ViVa-Questions

Q. 1 What is Cryptography?

Ans. : Cryptography is a process of hiding information while transmitting, storage, and processing of data by using different complex algorithms and methods.

Q. 2 What is the goal of Cryptography?

Ans. : The goal of Cryptography is Confidentiality, Integrity, Availability, and Non-Repudiation of IT system.

Q. 3 What is CIA?

Ans. : Confidentiality, Integrity, and Availability (CIA) is a popular model which is designed to develop a security policy. CIA model consists of three concepts:

(i) Confidentiality: Ensure the sensitive data is accessed only by an authorized user.

(ii) Integrity: Integrity means the information is in the right format.

(iii) Availability: Ensure the data and resources are available for users who need them.

Q. 4 What is the importance of a Cryptography?

Ans. : As we move towards the digital economy, cryptography plays a crucial role in securing your digital assets from hackers by encrypting it.

Q. 5 What is a key?

Ans. : In cryptography a key is a piece of information used in combination with an algorithm (a cipher) to transform plaintext into ciphertext (encryption) and vice versa (decryption).

Q. 6 Specify the four categories of security threads?

Ans. : (i) Interruption, (ii) Interception , (iii) Modification, (iv) Fabrication

Q. 7 Explain active and passive attack with example?

Ans. : **Passive attack :** Monitoring the message during transmission. E.g.: Interception

Active attack : It involves the modification of data stream or creation of false data stream. E.g.: Fabrication, Modification, and Interruption.

Q. 8 Define integrity and non-repudiation?

Ans. : **Integrity :** Service that ensures that only authorized person able to modify the message.

Non repudiation : This service helps to prove that the person who denies the transaction is true or false.

Q. 9 Define confidentiality and authentication.

Ans. : **Confidentiality :** It means how to maintain the secrecy of message.

Authentication : It ensures that the information in a computer system and transmitted information are accessible only for reading by authorized person.

Q. 10 Define cryptanalysis.

Ans. : It is a process of attempting to discover the key or plain text or both.

Q. 11 What is Symmetric Encryption?

Ans. : Symmetric Encryption is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetric encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages.

Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Q. 12 What is Asymmetric Encryption?

Ans. : Asymmetric encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text.

- Firstly, a public key must be made public in order to encrypt the data.
- Secondly, a private key used to decrypt the data.

The public key and the private key are not the same thing but they are related. You create your message then encrypt it with the recipient's public key. After that, if the recipient wants to decrypt your message, he/she would have to do it with his/her private key.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes EIGammal, RSA, DSA.

Q. 13 Define Security attacks.

Ans. : Any action that compromises the security of information owned by an organization is called security attack.

Q. 14 Define security mechanism.

Ans. : It is process that is designed to detect prevent, recover from a security attack. Example: Encryption algorithm, Digital signature, Authentication protocols.

Q. 15 Define Security service.

Ans. : A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Q. 16 What are Ciphers?

Ans. : Cipher is a process of creating data in a non-readable form. In other words, you can say it is an algorithm responsible for the encryption and decryption of data.

Q. 17 What are the different types of Ciphers?

Ans. : Some of the ciphers are: Mono-alphabetic Ciphers, Polyalphabetic Ciphers, Transposition Ciphers, Steganography.

Q. 18 Define steganography.

Ans. : Hiding the message into some cover media. It conceals the existence of a message.

Q. 19 What is RSA in the field of Cryptography?

Ans. : RSA (Rivest–Shamir–Adleman) is an asymmetric cryptographic algorithm. It consists of two keys: Public and Private keys. The private key holds only by the owner of that key, and the corresponding public key is available to different persons. If encryption is happening with the private key, decryption can be done with the public key, and vice versa depends on the usage of asymmetric encryption.

Q. 20 How fast is RSA?

Ans. : RSA is asymmetric encryption, so it is definitely slow compared to symmetric encryption, such as DES. On average, DES is approximately 100 times faster than RSA.

Q. 21 What is the major difference between the Symmetric and Asymmetric Key Algorithm?

Ans. : The major difference between the Symmetric and Asymmetric Key algorithms is using the same key in the case of the Symmetric Key algorithm while using different keys (public and private key) in the case of the Asymmetric Key Algorithm.

Q. 22 What is Transposition Cipher?

Ans. : Transposition ciphers is an encryption algorithm based on rearranging letters of the original message and convert it into a non-readable form.

Q. 23 Define product cipher.

Ans. : Product cipher performs two or more basic ciphers in sequence in such a way that the final result or product is crypto logically stronger than any of the component ciphers.

Q. 24 What are the advantages of the Symmetric Key Algorithm?

Ans. : The main advantage of the Symmetric Key Algorithm is the fast speed of encryption in comparison with the Asymmetric Key Algorithm. Another important advantage of this algorithm is the property of extreme security that makes it unbreakable.

Q. 25 What is Block Cipher?

Ans. : Block cipher is a method of encrypting data using cryptographic keys and algorithms to apply to a block or chunks of the message simultaneously rather than individually. The transposition cipher is an example of Block cipher.

Q. 26 What is Stream Cipher?

Ans. : In this cipher, the cryptographic algorithm is used to encrypt or decrypt a message one bit or character at a time. The Caesar cipher is an example of the stream cipher.

Q. 27 List out different types of encryption algorithms.

Ans. : Currently many cryptographic algorithms available to secure data. Some of them are:

DES/ Triple DES, Blowfish, AES, MD5, RSA.

Q. 28 List down some Hashing Algorithms.

Ans. : Hashing algorithms are used to convert data of any length into fixed-size hash value. Some hash algorithms are: Message Digest (MD), Secure Hash Function (SHA).

Q. 29 What is the Data Encryption Standard (DES)?

Ans. : DES or Data Encryption Standard is a symmetric-key algorithm to encrypt data into a non-readable form. DES uses the same key of size 56 bits to encrypt and decrypt data.

Q. 30 What is Triple DES (3DES)?

Ans. : Triple-DES is a type of symmetric-key algorithm and uses 168 bits key (three 56 bits keys) to encrypt or decrypt a message. It is considered a strong algorithm than DES.

Q. 31 What is the Advanced Encryption Standard (AES)?

Ans. : Advanced Encryption Standard (AES) is a symmetric key block cipher used to encrypt and decrypt messages.

Q. 32 What are Confusion and Diffusion in Cryptography?

Ans. :

- **Confusion** means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two. The property of confusion hides the relationship between the ciphertext and the key. This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected. Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.
- **Diffusion** means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change. Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. The idea of diffusion is to hide the relationship between the ciphertext and the plain text. This will make it hard for an attacker who tries to find out the plain text and it increases the redundancy of plain text by spreading it across the rows and columns; it is achieved through transposition of algorithm and it is used by block ciphers only.

Q. 33 Differentiate between IDS and IPS.

Ans. : Intrusion Detection System (IDS) detects intrusions. The administrator has to be careful while preventing the intrusion. In the Intrusion Prevention System (IPS), the system finds the intrusion and prevent it.

Q. 34 What is a Firewall?

Ans. : It is a security system designed for the network. A firewall is set on the boundaries of any system or network which monitors and controls network traffic. Firewalls are mostly used to protect the system or network from malware, worms, and viruses. Firewalls can also prevent content filtering and remote access.

Q. 35 Explain Traceroute

Ans. : It is a tool that shows the packet path. It lists all the points that the packet passes through. Traceroute is used mostly when the packet does not reach the destination. Traceroute is used to check where the connection breaks or stops or to identify the failure.

Q. 36 Differentiate between HIDS and NIDS.

Ans. :

Parameter	HIDS	NIDS
Usage	HIDS is used to detect the intrusions.	NIDS is used for the network.
What does it do?	It monitors suspicious system activities and traffic of a specific device.	It monitors the traffic of all device on the network.

Q. 37 Explain SSL

Ans. : SSL stands for Secure Sockets Layer. It is a technology creating encrypted connections between a web server and a web browser. It is used to protect the information in online transactions and digital payments to maintain data privacy.

Q. 38 What do you mean by data leakage?

Ans. : Data leakage is an unauthorized transfer of data to the outside world. Data leakage occurs via email, optical media, laptops, and USB keys.

Q. 39 Explain the brute force attack. How to prevent it?

Ans. : It is a trial-and-error method to find out the right password or PIN. Hackers repetitively try all the combinations of credentials. In many cases, brute force attacks are automated where the software automatically works to login with credentials. There are ways to prevent Brute Force attacks. They are:

- Setting password length.
- Increase password complexity.
- Set limit on login failures.

Q. 40 What is port scanning?

Ans. : It is the technique for identifying open ports and service available on a specific host. Hackers use port scanning technique to find information for malicious purposes.

Q. 41 What is a VPN?

Ans. : VPN stands for Virtual Private Network. It is a network connection method for creating an encrypted and safe connection. This method protects data from interference, snooping, censorship.

Q. 42 What is MITM attack?

Ans. : A MITM or Man-in-the-Middle is a type of attack where an attacker intercepts communication between two persons. The main intention of MITM is to access confidential information.

Q. 43 Explain botnet.

Ans. : It's a number of internet-connected devices like servers, mobile devices, IoT devices, and PCs that are infected and controlled by malware.

Q. 44 What is the main difference between SSL and TLS?

Ans. : The main difference between these two is that SSL verifies the identity of the sender. SSL helps you to track the person you are communicating to. TLS offers a secure channel between two clients.

Q. 45 What is hacking?

Ans. : Hacking is a process of finding weakness in computer or private networks to exploit its weaknesses and gain access. For example, using password cracking technique to gain access to a system.

Q. 46 Who are hackers?

Ans. : A Hacker is a person who finds and exploits the weakness in computer systems, smartphones, tablets, or networks to gain access. Hackers are well experienced computer programmers with knowledge of computer security.

Q. 47 What is network sniffing?

Ans. : Network sniffing is a tool used for analyzing data packets sent over a network. This can be done by the specialized software program or hardware equipment. Sniffing can be used to:

- Capture sensitive data such as password.
- Eavesdrop on chat messages
- Monitor data package over a network

Q. 48 What is SSH?

Ans. : SSH stands for Secure Socket Shell or Secure Shell. It is a utility suite that provides system administrators secure way to access the data on a network.

Q. 49 Is SSL protocol enough for network security?

Ans. : SSL verifies the sender's identity, but it does not provide security once the data is transferred to the server. It is good to use server-side encryption and hashing to protect the server against a data breach.

Q. 50 Explain vulnerabilities in network security.

Ans. : Vulnerabilities refer to the weak point in software code which can be exploited by a threat actor. They are most commonly found in an application like SaaS (Software as a service) software.

Q. 51 List out some of the common cyber-attack.

Ans. : Following are the common cyber-attacks which can be used by hackers to damage network:

Malware, Phishing, Password attacks, DDoS, Man in the middle.

Q. 52 How to make the user authentication process more secure?

Ans. : In order to authenticate users, they have to provide their identity. The ID and Key can be used to confirm the user's identity. This is an ideal way how the system should authorize the user.

Q. 53 What are the risks associated with public Wi-Fi?

Ans. : Public Wi-Fi has many security issues. Wi-Fi attacks include karma attack, sniffing, war-driving, brute force attack, etc. Public Wi-Fi may identify data that is passed through a network device like emails, browsing history, passwords, and credit card data.

Q. 54 Explain the main difference between Diffie-Hellman and RSA.

Ans. : Diffie-Hellman is a protocol used while exchanging key between two parties while RSA is an algorithm that works on the basis two keys called private and public key.

Q. 55 Explain the difference between stream cipher and block cipher.

Ans. :

Parameter	Stream Cipher	Block Cipher.
How does it work?	Stream cipher operates on small plaintext units	Block cipher works on large data blocks.
Code requirement	It requires less code.	It requires more code.
Usage of key	Key is used only once.	Reuse of key is possible.
Application	Secure Socket layer.	File encryption and database.
Usage	Stream cipher is used to implement hardware.	Block cipher is used to implement software.

Q. 56 What is the abbreviation of ECB and CBC?

Ans. : The full form of ECB is Electronic Codebook, and the full form of CBC is Cipher Block Chaining.

Q. 57 Explain a buffer overflow attack.

Ans. : Buffer overflow attack is an attack that takes advantage of a process that attempts to write more data to a fixed-length memory block.

Q. 58 Define Spyware.

Ans. : Spyware is a malware that aims to steal data about the organization or person. This malware can damage the organization's computer system.

Q. 59 What is a computer virus?

Ans. : A virus is a malicious software that is executed without the user's consent. Viruses can consume computer resources, such as CPU time and memory. Sometimes, the virus makes changes in other computer programs and insert its own code to harm the computer system.

Q. 60 What do you mean by a worm?

Ans. : A Worm is a type of malware which replicates from one computer to another.

Q. 61 State the difference between virus and worm.

Ans. :

Parameter	Virus	Worm
How they infect a computer?	It inserts malicious code into a specific file or program.	Generate it's copy and spread using email client.
Dependency	Virus need a host program to work	They do not require any host to function correctly.
Linked with files	It is linked with .com, .xls, .exe, .doc, etc.	It is linked with any file on a network.
Affecting speed	It is slower than worm.	It faster compared to a virus.

Q. 62 Name some tools used for packet sniffing.

Ans. : Following are some tools used for packet sniffing: Tcpdump, Kismet, Wireshark, NetworkMiner, Dsniff.

Q. 63 What is a distributed denial-of-service attack (DDoS)?

Ans. : It is an attack in which multiple computers attack website, server, or any network resource.

Q. 64 Explain honeypot.

Ans. : Honeypot is a decoy computer system which records all the transactions, interactions, and actions with users.

Q. 65 What is Backdoor?

Ans. : It is a malware type in which security mechanism is bypassed to access a system.

Q. 66 Is it right to send login credentials through email?

Ans. : It is not right to send login credentials through email because if you send someone userid and password in the mail, chances of email attacks are high.

Q. 67 Explain phishing.

Ans. : It is a technique used to obtain a username, password, and credit card details from other users.

Q. 68 Explain security threat

Ans. : Security threat is defined as a risk which can steal confidential data and harm computer systems as well as organization.

Q. 69 What are physical threats?

Ans. : A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.