its types.

Ans: A firewall is a system that monitors and controls network traffic based on predefined rules. Firewalls can be either software or hardware, or both, depending on their structure and functionality, Some common types of firewalls are:

- Packet filters
- Stateful inspection firewalls

- Next-generation firewalls
- Circuit-level gateways.

PART-B **3 x 5M=15M**

2) Explain the model of Network security with neat diagram?

Ans: A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

- For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message. Now, the transmission of a message from sender to receiver needs a medium i.e. **Information channel** which is an **Internet** service.

- A logical route is defined through the network (Internet), from sender to the receiver and using the **communication protocols** both the sender and the receiver established communication.

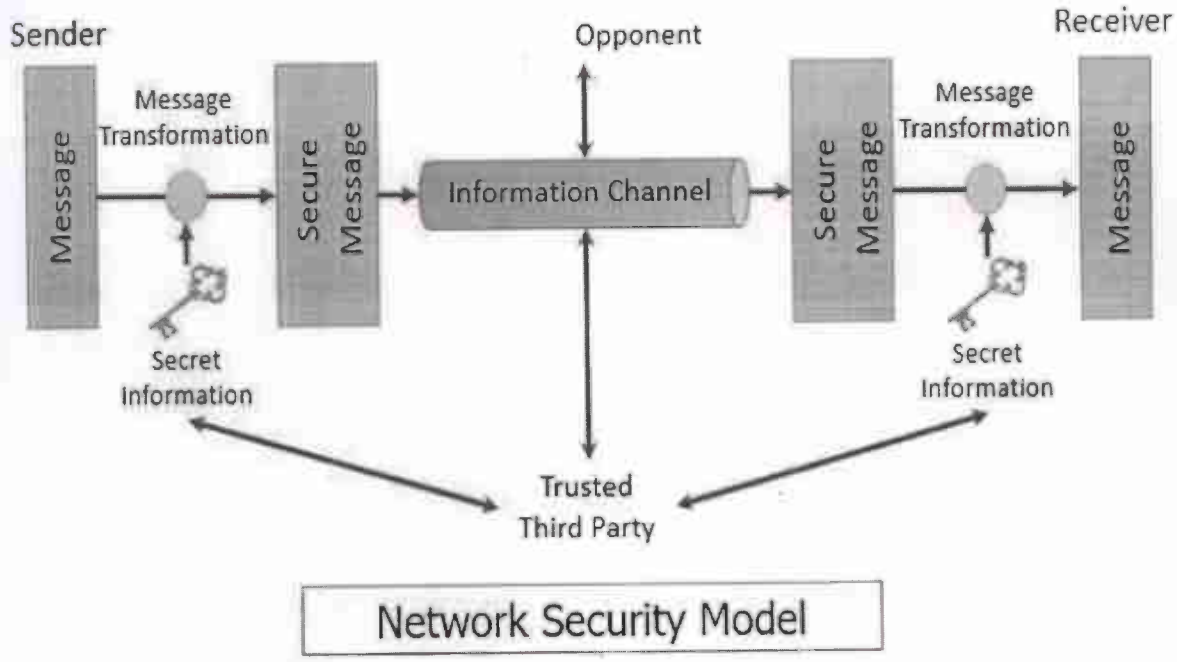
- We are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel. Any security service would have the **three components** discussed below:

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the **encryption** of the message.

It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the **secret information** between sender and receiver of which the opponent must not any clue. Yes, we are talking of the **encryption key** which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. There must be a **trusted third party** which should take the responsibility of **distributing the secret information** (key) to both the communicating parties and also prevent it from any opponent.



Network Security Model

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

In this section, we will be discussing the general '**network security model**' where we will study how messages are shared between the sender and receiver securely over the network. And we will also discuss the '**network access security model**' which is designed to secure your system from unwanted access through the network

For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message. Now, the transmission of a message from sender to receiver needs a medium i.e. **Information channel** which is an **Internet** service.

A logical route is defined through the network (Internet), from sender to the receiver and using the **communication protocols** both the sender and the receiver established communication.

Well, we are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel. Any security service would have the **three components** discussed below:

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the **encryption** of the message.

It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the **secret information** between sender and receiver of which the opponent must not any clue. Yes, we are talking of the **encryption key** which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. There must be a **trusted third party** which should take the responsibility of **distributing the secret information** (key) to both the communicating parties and also prevent it from any opponent.

Now we will study a general network security model with the help of the figure given below:
The network security model presents the two communicating parties **sender** and **receiver** who mutually agrees to exchange the information. The sender has information to share with the receiver.

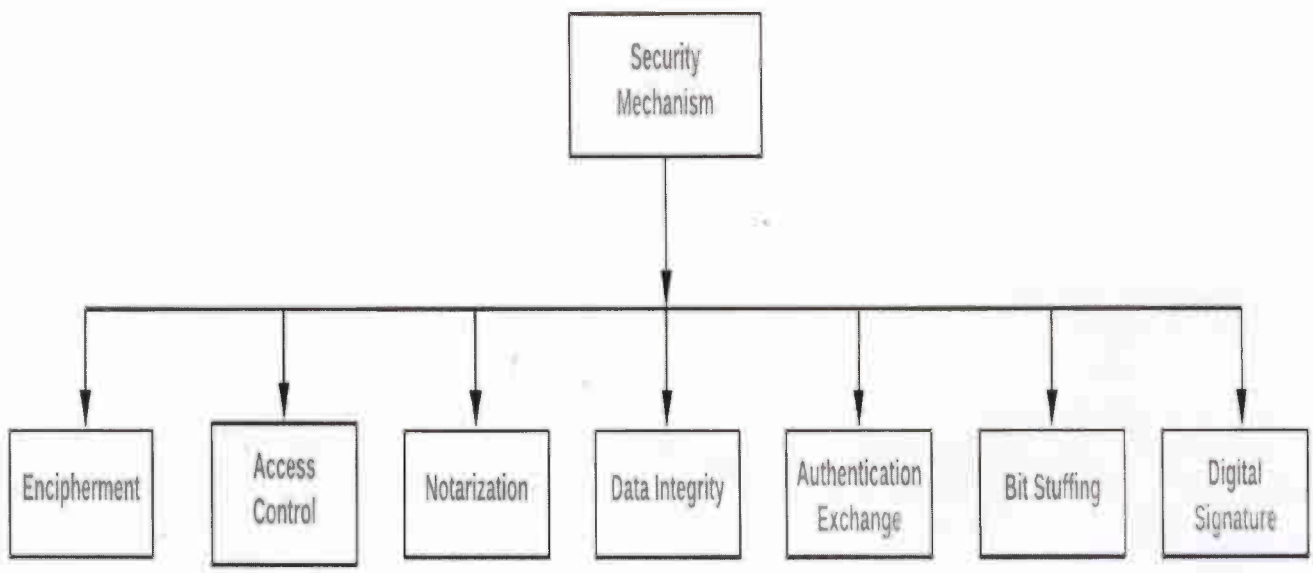
But sender cannot send the message on the information cannel in the readable form as it will have a threat of being attacked by the opponent. So, before sending the message through the information channel, it should be **transformed** into an unreadable format.

Secret information is used while transforming the message which will also be required when the message will be retransformed at the recipient side. That's why a trusted third party is required which would take the responsibility of distributing this secret information to both the parties involved in communication

(OR)

3) Discuss various security mechanisms in Information and Cyber Security?

Ans: Network Security is field in computer technology that deals with ensuring security of computer network infrastructure. As the network is very necessary for sharing of information whether it is at hardware level such as printer, scanner, or at software level. Therefore security mechanism can also be termed as is set of processes that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.



Types of Security Mechanism are :

Encipherment :
This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

Access Control :
This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

Notarization :
This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

Data Integrity :
This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.

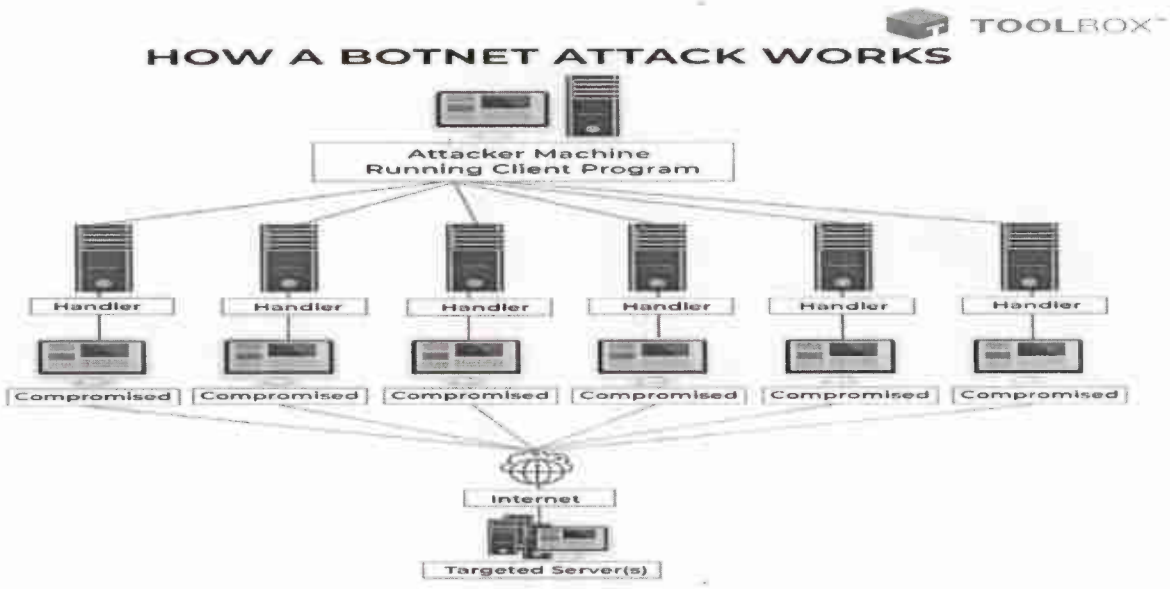
Authentication exchange :
This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not

Bit stuffing :
This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.

Digital Signature :
This security mechanism is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

4) Discuss in detail Botnets and its working in Cyber security

Ans: A botnet is defined as a cyberattack that uses multiple networked devices to run one or more bots on each device and then uses this swarm of infected devices to attack a server, company website, or other devices or individuals.'



A botnet (the abbreviated form of "robot network") is a network of malware-infected computers controlled by a single attacking party known as the bot-master. Another threat actor called the bot-herder converts the swarm's components into bots.

Typically, the bot herder will hijack a network of computer systems to create a botnet and then use it to execute various types of cyberattacks like scams, brute force attacks, malware invasions, etc. A bot-master then directs a group of hacked computers using remote commands. After compiling the bots, the herder utilizes command programming to control their other behaviors and aid the bot-master in fulfilling the ultimate ulterior motive.

How to Protect Yourself From Botnets

You require an all-inclusive strategy ranging from good surfing habits to software updates to anti-virus protection to prevent botnet infection. Listed below are some essential methods to keep botnets away.

Updating your operating system is a good malware preventative measure.

Beware of phishing emails and avoid email attachments from suspicious sources.

Refrain from clicking on suspicious links and be careful about which site you use for downloading information.

Install anti-virus, anti-spyware, and firewalls on your systems.

If you are a website owner, establish a multi-factor verification method and implement DDoS protection tools. This will safeguard your website from botnet attacks.

Following these steps will help you guard your network and devices from hackers. This sums up this tutorial on what is a botnet.

(OR)

5) Explain how cyber stalking works in real life?

Ans: Cyberstalking refers to the use of the internet and other technologies to harass or stalk another person online, and is potentially a crime

Cyberstalking does not necessarily involve direct communication, and some victims may not even realize that they are the victims of online stalking. The victims can be monitored through various methods and the information gathered can be later used for crimes such as identity theft. Some stalkers even go as far as harassing the victims offline as well and even contacting their friends.

Cyberstalking Examples

Cyberstalkers use a variety of tactics and techniques to humiliate, harass, control, and intimidate their victims. Many cyberstalkers are technologically savvy as well as creative in their ways. Here are some examples of how Cyberstalking might take place:

- Posting offensive, suggestive, or rude comments online
- Sending threatening, lewd, or offensive emails or messages to the victim
- Joining the same groups and forums as the victim
- Releasing the victim's confidential information online
- Tracking all online movements of the victim through tracking devices
- Using technology for blackmailing or threatening the victim
- Excessively tagging the victim in irrelevant posts
- Engaging with all online posts made by the victim
- Creating fake profiles on social media to follow the victim
- Posting or distributing real or fake photos of the victim
- Excessively sending explicit photos of themselves to the victim
- Making fake posts intended to shame the victim
- Repeatedly messaging the victim
- Hacking into the victim's online accounts
- Attempting to extort explicit photos of the victim
- Sending unwanted gifts or items to the victim
- Using hacking tools to get into the victim's laptop or smartphone camera and secretly record them
- Continuing harassment even after being asked to stop.

Cyberstalking Statistics

As people begin to rely more and more on technology, the incidence of cyberstalking increase. Law enforcement and government agencies continue to study the crime in order to learn how to better deter criminals from engaging in this crime of control, fear, and intimidation. The national advocacy group Survivors in Action admit that cyberstalking statistics are often difficult to come by, as a great deal of this activity goes unreported.

The majority of cyberstalking victims are between 18 and 29 years of age.

Roughly 56 percent of cyberstalkers are male

Women make up 60 percent of victims

In over 70 percent of cyberstalking cases, the victim and perpetrator live in different states

Nearly 50 percent of cyberstalkers are the victim's ex, and 15 percent are an online acquaintance of the victim

Stalker & Cyberstalking Typologies

Rejected Stalkers/Cyberstalkers: This type of stalker/cyberstalker is motivated to pursue their victim in an attempt to reverse what they perceive as a wrongful set of circumstances causing a prior divorce, separation or termination of a relationship. These offenders either feel misunderstood hoping to reverse the breakup or feel angry and seeking revenge because their attempts at reconciliation with the victim have failed in the past.

Resentful Stalkers/Cyberstalkers: This type of stalker/cyberstalker can be dangerous given their perceived motivation for stalking. Resentful stalkers/cyberstalkers are fully aware the victim is cognizant of the stalking but continues to fulfill a distorted vendetta he/she feels is warranted. Fear and distress experienced by the victim are the goals of this type of stalker/cyberstalker. For this type of profile, the stalker/cyberstalker believes the victim both deserves and requires being frightened because they have caused them and/or others anguish and distress.

Intimacy Seekers: This type of stalker/cyberstalker does not have ill will towards their victim. They simply want a loving relationship with them. Intimacy seekers view their victims as their soulmate destined to be together at all costs. Within their mind, they believe it is their job and purpose to make sure the destiny of a loving relationship is fulfilled. Intimacy seeking stalkers/cyberstalkers are often the segment of men or women who target celebrities and public figures. Blinded by their distorted perceptions of a destined love, they lose sight of the distress and fear they are causing the person they target.

Incompetent Suitors: This type of stalker/cyberstalker is deeply enamored with their victim. Their interest in the target can reach a state of fixation whereby their entire waking life is focused on the endeavor of one day becoming a couple. They tend to lack social, communication or courting skills and may feel entitled that their fantasy of a loving relationship is inevitable. Feeling entitled and/or deserving of a relationship with the victim inspires the stalker/cyberstalker to gradually increase their frequency of contact. Although like the Intimacy

Seeker stalker/cyberstalker, Incompetent Suitors are more gradual in their means and methods of contact.

Predatory Stalkers/Cyberstalkers: Of the six types, the predatory stalker/cyberstalker can be the most dangerous and determined. This type of stalker/cyberstalker is motivated by a perverted sexual need. They actively engage in planning an attack along with fantasizing about sexual acts with their victim. They do not have feelings of love for their victim, nor are they motivated by a belief in predestination. Their fuel to dominate and victimize resembles the psychopath experiencing little to no remorse for the welfare of their target.

1

Ghost Cyberstalkers: Not included in Dr. Mullen's five stalker profiles, the ghost cyberstalker is unique to the Information Age. They are online assailants who their target cannot identify. Using Cyberstealth, the ghost cyberstalker inspires fear and/or repeatedly makes direct or indirect threats of physical harm. They can represent an amalgamation of the other five types, be a predatory troll or a sadistic online user with no connection to their victim. Ghost cyberstalkers rely upon the veil of anonymity afforded to all online users.

6) What is cryptography? Discuss the private key cryptography with neat diagram.

Ans: Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

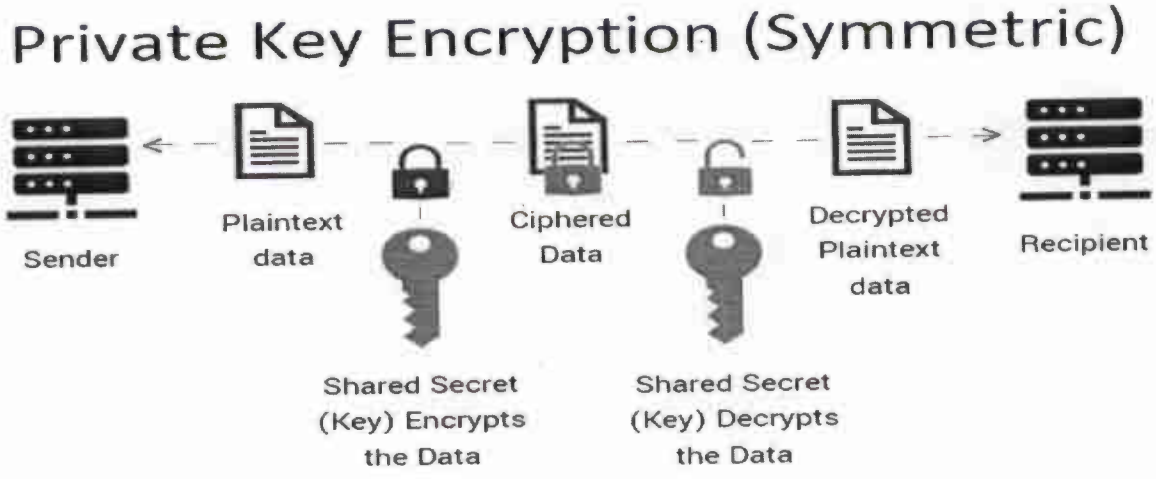
The prefix "crypt" means "hidden" and suffix "graphy" means "writing". In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it.

Private Key Cryptography

Private key encryption is the original type of encryption. Dating back to the advent of cryptography, private key cryptosystems were the first and continue to be the most common. When using private key cryptography, both parties much each possess, or at least exchange the private key. The word "key" can be a bit misleading — the key itself is really just the cipher that's used to scramble and unscramble the data being encrypted.

With an ancient cipher, like the Caesar cipher, the private key was simply a number that corresponded to the number each alphabetical character needed to be shifted. In current digital encryption schemes, the keys are now prohibitively difficult algorithms that no modern computer could ever efficiently crack.

The one thing that remains the same with all private key systems is that the same key can both encrypt and decrypt. Private key encryption is sometimes called symmetric encryption.



Components of Private Key Encryption:

Plain Text:

This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.

Cipher Text:

The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.

Encryption Algorithm:

The encryption algorithm is used to convert plain text into cipher text.

Decryption Algorithm:

It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text

Secret Key: Same key used by both sender and receiver for encrypting and decrypting the data

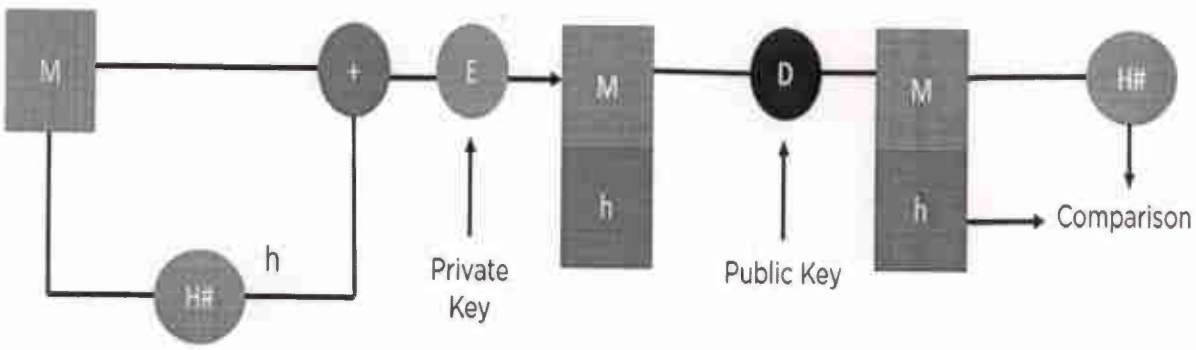
(OR)

7) Describe Digital Signature Algorithm with neat diagram.

Ans: The digital signature block diagram outlines the process of creating and verifying digital signatures. The process begins with a message being sent from one party to another. This message is then run through a **cryptographic hashing algorithm**, which produces a hash of the message. Then, the hash is encrypted using the sender's private key.

necessary to avoid tampering and digital modification or forgery during the transmission of official documents.

With one exception, they work on the public key cryptography architecture. Typically, an asymmetric key system encrypts using a public key and decrypts with a private key. For digital signatures, however, the reverse is true. The signature is encrypted using the private key and decrypted with the public key. Because the keys are linked, decoding it with the public key verifies that the proper private key was used to sign the document, thereby verifying the signature's provenance.



M – Plaintext H - Hash function h - Hash digest '+' - Bundle both plaintext and digest E – Encryption D – Decryption

The image above shows the entire process, from the signing of the key to its verification. So, go through each step to understand the procedure thoroughly.

- Step 1: M, the original message is first passed to a hash function denoted by H# to create a digest.
- Step 2: Next, it bundles the message together with the hash digest h and encrypts it using the sender's private key.
- Step 3: It sends the encrypted bundle to the receiver, who can decrypt it using the sender's public key.
- Step 4: Once it decrypts the message, it is passed through the same hash function (H#), to generate a similar digest.
- Step 5: It compares the newly generated hash with the bundled hash value received along with the message. If they match, it verifies data integrity.

There are two industry-standard ways to implement the above methodology. They are:

RSA Algorithm

DSA Algorithm

A. Nageswara Rao —

Dr. K. RubenRaju —

P. Vijaykumar —