Information Security and Cyber Law PYQ 2022

Section-A

Q1. A. Explain any two critical characteristics of information.

Ans1 a Two critical characteristics of information are:

Accuracy: The accuracy of information refers to the degree to which it is correct, reliable, and error-free. Accuracy is important because it ensures that the information being used is correct and trustworthy. Inaccurate information can lead to incorrect decisions and actions, which can have serious consequences. For example, inaccurate information about a patient's medical condition can result in incorrect treatment, leading to worsening of their health.

Timeliness: The timeliness of information refers to the degree to which it is available when needed. Timeliness is important because it ensures that information is available when it is needed to make decisions or take actions. Delays in accessing information can lead to missed opportunities or incorrect decisions. For example, if a business owner is not able to access timely sales data, they may make decisions based on outdated information, which can lead to missed opportunities or incorrect decisions.

B. Differentiate between substitution cipher and transposition cipher with example.

Ans1 b Substitution cipher and transposition cipher are two types of encryption techniques used to secure data.

Substitution cipher involves replacing each plaintext letter with a different ciphertext letter. This means that the letters in the original message are substituted with other letters or symbols according to a fixed system or key. For example, one of the simplest substitution ciphers is the Caesar Cipher, in which each letter in the plaintext message is shifted by a fixed number of positions in the alphabet. So, if the shift is three, the letter A would be replaced with D, B with E, and so on.

Example:

Plaintext: HELLO WORLD

Ciphertext: KHOOR ZRUOG

In the above example, each letter in the plaintext message has been replaced by the letter three positions down the alphabet.

Transposition cipher, on the other hand, involves rearranging the order of the letters in the plaintext message to create the ciphertext. In this technique, the letters themselves are not changed, but their positions in the message are shuffled according to a specific pattern. For example, a simple transposition cipher is columnar transposition, where the plaintext is arranged in a grid of a fixed number of columns, and the letters are read out column by column.

Example:

Plaintext: THE QUICK BROWN FOX

Ciphertext: TEBOKO XUI QNWCR HF

In the above example, the plaintext message has been arranged in a grid of 4 columns and then read out column by column to create the ciphertext.

In summary, substitution cipher replaces each letter of the plaintext message with a different letter or symbol, while transposition cipher rearranges the letters in the message to create the ciphertext without changing the letters themselves.

C. Name any two password cracking tools.

Ans1 c There are many password cracking tools available, but two commonly used ones are:

John the Ripper: It is a free and open-source password cracking tool that can be used on a variety of operating systems. It is known for its ability to crack many types of passwords, including Unix passwords, Windows LM and NTLM hashes, and more.

Hashcat: This is another popular password cracking tool that is used to crack a variety of password hashes. It can be used on multiple operating systems and supports a wide range of hash types, including MD5, SHA-1, SHA-256, and more. It is known for its speed and efficiency in cracking passwords.

D. Give the section number that covers the following areas:

(i) Punishment for cyber terrorism

(ii) Punishment for identity theft

Ans1 d (i) Punishment for cyber terrorism: Section 66F of the Information Technology Act, 2000.

(ii) Punishment for identity theft: Section 66C of the Information Technology Act, 2000.

E. Differentiate between Law and Ethic

Ans1 e Law and ethics are two distinct concepts, although they are often intertwined in practice. Here are the differences between the two:

Definition:

Law is a set of rules and regulations that are formally enacted by a government body, such as the legislature or the judiciary, and are enforced by the state. Ethics, on the other hand, are a set of moral principles that guide individual or group behaviour, beliefs, and values. Ethics are not formally enforced by the state, but rather are enforced by individuals or organizations themselves.

Enforcement:

Law is enforced by the state, which has the authority to punish those who violate the law. Ethics are enforced by individuals or organizations, who may choose to punish those who violate ethical principles through social, professional, or personal consequences.

Scope:

Law is a formal system of rules that govern society as a whole and is enforced by the state. Ethics, however, are often more subjective and can vary between cultures, organizations, and individuals.

Flexibility:

Law is often more rigid and less flexible than ethics. Once a law is enacted, it can be difficult to change or modify, whereas ethical principles can be more adaptable and change over time.

For example, the law may prohibit stealing, while ethical principles may prohibit lying or cheating. Violating the law can result in criminal charges, fines, or imprisonment, while violating ethical principles can result in social or professional consequences, such as loss of reputation or loss of employment opportunities.

F. Full form of the following:

(i)ACL

Ans (i) ACL stands for Access Control List.

(ii) DIP

Ans (ii) DIP stands for Data In-Place.

G. Write a short note on Digilocker.

Ans1 g DigiLocker is an online service provided by the Government of India that allows citizens to store and access electronic versions of their important documents, such as Aadhaar card, driving license, PAN card, and educational certificates, among others. It is a secure and cloud-based platform that offers a convenient way for individuals to access their important documents anytime and anywhere, without the need for physical copies.

DigiLocker offers several benefits, such as reducing the need for physical storage space, eliminating the risk of lost or damaged documents, and providing easy access to important documents, especially during emergencies. It also offers enhanced security features, such as two-factor authentication and 256-bit SSL encryption, to ensure the privacy and security of the documents stored on the platform.

The service is free of cost and is available to all citizens who have a valid Aadhaar card. To use the service, users need to create a DigiLocker account and link it to their Aadhaar number. They can then access and upload their electronic documents to the platform, which can be accessed using their login credentials. The platform also allows users to share their documents with other government agencies and departments, such as universities and employers, thereby reducing the need for physical copies and streamlining the verification process.

H. List four requirements for secure email.

Ans1 h Four requirements for secure email are:

Encryption: Secure email requires encryption of the content of the email to protect it from being intercepted or read by unauthorized users. Encryption makes the email message unreadable by anyone other than the intended recipient.

Digital Signatures: Digital signatures provide a means of verifying the authenticity of the email sender and ensuring that the email has not been tampered with during transmission. It uses cryptographic algorithms to generate a unique digital signature that can be used to authenticate the sender.

Authentication: Authentication is the process of verifying the identity of the sender and recipient of an email. This can be done through the use of secure login credentials or other authentication methods such as digital certificates.

Anti-virus and Anti-spam protection: Secure email requires protection against malicious software such as viruses and spam. This protection is necessary to prevent these types of attacks from compromising the security of the email system and the information it contains.

I. Differentiate between logical bomb and droppers.

Ans1 I Both logical bomb and droppers are malicious software that can cause harm to a computer system, but they function differently.

A logical bomb is a type of malware that is programmed to execute a malicious action when specific conditions are met. These conditions could be a specific date, time, or triggered by a particular user action. The purpose of a logical bomb is usually to destroy or modify data, disrupt the functioning of a system, or deny access to the system. For example, a programmer may create a logical bomb to delete all data on a system on a particular date.

On the other hand, droppers are programs that are designed to "drop" and install malware onto a target system. Droppers themselves are not malicious, but they are used as a delivery mechanism for other types of malware such as viruses, Trojans, or ransomware. A dropper typically exploits vulnerabilities in a system or uses social engineering techniques to trick the user into installing the malicious software.

In summary, a logical bomb is a type of malware that is triggered by specific conditions to carry out malicious actions, while a dropper is a program used to deliver malware onto a target system.

J. Define vulnerability. Explain different types of vulnerability.

Ans1 j In cybersecurity, vulnerability refers to a weakness or flaw in a system or software that can be exploited by attackers to compromise the security of the system. There are several types of vulnerabilities that exist:

Software Vulnerability: This type of vulnerability is present in the software code and can be exploited by an attacker to take control of a system or to steal sensitive information. Software vulnerabilities are often exploited by attackers through the use of malware.

Network Vulnerability: Network vulnerabilities are weaknesses in the network infrastructure that can be exploited by attackers to gain unauthorized access to a system or to steal data. These vulnerabilities can be caused by outdated or unpatched software, weak passwords, or poor network design.

Physical Vulnerability: This type of vulnerability refers to weaknesses in the physical security of a system or location. Physical vulnerabilities can include things like unlocked doors or windows, weak access controls, or lack of surveillance cameras.

Human Vulnerability: Human vulnerabilities refer to weaknesses in human behaviour that can be exploited by attackers. These vulnerabilities can include things like phishing scams, social engineering attacks, or weak passwords.

It is important to identify and address vulnerabilities in a timely manner to prevent security breaches and protect sensitive information. Regular security assessments and updates can help to identify and address vulnerabilities in a system or network.

Section-B

Q2 A. Expand and explain the term IRP.

Ans. IRP stands for Incident Response Plan. It is a predefined plan that outlines the procedures and steps that must be followed in the event of a security breach, cyber-attack, or any other incident that poses a threat to an organization's network or systems.

An IRP is a crucial part of an organization's overall security strategy. It helps to minimize the damage caused by the incident and ensures a quick and efficient response. The main objective of an IRP is to contain and control the incident, assess the damage, and restore the affected systems and services to normal operations as quickly as possible.

The key components of an IRP typically include:

Incident response team: This team is responsible for implementing the plan and consists of individuals from various departments, such as IT, security, legal, and public relations.

Incident identification and reporting: This section outlines the procedures for identifying and reporting an incident, including who to contact and what information to gather.

Incident assessment and classification: This section outlines how the incident will be assessed and classified based on its severity, impact, and type.

Incident response procedures: This section outlines the procedures that must be followed in response to the incident, including containment, investigation, and recovery.

Communication and notification procedures: This section outlines how internal and external stakeholders will be notified of the incident and how communication will be managed.

Recovery procedures: This section outlines the steps that must be taken to recover from the incident and restore normal operations.

Overall, an IRP is critical for ensuring that an organization can respond quickly and effectively to any security incident, minimizing the damage and ensuring the organization can get back to business as usual as quickly as possible.

B. Encrypt the text "Cyber Forensics" using

(i) Caesar Cipher with key as 3

(ii) Rail Fence Cipher with key as 5

Ans2 b i) Using Caesar Cipher with key as 3:

Each letter in the plaintext is shifted by 3 positions to get the ciphertext.

A becomes D, B becomes E, C becomes F, and so on.

Plaintext: CYBER FORENSICS

Ciphertext: FBEHU IRUQHVFLV

(ii) Using Rail Fence Cipher with key as 5:

The plaintext is written diagonally and then read row by row to get the ciphertext.

The key determines the number of rows used to write the plaintext diagonally.

Plaintext: CYBER FORENSICS

Key = 5:

C . . . . R . . . . S . . . .

. Y . . E . O . . F . N . . I

. . B . E . . R . O . E . C .

. . . F . . . N . . I . . .

. . . . H . . . V . . . . S

Ciphertext: CRSFYEOFNICBEROECHFNVHS

Q3. A. What is a firewall and what are the various categories of firewall?

Asn3 A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Its main purpose is to block unauthorized access while allowing legitimate communication.

There are several categories of firewalls:

Packet filtering firewall: This type of firewall examines each packet that passes through it and accepts or rejects it based on specific rules. It filters packets based on source and destination addresses, ports, and protocols.

Stateful inspection firewall: This type of firewall examines the state of the connection and the context of the packet to determine if it is legitimate. It maintains a record of all the connections passing through it and only allows packets that are part of an established connection.

Proxy firewall: This type of firewall acts as an intermediary between two or more systems. It receives and examines all the traffic before forwarding it to the destination. It can filter traffic based on application layer protocols.

Next-generation firewall: This type of firewall integrates several security functions, including intrusion prevention, application control, and antivirus filtering. It uses deep packet inspection to analyze traffic and identify threats.

Cloud firewall: This type of firewall is hosted in the cloud and is managed by a cloud provider. It provides protection for cloud-based applications and services.

Firewalls are an essential component of network security and are used to protect networks from unauthorized access and attacks.

B. Differentiate between Symmetric and Asymmetric key encryption.

Ans3 b Symmetric and asymmetric key encryption are two methods of cryptography used to secure data transmission. The main difference between the two is in the way the encryption and decryption keys are generated and shared.

Symmetric key encryption, also known as shared secret encryption, uses a single key for both encryption and decryption. This means that the same key is used by both the sender and the receiver to encrypt and decrypt the message. The encryption key is generated by the sender and then securely shared with the receiver. The receiver uses the key to decrypt the message. Examples of symmetric key encryption algorithms include Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

Asymmetric key encryption, also known as public-key encryption, uses two different keys - a public key and a private key. The public key is shared with anyone who wants to send an encrypted message, while the private key is kept secret by the owner. The sender uses the recipient's public key to encrypt the message, and the recipient uses their private key to decrypt it. The advantage of asymmetric key encryption is that it provides a way for people to securely communicate without needing to share a secret key. Examples of asymmetric key encryption algorithms include RSA and Elliptic Curve Cryptography (ECC).

In summary, symmetric key encryption uses the same key for both encryption and decryption, while asymmetric key encryption uses two different keys - a public key and a private key - for encryption and decryption.

Q4.A. Give examples of Cyber Crimes where:

(i) **Computers are used to commit crime**
(ii) **Computers become target of crime**

Ans4 a i) Examples of cyber crimes where computers are used to commit crime are:

Hacking: Unauthorized access to computer systems or networks for malicious purposes.

Malware attacks: The use of viruses, Trojans, and other malicious software to steal data, damage systems, or disrupt operations.

Phishing: The use of fake emails, websites, or messages to trick people into revealing personal or financial information.

Cyberbullying: The use of electronic communication to harass, threaten, or intimidate someone.

Cyberstalking: The use of the internet, social media, or other electronic means to harass or intimidate someone.

(ii) Examples of cyber crimes where computers become the target of crime are:

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: These attacks flood a computer or network with traffic, making it unavailable to legitimate users.

Cyber espionage: The theft of sensitive information or trade secrets from computer systems or networks.

Ransomware attacks: Malware that encrypts data or locks users out of their systems until a ransom is paid.

Cyber vandalism: The intentional destruction or defacement of websites, databases, or other computer resources.

Cyber terrorism: The use of computer networks and systems to launch attacks that cause widespread fear or harm.

B. What is risk management and why is the identification of risks and vulnerability to assets so important in risk management?

Ans4 b Risk management is the process of identifying, assessing, and prioritizing risks to minimize, monitor, and control the impact of uncertain events on an organization's objectives. It is an essential process for any organization that wants to ensure the smooth functioning of its operations while protecting its assets, reputation, and stakeholders from potential threats and uncertainties.

The identification of risks and vulnerability to assets is critical in risk management because it allows organizations to prioritize their resources and efforts towards the most significant risks and vulnerabilities that could potentially harm their operations. By understanding the risks and vulnerabilities to assets, organizations can develop effective risk management strategies and implement appropriate controls to mitigate or prevent the impact of such risks.

Moreover, the identification of risks and vulnerabilities enables organizations to evaluate their overall risk exposure and develop risk management policies and procedures that align with their risk appetite and tolerance. This helps organizations to achieve their objectives by providing them with a structured and systematic approach to risk management that ensures a balance between risk and reward.

In summary, the identification of risks and vulnerabilities to assets is crucial in risk management because it enables organizations to understand the potential impact of risks on their operations and stakeholders, develop effective risk management strategies, and align their risk management policies with their overall objectives and risk appetite.

Q5. A. What is an IDS. Explain how do signature-based IDS differ from heuristic IDS.

Ans5 a IDS stands for Intrusion Detection System, which is a software or hardware solution designed to detect and prevent unauthorized access or attacks on a computer network or system. The IDS works by monitoring network traffic and system activity for known or suspicious patterns of behaviour that may indicate an attempted or successful attack.

There are two types of IDS, signature-based IDS and heuristic IDS. Signature-based IDS relies on a database of known attack signatures, which is essentially a collection of patterns and rules that represent known malicious activities. When network traffic or system activity matches one of the signatures in the database, the IDS alerts the security team about the attempted attack.

On the other hand, heuristic IDS uses algorithms and statistical models to detect abnormal patterns of behaviour that may indicate an attack. Unlike signature-based IDS, heuristic IDS does not rely on a database of known attack signatures. Instead, it uses artificial intelligence and machine learning techniques to learn the normal behaviour of a network or system and identify deviations from the normal behaviour.

The main difference between the two types of IDS is that signature-based IDS is effective at detecting known attacks, while heuristic IDS can detect new and unknown attacks. However, signature-based IDS can generate false positives if the database of attack signatures is not kept up-to-date, while heuristic IDS can generate false negatives if the algorithm fails to detect a new attack pattern. Therefore, a combination of both types of IDS can provide comprehensive network security.

B. Explain Section 72 for breach of Confidentiality and Privacy.

Ans5 b Section 72 of the Information Technology Act, 2000 deals with the penalty for breach of confidentiality and privacy of an individual. The section states that any person who, in the course of their work, has secured access to any electronic record, book, register, correspondence, information, document or other material which is under the control of a company or firm, and has obtained such access with the intent to cause or knowing that he is likely to cause injury to any person, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to INR 1,00,000, or with both.

In other words, if any person who has access to electronic records or information belonging to a company or firm, intentionally discloses or provides access to such information to any third party, then such person can be penalized under this section. This section is applicable to all individuals, including employees, who have access to electronic records and are entrusted with maintaining the confidentiality and privacy of such records.

It is important to identify and mitigate risks and vulnerabilities in order to prevent breaches of confidentiality and privacy. The section is meant to ensure that individuals who have access to electronic records are aware of their responsibilities and are held accountable for any breach of confidentiality and privacy.

Q6. A. Differentiate between

(i) Virus and Trojan Horse

Ans. A virus is a malicious code that replicates itself and spreads to other files and systems, often causing damage to the system. A Trojan horse is a type of malware that disguises itself as a harmless file or program but actually carries a malicious payload. While viruses are designed to spread themselves, Trojan horses are designed to trick the user into executing the malicious code.

(ii) Private key and public key

Ans. Private key and public key are the two components of asymmetric key encryption. A private key is a secret key that is kept by the owner and is used to decrypt messages that have been encrypted using the corresponding public key. A public key is available to anyone who wants to send a message to the owner of the private key. The sender encrypts the message using the public key, which can only be decrypted by the owner of the corresponding private key. In short, private keys are kept secret and used for decryption, while public keys are shared and used for encryption.

B. Explain Man-in-the-middle attack.

Ans6 b A Man-in-the-middle (MITM) attack is a type of cyber attack where an attacker intercepts communication between two parties and eavesdrops or manipulates the communication. In a MITM attack, the attacker positions himself/herself between the two communicating parties and captures the data that is being transmitted. The attacker then has the ability to read, modify, or delete the data being transmitted, without either party being aware of the attack.

A MITM attack can be carried out in various ways. One common method is through the use of a spoofed Wi-Fi network, where the attacker creates a fake wireless access point with a name similar to a legitimate access point. When unsuspecting users connect to the fake network, the attacker can intercept all the data that passes through the network.

Another method is through DNS spoofing, where the attacker redirects the user to a fake website by altering the DNS records. This enables the attacker to steal login credentials, credit card information, or other sensitive data.

MITM attacks can also occur on encrypted connections, such as SSL or TLS. In this case, the attacker intercepts the encrypted communication and decrypts it, revealing the sensitive data.

To protect against MITM attacks, users can take several measures, such as using a Virtual Private Network (VPN) to encrypt their communication, avoiding public Wi-Fi networks, and ensuring that websites they visit use HTTPS encryption. Additionally, software-based security solutions such as intrusion detection systems and firewalls can help to prevent and detect MITM attacks.

C. Justify the statement, "Successful Organization should have 2 multiple layers of security".

Ans6 c The statement "Successful organization should have 2 multiple layers of security" is justified because it emphasizes the need for a comprehensive security approach. A single layer of security, no matter how robust, is often not enough to protect an organization's digital assets from various cyber threats.

Multiple layers of security provide additional protection against security breaches and unauthorized access to critical data, systems, and networks. Each layer in the security system should have its own security mechanisms and should be designed to complement other layers.

For instance, implementing firewalls, intrusion detection and prevention systems, access control mechanisms, encryption, and other security measures at multiple layers will create a more resilient security system. In the event that one layer of security is breached, the additional layers of security will make it harder for attackers to reach the critical data and systems.

Moreover, the multiple layers of security approach also make it possible to identify and isolate a threat early on, minimizing the damage it can cause to the organization. This approach can help prevent financial losses, reputational damage, and legal liabilities associated with data breaches and cyber attacks.

In conclusion, successful organizations recognize the importance of implementing multiple layers of security to safeguard their critical data, systems, and networks from cyber threats. This approach helps to reduce the risk of security breaches and provides a more robust and resilient security system.

Q7. A. Explain the terms

(i) Hacker

(ii) Encryption

(iii)Botnet

(iv key

Ans7 a i) Hacker: A hacker is a person who uses his/her technical expertise and knowledge to find vulnerabilities and exploit weaknesses in computer systems and networks for various purposes. Hackers can be classified into three categories based on their intentions: white hat hackers, black hat hackers, and gray hat hackers.

(ii) Encryption: Encryption is the process of converting plain text or data into a coded form using an algorithm to protect its confidentiality and integrity. The encrypted data can only be deciphered by those who have the key to unlock the code.

(iii) Botnet: A botnet is a network of computers that have been infected with malicious software (malware) and are under the control of a remote attacker. Botnets are commonly used to launch DDoS attacks, steal sensitive information, and send spam emails.

(iv) Key: A key is a unique code or password used in encryption algorithms to secure data. It is used to encrypt and decrypt the data, and only those who have the correct key can access the encrypted data. Keys can be of different types, such as symmetric key and asymmetric key.

B. What is the need of a security policy? Explain different types of security policies.

Ans7 b A security policy is a document that outlines an organization's rules, regulations, and procedures related to information security. It helps to define the expectations of users, establish standards for behaviour, and minimize risks to the organization's security. The need for a security policy arises from the growing number of security threats and cyber-attacks on organizations, which can lead to financial loss, reputation damage, and legal liabilities.

There are several types of security policies, including:

Access Control Policy: It outlines the measures for granting access to the organization's resources to authorized personnel only. It defines the levels of access for different users, such as employees, contractors, and partners.

Password Policy: It defines the guidelines for creating and managing passwords, such as length, complexity, and frequency of password changes. It also specifies the rules for storing, sharing, and protecting passwords.

Network Security Policy: It outlines the measures for securing the organization's network infrastructure, such as firewalls, routers, and switches. It defines the protocols for data transfer, remote access, and monitoring of network traffic.

Incident Response Policy: It defines the procedures for detecting, reporting, and responding to security incidents, such as data breaches, malware infections, and denial-of-service attacks. It outlines the roles and responsibilities of the incident response team and the steps for remediation and recovery.

Physical Security Policy: It outlines the measures for securing the organization's physical assets, such as buildings, facilities, and equipment. It defines the access control measures, video surveillance, and alarm systems for preventing unauthorized access and theft.

Acceptable Use Policy: It outlines the guidelines for the acceptable use of the organization's resources, such as computers, networks, and internet services. It defines the restrictions on accessing inappropriate websites, downloading unauthorized software, and sending unsolicited emails.

In conclusion, having a security policy is crucial for every organization to ensure the safety and integrity of its assets. It helps to establish a culture of security, compliance, and risk management, and enables the organization to respond effectively to security incidents and emerging threats.

Q8. A. What is access control? How do Discretionary access control differ from Mandatory and Role-based access control?

Ans8 a Access control is a security mechanism that manages and controls access to resources and systems within an organization. It ensures that authorized users have access to only those resources that they need, while unauthorized users are denied access.

Discretionary access control (DAC) is a type of access control in which the resource owner determines who can access the resource and what level of access they have. The resource owner is responsible for granting and revoking access privileges. DAC is commonly used in small organizations or in situations where the resources are not highly sensitive.

Mandatory access control (MAC) is a type of access control in which access to resources is determined by a central authority. The central authority sets the security policies and determines the level of access that each user is allowed. MAC is commonly used in large organizations or in situations where the resources are highly sensitive.

Role-based access control (RBAC) is a type of access control in which access to resources is based on the user's role or position within the organization. Users are assigned roles based on their job responsibilities, and their access to resources is determined by their role. RBAC is commonly used in organizations with a large number of users and resources, as it simplifies the management of access control policies.

B. Hackers are motivated by various factors. Explain them in detail.

Ans8 b Hackers are individuals or groups who use their technical knowledge and expertise to gain unauthorized access to computer systems and networks. They are motivated by a variety of factors, ranging from financial gain to activism to personal entertainment. Here are some of the common motivations of hackers:

Financial gain: Some hackers are motivated by the prospect of making money through cybercrime. They may steal credit card numbers, login credentials, or other sensitive information that can be sold on the black market.

Activism: Some hackers are motivated by political or social causes. They may use their skills to disrupt or deface websites, leak sensitive information, or launch denial-of-service attacks to draw attention to their cause.

Personal entertainment: Some hackers simply enjoy the thrill of breaking into computer systems and causing mischief. They may engage in pranks or other harmless activities, or they may cause serious damage by deleting files, altering data, or stealing sensitive information.

Revenge: Some hackers may be motivated by a desire for revenge against an individual or organization that has wronged them. They may seek to embarrass, expose, or harm their target through cyber attacks.

Intellectual challenge: Some hackers are motivated by the intellectual challenge of breaking into complex computer systems and networks. They may view hacking as a way to test their technical skills and knowledge.

Espionage: Some hackers may be motivated by a desire to steal sensitive information from governments, businesses, or other organizations. They may engage in sophisticated attacks aimed at infiltrating computer networks and exfiltrating classified or proprietary data.

Discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC) are three common approaches to access control in computer systems. In DAC, access rights are assigned at the discretion of the owner or administrator of the resource. In MAC, access is granted based on a set of predefined rules and policies, often determined by a central authority. In RBAC, access is based on the role of the user within the organization or system. Each approach has its own strengths and weaknesses, and the appropriate approach depends on the needs and requirements of the organization or system.

Q9. Write a short notes on:

(i) Cryptology

(ii) Steganography

(iii)WhiteH a tHacker

(iv)Password Attack

(v)Mail Bomb

Ans9 (i) Cryptology: Cryptology is the study of techniques used for secure communication in the presence of third parties. It includes both cryptography and cryptanalysis. Cryptography refers to the techniques used to protect the confidentiality, integrity, and authenticity of data, while cryptanalysis involves breaking cryptosystems and decoding encrypted messages without the key.

(ii) Steganography: Steganography is the practice of hiding secret messages within other non-secret data to avoid detection. This can be done by embedding the message within an image, audio or video file, or even within another text file.

(iii) White Hat Hacker: A White Hat Hacker is an ethical hacker who uses their skills to help organizations and governments identify and fix security vulnerabilities. They perform security assessments, penetration testing, and other security-related tasks to ensure that systems are secure and that sensitive information is protected.

(iv) Password Attack: Password attack refers to the process of cracking a password-protected system by using various techniques such as brute force, dictionary attack, rainbow table attack, and social engineering.

(v) Mail Bomb: A mail bomb is a type of denial-of-service attack in which the attacker sends a large number of emails to the target's email account, causing the email server to crash or become overloaded, making it impossible for the target to receive any legitimate emails.