**CS VIVA**

**1] Blockchain :**

**Blockchain is a distributed database technology that is used to maintain a growing list of records, called blocks, in a secure and tamper-resistant way. Each block contains a timestamp and a link to the previous block, forming a chain of blocks that is protected by cryptography.**

**2] Security in blockchain:**

**Blockchain provides a number of security benefits, including:**

* **Decentralization: Blockchain is a decentralized technology, which means that it is not controlled by any single entity. This makes it resistant to tampering or censorship, as there is no central point of failure that attackers can target.**
* **Cryptography: Blockchain uses cryptographic techniques, such as hashing and digital signatures, to secure the data and protect against unauthorized access. These techniques make it difficult for attackers to alter the data or forge transactions.**
* **Consensus: In a blockchain network, all participating nodes must agree on the state of the ledger in order for a new block to be added. This consensus mechanism helps to ensure the integrity and reliability of the data.**

**3] DES:**

**The Data Encryption Standard (DES) is a symmetric-key cryptographic algorithm that was developed by IBM in the 1970s. It was widely used for many years, but has since been replaced by more secure algorithms, such as the Advanced Encryption Standard (AES).**

**DES uses a fixed block size of 64 bits, and a key size of 56 bits. It uses a combination of substitution and permutation operations to transform the plaintext data into ciphertext. The specific operations used and the order in which they are applied are determined by the key.**

**To decrypt the ciphertext and restore the original plaintext data, the recipient of the ciphertext must have the same cryptographic key that was used to encrypt the data. The DES algorithm uses the key to perform the reverse transformations on the ciphertext, restoring the original data.**

**Overall, while DES was once a widely-used cryptographic algorithm, it has since been replaced by more secure algorithms, such as AES. It is still used in some legacy systems, but its use is generally discouraged due to its relatively short key length and potential vulnerabilities.**

**ADVANTAGES**

**DES does have some advantages, including:**

* **Wide adoption: DES was a widely-used algorithm, and as a result, it is supported by a wide range of operating systems, libraries, and hardware devices. This makes it easy to use and deploy in existing systems.**
* **Efficiency: DES is a relatively efficient algorithm, which means that it can encrypt and decrypt data quickly without requiring a lot of computational resources. This makes it well-suited for use in resource-constrained environments, such as mobile devices or embedded systems.**
* **Flexibility: DES supports a number of different modes of operation, which allows it to be used in a variety of different applications. For example, it can be used in block cipher mode to encrypt data, or in stream cipher mode to encrypt data streams.**

**DISADVANTAGES**

**DES does have some disadvantages, including:**

* **Security: DES is no longer considered to be a secure algorithm. Its key length of only 56 bits is relatively short, and it has been shown to be vulnerable to various attacks, such as brute-force attacks and differential cryptanalysis.**
* **Key management: Like all cryptographic algorithms, DES relies on the use of a cryptographic key to encrypt and decrypt data. Proper key management is essential to ensure the security of the encryption, but it can also be difficult and time-consuming.**
* **Size of the plaintext: DES is a block cipher, which means that it operates on fixed-size blocks of data. This can be a disadvantage when encrypting large amounts of data, as the plaintext must be broken down into blocks before it can be encrypted.**

**4] AES**

**The Advanced Encryption Standard (AES) is a widely-used cryptographic algorithm that is used to encrypt and decrypt data. It is a symmetric block cipher, which means that the same cryptographic key is used to encrypt and decrypt the data.**

**The AES algorithm uses a fixed block size of 128 bits, and supports three different key sizes: 128 bits, 192 bits, and 256 bits. The longer the key size, the more secure the encryption, but longer key sizes also require more computational resources to encrypt and decrypt the data.**

**The AES algorithm uses a number of different mathematical operations, such as substitution, permutation, and XOR, to transform the plaintext data into ciphertext. The specific operations used and the order in which they are applied are determined by the cryptographic key.**

**To decrypt the ciphertext and restore the original plaintext data, the recipient of the ciphertext must have the same cryptographic key that was used to encrypt the data. The AES algorithm uses the key to perform the reverse transformations on the ciphertext, restoring the original data.**

**Overall, the AES algorithm is a widely-used cryptographic algorithm that is used to encrypt and decrypt data. It is known for its security and efficiency, and is used in many applications, including online banking, secure messaging, and internet shopping.**

**ADVANTAGES**

**Some of the main advantages of AES include:**

* **Security: AES is considered to be a very secure algorithm. It has been extensively studied and tested by cryptographers, and is widely considered to be resistant to attacks.**
* **Efficiency: AES is a highly efficient algorithm, which means that it can encrypt and decrypt data quickly and without requiring a lot of computational resources. This makes it well-suited for use in resource-constrained environments, such as mobile devices or embedded systems.**
* **Flexibility: AES supports three different key sizes (128 bits, 192 bits, and 256 bits), which provides a trade-off between security and efficiency. This allows users to choose the key size that is most appropriate for their specific needs.**

**DISADVANTAGES**

**Some of the main disadvantages of AES include:**

* **Key management: Like all cryptographic algorithms, AES relies on the use of a cryptographic key to encrypt and decrypt data. Proper key management is essential to ensure the security of the encryption, but it can also be difficult and time-consuming.**
* **Size of the plaintext: AES is a block cipher, which means that it operates on fixed-size blocks of data. This can be a disadvantage when encrypting large amounts of data, as the plaintext must be broken down into blocks before it can be encrypted.**
* **Vulnerability to quantum computers: While AES is currently considered to be secure against classical computers, it is vulnerable to attacks by quantum computers. As quantum computing technology continues to advance, it is possible that AES may become less secure in the future.**

**5] SSL :** SSL, or Secure Sockets Layer, is a widely-used security protocol for establishing encrypted links between a web server and a client, such as a web browser. SSL is used to secure sensitive information, it can be a useful tool for enhancing the security of a blockchain network and protecting the privacy of its users.

**6] Dos ddos :**

**A Denial of Service (DoS) attack is a type of cyber attack that is designed to make a network or system unavailable to its intended users. DoS attacks typically involve flooding the target with excessive traffic or requests, overwhelming its resources and preventing it from responding to legitimate requests.**

**A Distributed Denial of Service (DDoS) attack is a variation of a DoS attack that uses multiple compromised devices, often distributed across the internet, to attack the target. This makes DDoS attacks more difficult to detect and mitigate, as the traffic comes from multiple sources.**

**Both DoS and DDoS attacks can have serious consequences, such as disrupting business operations, damaging the target's reputation, and causing financial losses. They can also be used as a smokescreen for other types of attacks, such as data breaches or malware infections.**

**To protect against DoS and DDoS attacks, organizations should implement effective security measures, such as firewalls, intrusion detection and prevention systems, and network segmentation. It is also important to monitor network traffic for signs of an attack, and to have a plan in place for responding to an attack.**

**7] IPSec:**

**IPsec (Internet Protocol Security) is a suite of protocols and algorithms that is used to provide security for internet communication. It is designed to protect the confidentiality, integrity, and authenticity of data transmitted over the internet, and is widely used to secure virtual private networks (VPNs), internet-based voice and video calls, and other applications.**

**IPsec is widely used because it is flexible and can be used with a variety of different network protocols, such as IPv4 and IPv6. It is also supported by many operating systems and devices, making it easy to deploy and use.**

**Overall, IPsec is a suite of protocols and algorithms that is used to provide security for internet communication. It is widely used to secure VPNs, voice and video calls, and other applications, and is known for its flexibility and support for a variety of network protocols.**

**8] MQTT: MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol for use on top of the TCP/IP protocol. It is designed for connections with remote locations where a "small code footprint" is required, or the network bandwidth is limited. The protocol is designed to be used in embedded systems, sensors, and mobile devices where battery power and low bandwidth are critical resources.**

**9. HTTPS: HTTPS (Hypertext Transfer Protocol Secure) is a secure version of the HTTP protocol that is used to transmit data over the internet. It is commonly used to protect the confidentiality of data exchanged between a web server and a client, such as a web browser. HTTPS uses the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to encrypt the data transmitted between the server and the client, making it much harder for an attacker to intercept and read the data. This added security is important for sensitive information, such as online transactions or login credentials.**

**(How is secure?):**

**HTTPS is secure because it uses the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to encrypt the data transmitted between the server and the client. This encryption makes it much harder for an attacker to intercept and read the data.**

**When a client, such as a web browser, connects to a web server using HTTPS, the server sends the client a copy of its SSL or TLS certificate. The client then uses this certificate to verify the identity of the server, and to establish a secure, encrypted connection. Once the connection is established, all data transmitted between the client and the server is encrypted and secure.**

**In addition to encryption, HTTPS also provides authentication, which ensures that the client is communicating with the correct server. This is important because it helps prevent man-in-the-middle attacks, in which an attacker intercepts and alters the data transmitted between the client and the server.**

**Overall, HTTPS provides a high level of security for online communication, and is widely used to protect sensitive information, such as online transactions and login credentials.**

**10. What is concept of Hyperledging?**

**Hyperledger is a collaborative effort to advance cross-industry blockchain technologies. It is an open-source project that aims to help organizations build and run secure and scalable distributed ledger applications.**

**The term "hyperledger" refers to the collective name for the various blockchain-based projects that are being developed under the umbrella of the Linux Foundation's Hyperledger project. These projects are designed to support a variety of applications and use cases, including supply chain management, identity management, and financial services.**

**The main advantage of using a hyperledger is that it allows organizations to build and use distributed ledger applications in a way that is secure, transparent, and tamper-resistant. This can help organizations to improve the efficiency and trustworthiness of their business processes, and to share data and assets securely across different entities.**

**In summary, hyperledger is a technology that enables organizations to build and use secure and scalable distributed ledger applications. It is an open-source project that is being developed by the Linux Foundation's Hyperledger project.**

**11. Types of DoS Attacks**

**There are several different types of DoS (Denial of Service) attacks. Some common types of DoS attacks include:**

* **Flooding attacks: These attacks attempt to overwhelm a network or server with a high volume of traffic, making it unable to process legitimate requests. Examples of flooding attacks include SYN floods and UDP floods.**
* **Application-level attacks: These attacks target specific applications or services, such as web servers, DNS servers, or databases. Examples of application-level attacks include HTTP floods and Slowloris attacks.**
* **Protocol attacks: These attacks exploit vulnerabilities in the underlying protocols that govern internet communication, such as TCP/IP or HTTP. Examples of protocol attacks include teardrop attacks and ping of death attacks.**
* **Distributed attacks: These attacks use multiple compromised devices, such as computers or IoT devices, to launch the attack simultaneously. This can make the attack more powerful and harder to defend against. Examples of distributed attacks include DDoS (Distributed Denial of Service) attacks and botnet attacks.**

**Overall, DoS attacks are designed to disrupt or disable the normal functioning of a network or server, making it unavailable to users. They can cause significant harm to organizations, and can be difficult to defend against.**

**12. Types of Blockchain (Public/Private/Consortium/Hybrid)**

**There are four main types of blockchain:**

1. **Public blockchains: These are decentralized networks that are open to anyone. Anyone can join the network, view the data stored on the blockchain, and participate in the consensus process to verify and validate transactions. Examples of public blockchains include the Bitcoin and Ethereum networks.**
2. **Private blockchains: These are networks that are permissioned, meaning that only authorized users are allowed to access the network and view the data stored on the blockchain. Private blockchains are typically owned and operated by a single organization or group of organizations.**
3. **Consortium blockchains: These are networks that are permissioned, but are not owned and operated by a single organization. Instead, they are governed by a consortium or group of organizations that have agreed to work together to maintain the blockchain and manage the consensus process.**
4. **Hybrid blockchains: These are networks that combine elements of public and private blockchains. For example, a hybrid blockchain might allow anyone to access and view the data stored on the blockchain, but only authorized users would be able to participate in the consensus process and validate transactions.**

**Overall, the type of blockchain that is used depends on the specific needs and requirements of the organizations or individuals involved. Public blockchains offer the highest level of decentralization and openness, while private and consortium blockchains offer more control and permissioning. Hybrid blockchains offer a balance between the two.**

**13. What is cyber forensic?**

**Cyber forensic, or computer forensic, is the practice of collecting, analyzing, and presenting digital evidence in a way that is admissible in a court of law. It involves the use of specialized techniques and tools to identify, preserve, and extract evidence from digital devices, such as computers, smartphones, and servers.**

**Cyber forensic experts are typically employed by law enforcement agencies or private companies to investigate crimes that involve computers or other digital devices. They may be called upon to analyze digital evidence in cases involving fraud, cyberbullying, hacking, or other types of digital wrongdoing.**

**In order to perform a cyber forensic investigation, experts must follow a strict set of guidelines to ensure the integrity of the evidence. This includes seizing the digital devices in a way that preserves the evidence, making a forensic copy of the devices' data, and analyzing the data using specialized tools and techniques. The findings of a cyber forensic investigation can then be used as evidence in a court of law.**

**Overall, cyber forensic is a specialized field that involves the collection and analysis of digital evidence to support criminal investigations and legal proceedings. It plays a critical role in helping to identify and prosecute individuals who engage in digital wrongdoing.**

**14. What are cryptographic algorithms you learned ??**

**Cryptographic algorithms, or cryptographic ciphers, are mathematical algorithms that are used to encrypt and decrypt data.**

**Some examples of cryptographic algorithms include AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), and ECC (Elliptic Curve Cryptography). These algorithms are widely used in applications such as online banking, secure messaging, and internet shopping to protect the confidentiality and integrity of data.**

**15. Full form of RSA and how it works in short**

**RSA (Rivest–Shamir–Adleman) is a widely-used public key cryptographic algorithm. It is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman, who first described the algorithm in 1977.**

**In the RSA algorithm, the security of the encryption is based on the computational difficulty of factoring large numbers. To encrypt a message, the sender first generates a pair of large prime numbers, and multiplies them together to produce a third number, known as the modulus. The sender then selects a public exponent, and uses these values to compute the public key.**

**To decrypt the message, the recipient uses a private key, which is derived from the modulus and the private exponent. The private exponent is chosen in such a way that it can be used to easily compute the original prime factors from the modulus, but it is difficult to derive the private exponent from the public key.**

**In summary, RSA is a widely-used public key cryptographic algorithm that is based on the computational difficulty of factoring large numbers. It is used to securely transmit information over the internet and to verify the authenticity of digital signatures.**

**16. Coap protocol,**

**The Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained devices and networks in the Internet of Things (IoT). It is designed to be simple and lightweight, making it well-suited for use in resource-constrained environments, such as low-power sensors and wireless devices.**

**CoAP is based on the HTTP protocol, and uses a similar message format and request-response model. However, it has a number of differences that make it more suitable for use with IoT devices. For example, CoAP supports UDP (User Datagram Protocol) as a transport layer, which is more efficient and less resource-intensive than TCP (Transmission Control Protocol), the transport layer used by HTTP.**

**In addition, CoAP supports asynchronous messaging, which allows multiple devices to communicate with each other without the need for a central server or broker. This can help to improve the scalability and reliability of IoT networks.**

**Overall, CoAP is a specialized protocol that is designed for use in IoT environments. It offers a simple and lightweight way for constrained devices to communicate with each other and with the broader internet.**

**17. Transport layers attacks**

**Transport Layer Security (TLS) is a cryptographic protocol that is used to provide secure communications on the internet. It is a successor to the Secure Sockets Layer (SSL) protocol, and is designed to provide data confidentiality, integrity, and authenticity between two communicating applications.**

**TLS is typically used to secure communications between a web server and a client, such as a web browser. When a client connects to a server using TLS, the server sends the client a copy of its TLS certificate. The client then verifies the identity of the server, and establishes an encrypted connection using the TLS protocol.**

**Once the connection is established, all data transmitted between the client and the server is encrypted and secure. This helps to protect the confidentiality and integrity of the data, and prevents attackers from eavesdropping on or tampering with the communication.**

**In summary, TLS is a cryptographic protocol that is used to provide secure communications on the internet. It is an important tool for protecting the confidentiality and integrity of data transmitted over the internet, and is widely used to secure web communications and other applications.**

**18. Types of attack**

**There are many different types of cyber attacks, and new types are constantly being developed. Some common types of cyber attacks include:**

* **Malware attacks: These attacks involve the use of malicious software, such as viruses, worms, or Trojans, to compromise the security of a computer or network. Malware can be delivered through email attachments, downloads, or infected websites, and can be used to steal sensitive information, disrupt operations, or gain unauthorized access to a system.**
* **Phishing attacks: These attacks involve the use of fraudulent emails or websites to trick users into revealing sensitive information, such as login credentials or financial data. Phishing attacks often use authentic-looking logos and branding to make the emails or websites appear legitimate, and can be difficult to detect.**
* **Denial of Service (DoS) attacks: These attacks involve overwhelming a network or server with traffic, making it unavailable to users. DoS attacks can be launched using multiple compromised devices, known as a botnet, to amplify the attack and make it more powerful.**
* **SQL injection attacks: These attacks involve injecting malicious code into a database through a vulnerable web application. SQL injection attacks can be used to gain access to sensitive information, or to modify or delete data from the database.**

**Overall, cyber attacks are a major threat to organizations and individuals, and can have serious consequences, including financial losses, reputational damage, and legal liabilities. It is important for organizations to implement effective cybersecurity measures to protect against these attacks.**

**19. What is Vulnerability**

**In the context of computer security, a vulnerability is a weakness or flaw in a system, network, or software application that can be exploited by attackers to gain unauthorized access or perform other malicious actions. Vulnerabilities can arise from a variety of sources, including poor design or implementation, software bugs, or user error.**

**Vulnerabilities can have serious consequences, such as allowing attackers to steal sensitive data, disrupt operations, or gain access to sensitive systems. They can also be used as entry points for more sophisticated attacks, such as malware infections or ransomware attacks.**

**To protect against vulnerabilities, organizations and individuals should implement effective security measures, such as regular patching and updates, strong password policies, and firewalls. It is also important to monitor systems and networks for signs of vulnerabilities, and to respond quickly to any potential threats.**

**Overall, vulnerabilities are weaknesses in systems or software that can be exploited by attackers to gain unauthorized access or perform malicious actions. They are a major concern in the field of computer security, and require effective measures to prevent and mitigate their impact.**

**20. ransomware ?**

**Ransomware is a type of malicious software that encrypts a victim's files and demands a ransom payment in order to restore access. Ransomware typically spreads through phishing emails or malicious websites, and can infect a computer or network quickly and easily.**

**Once a computer is infected with ransomware, the attackers will encrypt the victim's files, making them inaccessible. The attackers will then demand a ransom payment, typically in the form of cryptocurrency, in exchange for the decryption key that is needed to restore access to the files.**

**Ransomware attacks can be highly disruptive and costly, as they can prevent organizations from accessing critical data and systems. They can also result in significant financial losses, as victims may be forced to pay the ransom in order to regain access to their files.**

**To protect against ransomware attacks, organizations and individuals should implement effective security measures, such as regular backups, strong passwords, and up-to-date antivirus software. It is also important to be cautious when opening emails or downloading files from unknown sources.**

**Overall, ransomware is a type of malicious software that encrypts a victim's files and demands a ransom payment in order to restore access. It is a serious threat that can cause significant harm to organizations and individuals.**

**21. Hashing**

**In the context of cybersecurity, hashing is a technique that is used to protect the integrity of data. It involves the use of a cryptographic hash function, which is a mathematical algorithm that maps data of any size to a fixed-size output called a hash value.**

**The main advantage of hashing is that it is a one-way process, which means that it is impossible to recreate the original data from the hash value. This makes it a useful tool for ensuring the integrity of data, as any changes to the original data will result in a different hash value.**

**For example, a sender can compute the hash value of a message using a cryptographic hash function, and include the hash value in the message. When the recipient receives the message, they can compute the hash value of the message using the same hash function. If the recipient's hash value matches the original hash value, they can be confident that the message has not been altered in transit.**

**Overall, hashing is a useful technique for protecting the integrity of data. It is a one-way process that is used to ensure that data has not been tampered with, and is an important component of many cryptographic protocols and systems.**

**22. Authentication and authorization**

**Authentication and authorization are two closely-related concepts in the field of cybersecurity.**

**Authentication is the process of verifying the identity of a user, device, or system. This typically involves the use of credentials, such as a username and password, to prove that the entity is who or what it claims to be.**

**Authorization, on the other hand, is the process of granting access to resources or services based on the authenticated identity of the user, device, or system. This typically involves checking the authenticated identity against a set of permissions or rules to determine what actions the entity is allowed to perform.**

**Together, authentication and authorization form the basis of access control in computer systems. They are used to ensure that only authorized users, devices, or systems are able to access sensitive resources or services, and that they can only perform actions that they are permitted to perform.**

**Overall, authentication and authorization are critical components of cybersecurity. They are used to verify the identity of users, devices, and systems, and to control access to resources and services.**

**23. Aes working**

**The Advanced Encryption Standard (AES) is a widely-used cryptographic algorithm that is used to encrypt and decrypt data. It is a symmetric block cipher, which means that the same cryptographic key is used to encrypt and decrypt the data.**

**The AES algorithm uses a fixed block size of 128 bits, and supports three different key sizes: 128 bits, 192 bits, and 256 bits. The longer the key size, the more secure the encryption, but longer key sizes also require more computational resources to encrypt and decrypt the data.**

**The AES algorithm uses a number of different mathematical operations, such as substitution, permutation, and XOR, to transform the plaintext data into ciphertext. The specific operations used and the order in which they are applied are determined by the cryptographic key.**

**To decrypt the ciphertext and restore the original plaintext data, the recipient of the ciphertext must have the same cryptographic key that was used to encrypt the data. The AES algorithm uses the key to perform the reverse transformations on the ciphertext, restoring the original data.**

**Overall, the AES algorithm is a widely-used cryptographic algorithm that is used to encrypt and decrypt data. It is known for its security and efficiency, and is used in many applications, including online banking, secure messaging, and internet shopping.**

**24. Digital signature**

**In the context of cybersecurity, a digital signature is a mathematical technique that is used to verify the authenticity and integrity of a digital document or message. It is similar to a handwritten signature on a paper document, but is generated and verified using cryptographic algorithms and a digital certificate.**

**A digital signature uses a pair of keys, a private key and a public key, to generate and verify the signature. The private key is kept secret by the signer, while the public key is made available to anyone who needs to verify the signature.**

**25. diff between aes and des algorithms**

**While both algorithms are used for encrypting and decrypting data, there are some significant differences between them.**

**One of the main differences between DES and AES is the key size. DES uses a key size of 56 bits, while AES supports three different key sizes: 128 bits, 192 bits, and 256 bits. The longer the key size, the more secure the encryption, but longer key sizes also require more computational resources to encrypt and decrypt the data.**

**Another difference between DES and AES is the block size. DES uses a fixed block size of 64 bits, while AES uses a fixed block size of 128 bits. This means that AES can encrypt larger blocks of data in a single operation, making it more efficient for encrypting large amounts of data.**