Cyber security

1 → Intrusion Detection System
It is the process of monitoring the events occuring a Computer System or network and analyzing them For sign of possible incidents.

Intrusion Prevention System
It is software that has all the capabilities of an intrusion system and can also attempt to stop incidents.

2. Biometrics is the analysis of unique biological and physiological characteristics with the aim of confirming a person's identity.
Common types of biometric identifiers are:- Fingerprint, voice, iris, Facial, etc.

3. It is the process of extracting data as a proof for a crime while Following proper Investigation rules to nab the culprit.

Cyber Forensics is also known as computer Forensics

It can recover deleted Files, Chat logs, emails, etc.
It can also get deleted SMS, Phone calls

→ It can identify which user ran which program.

~~Needs of Cyber Forensics~~

4. → Airport security :→ Biometrics technology are used to verify passenger identity.

→ Law Enforcement
Many Agencies uses biometric to identify Criminal and Investigate them.

→ Banking Sector
Banking sector also uses biometrics in order to delievery seamless expesience to Customers.

→ Mobile phones
All new mobile phones are now integrated with biometric such as Touch ID, Facial recognition, Fingerprint, voice and irips.

Page No.
Date

Malware

5. It is a term to describe malicious software, including spyware, ransomware, viruses and worms
There are large variety of malware

1. Viruses
It is a malicious code designed to spread From device to device.

2. Trojans
It is a type of malicious code or software that looks legitimate but can take of your computer.

3. Worms :→
It is a type of malware that spread Copies of itself from computer to Computer.
It's main objective is to eat the system resources.

(6)→ Symmetric Cryptography
It is a Algorithm in which the Key For encryption and decryption are Same.
Ex- Caesar Cipher

It is of two types

Page No.
Date

Block Cipher
Encrypt data in one block at a time
used For single message

Stream Cipher
Encrypt data in one bit or byte at a time

Assymmetric Encryption
It uses a pair of keys of encryption
Public key For encryption
Private key For decryption

Message encoded using public key can only be decrypted/decoded by the private key.

~~Types~~ Two most popular algorithms are

RSA

→ In this Both public and private key are interchangeable.

→ Most popular public key algorithms.

El Gamal

less common than RSA, It used protocol like PGP [Pretty Good privacy]

7. Uses of Firewall
1. Prevents unauthorized Remote Access
2. It make online gaming safely.
3. We can block unsuitable content with Firewall

8. Difference.

DOS	DDOS
DOS stands For Denial of service.	DDOS stands for distributive Denial of service.
DOS is slower as compare to DDOS	It is faster.
They are easy to trace	They are difficult to trace
Single device is used with DOS tools	Bots are used to attack at same time

9. Advantage of cyber security
1. Data protection From unauthorised access, loss or deletion.
2. Protects system against viruses, worms, spyware.
3. Give privacy to users
4. Protects system From being hacked.
5. Minimize Computer Freezes and Crashes.

10. Authorization

It is a security mechanism to determine access levels. ~~or~~

It is the function of specifying access rights / privileges to resources.

It is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.

11) Ans The Full form of SOAP is Simple Object Access Protocol.

12) Ans A Data Breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed stolen or used by an individual unauthorized to do so.

13) What is Malware ? Explain any 3 types of Malware in detail.

Ans Malware is intrusive software that is designed to damage and distroy computers and computer system.

* Malware is a contraction for "malicious software".
* The 4 types of Malware are —
  (i) Computer Virus
  (ii) Worm
  (iii) Spyware
  (iv) Adware

(i) Computer Virus – is a piece of software that can be attached to another program or file. Virus spreads when the infected file is passed from system to system. Normally, viruses are written to do harm to your computer, like destroy system files.

(ii) Worm : Worm is very similar to virus, The design is same but, worm is capable of moving from system to system without any human action. Like viruses, worms are often

associated with causing damage to computer system.

(iii) * Spyware : Spyware may spread like virus or worms, but spyware having a special purpose to steal private information from your computer for a third party.

14) What is Cyber Security?

Ans Cyber Security is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

15) What is the Full form of SOAP?

Ans Full form of SOAP is Simple Object Access protocol.

16) What is Man in Middle Attack?

Ans A Man in Middle attack is a cyber attack where an attacker relays and possibly alters communication between two parties who believe they are communicating directly. This allow attacker to relay communication, listen in and even modify what each party is saying.

17) Explain any 3 advantages of Cyber Security —

Ans * It protect business against ransomeware, malware, social engineering and phising
* It protects end-users.
* It gives good protection for both data as well as networks.
* Increase recovery after a breach.

18) Write a short note on : Virtual Private Network.

Ans Virtual Private network is a way to extend a private network using a public network such as the internet. The name only suggests that it is a Virtual Private Network.

* User can be a part of a local network sitting at a remote location. It make use of tunneling protocols to establish a secure connection.

19.) Explain System Security in Detail.

Ans System Security is a process of ensuring the confidentiality and integrity of the OS.

* A System is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of various malicious threats and unauthorized access.
* The Security of a System can be threatened via two violations -
  - → Threat
  - → Attacks
* Security System goals :-
  (i) Integrity
  (ii) Secrecy
  (iii) Availability

20) List tools of Cyber Security. Explain any two tools with its features.

Ans Different

Tools of Cyber Security are —

(1.) Firewalls
(2.) Antivirus Software
(3.) Wireshark
(4.) Nmap
(5.) Ncat
(6.) Metasploit
(7.) John the Ripper

(1) Firewall:

Firewall is the core of security tools, its job is to prevent unauthorized access to or from a private network. It can be implemented as hadware, software or combination of both.

(2.) Wireshark

Wireshark is the world's best network analyzer tool. It is an open-source software that enables you to inspect real-time data on a live Network.

* Wireshark support all major network protocol and media types.

21) Digital Signature?

Ans: MAC (Message Authentication Code) was used to provide Message Integrity and Message Authentication but it needs symmetric key established between sender and receiver. A digital signature on other hand uses pair of asymmetric keys.

A valid digital signature helps the receiver to know the message comes from the authentic sender and is not altered in between.

What is a Signature?
We sign a document to show that is approved by us or created by us. The signature is proof to the recipient that this document is coming from the correct source. The signature on the document simply means the document is authentic.

When A sends a message to B, B needs to check the authenticity of the message and confirm it comes from A and not C. So, B can ask A to sign the message electronically. The electronic signature proves the identity of A is also called a digital signature.

Conventional Signature Vs Digital Signature

Conventional Signature	**Digital Signature**
A conventional Signature is part of a document. For example, when we sign a cheque, the signature is present on the cheque not on a separate document.	A digital signature is not part of a document. This means the sender sends two documents message and signature.
To verify conventional signatures the recipient compares the signature on the document with the signature on file. So, recipient needs to have a copy of this signature on file for comparison.	To verify digital signatures the recipient applies verification technique to a combination of message and the signature to verify authenticity. So here a copy of the signature is not stored anywhere.
the One-to-Many relationships between document and signature.	One to One relationship between message and signature. Every message has its own signature.
Copy of signed document can be distinguished from the original signature on file.	No distinction can be made unless there is a factor of time(timestamp) on the document.

- Digital Signature needs a public key system. The sender uses a private key to sign a document and the verifier uses the public key to verify the document.

Cryptography Vs Digital Signature

- In Cryptosystem uses private and public keys of the receiver.
- In Digital signature uses private and public keys of the sender.

Process of Digital Signature

1.Signing the document
2.Signing a digest

Signing the document

- Encrypt the document using the private key of the sender.
- Decrypt the document using the public key of the sender.

Signing a digest

- Using public keys is very inefficient if we are dealing with long messages. The solution is to sign a digest of the message.
- Message digest has one to one relationship with a message.
- A digest can be made out of messages at the sender's site.
- Digest then goes through the signing process using the sender's private key.
- Sender then sends a message and signature to the receiver.
- At the receiver site using the public hash function, a digest is created out of the message it received.
- Using verification process authentication of signature is determined.

Features of Digital Signature

Message Integrity
It is preserved by using the hash function in signing and verifying algorithms.

Message Authentication
The message is verified using the public key of the sender. When A sends a message to B . B uses the public key of A for verification and A public key cannot create the same signature as C's private key.

Message Nonrepudiation
To provide a message non-repudiation trusted third party is needed.

- A creates a signature from the message and sends a message to B and a signature to the trusted centre.
- The centre validates A public key and verifies messages that come from A.
- The centre saves a copy of the message with sender identity, receiver identity, and timestamp.
- The centre uses a private key to create a new signature.
- The centre sends a message, a new signature, A's identity, B's identity to B.
- B verifies the message using the public key of the trusted centre.

In the future, if A denies that no message is sent from its site, the centre can show a copy of the saved message.

22) Explain any three authentication mechanisms/ patterns in details.

Ans 1. Password-based authentication

Passwords are the most common methods of authentication. Passwords can be in the form of a string of letters, numbers, or special characters. To protect yourself you need to create strong passwords that include a combination of all possible options.

However, passwords are prone to phishing attacks and bad hygiene that weakens effectiveness. An average person has about 25 different online accounts, but only 54% of users use different passwords across their accounts.

The truth is that there are a lot of passwords to remember. As a result, many people choose convenience over security. Most people use simple passwords instead of creating reliable passwords because they are easier to remember.

The bottom line is that passwords have a lot of weaknesses and are not sufficient in protecting online information. Hackers can easily guess user credentials by running through all possible combinations until they find a match.

2. Multi-factor authentication

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Examples include codes generated from the user's smartphone, Captcha tests, fingerprints, voice biometrics or facial recognition.

MFA authentication methods and technologies increase the confidence of users by adding multiple layers of security. MFA may be a good defence against most account hacks, but it has its own pitfalls. People may lose their phones or SIM cards and not be able to generate an authentication code

3. Biometric authentication

Biometrics authentication is a security process that relies on the unique biological characteristics of an individual. Here are key advantages of using biometric authentication technologies:

- Biological characteristics can be easily compared to authorized features saved in a database.
- Biometric authentication can control physical access when installed on gates and doors.
- You can add biometrics into your multi-factor authentication process.

Biometric authentication technologies are used by consumers, governments and private corporations including airports, military bases, and national borders. The technology is increasingly adopted due to the ability to achieve a high level of security without creating friction for the user. Common biometric authentication methods include:

- **Facial recognition**—matches the different face characteristics of an individual trying to gain access to an approved face stored in a database. Face recognition can be inconsistent when comparing faces at different angles or comparing people who look similar, like close relatives. Facial liveness like ID R&D's passive facial liveness prevents spoofing.
- **Fingerprint scanners**—match the unique patterns on an individual's fingerprints. Some new versions of fingerprint scanners can even assess the vascular patterns in people's fingers. Fingerprint scanners are currently the most popular biometric technology for everyday consumers, despite their frequent inaccuracies. This popularity can be attributed to iPhones.
- **Speaker Recognition** —also known as voice biometrics, examines a speaker's speech patterns for the formation of specific shapes and sound qualities. A voice-protected device usually relies on standardized words to identify users, just like a password.
- **Eye scanners**—include technologies like iris recognition and retina scanners. Iris scanners project a bright light towards the eye and search for unique patterns in the coloured ring around the pupil of the eye. The patterns are then compared to approved information stored in a database. Eye-based authentication may suffer inaccuracies if a person wears glasses or contact lenses.

23) Explain hashing functions/algorithms in detail.

Ans:

One main use of hashing is to compare two files for equality. Without opening two document files to compare them word-for-word, the calculated hash values of these files will allow the owner to know immediately if they are different.

Hashing is also used to verify the integrity of a file after it has been transferred from one place to another, typically in a file backup program like SyncBack. To ensure the transferred file is not corrupted, a user can compare the hash value of both files. If they are the same, then the transferred file is an identical copy.

- Types of Hashing

There are many different types of hash algorithms such as RipeMD, Tiger, xxhash and more, but the most common type of hashing used for file integrity checks are MD5, SHA-2 and CRC32.

MD5 - An MD5 hash function encodes a string of information and encodes it into a 128-bit fingerprint. MD5 is often used as a checksum to verify data integrity. However, due to its age, MD5 is also known to suffer from extensive hash collision vulnerabilities, but it's still one of the most widely used algorithms in the world.

SHA-2 – SHA-2, developed by the National Security Agency (NSA), is a cryptographic hash function. SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256.

CRC32 – A cyclic redundancy check (CRC) is an error-detecting code often used for detection of accidental changes to data. Encoding the same data string using CRC32 will always result in the same hash output, thus CRC32 is sometimes used as a hash algorithm for file integrity checks. These days, CRC32 is rarely used outside of Zip files and FTP servers.

24) Explain Identity and Access Management in Cyber Security?

Ans:

Identity Access and Management is abbreviated as IAM. In simple words, it restricts access to sensitive data while allowing employees to view, copy and change content related to their jobs. This information can range from sensitive information to company-specific information.

It refers to the IAM IT security discipline as well as the framework for managing digital identities. It also deprives the provision of identity, which allows access to resources and performing particular activities.

When you exceed your target, IAM ensures that the appropriate resources, such as the database, application, and network, are accessible. Everything is proceeding according to plan.

25) List any five attacks of cyber security. Explain any two in detail?

Ans: Types of cyber-Attacks

Malware

Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:

- Blocks access to key components of the network (ransomware)
- Installs malware or additional harmful software
- Covertly obtains information by transmitting data from the hard drive (spyware)
- Disrupts certain components and renders the system inoperable

Phishing

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. Phishing is an increasingly common cyberthreat.

What Is Phishing?

Man-in-the-middle attack

Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor's device and the network. Without knowing, the visitor passes all information through the attacker.

2. Once malware has breached a device, an attacker can install software to process all of the victim's information.

Denial-of-service attack

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfil legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a distributed-denial-of-service (DDoS) attack.

SQL injection

A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

Zero-day exploit

A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. Zero-day vulnerability threat detection requires constant awareness.

26) Explain Intrusion Prevention System and Intrusion Detection System.

Ans: Intrusion detection is the process of monitoring the events occurring in your network and analysing them for signs of possible incidents, violations, or imminent threats to your security policies.

Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of your network to detect and stop potential incidents.

The three IDS detection methodologies are typically used to detect incidents.

- **Signature-Based Detection** compares signatures against observed events to identify possible incidents. This is the simplest detection method because it compares only the current unit of activity (such as a packet or a log entry, to a list of signatures) using string comparison operations.
- **Anomaly-Based Detection** compares definitions of what is considered normal activity with observed events in order to identify significant deviations. This detection method can be very effective at spotting previously unknown threats.
- **Stateful Protocol Analysis** compares predetermined profiles of generally accepted definitions for benign protocol activity for each protocol state against observed events in order to identify deviations.

27) What is Cryptography?

Ans: Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Modern cryptography concerns itself with the following four objectives:

1. **Confidentiality.** The information cannot be understood by anyone for whom it was unintended.
2. **Integrity.** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
3. **Non-repudiation.** The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.
4. **Authentication.** The sender and receiver can confirm each other's identity and the origin/destination of the information.

28) What is Authentication?

Ans: Authentication is a term that refers to the process of proving that some fact or some document is genuine. In computer science, this term is typically associated with proving a user's identity. Usually, a user proves their identity by providing their **credentials**, that is, an agreed piece of information shared between the user and the system.

29) What is Encryption and Decryption? Write your answer with example?

Ans:

	Encryption	Decryption
1.	Encryption is the process of converting normal message into meaningless message.	While decryption is the process of converting meaningless message into its original form.
2.	Encryption is the process which take place at sender's end.	While decryption is the process which take place at receiver's end.
3.	Its major task is to convert the plain text into cipher text.	While its main task is to convert the cipher text into plain text.
4.	Any message can be encrypted with either secret key or public key.	Whereas the encrypted message can be decrypted with either secret key or private key.
5.	In encryption process, sender sends the data to receiver after encrypted it.	Whereas in decryption process, receiver receives the information (Cipher text) and convert into plain text.

30) Explain CIA Model.

Ans: When we discuss data and information, we must consider the CIA triad. The CIA triad refers to an information security model made up of the three main components: confidentiality, integrity and availability. Each component represents a fundamental objective of information security.

The three components of the CIA triad are discussed below:

1. **Confidentiality:** This component is often associated with secrecy and the use of encryption. Confidentiality in this context means that the data is only available to authorized parties. When information has been kept confidential it means that it has not been compromised by other parties; confidential data are not disclosed to people who do not require them or who should not have access to them. Ensuring confidentiality means that information is organized in terms of who needs to have access, as well as the sensitivity of the data. A breach of confidentiality may take place through different means, for instance hacking or social engineering.

2. **Integrity:** Data integrity refers to the certainty that the data is not tampered with or degraded during or after submission. It is the certainty that the data has not been subject to unauthorized modification, either intentional or unintentional. There are two points during the transmission process during which the integrity could be compromised: during the upload or transmission of data or during the storage of the document in the database or collection.

3. **Availability:** This means that the information is available to authorized users when it is needed. For a system to demonstrate availability, it must have properly functioning computing systems, security controls and communication channels. Systems defined as critical (power generation, medical equipment, safety systems) often have extreme requirements related to availability. These systems must be resilient against cyber threats, and have safeguards against power outages, hardware failures and other events that might impact the system availability.

30.) Explain CIA Model:

Confidentiality:

⇒ It is

⇒ Confidentiality, integrity, and availability, also known as the CIA triad, is a model design to guide an an organisation policy and information security.

Confidentiality:

⇒ It is the ability not to disclose information to unauthorized persons, programs, or processes.

⇒ It requires measures to ensure that only authorise persons have access to information, and while unauthorized persons are denied access to them

⇒ If confidentiality is compromised, this can lead to loss of privacy and disclosure of confidential informatio to the public or other persons.

PAGE:
DATE: / /

Integrity:

⇒ It means that protection against improper modification and destruction of information, ensuring that information cannot be changed undetected and ensuring the integrity of the information.

⇒ It is based on encryption & hashing to ensure the best possible protection against cyber attacks.

Availability:

⇒ It ensures that information is available to those in need that includes timely and reliable access, regardless of the time of day, place or other factors.

3.) Symmetric key	Asymmetric key
1.) It only requires a single key for both encryption and decryption.	1.) It requires two key one to encrypt and the other one to decrypt.
2.) The encryption process is very fast.	2.) The encryption process is slow.
3.) It only provides confidentiality	3.) It provides confidentiality, authenticity and non-repudiation.
4.) It is used when a large amount of data is required to tranfer	4.) It is used to transfer small amount of data.
5.) ex- 3DES, AES etc	5.) Ex- ECC, ElGamal, DSA & RSA.

32.) ⇒ Identity and access ~~mangers~~ management is the security discipline that makes it possible for the right entities to use the right resources when they need to without ~~inf~~ interference, using the devices they want to use.

⇒ It restricts access to sensitive data while allowing employees to view, copy and change content related to their jobs.

33.) It is a technique of securing information and communication through use of codes in a particular form so that only those for whom it is intended can read & process it.

36.) Write any one difference between DoS & DDoS.

⇒ DoS:

→ In DoS attack single system targets the victims system.

DDoS:

→ In DDoS multiple system attacks the victims system

38.) It is a method of hiding secret data, by embedding it into unsecret file like audio, video, image or text file.
It is one of the methods employed to protect secret or sensitive data from malicious attacks.
ex- Audio, Steganography, Text Steganography, Video etc.

PAGE:
DATE: / /

39.)

40.) It is a technique which is used to validate the authenticity and integrity of the message.

⇒ The basic idea behind the Digital Signature is to sign a document. When we send a document electronically, we can also sign it.

⇒ In digital signature, a ~~public~~ private key encryption technique is used to sign a document while the public key is used for decryption.

⇒ It cannot be achieved by using secret key encryption.

41.) These are the five attacks of cyber security:

1.) Phishing attack
2.) Man-In-the-Middle attack
3.) DoS attack
4.) SQL Injection
5.) Brute-Force Attack

DoS attack

⇒ It is designed to slow or take down machines or networks making them inaccessible for the people who need them.

⇒ It make networks and the resource that rely on them inaccessible for those who use them.

⇒ DoS attacks are one of the oldest cybercrime tactics, but they are increasingly damging and disruptive to organization of all sizes.

⇒

PAGE:
DATE: / /

Man in the middle attack:

⇒ It is a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. Once the attackers interrupt the traffic they can filter and steal data.

42.) ⇒ A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

⇒ It is one of the algorithms which calculates a string value from a file, which is of a fixed size. Basically, it contains blocks of data, which is transformed into a short fixed length key or value from the original string.