LGG_1416_2023

INFORMATION SECURITY PYQS

Qs. Briefly explain OSI security Architecture. [4M]

OSI Security Architecture is categorized into three broad categories namely Security Attacks, Security mechanisms, and Security Services.

1. Security Attacks:

A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization's safety.

They are further classified into 2 sub-categories:

A. Passive Attack:

Attacks in which a third-party intruder tries to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission or eave-dropping the transmission is called Passive Attacks. These types of attacks involve the attacker observing or monitoring system, network, or device activity without actively disrupting or altering it. Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption.
Here, both the sender and receiver have no clue that their message/ data is accessible to some third-party intruder. The message/ data transmitted remains in its usual form without any deviation from its usual behavior. This makes passive attacks very risky as there is no information provided about the attack happening in the communication process. One way to prevent passive attacks is to encrypt the message/data that needs to be transmitted, this will prevent third-party intruders to use the information though it would be accessible to them.

Passive attacks are further divided into two parts based on their behavior:

- **Eavesdropping: This involves the attacker intercepting and listening to communications between two or more parties without their knowledge or consent. Eavesdropping can be performed using a variety of techniques, such as packet sniffing, or man-in-the-middle attacks.**
- **Traffic analysis: This involves the attacker analyzing network traffic patterns and metadata to gather information about the system, network, or device. Here the intruder can't read the message but only understands the pattern and length of encryption.**

Traffic analysis can be performed using a variety of techniques, such as network flow analysis, or protocol analysis.

B. Active Attacks:

Active attacks refer to types of attacks that involve the attacker actively disrupting or altering system, network, or device activity. Active attacks are typically focused on causing damage or disruption, rather than gathering information or intelligence. Here, both the sender and receiver have no clue that their message/ data is modified by some third-party intruder. The message/ data transmitted doesn't remain in its usual form and shows deviation from its usual behavior. This makes active attacks dangerous as there is no information provided of the attack happening in the communication process and the receiver is not aware that the data/ message received is not from the sender.

Active attacks are further divided into four parts based on their behavior:

- **Masquerade** is a type of attack in which the attacker pretends to be an authentic sender in order to gain unauthorized access to a system. This type of attack can involve the attacker using stolen or forged credentials, or manipulating authentication or authorization controls in some other way.
- **Replay** is a type of active attack in which the attacker intercepts a transmitted message through a passive channel and then maliciously or fraudulently replays or delays it at a later time.
- **Modification** of Message involves the attacker modifying the transmitted message and making the final message received by the receiver look like it's not safe or non-meaningful. This type of attack can be used to manipulate the content of the message or to disrupt the communication process.
- **Denial of service (DoS)** attacks involve the attacker sending a large volume of traffic to a system, network, or device in an attempt to overwhelm it and make it unavailable to legitimate users.

2. Security Mechanism

The mechanism that is built to identify any breach of security or attack on the organization, is called a security mechanism. Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access, tampering, or other security threats. Security

mechanisms can be implemented at various levels within a system or network and can be used to provide different types of security, such as confidentiality, integrity, or availability.

Some examples of security mechanisms include:

- **Encipherment (Encryption)**
- **Digital signature**
- **Traffic padding**
- **Routing control**

3. Security Services:

Security services refer to the different services available for maintaining the security and safety of an organization. They help in preventing any potential risks to security.

Security services are divided into 5 types:

- **Authentication** is the process of verifying the identity of a user or device in order to grant or deny access to a system or device.
- **Access control** involves the use of policies and procedures to determine who is allowed to access specific resources within a system.
- **Data Confidentiality** is responsible for the protection of information from being accessed or disclosed to unauthorized parties.
- **Data integrity** is a security mechanism that involves the use of techniques to ensure that data has not been tampered with or altered in any way during transmission or storage.
- **Non- repudiation** involves the use of techniques to create a verifiable record of the origin and transmission of a message, which can be used to prevent the sender from denying that they sent the message.

Qs. What are Rabbit and Logic Bombs? [2M]

Rabbit:

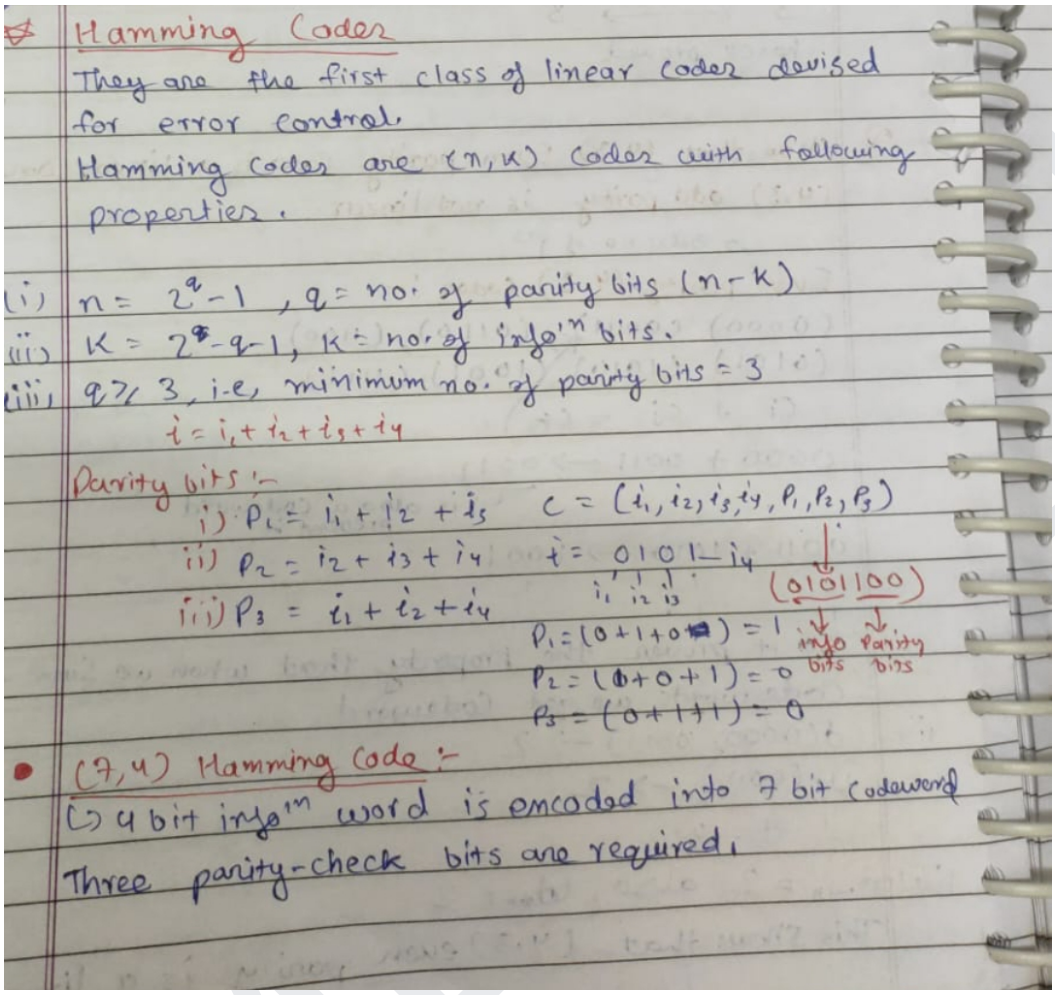
A fork bomb (also known as a "rabbit virus") is a denial of service (DoS) attack in which the fork system call is recursively used until all system resources execute a command. The system eventually becomes overloaded and is unable to respond to any input.

LGG_1416_2023

Logic Bomb:

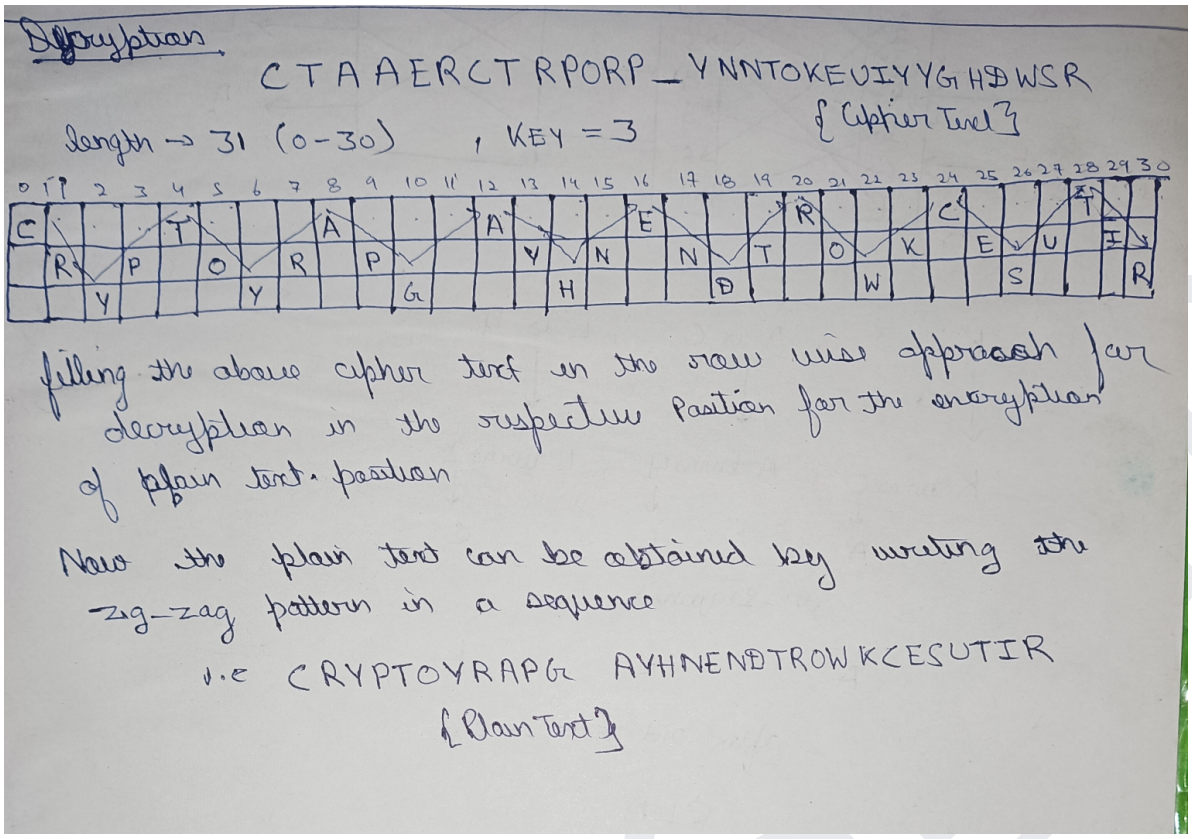
A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files, should they ever be terminated from the company.

Qs. What are the various parameters of the hamming code? [4M]



Qs. Decrypt the following message using rail fence cipher with key=3: [4M]

"CTAAERCTRPORP YNNTOKEUIYYGHDWSR".



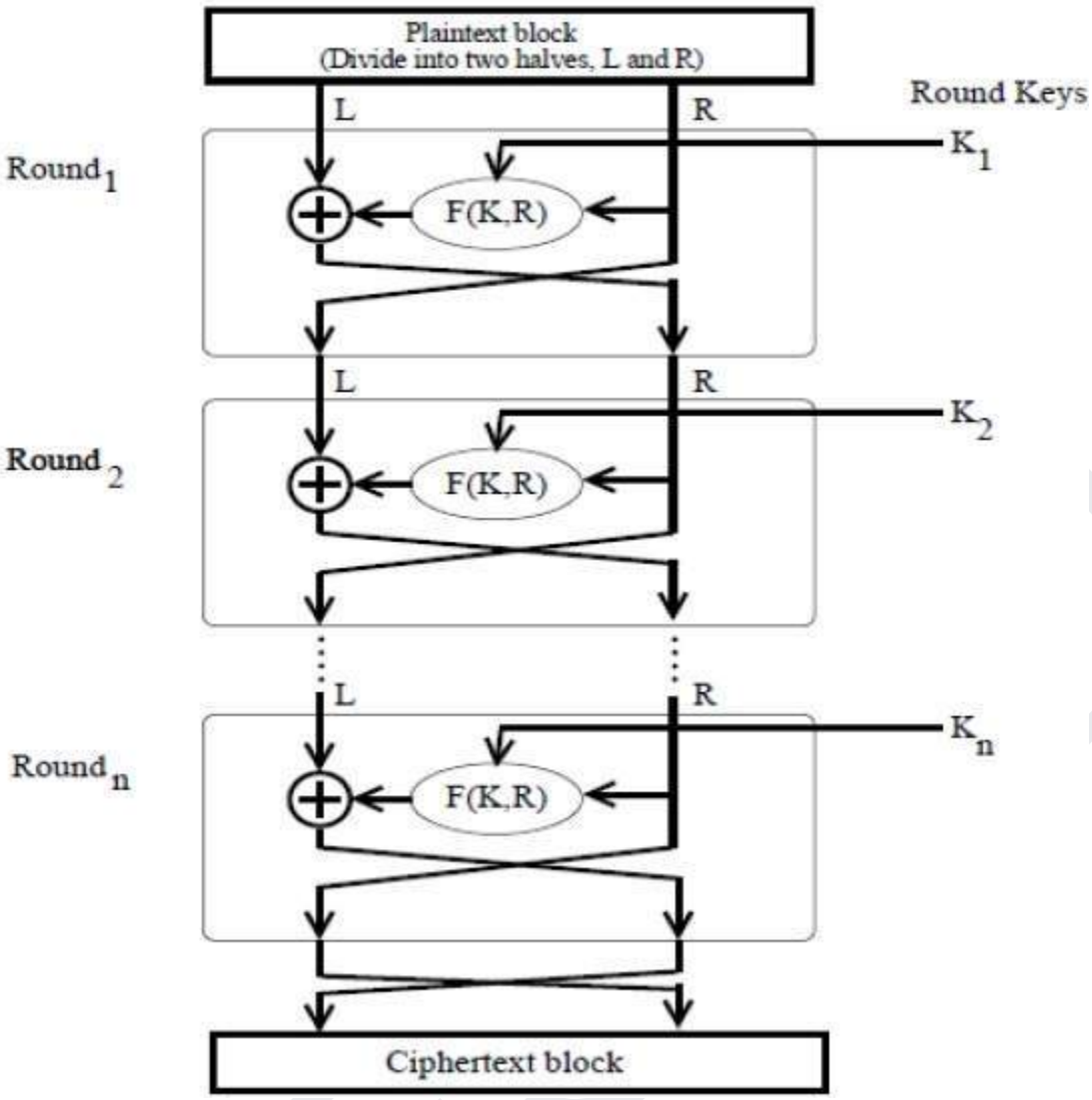
Qs.(a) Explain the Feistel cipher structure in detail. [6M]

Feistel Cipher is a design model from which many different block ciphers are derived. DES is one example of a Feistel Cipher. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption and decryption.

Encryption Process

The encryption process uses the Feistel structure consisting of multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step.

Feistel Structure is shown in the following illustration –



The input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half.

In each round, the right half of the block, R, goes through unchanged. But the left half, L goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two inputs – the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.

In real implementation of the Feistel Cipher, such as DES, instead of using the whole encryption key during each round, a round-dependent key (a subkey) is derived from the encryption key. This

means that each round uses a different key, although all these subkeys are related to the original key.

The permutation step at the end of each round swaps the modified L and unmodified R. Therefore, the L for the next round would be R of the current round. And R for the next round will be the output L of the current round.

Above substitution and permutation steps form a 'round'. The number of rounds are specified by the algorithm design.

Once the last round is completed then the two sub blocks, 'R' and 'L' are concatenated in this order to form the ciphertext block.

The difficult part of designing a Feistel Cipher is the selection of round function 'f'. In order to be an unbreakable scheme.

Decryption Process

The process of decryption in Feistel cipher is almost similar. Instead of starting with a block of plaintext, the ciphertext block is fed into the start of the Feistel structure and then the process thereafter is exactly the same as described in the given illustration.

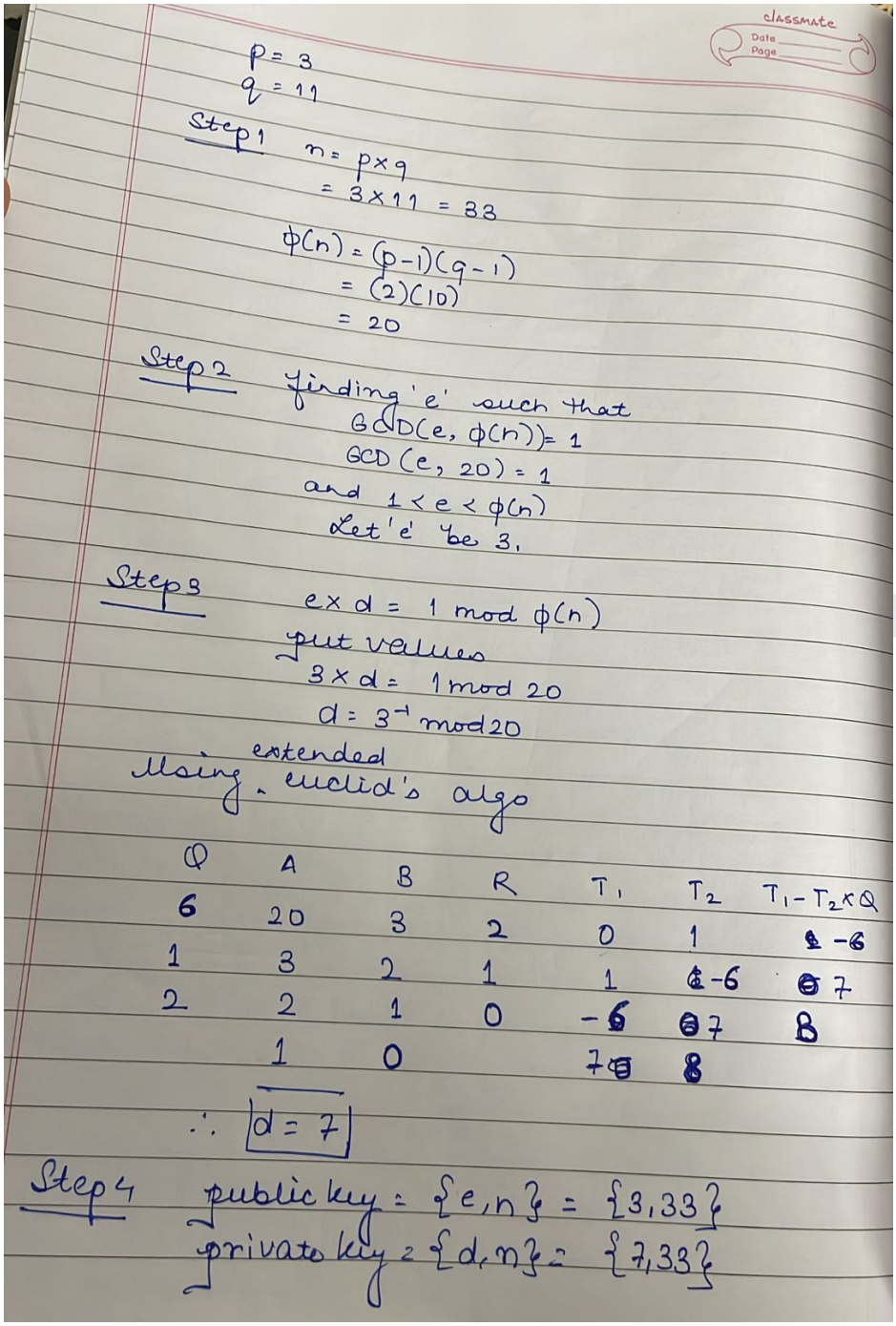
The process is said to be almost similar and not exactly the same. In the case of decryption, the only difference is that the subkeys used in encryption are used in the reverse order.

The final swapping of 'L' and 'R' in the last step of the Feistel Cipher is essential. If these are not swapped then the resulting ciphertext could not be decrypted using the same algorithm.

Number of Rounds

The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide a more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes. Number of rounds in the systems thus depend upon efficiency–security tradeoff.

(b) Perform the encryption of plain text (m)=2 and decryption of the generated cipher text (c) using the RSA algorithm.(Given: p=3,q=11) [4M]



$p = 3$
$q = 11$

Step 1 $n = p \times q$
$= 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1)$
$= (2)(10)$
$= 20$

Step 2 finding 'e' such that
$GCD(e, \phi(n)) = 1$
$GCD(e, 20) = 1$
and $1 < e < \phi(n)$
Let 'e' be 3.

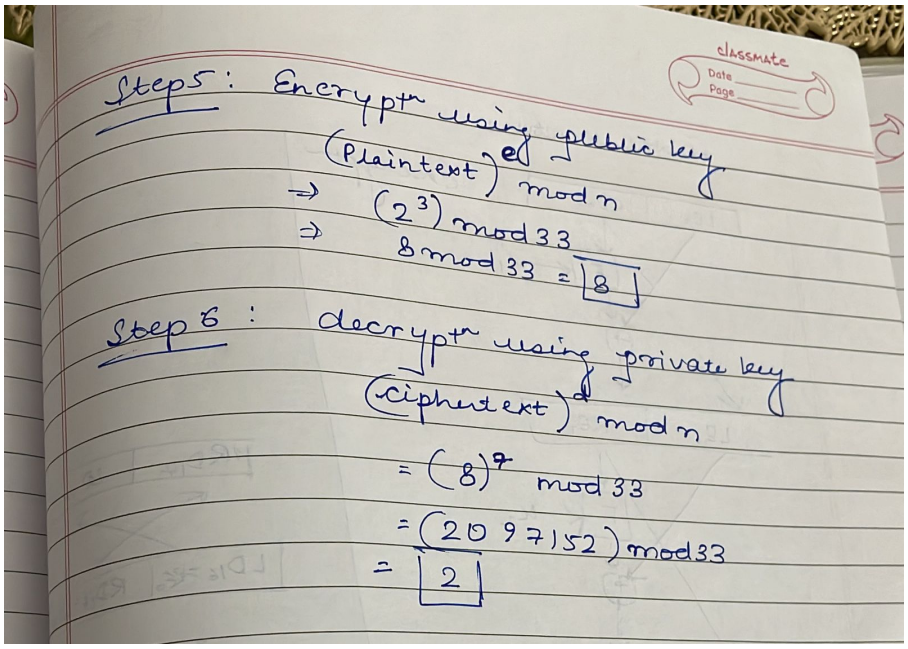
Step 3 $e \times d = 1 \bmod \phi(n)$
put values
$3 \times d = 1 \bmod 20$
$d = 3^{-1} \bmod 20$
using extended euclid's algo

Q	A	B	R	T_1	T_2	$T_1 - T_2 \times Q$
6	20	3	2	0	1	-6
1	3	2	1	1	-6	7
2	2	1	0	-6	7	8
	1	0		7	8	

$\therefore \boxed{d = 7}$

Step 4 public key = $\{e, n\} = \{3, 33\}$
private key = $\{d, n\} = \{7, 33\}$

LGG_1416_2023



Qs. Briefly explain zero-day attack. [2M]

A zero-day attack refers to a cyber attack that exploits a previously unknown vulnerability in software or hardware. It occurs before the vulnerability is known to the software vendor or security community, giving no time for them to develop a patch or fix. Attackers can take advantage of this window of opportunity to infiltrate systems, steal data, or cause other types of damage. The term "zero-day" implies that the attack occurs on the same day the vulnerability is discovered or disclosed, with zero days available for the affected party to protect against it.

Qs. Differentiate among resident virus, transient virus, boot sector virus and polymorphic virus. [4M]

Resident Virus:

A resident virus is a type of computer virus that lodges itself within a computer's memory and remains active even after the initial infection has taken place. It achieves this by attaching itself to a specific program or file and then loading itself into memory when that program or file is executed. Once in memory, the resident virus can infect other files or programs, increasing its spread throughout the system. It stays resident in memory and can continue its malicious activities as long as the computer is running.

Transient Virus:

LGG_1416_2023

A transient virus is a type of computer virus that does not remain permanently in the computer's memory. Instead, it executes its malicious code and performs its intended actions when an infected program or file is executed. Once the execution is complete, the transient virus does not remain active in memory. It relies on infected programs or files to spread to other systems.

Boot Sector Virus:

A boot sector virus infects the boot sector or the master boot record (MBR) of a computer's hard drive or other storage media. The boot sector is a crucial part of the system that contains instructions for the computer to start up. By infecting the boot sector, the virus gains control during the boot process, allowing it to load itself into memory and execute its malicious code before the operating system is fully loaded. Boot sector viruses can spread when infected media, such as a floppy disk or USB drive, is used on multiple computers.

Polymorphic Virus:

A polymorphic virus is a sophisticated type of computer virus that has the ability to change its own code or signature each time it infects a new file or program. By altering its appearance, the polymorphic virus can evade detection by traditional antivirus software that relies on known signatures to identify threats. This constant code mutation makes it challenging for security solutions to identify and eliminate the virus effectively. Polymorphic viruses often employ encryption or obfuscation techniques to generate new variants and make their detection more difficult.

Qs. What is stack smashing? How can we protect our stack from being overwritten by the attacker? [4M]

Stack smashing, also known as a stack buffer overflow, is a type of vulnerability in software that occurs when a program writes more data to a stack buffer than it can hold. This can happen when an attacker deliberately inputs more data than expected, causing the excess data to overflow into adjacent memory locations, potentially overwriting critical information or code.

To protect the stack from being overwritten by an attacker, several mitigation techniques can be employed:

LGG_1416_2023

1. Buffer Overflow Protection: Developers should implement proper input validation and bounds checking to ensure that data being written to stack buffers does not exceed the allocated space. Using secure coding practices and libraries that provide bounds checking can help prevent buffer overflow vulnerabilities.

2. Stack Canaries: Stack canaries, or stack cookies, are random values placed between variables and control data on the stack. Before a function returns, the canary value is checked to ensure it has not been modified. If the canary value has changed, it indicates a stack buffer overflow, and the program can terminate to prevent further exploitation.

3. Address Space Layout Randomization (ASLR): ASLR is a technique that randomizes the memory layout of a program, including the stack. By randomizing memory locations, it becomes more challenging for an attacker to predict the location of the stack and execute a successful stack smashing attack.

4. Data Execution Prevention (DEP): DEP is a security feature that prevents the execution of code from memory regions that are intended for data storage, such as the stack. DEP helps to mitigate certain types of stack smashing attacks by marking the stack as a non-executable region.

5. Compiler-Based Protections: Modern compilers often provide options or flags that enable additional security features to protect against stack smashing attacks. These features may include stack canary generation, stack alignment, and other optimizations that make it harder for attackers to exploit stack vulnerabilities.

It is essential to note that employing multiple layers of protection and staying updated with security patches and software updates are crucial to maintaining a secure system.

{REPEATED AND SIMILAR TOPIC}

[[Qs. 1)Define copyright infringement and Patent infringement{PIRACY se regarding answer rhega niche likha hua he-**}. [2M]**

LGG_1416_2023

Qs. 2)Describe the terms copyright, piracy and patents. Also distinguish between patents and copyrights. [5M]

Qs. 3)Describe the terms copyright, piracy and patents. Also distinguish between patents and copyrights.[5M]]]

Answer

- **Overview On Copyright**
  - **Copyright is the form of legal shield conferred to the authors of "original work of authorship" that enclose dramatic, literary, artistic, musical, and other intellectual works, both published and unpublished. Moreover, its copyright safeguards the form of expression, not the idea behind it.**
  - **For example: The copyright could be conferred to the description of the specified equipment. However, this would only protect the description against any sort of replication activity; it would never disallow others from creating their own description.**
  - **The copyright is granted by the copyright office of the library of congress. An artwork under copyright protection prevents the intervention of defaulters seeking to derive revenue from it.**

- **Overview Of Patent**
  - **Since patents represent the legal articles, they could be hard to obtain. The applicant might have to wait for a year for the approval of the patent application. The most challenging aspect of the patent application is the review phase, in which the patent examiner conducts an in-depth review of the invention on the predetermined grounds.**
  - **The examiner continues to test the specimen until he/she gets satisfied and finds the invention groundbreaking in every aspect and also ensures it doesn't overlap with the previous invention. The review might persist for a couple of months and even a year, depending on the invention's complexity. There are a lot of distinctions involved in obtaining the patent for an invention.**
  - **Once your invention qualified for the patent, you would secure the right to use the invention on your own terms, be it a matter of selling the invention or raising funds for the business. In short, the patent sets an exclusive right for the inventor, which renders him/her complete authority over its inventions.**
  - **A patent does not apply to the idea until it transforms into a materialistic form that offers solutions to a problem. In general, the patent can be obtained for the process, composition of matter, and equipment.**

LGG_1416_2023

- **Overview of piracy(software)**
    - **Software piracy is the act of illegally using, copying, modifying, distributing, sharing, or selling computer software protected by copyright laws. A software pirate is anyone who intentionally or unintentionally commits these illegal acts.**
    - **You don't have to be a hacker to become a software pirate. It's enough to use illegal software or copy and share legal software without the author's consent.**

Key Differences Between Patent And Copyright

Copyright	Patent
Copyright is regulated by the Copyright Act, 1957	A patent is regulated by the Patents Act, 1970.
It is a legal right conferred to the creator of artistic work. It encompasses the right of adaptation of work, reproduction, distribution, etc.	A patent refers to a statutory right conferred by the government to protect an invention for a limited timeframe. Under the specified patent law, the invention cannot be sold, remade, imported without the inventor's permission.
Copyright has a limited scope of applicability as it can't be applied to all sorts of work. It is typically applied on artistry work, namely – poetry, music, film, artwork, and photography,	A patent protects the technical enhancement, which adheres to novelty and uniqueness.
Copyright registration serves the validity period of 60 years and even exists after the demise of the owner.	A patent registration lasts for 20 years from the date on which the application was filed.
Through copyright registration, the owner can reproduce and distribute the original work without any hassle.	A patent is granted to the invention, such as composition involved in an element or particular process.

Copyright Act averts the activity of duplicity and replication of the original work,	A patent prevents others from stealing the notion behind the invention and also deployed prevention measures to avert selling and importing the patented item.
Artists and creators can apply for copyright registration anytime.	A patent for an invention cannot be obtained once disclosed to the general public or made available in the marketplace.

Key Points To Remember On Copyright And Patent

- Copyright serves authors; meanwhile, patent focuses on inventors.
- Companies typically adopt copyright to safeguard their intellectual and creative works.
- Copyright emphasizes art, music, and photography. In comparison, the patent is applied to technologies and medical devices.
- Copyright registration renders the time limit from 70-170 years, depending on the type of artwork. On the contrary, the patent last for 15-20 years.

[[Qs. 1)Does VPN provide link encryption or end-to-end encryption? Justify your answer. (3M)

Qs. 2)Compare link encryption and end-to-end encryption.(5M)]]

Ans 1

VPN (Virtual Private Network) provides link encryption.

A VPN creates a secure tunnel between the user's device and the VPN server, which encrypts all data passing through it. This means that the data is protected from interception and eavesdropping while it is in transit over the internet. The encryption used by the VPN provides link encryption, as it protects the communication link between the user's device and the VPN server.

However, VPNs do not typically provide end-to-end encryption, as the decrypted data is often visible to the VPN provider. This means that the user's data is protected from third-party interception, but the VPN provider can still access and potentially monitor the data passing through its servers.

Some VPN providers offer end-to-end encryption as an additional layer of security

LGG_1416_2023

Ans 2

Link encryption, also known as transport encryption, is a security protocol that encrypts data as it is transmitted between two points on a network, such as between a user's device and a server. This type of encryption typically uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to encrypt data while it is in transit, and it can help protect against interception or eavesdropping by attackers.

End-to-end encryption, on the other hand, is a more comprehensive approach that encrypts data from the point of origin to the point of destination. This means that the data is encrypted on the user's device and remains encrypted as it travels through various servers and networks until it reaches its intended recipient. Only the sender and the recipient have the key to decrypt the data, and even the service provider cannot access the content.

One key difference between link encryption and end-to-end encryption is the level of protection they offer. While link encryption can protect data from interception during transmission, it does not guarantee that the data will remain secure throughout the entire journey. End-to-end encryption, on the other hand, provides a higher level of security by ensuring that data is protected at all times, regardless of where it travels.

Another difference between the two approaches is their impact on performance. Link encryption can cause some performance overhead due to the need to encrypt and decrypt data at each hop in the network. End-to-end encryption can also impact performance, but it typically has less of an impact since the encryption and decryption only occurs at the endpoints.

[[Qs. 1)List the various types of separation used in security methods of an operating system.[2M]

Qs. 2)Explain the various types of Separation used in the security methods of an Operating System [5M]

Qs. 3)What are the different ways in which operating system can support separation and sharing? Explain.[5M]

Qs. 4)Explain the ways in which operating system can support separation and sharing. [3M]

Qs. 5)Explain the ways in which operating system can support separation and Sharing.[5M]]]

LGG_1416_2023

Operating systems provide mechanisms for separation and sharing of resources among multiple processes or users to ensure system security. Below are different ways in which operating systems can support separation and sharing:

1. Process isolation: An operating system can create isolated processes, where each process runs independently and has its own virtual memory space, preventing one process from accessing another process's memory. This ensures that if one process is compromised, it cannot affect other processes.
2. File permissions: Operating systems can use file permissions to control access to files and directories. By setting file permissions, the operating system can restrict users or processes from accessing certain files, directories or system resources, preventing unauthorized access or modification of sensitive data.
3. User account control: Operating systems can enforce user account control to ensure that only authorized users can access system resources. User accounts can be assigned different permissions based on their roles, and access can be further restricted by implementing authentication mechanisms such as passwords, biometrics or two-factor authentication.
4. Virtualization: Operating systems can use virtualization technology to create multiple isolated virtual machines that can run different operating systems or applications. This allows multiple users or processes to share the same physical hardware resources while keeping them separate from each other, preventing any unauthorized access.
5. Sandboxing: Operating systems can use sandboxing techniques to restrict the execution of an application or process to a controlled environment, preventing it from accessing other system resources. This ensures that even if the application is compromised, it cannot access or affect other processes or data on the system.

[[Qs. 1) Describe Salami attack and explain why salami attacks persist?[3M]

Qs. 2)Describe salami attack with the help of an example and explain why salami attacks persist[2+1+1M]]]

Salami attack is a type of financial fraud where the perpetrator steals small amounts of money over a long period of time. In a salami attack, the fraudster takes a small amount of money from a large number of transactions, with the aim of avoiding detection. The stolen money is so small that it goes unnoticed by the victims, but when added together, it amounts to a substantial sum.

LGG_1416_2023

For example, imagine a bank employee who has access to a large number of customer accounts. Instead of stealing a large sum of money from a single account, the employee transfers small amounts of money from each account into a separate account he controls. Over time, the employee siphons off a large amount of money while avoiding detection, as the amount stolen from each account is too small to raise suspicion.

Salami attacks persist because they are difficult to detect. The small amounts stolen are often not noticed by victims, and the fraudulent transactions may not trigger any alarms or alerts that would raise suspicions. The perpetrator can also cover their tracks by manipulating records, falsifying documents or creating fake accounts. Additionally, salami attacks are typically carried out over a long period of time, which makes it difficult to identify patterns or trends that would indicate fraudulent activity.

[[Qs. 1) Describe Non-malicious program errors. Name any two such errors.[5M]

Qs. 2)What do you understand by Non-malicious program error? Explain buffer-overflow attack and its security implications[5M]]]

A non-malicious program error refers to a programming mistake that causes a program to behave unexpectedly or incorrectly. Such errors are usually caused by unintentional programming errors, such as syntax errors, logical errors, or memory-related errors.

One common type of non-malicious program error that can be exploited by attackers is a buffer-overflow error. A buffer-overflow error occurs when a program attempts to store more data in a buffer (temporary storage area) than it can hold. This can cause the program to crash or behave unpredictably.

An attacker can exploit a buffer-overflow error by sending more data to the program than it can handle, causing the extra data to overflow into adjacent memory locations. If the attacker can control the overflow data, they may be able to overwrite critical system memory or execute arbitrary code, potentially allowing them to take control of the system or steal sensitive data.

Buffer-overflow attacks are particularly dangerous because they can be used to bypass security measures, such as data validation or access controls, that are in place to prevent unauthorized access to a system. Additionally, buffer-overflow attacks can be difficult to detect and prevent, as they often rely on exploiting subtle programming errors that may go unnoticed during normal use.

To mitigate the risk of buffer-overflow attacks, programmers can use secure coding practices, such as bounds checking and input validation, to prevent buffer-overflow errors from occurring. Additionally, software developers can use specialized tools, such as static analysis tools and runtime protection mechanisms, to detect and prevent buffer-overflow attacks at runtime. Finally, system administrators can employ security measures, such as firewalls and intrusion detection

systems, to monitor for suspicious network traffic and block or alert on potential buffer-overflow attacks.

[[Qs. 1)What are digital signatures? How can they contribute to the security of downloading an running software from the Internet?[5M]

Qs. 2)Write short notes on the following:[5M]

(a) Digital signatures

Qs. 3)Differentiate between the following: [2M]

(a) Digital Signature and conventional signature]]

Ans 1

Digital signatures are a method of verifying the authenticity and integrity of digital data, such as documents, software, or other files. They are essentially electronic fingerprints that are unique to a specific piece of data and are used to ensure that the data has not been tampered with or altered since it was signed.

In the context of downloading and running software from the internet, digital signatures can help to ensure that the software being downloaded is genuine and has not been modified or tampered with by an attacker. When software is signed with a digital signature, the signature is a cryptographic hash that is unique to that specific version of the software. This hash can be used to verify that the software has not been modified since it was signed, providing assurance that the software has not been compromised.

By verifying the digital signature of a software package, users can be confident that the software they are downloading is genuine and has not been tampered with. This can help to prevent malicious software from being downloaded and installed on a user's system, which can lead to data loss, theft, or other security breaches.

ANS 3

A conventional signature is a physical signature that is written on a document by hand. It is used to provide authentication and proof of agreement, and can be used to verify the identity of the signer. However, it can

be forged or copied, and does not offer any protection against alteration or tampering of the document after it has been signed.

On the other hand, a digital signature is an electronic signature that uses a cryptographic algorithm to provide authentication, integrity, and non-repudiation of electronic data. It involves using a private key to create a digital signature that is unique to a particular document or message. The signature can then be verified using the corresponding public key to ensure that the data has not been tampered with or altered since it was signed. Digital signatures are more secure than conventional signatures because they are difficult to forge or copy, and provide protection against tampering or alteration of the signed data.

[[Qs. 1)What is the difference between passive and active security attacks? Explain by giving suitable examples,(5M)

Qs. 2)Which attack, active or passive, is more difficult to detect and why ?[5M]]]

Active Attack	Passive Attack
• In an active attack, Modification in information takes place.	• While in a passive attack, Modification in the information does not take place.
• Active Attack is a danger to Integrity as well as availability.	• Passive Attack is a danger to Confidentiality.
• In an active attack, attention is on prevention.	• While in passive attack attention is on detection.
• Due to active attacks, the execution system is always damaged.	• While due to passive attack, there is no harm to the system.
• In an active attack, Victim gets informed about the	• While in a passive attack, Victim does not get informed about the attack.

attack.

• In an active attack, System resources can be changed.	• While in passive attack, System resources are not changing.
• Active attack influences the services of the system.	• While in a passive attack, information and messages in the system or network are acquired.
• In an active attack, information collected through passive attacks is used during execution.	• While passive attacks are performed by collecting information such as passwords, and messages by themselves.
• An active attack is tough to restrict from entering systems or networks.	• Passive Attack is easy to prohibit in comparison to active attack.
• The duration of an active attack is short.	• The duration of a passive attack is long.
• The prevention possibility of active attack is High	• The prevention possibility of passive attack is low.
• Complexity is High	• Complexity is low.

Ans 2

Passive attacks are generally more difficult to detect compared to active attacks.

In a passive attack, the attacker simply eavesdrops on the communication between two parties without altering the contents of the communication. This means that the attack is not causing any noticeable disturbance in the network or communication channel, and the parties involved may not even be aware that they are being monitored. As a result, passive attacks can be harder to detect since there may not be any obvious signs of malicious activity.

LGG_1416_2023

On the other hand, active attacks involve an attacker making changes to the communication between two parties. This often involves injecting new data or modifying existing data in order to disrupt the communication, steal data, or manipulate the flow of information. Active attacks can be easier to detect since they often cause disruptions or abnormal behaviors in the network or communication channel.

That being said, both types of attacks can be difficult to detect if the attacker is skilled and takes steps to remain hidden. It's important for security professionals to have a layered approach to security that includes monitoring, intrusion detection, and other defensive measures to detect and mitigate both active and passive attacks.

[[Qs. 1)Differentiate between the terms authentication and authorization with the help of suitable example(s). [5M]

Qs. 2)Differentiate between Authentication and Authorisation,(2M)]]

Ans

Authentication refers to the process of verifying the identity of a user, device, or entity before granting access to a system or resource. It involves confirming that the user is who they claim to be, typically through the use of credentials such as usernames, passwords, or biometric data.

For example, when a user logs into a website or an application, they are required to enter their username and password. The system then verifies the user's credentials and grants access to the site or application if the credentials are valid. In this case, authentication is used to confirm the identity of the user before allowing them to access the system.

Authorization, on the other hand, refers to the process of granting or denying access to a particular resource or system based on the authenticated user's permissions or privileges. It involves determining what actions a user is allowed to perform, and what resources they are authorized to access.

For example, once a user has been authenticated and logged into a website, the system will then determine what level of access the user has to different areas of the site. An administrator may have access to all areas of the site, while a regular user may only have access to certain parts. In this case, authorization is used to control what actions the user is allowed to perform and what resources they are authorized to access.

LGG_1416_2023

In summary, authentication is the process of verifying the identity of a user, while authorization is the process of determining what actions a user is allowed to perform once they have been authenticated.

[[Qs. 1)With the help of an example, explain the SQL injection attack and defense from this attack. [5M]

Qs. 2)With the help of an example, explain the SQL injection attack and defense from this attack.[5M]

Qs. 3)With the help of an example, explain SQL injection attack and the defense from this attack.[5M]]]

Ans 3

SQL injection attack is a type of cyber attack that involves exploiting vulnerabilities in a web application's input validation process to execute malicious SQL commands. Attackers use this technique to access and manipulate a web application's database, which may contain sensitive information such as user credentials or financial data.

For example, consider a web application that allows users to search for products by entering a search term into a text box. The application takes the user's input and uses it to construct a SQL query to retrieve matching products from the database. An attacker can exploit this input validation process by entering a malicious SQL command into the search box. For instance, the attacker could enter a search term like "' OR 1=1; --", which would be interpreted as part of the SQL query and cause the application to retrieve all the products in the database instead of the intended search results.

To defend against SQL injection attacks, web application developers can implement various measures such as input validation, parameterized queries, and stored procedures. Input validation involves filtering and sanitizing user input to ensure that it is safe and does not contain any malicious code. Parameterized queries involve separating the SQL code from the user input by using placeholders for user input, which are then replaced with sanitized values before the query is executed. Stored procedures involve predefining the SQL commands on the database server, which can be called by the application without the need for dynamic SQL generation.

Another effective defense against SQL injection attacks is the use of web application firewalls (WAFs), which can detect and block malicious SQL commands before they reach the application.

LGG_1416_2023

WAFs use a set of predefined rules and heuristics to identify and block suspicious requests based on their content and behavior.

In summary, SQL injection attacks are a serious threat to web applications that rely on SQL databases. By implementing measures such as input validation, parameterized queries, and stored procedures, and using web application firewalls, developers can defend against SQL injection attacks and ensure the security of their applications and databases.

[[Qs. 1)Describe public key infrastructure (PKI).[5M]

Qs. 2)Explain Public Key Infrastructures (PKI) along with the types of models. [5M]

Qs. 3)Explain Public Key Infrastructures (PKI) along with the types of models. [5M]]]

Ans

Public Key Infrastructure (PKI) is a system of hardware, software, policies, and procedures that enable the secure exchange of digital information using public key cryptography. It provides a framework for managing digital certificates, which are used to authenticate and secure electronic communication and transactions.

PKI consists of several key components, including:

1. Certificate Authority (CA): A trusted third-party organization that issues and manages digital certificates.

2. Registration Authority (RA): An entity responsible for verifying the identity of certificate holders and issuing digital certificates.

3. Certificate Revocation List (CRL): A list of digital certificates that have been revoked or are no longer valid.

4. Certificate Repository: A database or repository where digital certificates can be stored and retrieved.

PKI operates based on the concept of a public-private key pair. A user creates a public-private key pair, and the public key is distributed to others while the private key is kept secret. The public key is used for encrypting data and verifying digital signatures, while the private key is used for decrypting data and generating digital signatures.

There are two main PKI models: hierarchical and web-of-trust.

LGG_1416_2023

1. Hierarchical PKI: In this model, a root Certificate Authority(CA) issues digital certificates to subordinate CAs, which in turn issue digital certificates to end-users. This creates a hierarchy of trust, with the root CA at the top of the chain and end-users at the bottom. This model is commonly used in enterprise environments.

2. Web-of-Trust PKI: In this model, there is no central authority or hierarchy of trust. Instead, users rely on each other to verify the authenticity of digital certificates. This model is commonly used in decentralized environments, such as peer-to-peer networks or open-source software development.

In summary, PKI is a system for managing digital certificates that provide authentication and security for electronic communication and transactions. There are two main PKI models: hierarchical and web-of-trust, each with its own advantages and use cases.

{Note: questions on chiper}

[[{Note: questions on transposition and substitution chiper}

Qs. 1)Explain columnar transposition by giving suitable example.[3M]

Qs. 2)What is transposition cipher? Explain with an example. [5M]

Qs. 3)Explain transposition cipher with a suitable example. [3M]

Qs. 4)What is the step to quickly test a piece of ciphertext to find out whether it was a result of simple transposition or substitution? [2M]]]

Answer. 1)

Given a plain-text message and a numeric key, cipher the given text using Columnar Transposition Cipher

The Columnar Transposition Cipher is a form of transposition cipher. Columnar Transposition involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one.

Examples:

Encryption

LGG_1416_2023

Input : Geeks for Geeks

Key = HACK

Output : e kefGsGsrekoe_

Decryption

Input : e kefGsGsrekoe_

Key = HACK

Output : Geeks for Geeks

Encryption

In a Columnar transposition cipher, the order of the alphabets is re-arranged to obtain the cipher-text.

1. **The message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.**
2. **Width of the rows and the permutation of the columns are usually defined by a keyword.**
3. **For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "3 1 2 4".**
4. **Any spare spaces are filled with nulls or left blank or placed by a character (Example:"_").**
5. **Finally, the message is read off in columns, in the order specified by the keyword.**

Encryption

Given text = Geeks for Geeks
Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print Characters of column 1,2,3,4
Encrypted Text = e kefGsGsrekoe_

Decryption

1. **To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.**
2. **Then, write the message out in columns again, then re-order the columns by reforming the key word.**

Answer. 2 or 3)

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

{EXAMPLE is columnar T.C mentioned in above i.e Qs. 1)}

Answer. 4)

Transposition cipher: This type of cipher involves changing the positions of the characters but leaving the identity of the characters the same without changing.

Substitution Cipher: This type of cipher involves changing the characters. In short it replaces one character with another.

LGG_1416_2023

These two types of ciphers can be differentiated by using the monogram frequencies. The English language has a very specific frequency distribution and this is not changed by the transposition cipher. The other ciphers change this distribution, so the frequencies can be used to tell what type of cipher it is.

*****Describe how can we go about attempting to break simple ciphers.{NOTE:IT CAN BE ASKED IN 5M QS }**

Steps that I would follow to crack simple ciphers are:

1. Look for single letter words in the ciphertext: The most common single letter words are "a" and "I".

2. Count how many times each letter appears in the ciphertext: This is done by using frequency analysis. In the English language a few words appear a greater number of times when compared to the others. The most common letter that appears a greater number of times is "e".

3. Try to replace the letters by guess or by using the frequency analysis: Change the letters in the ciphertext and look for words that reveal what the actual plaintext is.

4. Find repeating letter patterns: Look for letters that are repeating. The most common English letter groups are: TH, ING, RE, ION.

5. Try to decode 2, 3, 4 letter words: The most common 2, 3 and 4 letter words are "of", "to", "in", "is", "it", "the", "and", "for", "was" and "that". Try replacing the words with these words and see if they fit in.***

[[Qs. 1)Describe the use of Vigenere cipher with the help of suitable example.[5M]

Qs. 2)Explain encryption and decryption of Vernam cipher with suitable example(4M)

Qs. 3)What do you mean by one time pads? Explain Vernam cipher with an example: [4M]

Qs. 4)Use the Additive cipher to encrypt the message "HelloAbraham" with key = 10. [3M]

Qs. 5)Explain whether the following cipher is monoalphabetic or not. Given reason also [2M]

Plain text: Frittata

Ciphertext: LTOHHQJQ

Qs. 6) (a)Describe Playfair Cipher encryption.

(b)Encrypt the plaintext "This is Good" using playfair cipher and the following

key :

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

[3+2M]]]

Answer. 1)

Vigenere Cipher is an encryption and decryption algorithm. It is a type of polyalphabetic substitution cipher, which means that the cipher alphabet is changed regularly during the encryption process. Due to this, the cipher becomes less vulnerable to cryptanalysis.

The encryption of the original text is done using the *Vigenère square or Vigenère table*.

- **The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.**
- **At different points in the encryption process, the cipher uses a different alphabet from one of the rows.**
- **The alphabet used at each point depends on a repeating keyword.**

Example:

Input : Plaintext : GEEKSFORGEEKS

LGG_1416_2023

Keyword : AYUSH

Output : Ciphertext : GCYCZFMLYLEIM

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

The plain text is then encrypted using the process explained below.

Encryption:

The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E, and column Y is C. The rest of the plaintext is enciphered in a similar fashion.

Table to encrypt – Geeks

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Decryption:

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next, we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.

A more easy implementation could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25].

Encryption

The plaintext(P) and key(K) are added modulo 26.

Ei = (Pi + Ki) mod 26

Decryption

Di = (Ei - Ki + 26) mod 26

Note: Di denotes the offset of the i-th character of the plaintext. Like offset of A is 0 and of B is 1 and so on.

Answer. 2)

The Vernam cipher is a substitution cipher where each plain text character is encrypted using its own key. This key — or key stream — is randomly generated or is taken from a one-time pad, e.g. a page of a book. The key must be equal in length to the plain text message. The fact that each character of the message is encrypted using a different key prevents any useful information being revealed through a frequency analysis of the cipher text.

To encrypt the message, each character of the plain text and the key will need to be converted to a numeric code. Fortunately, there are already coding schemes to do this, and we can use standard ASCII codes. As you may already know, in the ASCII coding system, each character is given a numeric code. For example, the letter 'H' is 72. This number has a binary representation of 01001000 (using 8 bits). { A-Z = 65-90, a-z = 97-122 }

To use the Vernam cipher, you will need to use an XOR operation. The operation's truth table is shown below:

INPUT A	INPUT B	OUTPUT Q
0	0	0
0	1	1
1	0	1
1	1	0

To apply the Vernam cipher, each bit of the binary character code for each letter of the plain text undergoes a XOR operation with the corresponding bit of each letter of the binary character code for the corresponding character from the key stream — this creates the cipher text.

In the below example, the message 'HELLO' will be encrypted using the key 'PLUTO'. The letters will be converted into 8-bit ASCII codes.

- **Encryption:**
  1. **Obtain the 8-bit ASCII code for each letter of the plain text:**

Plain text

H	01001000
E	01000101
L	01001100
L	01001100
O	01001111

2. **Obtain the 8-bit ASCII code for each letter of the key:**

Key

P	**01010000**
L	**01001100**
U	**01010101**
T	**01010100**
O	**01001111**

3. **Carry out the XOR operation, applying it to each corresponding pair of bits:**

Plain text	**01001000**	**01000101**	**01001100**	**01001100**	**01001111**
Key	**01010000**	**01001100**	**01010101**	**01010100**	**01001111**
Cipher text in binary	**00011000**	**00001001**	**00011001**	**00011000**	**00000000**

Cipher text(IN 8 bit binary):

00011000, 00001001, 00011001, 00011000, 00000000,

Cipher text(IN denary or decimal):

4, 9, 25, 24, 0

- **Decryption:**

  The same method is used to decrypt the message.

1. **Obtain the binary code for each character of the cipher text (here, you are converting from the denary code version of the cipher text that was produced in the encryption example):**

Cipher text

24	**00011000**
9	**00001001**
25	**00011001**
24	**00011000**
0	**00000000**

2. **Obtain the 8-bit ASCII code for each letter of the key:**

Key

P	**01010000**
L	**01001100**
U	**01010101**
T	**01010100**
O	**01001111**

3. **Carry out the XOR operation, applying it to each corresponding pair of bits:**

Cipher text	00011000	00001001	00011001	00011000	00000000
Key	01010000	01001100	01010101	01010100	01001111
Plain text	01001000	01000101	01001100	01001100	01001111
Plain text converted back into characters	H	E	L	L	O

Answer. 3)

One-time pad: In cryptography, a one-time pad is a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key.

{REST SOLN DONE IN QS. 2}

Answer. 4)

{IMPORTANT: Additive cipher also Known as shift Cipher[*ISKO RECHECK KAR LENA YE MENE KHUD SOLVE KIYA HE***]}**

Plain text: "HelloAbraham"

Key: 10

As in additive cipher we replace plaintext with the corresponding alphabet by adding key no to given plain text alphabet.

here we encrypt one character at a time, each character will shift 10 character down,

"H" will encrypted to "R",

H+10=R,

Similarly ,

“e” encrypted to “o”,

“l” encrypted to “v”,

“l” encrypted to “v”,

“o” encrypted to “y”,

“A” encrypted to “K”,

“b” encrypted to “l”,

“r” encrypted to “b”,

“a” encrypted to “k”,

“h” encrypted to “r”,

“a” encrypted to “k”,

“m” encrypted to “w”,

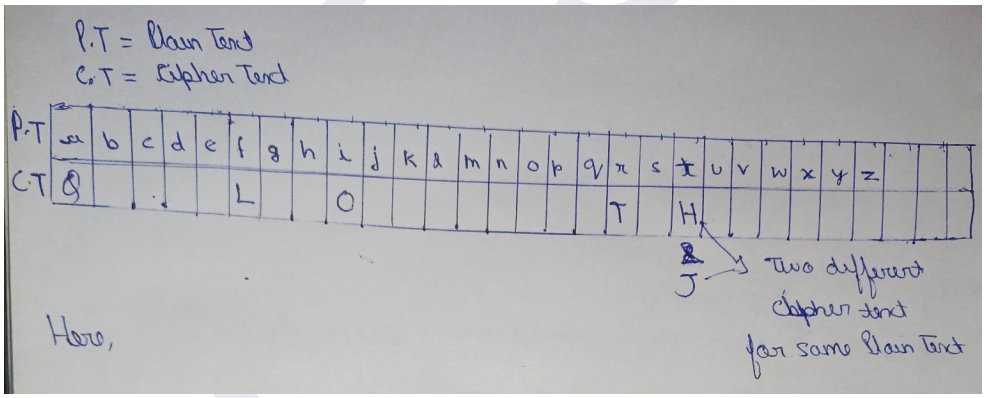
therefore on encrypting “HelloAbraham” we get “RovvyKlbkrkw”

Answer. 5)

{Note:*ISKO RECHECK KAR LENA YE MENE KHUD SOLVE KIYA HE***}**

Here, Plain text: Frittata

and Ciphertext: LTOHHQJQ



As we know that, A monoalphabetic substitution is a cipher in which each occurrence of a plaintext symbol is replaced by a corresponding ciphertext symbol to generate ciphertext. The key for such a cipher is a table of the correspondence or a function from which the correspondence is computed.

LGG_1416_2023

Here for one plain text “t” there are two cipher texts i.e H and J.

so, it cannot be a monoalphabetic cipher.

Answer. 6)

(a)Playfair cipher:

The Playfair cipher encryption technique can be used to encrypt or encode a message. It operates exactly like typical encryption. The only difference is that it encrypts a digraph, or a pair of two letters, as opposed to a single letter.

An initial 5×5 matrix key table is created. The plaintext encryption key is made out of the matrix’s alphabetic characters. in which we shouldn’t repeat the letters. There are 26 alphabets, however, there are only 25 spaces in which we can place a letter. The matrix will delete the extra letter because there is an excess of one letter (typically J). Despite this, J is there in the plaintext before being changed to I.

(b)

{{{NOTE: THIS IS WORKING ALGORITHM FOR PLAY CIPHER (ISKO SAMAJ LENA SAARE QS HOJAYNGE ISSE RELATED BAKI YE QS MENE SOLVE KARDIA HAIN ISKE BAAD)

The Playfair Cipher Encryption Algorithm:

The Algorithm consists of 2 steps:

1. Generate the key Square(5×5):
    - The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

    - The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the

alphabet in order.

2. Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.
   For example:
   PlainText: "instruments" After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

{NOTE: WORKING RULE EXAMPLE

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: "hello"

After Split: 'he' 'lx' 'lo'

Here 'x' is the bogus letter.

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: "helloe"

AfterSplit: 'he' 'lx' 'lo' 'ez'

Here 'z' is the bogus letter. }

Rules for Encryption:

a) If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

For example:

Diagraph: "me"

Encrypted Text: cl

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Encryption: m -> c and e -> l

b) If both the letters are in the same row: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

For example:

Diagraph: "st"

Encrypted Text: tl

Encryption: s -> t and t -> l

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

c) If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

Diagraph: "nt"

Encrypted Text: rq

Encryption: n -> r and t -> q

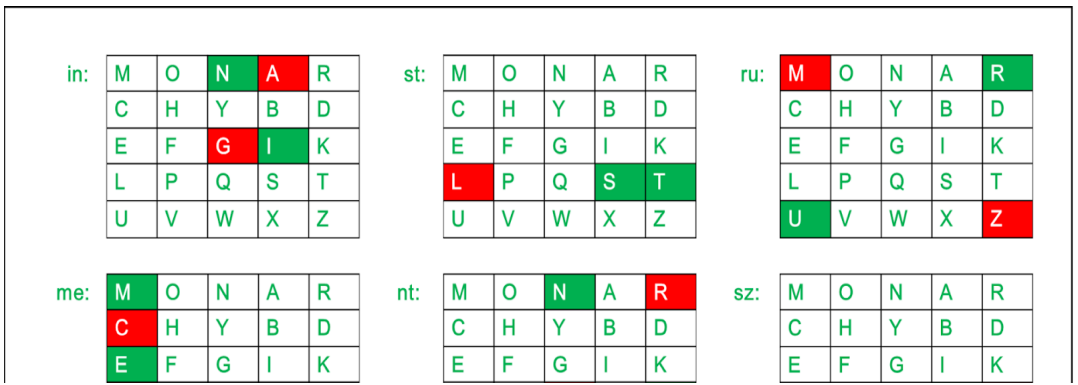
M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

***For example HERE:**

Plain Text: "instrumentsz"

Encrypted Text: gatlmzclrqtx

Encryption:



LGG_1416_2023

i -> g and n -> a

s -> t and t -> l

r -> m and u -> z

m -> c and e -> l

n -> r and t -> q

s -> t and z -> x ***

}}}

NOW GIVEN plaintext "This is good"

IN DIGRAPH "Th" "is" "is" "go" "od"

key :

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

now by using above secret key and playfair ciphertext encryption algorithm

Diagraph: "Th"

T->W and H->E

Encrypted Text: We

key :

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

LGG_1416_2023

Diagraph: "is"

I->N and S->O

Encrypted Text: no

key :

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

Diagraph: "is"

I->N and S->O

Encrypted Text: no

key :

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

Diagraph: "go"

G->B and O->V

Encrypted Text: bv

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

Diagraph: "od"

key :

secret key =

L	G	D	B	A
Q	M	H	E	C
U	R	N	I/J	F
X	V	S	O	K
Z	Y	W	T	P

LGG_1416_2023

O->S and D->B

Encrypted Text: sb

therefore encrypted text will be "Weno no bvsb"

[[Qs. 1)Describe various categories of Computer/cyber Criminals by giving an example of each category.[5M]

Qs. 2)Who are Computer Criminals? Give examples[2M]]]

Computer Criminals are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit.

Computer Criminals are known to access the Computer Criminal underground markets found in the deep web to trade malicious goods and services, such as hacking tools and stolen data. Computer Criminal underground markets are known to specialize in certain products or services.

These are five types of computer criminals:

#1 The Social Engineer

Cyber criminals pretending to be someone else can trick unsuspecting employees to compromise data. In one scenario, a spoof email purporting to be from the CEO of the company directs an employee to send a PDF with employees' 1099 tax forms for an upcoming meeting with the Internal Revenue Service. The social engineer is able to capture Personally Identifiable Information (PII).

Employees should also ensure the "Reply To" address is, in fact, the email address of the requesting employee, and send this type of information via an encrypted email message." Beware time-sensitive requests, as social engineers sometimes use a sense of urgency to compel victims into unsafe behavior.

#2 The Spear Phisher

Social threats factored into just under one-third of confirmed data breaches, with phishing the tactic used in 92 percent of social-related attacks. An email can appear to be from a legitimate sender, but actually contain a malicious attachment or link that can give spear phishers access to banking credentials, trade secrets and other information that they are able to access.

"Companies can have employee training that both prepares and tests employees to recognize and respond to malicious phishing attempts,"

#3 The Hacker

Nearly two-thirds of confirmed data breaches involved leveraging weak, default or stolen passwords. Malware poses a serious threat, as it can capture keystrokes from an infected device even if employees use strong passwords with special characters and a combination of upper- and lower-case letters.

Still, strong passwords are the first line of defense against hackers, "Use multi-factor authentication, enforce strong password requirements, patch operating systems, software and apps, and increase redundancy and bandwidth".

#4 The Rogue Employee

Disgruntled employees present an insider threat to data. Insider threats accounted for 15 percent of breaches across all patterns, and they can be especially challenging for companies because employees often have both access to data and knowledge of what is stored and where.

Restricting access to sensitive data to only employees with an immediate need to use the data can help reduce the threat. Companies can limit, log and monitor internal account usage to protect against rogue employees, as well as protect against external attackers disguising themselves as legitimate users.

#5 The Ransom Artist

Bad actors have been modifying codes and implementing new ransom attack methods, sparking a rise in ransomware as the fifth most common form of malware, up from the 22nd most common in the 2014 Verizon Data Breach Incident Report. Many companies are paying ransom, often via anonymous bitcoin payments, to have their data restored.

"The people who fall victim to ransomware are not following the information security rules, including encryption and frequent backups,"

{{{{Note: Questions on DES}

[[Qs. 1)With suitable sketches, explain the working of Data Encryption Standard (DES) algorithm.[7M]

Qs. 2)Explain Data Encryption standard with the help of a diagram. [2M]

Qs. 3)With suitable sketches, explain the working of Data Encryption Standard (DES) algorithm.[7M]

Qs. 4)Explain Data Encryption standard with the help of a diagram. [7M]

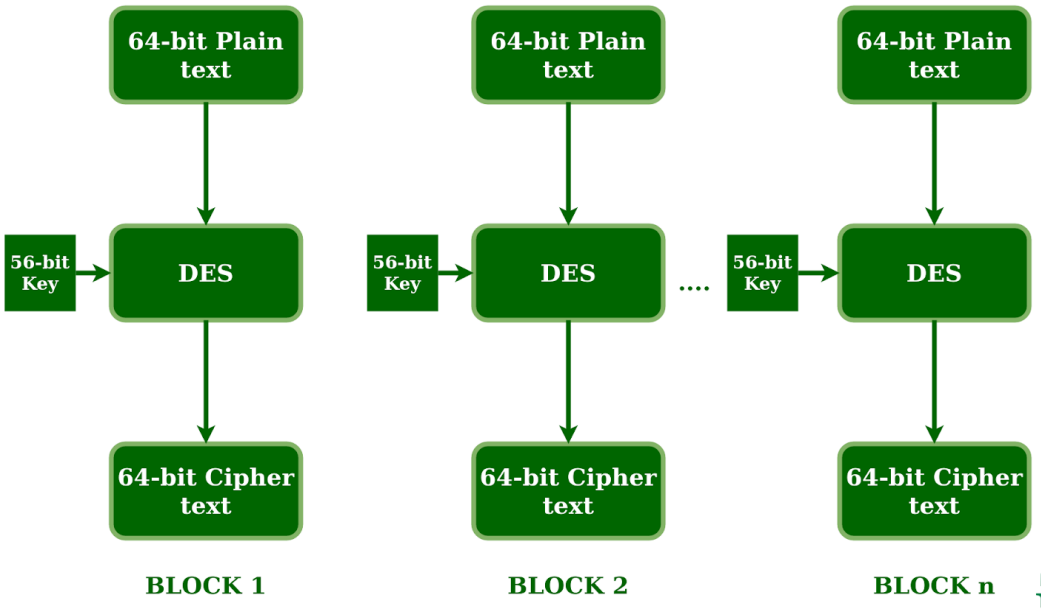
Qs. 5)Describe the steps of encryption using DES through a flow graph. [3M]

Qs. 6)With the help of block diagram, explain cycles of permutation and substitution in DES scheme.[5M]

Qs. 7)How many permutation tables are used in the Data Encryption Standard cipher ? [2M]]]

Answer. 1,2,3,4,5,6,7)

Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext. The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits.



The basic idea is shown in the figure:

We have mentioned that DES uses a 56-bit key. Actually, The initial key consists of 64 bits. However, before the DES process even starts, every 8th bit of the key is discarded to produce a 56-bit key. That is, bit positions 8, 16, 24, 32, 40, 48, 56, and 64 are discarded.

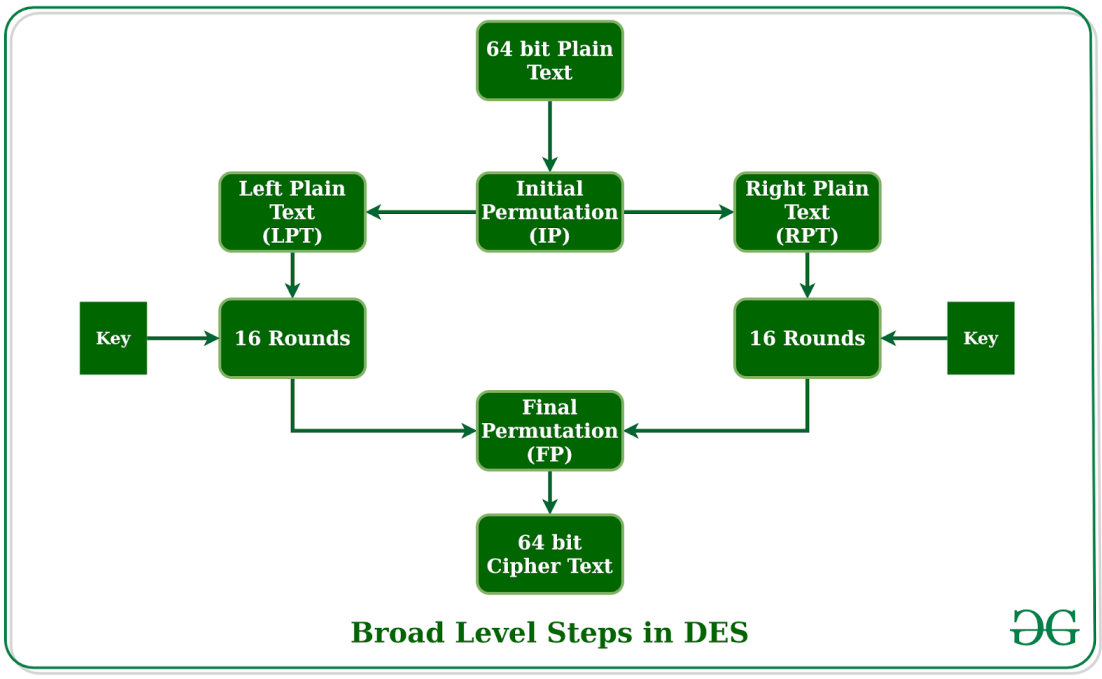
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64

Figure - discording of every 8th bit of original key

Thus, the discarding of every 8th bit of the key produces a 56-bit key from the original 64-bit key. DES is based on the two fundamental attributes of cryptography: substitution (also called confusion) and transposition (also called diffusion). DES consists of 16 steps, each of which is called a round. Each round performs the steps of substitution and transposition. Let us now discuss the broad-level steps in DES.

- **In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.**
- **The initial permutation is performed on plain text.**
- **Next, the initial permutation (IP) produces two halves of the permuted block; saying Left Plain Text (LPT) and Right Plain Text (RPT).**

- Now each LPT and RPT go through 16 rounds of the encryption process.
- In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the combined block
- The result of this process produces 64-bit ciphertext.



Initial Permutation (IP):

As we have noted, the initial permutation (IP) happens only once and it happens before the first round. It suggests how the transposition in IP should proceed, as shown in the figure. For example, it says that the IP replaces the first bit of the original plain text block with the 58th bit of the original plain text, the second bit with the 50th bit of the original plain text block, and so on.

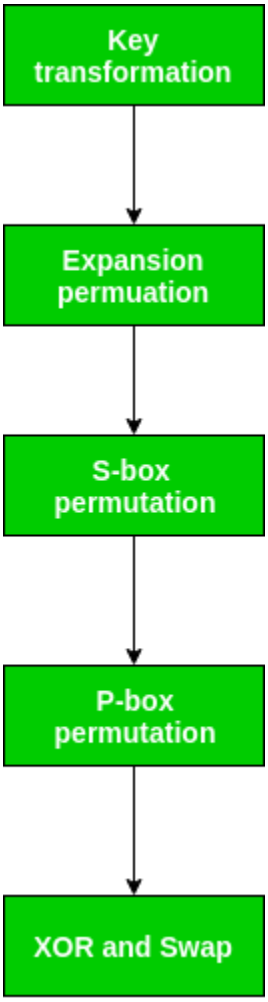
This is nothing but jugglery of bit positions of the original plain text block. the same rule applies to all the other bit positions shown in the figure.

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Figure - Initial permutation table

LGG_1416_2023

As we have noted after IP is done, the resulting 64-bit permuted text block is divided into two half blocks. Each half-block consists of 32 bits, and each of the 16 rounds, in turn, consists of the broad-level steps outlined in the figure.



Step-1: Key transformation:

We have noted that the initial 64-bit key is transformed into a 56-bit key by discarding every 8th bit of the initial key. Thus, for each a 56-bit key is available. From this 56-bit key, a different 48-bit Sub Key is generated during each round using a process called key transformation. For this, the 56-bit key is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round.

For example: if the round numbers 1, 2, 9, or 16 the shift is done by only one position for other rounds, the circular shift is done by two positions. The number of key bits shifted per round is shown in the figure.

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#key bits shifted	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Figure - number of key bits shifted per round

After an appropriate shift, 48 of the 56 bits are selected. for selecting 48 of the 56 bits the table is shown in the figure given below. For instance, after the shift, bit number 14 moves to the firstwposition, bit number 17 moves to the second position, and so on. If we observe the table , we will realize that it contains only 48-bit positions. Bit number 18 is discarded (we will not find it in the table), like 7 others, to reduce a 56-bit key to a 48-bit key. Since the key transformation process involves permutation as well as a selection of a 48-bit subset of the original 56-bit key it is called Compression Permutation.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Figure - compression permutation

Because of this compression permutation technique, a different subset of key bits is used in each round. That makes DES not easy to crack.

Step-2: Expansion Permutation:

Recall that after the initial permutation, we had two 32-bit plain text areas called Left Plain Text(LPT) and Right Plain Text(RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation. This happens as the 32-bit RPT is divided into 8 blocks, with each block consisting of 4 bits. Then, each 4-bit block of the previous step is then expanded to a corresponding 6-bit block, i.e., per 4-bit block, 2 more bits are added.

LGG_1416_2023

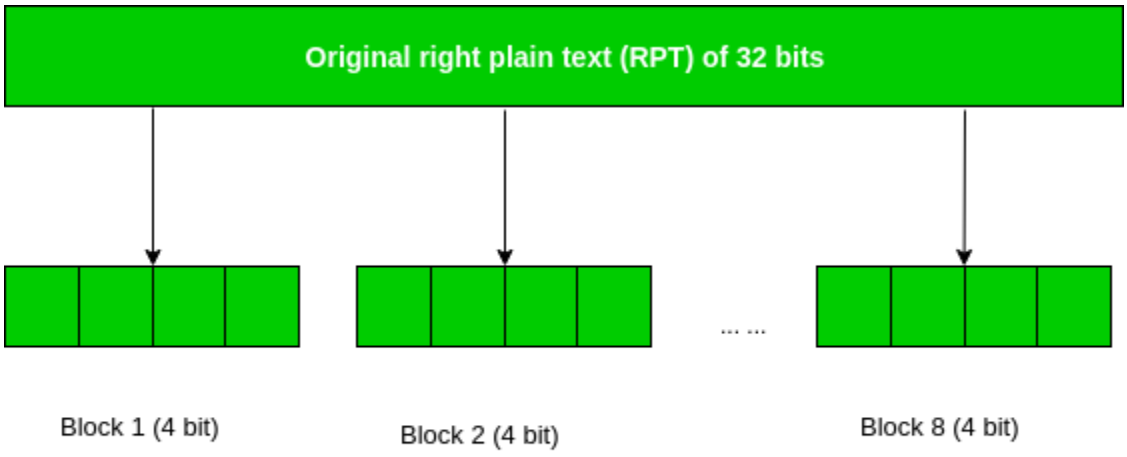


Figure - division of 32 bit RPT into 8 bit blocks

This process results in expansion as well as a permutation of the input bit while creating output. The key transformation process compresses the 56-bit key to 48 bits. Then the expansion permutation process expands the 32-bit RPT to 48-bits. Now the 48-bit key is XOR with 48-bit RPT and the resulting output is given to the next step, which is the S-Box substitution.

[[

Qs. 1)In a simplified version of DES, the 8-bit output from a round is divided into two blocks: The first block consists of the first 4 bits and the last four bits make the second block. The first block is the input for the first S box (S1) and the second block is the input for the second S-box (S2). The outputs of both the S-Boxes are then concatenated to form the final output. The S1 and S2 boxes are shown below.

S1-Box

101	010	001	110	011	100	111	000
001	100	110	010	000	111	101	011

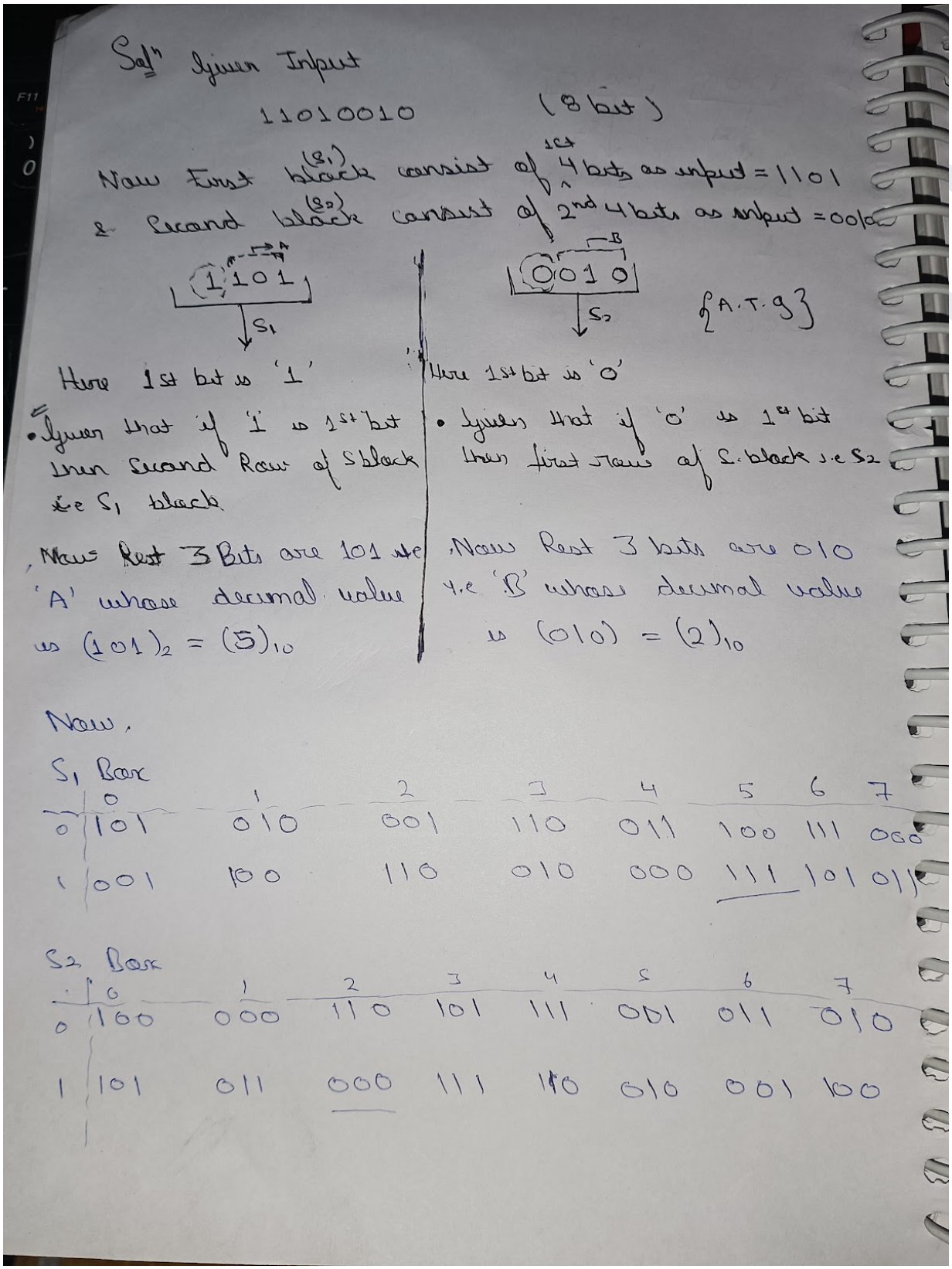
S2-Box

100	000	110	101	111	001	011	010
101	011	000	111	110	010	001	100

The S-boxes take 4 bits as input and produce 3 bits of output. The first bit of the input is used to select the row from the S-box. 0 for the first row and 1 for the second row. The last 3 bits are used to select the column. Based on this description, find the output of 11010010.[4M]

LGG_1416_2023

Answer. 1)



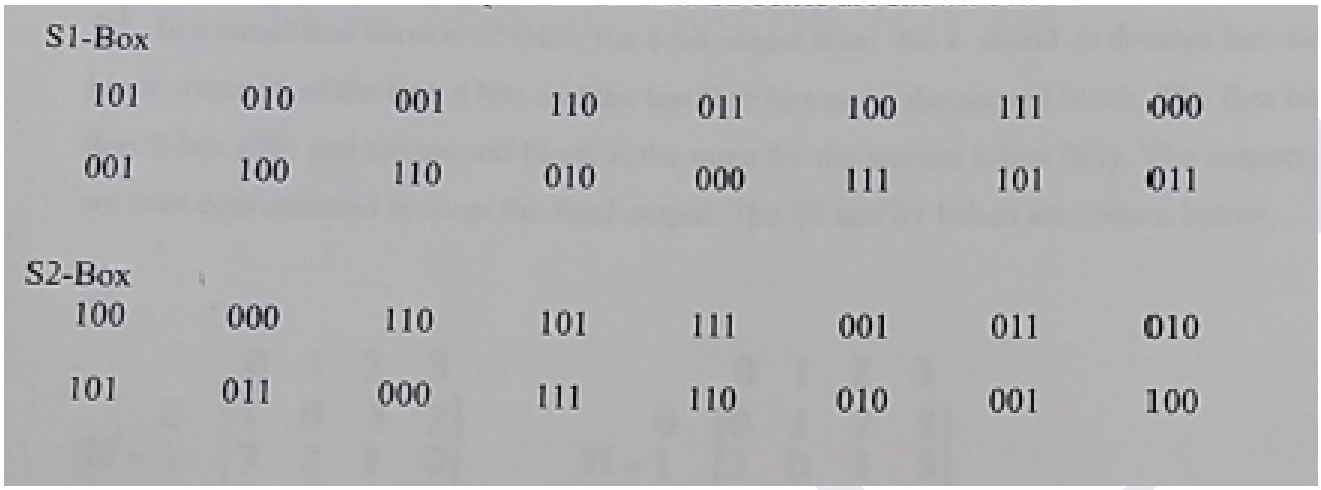
Here if we look in S_1 Block or box By using DES algorithm. The 5th column of the box in Second Row will be the output consisting of 3 bits i.e = 111

Similarly in S_2 Block, 2nd column of the block in ~~first~~ Row will be the output consisting of 3 bit i.e = 000

∴ Final output of 11010010 is "111000"

LGG_1416_2023

Qs. 2)In a simplified version of DES, the 8-bit output from a round is divided into two blocks. The first block consists of the first 4 hits and the last four bits make the second block. The first block is the input for the first S-box (S1) and the second block is the input for the second S-box (S2). The outputs of both the S-Boxes are then concatenated to form the final output. The S1 and S2 boxes are shown below.



S1-Box

101	010	001	110	011	100	111	000
001	100	110	010	000	111	101	011

S2-Box

100	000	110	101	111	001	011	010
101	011	000	111	110	010	001	100

The S-boxes take 4 bits as input and produce 3 bits of output. The first bit of the input is used to select the row from the S-box, 0 for the first row and 1 for the second row. The last 3 hits are used to select the column. Based on this description, find the output of 11011011. [4M]

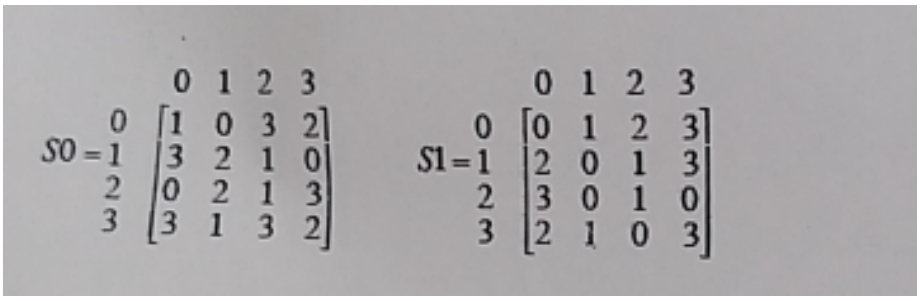
Answer. 2)

{NOTE: YE QUESTION FIRST QUESTION KI TARA HE PURA BS ISKI INPUT VALUE 11011011 HE, BAKI PROSS SAME HOGI.}

Qs. 3) (a) What is the purpose of S- Box in DES?

(b) In a simplified version of DES, the 8-hit output from the a round is divided into two blocks. The first block consists of the first 4 bits and the last four bits make the second block. The first block is the input for the first box (S0) and the second block is the input for the second S-box (S1). The outputs of both the S-Boxes are then concatenated to form the final output. The S0 and S1 boxes are shown below.

LGG_1416_2023



$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

The S-boxes operate as follows. The first and fourth input bits are treated as a 2-bit number that specify a row of the S-box, and the second and third input bits specify a column of the Sbox. The entry in that row and column, in base 2, is the 2-bit output of the S-Box. Given this information, find the output of 11010010. [5M]

Answer. 3)

(a)The role of the S-boxes in the function F is that the substitution includes a group of eight S-boxes.

Each of which take 6 bits as input and creates 4 bits as follows – The first and last bits of the input to box Si form a 2-bit binary number to choose one of four substitutions represented by the four rows in the table for Si. {where i=0,1,2,3}

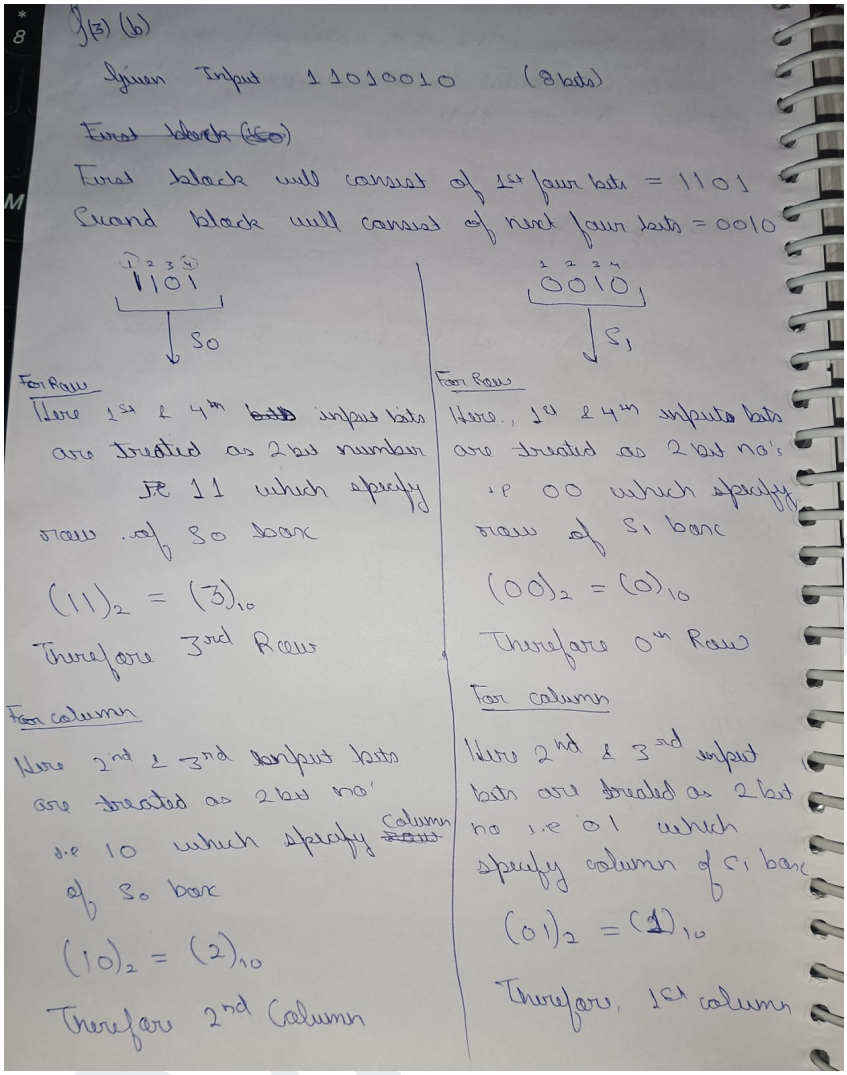
The middle four bits choose one of the sixteen columns. The decimal value in the cell chosen by the row and column is then transformed to its 4-bit description to make the output. For instance, in S1, for input 011001, the row is 01 and the column is 1100.The value in row 1, column 12 is 9, therefore the output is 1001.

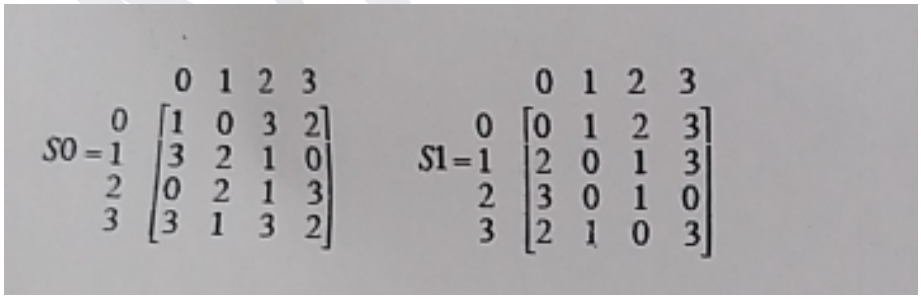
The principle of S-boxes is as follows –

- **Each S-box must have six bits of input and four bits of output.**
- **There is no output bit of an S-box should be too near to a linear function of the input bits. (The S-boxes are the only non-linear element of DES and their nonlinearity is the algorithm's strength.)**
- **Each "row" of an S-box should include all possible outputs. (This randomizes the output.)**
- **If two inputs to an S-box differ in actually one bit, their outputs must differ in minimum two bits.**
- **If two inputs to an S-box differ specifically in the middle two bits and their outputs should differ by minimum two bits.**

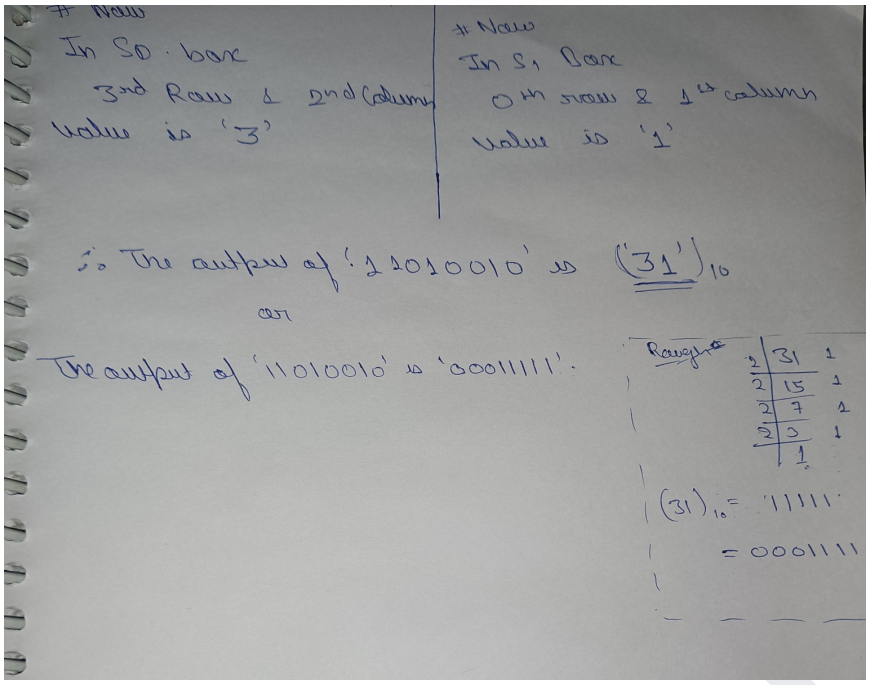
- **If two inputs to an S-box differ in their first two bits and agree on their last two, the two outputs should be dissimilar.**

(b)





$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$



Qs. 4)Discuss the purpose and procedure of S-Boxes in DES. Find the output of the input 1101 on s-box given below: [3+1M]

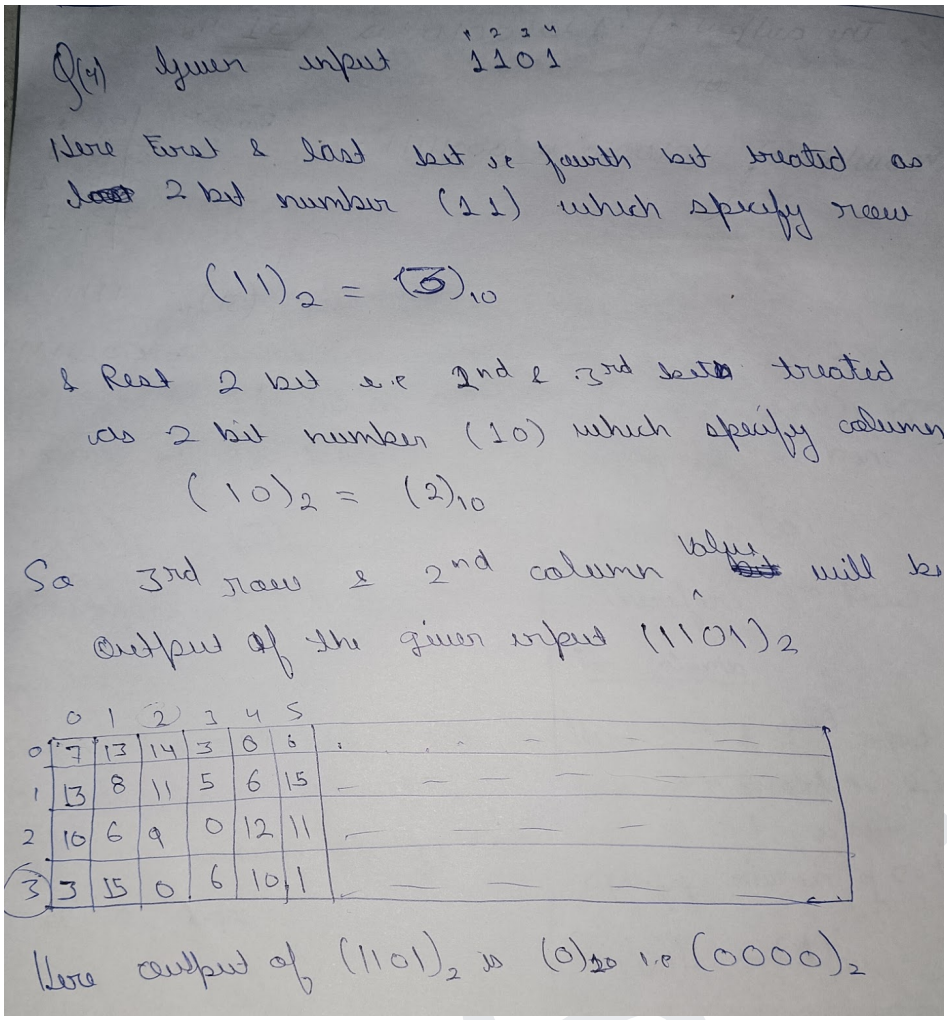
S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Answer. 4)

{NOTE: FIRST PART IS SIMILAR TO QS 3 PART (a) }

LGG_1416_2023



]]}}}

[[Qs. 1)Illustrate the use of fence register in protecting user's program.[3M]

Qs. 2)How a Fence Register can provide protection in an operating system? [5M]]]

Ans

A Fence Register is a hardware mechanism used to control the memory access of processes in an operating system. It is also known as a Memory Protection Register or a Segment Limit Register.

A Fence Register can provide protection in an operating system by setting the boundaries of the memory segments that a process can access. It is used to prevent a process from accessing memory areas that it is not authorized to access.

LGG_1416_2023

When a process tries to access memory outside the boundaries set by the Fence Register, it triggers a hardware exception, which can be handled by the operating system. This helps in preventing buffer overflow attacks and other types of memory-related security vulnerabilities.

In addition to providing memory protection, a Fence Register can also be used to implement a virtual memory system, which allows multiple processes to share the same physical memory without interfering with each other.

[[Qs. 1)Describe Buffer Overflow attack with the help of a suitable example.[5M]

Qs. 2)What is Buffer Overflow attack? Explain with suitable examples.[5M]

Qs. 3)Describe buffer overflow. What are its security implications? [5M]

Qs. 4)Write short notes on the following: [5M]

(a) Buffer overflow error]] **{NOTE: comes under "non malicious program errors"}**

Ans

Buffer overflow is a type of software vulnerability that occurs when a program writes more data to a buffer - a temporary storage area in memory - than it was designed to hold. As a result, the extra data overflows into adjacent memory areas, corrupting or overwriting data that should not be modified.

The security implications of buffer overflow can be severe. Attackers can exploit this vulnerability by sending input that exceeds the buffer size, which can cause the program to crash or behave unpredictably. In some cases, attackers can craft input that overwrites critical data, such as the return address on the stack, which can be used to execute arbitrary code or launch a denial-of-service attack.

One of the most common ways attackers exploit buffer overflow vulnerabilities is by injecting malicious code into the buffer. This code can then be executed by overwriting the return address on the stack with the address of the malicious code. This technique is known as a "stack-based buffer overflow" attack.

Another type of buffer overflow vulnerability is called a "heap-based buffer overflow". This occurs when a program allocates memory from the heap, but does not properly validate the size of the

data that is copied into the allocated buffer. This can allow an attacker to overwrite adjacent heap memory and potentially gain control of the program.

A buffer overflow vulnerability will typically occur when code:

1. Is reliant on external data to control its behavior
2. Is dependent on data properties that are enforced beyond its immediate scope
3. Is so complex that programmers are not able to predict its behavior accurately

To mitigate the security implications of buffer overflow, developers can use secure coding practices such as input validation and boundary checking to ensure that programs are not vulnerable to this type of attack.

[[Qs. 1)List three factors that should be considered when developing a security plan.[3M]

Qs. 2)Describe security planning. [5M]

Qs. 3)Describe various factors that should be considered while developing a security plan(5M)]]

Answer 1,2,3)

Developing a security plan involves considering various factors that can help ensure the security and protection of an organization's assets, data, and operations. Some of the key factors that should be considered while developing a security plan include:

1. Risk Assessment: Conducting a comprehensive risk assessment to identify potential security threats and vulnerabilities. This involves identifying assets, determining their value, and evaluating the likelihood and impact of potential threats.

2. Security Policies and Procedures: Establishing clear and concise security policies and procedures that outline how data and assets should be protected, who has access to them, and what actions should be taken in the event of a security breach.

3. Security Controls: Implementing appropriate security controls, such as firewalls, intrusion detection and prevention systems, access controls, and encryption, to mitigate security risks and protect against potential threats.

4. Employee Training and Awareness: Providing training and awareness programs for employees to educate them about security risks and how to prevent security breaches. This includes topics such as password management, social engineering, and phishing attacks.

5. Incident Response Plan: Developing an incident response plan that outlines how to respond to security incidents, including identifying and containing the incident, mitigating the damage, and recovering from the incident.

6. Compliance: Ensuring that the security plan complies with relevant laws, regulations, and industry standards, such as GDPR, HIPAA, and ISO 27001.

7. Continuous Improvement: Regularly reviewing and updating the security plan to address new threats and vulnerabilities, and to ensure that it remains effective in protecting the organization's assets and data.

Overall, developing a comprehensive security plan involves considering a wide range of factors to ensure that the organization is adequately protected against potential threats and risks.

[[Qs. 1)Write short notes on the following: [5]

(a)Cryptanalysis

Qs. 2)Define the following [2+2M]

(a) Cryptography

(b) Cryptanalysis

Qs. 3)Differentiate between cryptography and cryptanalysis. Explain Symmetric Key cryptography with the help of a diagram. [3M]]]

Answer. 1,2,3)

Cryptography refers to the process of encoding information in a way that only authorized parties can decode and understand it. Cryptography is used to protect the confidentiality, integrity, and authenticity of information, and it is achieved through various techniques such as encryption, digital signatures, and hash functions.

Cryptanalysis is the study of ciphertext, ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them. For example, cryptanalysts seek to decrypt ciphertexts without knowledge of the plaintext source, encryption key or the algorithm used to encrypt it; cryptanalysts also target secure hashing, digital signatures and other cryptographic algorithms.

LGG_1416_2023

A symmetric encryption scheme has five ingredients (Figure 3.1):

■ **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.

■ **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.

■ **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

■ **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible

■ **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

Symmetric key cryptography is a type of encryption technique that uses the same key for both encryption and decryption of the message. This means that the same secret key is used to both encrypt and decrypt the message

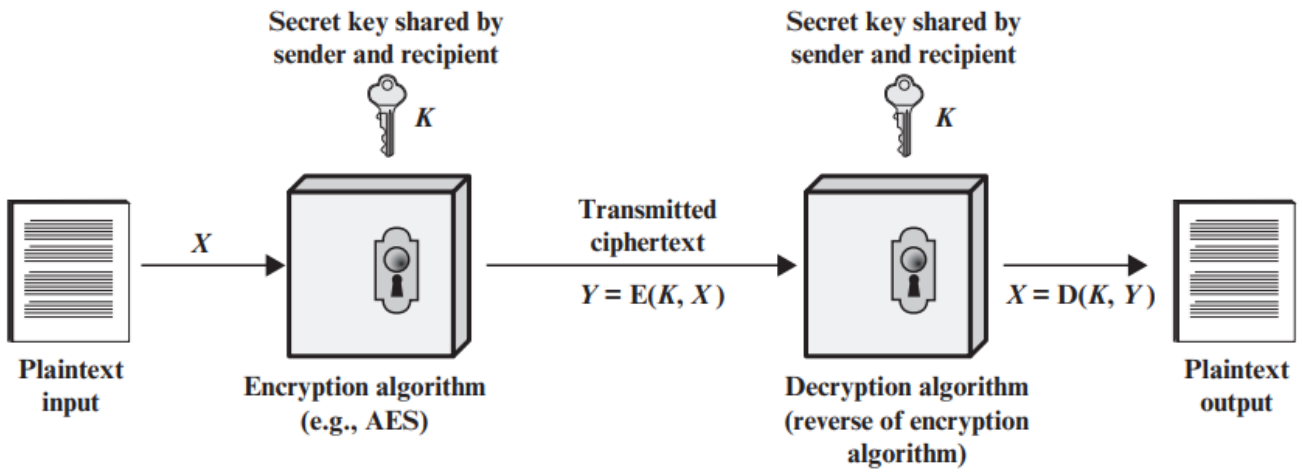


Figure 3.1 Simplified Model of Symmetric Encryption

LGG_1416_2023

[[Qs. 1)What is a Firewall? Give the names of the types of Firewall.[4M]

Qs. 2)What is a firewall? Explain various types of firewalls. [5M]]]

Ans

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and an untrusted external network, such as the internet, and helps to prevent unauthorized access, data theft, and other malicious activities.

There are several types of firewalls, including:

1. Packet Filtering Firewall: This is the simplest type of firewall that filters incoming and outgoing packets based on predefined rules, such as source and destination IP addresses, ports, and protocols. It examines each packet and either allows or blocks it based on the rules.

2. Stateful Inspection Firewall: This type of firewall is an advanced version of packet filtering firewall that keeps track of the state of network connections. It examines the packets and the context of the connection, such as the source and destination IP addresses, ports, and protocols, to determine if they are part of an existing connection or a new connection. It allows only the packets that are part of an established connection and blocks all others.

3. Application Firewall: This type of firewall works at the application layer and filters traffic based on the content of the packets, such as the type of application, data in the packets, and the commands used. It can identify and block specific applications or protocols, such as email, web browsing, and file sharing.

4. Next-Generation Firewall: This is an advanced type of firewall that combines traditional firewall functionality with additional security features, such as intrusion prevention, antivirus, and web filtering. It provides granular control over network traffic and can block advanced threats, such as malware and zero-day attacks.

5. Proxy Firewall: This type of firewall acts as an intermediary between the user and the internet. It intercepts all network traffic and replaces the source IP address with its own, making it difficult for attackers to identify the user's location. It can also filter web content and block access to malicious websites.

Overall, firewalls are essential network security tools that provide protection against a wide range of threats and attacks. The type of firewall you choose depends on your specific security requirements and the level of protection you need.

LGG_1416_2023

[[Qs. 1)Give the security requirements of a database system.[5M]

Qs. 2)Explain the security requirements of a database system. [3M]

Qs. 3)List out the security requirements of a database. [5M]]]

Ans

The security requirements of a database typically include:

1. Authentication: This refers to the process of verifying the identity of users who access the database. Authentication mechanisms such as usernames and passwords, biometric authentication, and multi-factor authentication help to ensure that only authorized users can access the database.

2. Authorization: This refers to the process of granting or denying access to specific resources within the database. Authorization mechanisms such as access control lists, roles, and permissions help to ensure that users can only access the data and functions they are authorized to use.

3. Data encryption: This involves the use of encryption algorithms to protect sensitive data from unauthorized access. Data can be encrypted at rest (i.e., stored in an encrypted format) and in transit (i.e., encrypted while being transmitted between systems).

4. Auditing and logging: This involves the recording of all activities and changes made to the database. Audit logs can be used to detect and investigate security incidents and to ensure compliance with regulatory requirements.

5. Backup and recovery: This involves regularly backing up the database to ensure that data can be restored in the event of data loss or corruption. Backup and recovery procedures should be tested regularly to ensure that data can be recovered quickly and accurately.

6. Vulnerability management: This involves regularly identifying and patching security vulnerabilities in the database software and associated applications. Vulnerability management can help to prevent unauthorized access and data breaches.

Overall, implementing these security requirements can help to ensure the confidentiality, integrity, and availability of a database and its data.

LGG_1416_2023

[[Qs. 1)Describe covert channel. List any two covert channels: [3M]

Qs. 2)Describe Covert channels. Explain any two types of covert channels. [2+3M]]]

Ans

Covert channels are communication channels that are hidden from normal security controls and are used to transfer information in a stealthy and unauthorized manner. These channels can be used by attackers to bypass security measures and steal sensitive data, or by insiders to leak confidential information.

There are several types of covert channels, including:

1. Timing Covert Channels: Timing channels exploit variations in the timing of system events to communicate information. For example, an attacker may use delays in network traffic or variations in CPU utilization to transmit data. Another example is a technique called steganography, in which information is hidden within other data, such as an image or audio file.

2. Storage Covert Channels: Storage channels use storage resources, such as disk space or memory, to store and transmit data. For example, an attacker may use unused disk space to store encrypted data that can later be retrieved by another party. Another example is a technique called data hiding, in which data is hidden within legitimate data structures, such as file headers or unused memory blocks.

3. Protocol Covert Channels: Protocol channels use variations in the behavior of network protocols to transmit data. For example, an attacker may use variations in the timing or size of network packets to transmit data that is hidden within legitimate traffic.

Overall, covert channels can be difficult to detect and prevent because they are designed to bypass security controls. However, security measures such as access controls, network segmentation, and encryption can help to reduce the risk of covert channel attacks. It is also important to regularly monitor and analyze network traffic to detect any suspicious behavior or patterns.

[[Qs. 1)Explain the different types of intrusion detection systems. [5M]

Qs. 2)What do you mean by Intrusion Detection and Prevention System? Explain any two types of IDPS. [1+2+2M]

LGG_1416_2023

Qs. 3)What do you mean by Intrusion Detection and Prevention System? Explain any two types of IDPS. [5M]]]

An Intrusion Detection and Prevention System (IDPS) is a network security technology that monitors network traffic and system activity for signs of malicious activity, such as unauthorized access attempts, malware infections, and network attacks. IDPSs work by analyzing network traffic patterns and comparing them against a database of known attack signatures, or by using behavioral analysis techniques to identify abnormal activity.

- **Network-based intrusion prevention system (NIPS):** Network-based intrusion prevention systems monitor entire networks or network segments for malicious traffic. This is usually done by analyzing protocol activity. If the protocol activity matches against a database of known attacks, the corresponding information isn't allowed to get through. NIPS are usually deployed at network boundaries, behind firewalls, routers, and remote access servers.
- **Wireless intrusion prevention system (WIPS):** Wireless intrusion prevention systems monitor wireless networks by analyzing wireless networking specific protocols. While WIPS are valuable within the range of an organization's wireless network, these systems don't analyze higher network protocols such as transmission control protocol (TCP). Wireless intrusion prevention systems are deployed within the wireless network and in areas that are susceptible to unauthorized wireless networking.
- **Network behavior analysis (NBA) system:** While NIPS analyze deviations in protocol activity, network behavior analysis systems identify threats by checking for unusual traffic patterns. Such patterns are generally a result of policy violations, malware-generated attacks, or distributed denial of service (DDoS) attacks. NBA systems are deployed in an organization's internal networks and at points where traffic flows between internal and external networks.
- **Host-based intrusion prevention system (HIPS)**: Host-based intrusion prevention systems differ from the rest in that they're deployed in a single host. These hosts are critical servers with important data or publicly accessible servers that can become gateways to internal systems. The HIPS monitors the traffic flowing in and out of that particular host by monitoring running processes, network activity, system logs, application activity, and configuration changes

[[Qs. 1)Explain various techniques of Viruses gaining control over a program with the help of suitable diagrams. [5M]

Qs. 2)Describe different kinds of malicious codes. Also explain how viruses attach ? [7M]

Qs. 3)Describe how the viruses are attached with the programs? [5M]

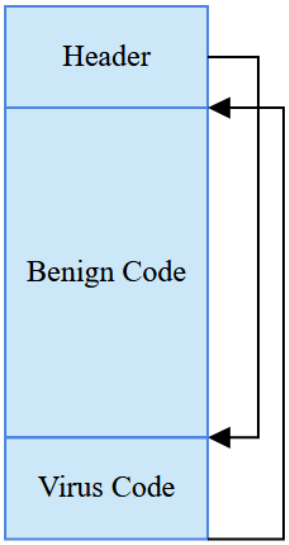
LGG_1416_2023

Qs. 4)Explain the various ways of virus attachments to a program. [4M]

Qs. 5)Describe how does the viruses gain control.[4M]]]

Viruses are malicious software programs that can infect computers and cause harm. One of the primary objectives of a virus is to gain control over a program, so that it can execute its malicious code. There are various techniques that viruses use to gain control over a program. Here are some of the most common techniques, along with suitable diagrams

1. Appending Technique: In this technique, the virus attaches itself to the end of a legitimate program, and modifies the program's entry point to point to the virus code. When the program is executed, the virus code runs first, and then passes control back to the legitimate program. The following diagram illustrates the appending technique:



2. Prepending Technique: This technique is similar to the appending technique, except that the virus code is added to the beginning of the program, rather than the end. The program's entry point is again modified to point to the virus code. The following diagram illustrates the prepending technique:

{will be same as appending place virus code in first}

3. Overwriting Technique: In this technique, the virus overwrites a section of the legitimate program's code with its own code. The virus then modifies the program's entry point to point to the virus code. When the program is executed, the virus code runs instead of the legitimate code.

4. Code Injection Technique: In this technique, the virus injects its code into the legitimate program's memory space, and then modifies the program's entry point to point to the virus code. When the program is executed, the virus code runs instead of the legitimate code.

It's worth noting that these techniques are just a few of the ways that viruses can gain control over a program. There are many other techniques that viruses can use, and new techniques are constantly being developed as antivirus software evolves to counter them.

[[Qs. 1)Explain the steps of Diffie-Hellman Key exchange protocol. What is the most common attack on this protocol? [5M]

Qs. 2) (a)Explain the steps of Diffie-Hellman Key exchange protocol. What is the most common attack on this protocol ? [5M]]]

Answer. 1 and 2)

The Diffie-Hellman key exchange protocol is a method for two parties to establish a shared secret key over an insecure channel. The protocol works as follows:

Step 1: Initialization

- Alice and Bob agree on a large prime number p and a primitive root g mod p.

- They keep p and g public and choose their own secret values a and b respectively.

Step 2: Public Key Exchange

- Alice computes A = g^a mod p and sends it to Bob.

- Bob computes B = g^b mod p and sends it to Alice.

Step 3: Secret Key Calculation

LGG_1416_2023

- Alice computes s = B^a mod p.

- Bob computes s = A^b mod p.

At this point, Alice and Bob both have the same secret key s, which they can use to encrypt their messages using a symmetric encryption algorithm.

The most common attack on the Diffie-Hellman key exchange protocol is the Man-in-the-Middle (MITM) attack. In this attack, an attacker intercepts the public keys A and B being exchanged between Alice and Bob, and then sends his own public key to each of them instead. This means that Alice and Bob each end up with a different secret key, one shared with the attacker, which can be used to decrypt all messages sent between Alice and Bob. To prevent this attack, a secure communication channel is required between Alice and Bob, or an authentication mechanism must be used to verify the public keys exchanged. One such mechanism is the use of digital signatures.

[[Qs. 1)Define Generator and Parity Check Matrix. [2M]

Qs. 2)How can parity check matrix be used to generate codeword? [2M]]]

Answer. 1 and 2)

Generator Matrix:

A generator matrix is a simple, yet particularly clever means of generating codes. They are an identity matrix combined with an arbitrary matrix. Multiplying a message in row matrix form by a generator matrix produces a codeword. the remainder of this section is step-by-step instructions for creating a generator matrix that will produce a code with eight codewords.

The first step is to define an identity matrix which is a matrix that any given matrix can be multiplied by without changing the value of the given matrix. This is accomplished by setting the principal diagonal elements to one and leaving the rest as zero. See figure one for an example. The matrix is of order three because a three-digit binary string can represent eight possible values which is the number of desired codewords.

3 X 3 Identity Matrix

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Figure 1

The next step is to define an arbitrary matrix (denoted by A). The size of the matrix determines the size of generated codewords. If m is the size of the identity matrix, and n is the desired length of codewords, then the arbitrary matrix should be of size m *(n-m). Six digit codewords suffice for the purposes of this article; therefore, the arbitrary matrix must be sized three by three (3*3)(six-digit length minus three-digit identity). Figure two is A as used by the remaining examples.

Arbitrary Matrix for 6 Digit Codewords

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Figure 2

The only thing left to do is combine the two matrices above together to form G. It's as simple as placing them side by side as shown in figure three.

Generator Matrix

$$G = [I_3|A]$$

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Figure 3

With the generator matrix (G) in hand, generating codewords is trivial. Multiplying any three-digit binary message in row matrix form produces a codeword. For example, the message 011 becomes

the codeword 011110 as shown in figure four. Notice the codeword is the original message with three parity bits appended. This happens because the generator matrix begins with an identity matrix.

Generating Codewords from Messages

$$[0 \quad 1 \quad 1]G = [0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0]$$

Figure 4

Parity Check Matrices:

Parity check matrices are derived from generator matrices. They are used during the decoding process to expose and correct errors introduced during transmission. Multiplying a parity check matrix by the transpose of a codeword exposes errors.

A parity check matrix (denoted as H) consists of the transpose of the arbitrary matrix combined with the identity matrix. As a refresher, the transpose of a matrix is simply the matrix flipped across it's diagonal so that the (i,j)th element in the matrix becomes the (j,i)th element. Figure 8 shows the parity check matrix that corresponds to the generator matrix from the running example.

Parity Check Matrix

$$H = [A^t | I_3]$$

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Figure 8

Multiplying the transpose of any valid codeword by the parity check matrix produces a zero-value result as demonstrated in figure 9.

Validating Code Words with H

$$H\begin{pmatrix}0\\1\\1\\1\\1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}, \quad H\begin{pmatrix}1\\1\\1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$$

Figure 9

Changing any of the bits in the codeword produces a non-zero result which indicates an error. Consider 011010, as shown in figure ten. The result does not equal zero so at least one of the bits is erroneous.

Invalid Codeword

$$H\begin{pmatrix}0\\1\\1\\0\\1\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix}$$

Figure 10

After identifying an inaccurate codeword, it may be possible to correct it using H. Continuing with the example above; the product of the codeword and H is equal to the fourth column in H. This indicates an error in the fourth bit and changing the fourth bit produces the correct codeword. See figure eleven for an illustration.

LGG_1416_2023

Error Checking with Parity Check Matrix

$$H\begin{pmatrix}0\\1\\1\\0\\1\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix}$$

$$H=\begin{bmatrix}1&0&1&1&0&0\\1&1&0&0&1&0\\0&1&1&0&0&1\end{bmatrix}$$

Error in 4th Column = 4th Bit is Erroneous

Figure 11

Because the example code is only capable of correcting a single error, changing more than one bit generates an irrecoverable codeword. However, with a more complex code, it is possible to correct multiple errors using the distinct sum of H rows and the nearest neighbor method.

[[Qs. 1)Explain the different phases of security systems development Life Cycle. [6M]

Qs. 2)Explain briefly the key principles of security? [3M]]]

Qs. 3)Discuss various aspects to be considered in computer security. [6M]

Answer. 1)

The Security System Development Life Cycle (SSDLC) is a framework used to manage the development, maintenance, and retirement of an organization's information security systems. The SSDLC is a cyclical process that includes the following phases:

Planning: During this phase, the organization identifies its information security needs and develops a plan to meet those needs. This may include identifying potential security risks and vulnerabilities, and determining the appropriate controls to mitigate those risks.

LGG_1416_2023

Analysis: During this phase, the organization analyzes its information security needs in more detail and develops a detailed security requirements specification.

Design: During this phase, the organization designs the security system to meet the requirements developed in the previous phase. This may include selecting and configuring security controls, such as firewalls, intrusion detection systems, and encryption.

Implementation: During this phase, the organization develops, tests, and deploys the security system.

Maintenance: After the security system has been deployed, it enters the maintenance phase, where it is updated, maintained, and tweaked to meet the changing needs of the organization.

Retirement: Eventually, the security system will reach the end of its useful life and will need to be retired. During this phase, the organization will plan for the replacement of the system, and ensure that data stored in it is properly preserved.

Answer. 2,3)

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

Confidentiality

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

Integrity

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

Availability

LGG_1416_2023

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers.

[[Qs. 1)Explain various types of attack in detail. [4M]

Qs. 2)List and explain any four types of deliberate software attacks. [4M]

Qs. 3)Describe the different categories of Attacks on Networks? [5M]]]

Answer. 1,2,3)

1. DoS and DDoS Attacks

A denial-of-service (DoS) attack is designed to overwhelm the resources of a system to the point where it is unable to reply to legitimate service requests. A distributed denial-of-service (DDoS) attack is similar in that it also seeks to drain the resources of a system. A DDoS attack is initiated by a vast array of malware-infected host machines controlled by the attacker. These are referred to as "denial of service" attacks because the victim site is unable to provide service to those who want to access it.

2. MITM Attacks

Man-in-the-middle (MITM) types of cyber attacks refer to breaches in cybersecurity that make it possible for an attacker to eavesdrop on the data sent back and forth between two people, networks, or computers. It is called a "man in the middle" attack because the attacker positions themselves in the "middle" or between the two parties trying to communicate. In effect, the attacker is spying on the interaction between the two parties.

Some ways to protect yourself and your organization from MITM attacks is by using strong encryption on access points or to use a virtual private network (VPN).

3. Phishing Attacks

LGG_1416_2023

A phishing attack occurs when a malicious actor sends emails that seem to be coming from trusted, legitimate sources in an attempt to grab sensitive information from the target. Phishing attacks combine social engineering and technology and are so-called because the attacker is, in effect, “fishing” for access to a forbidden area by using the “bait” of a seemingly trustworthy sender.

To execute the attack, the bad actor may send a link that brings you to a website that then fools you into downloading malware such as viruses, or giving the attacker your private information.

4. Whale-phishing Attacks

A whale-phishing attack is so-named because it goes after the “big fish” or whales of an organization, which typically include those in the C-suite or others in charge of the organization. These individuals are likely to possess information that can be valuable to attackers, such as proprietary information about the business or its operations.

5. Spear-phishing Attacks

Spear phishing refers to a specific type of targeted phishing attack. The attacker takes the time to research their intended targets and then write messages the target is likely to find personally relevant. These types of attacks are aptly called “spear” phishing because of the way the attacker hones in on one specific target. The message will seem legitimate, which is why it can be difficult to spot a spear-phishing attack.

6. Ransomware

With Ransomware, the victim’s system is held hostage until they agree to pay a ransom to the attacker. After the payment has been sent, the attacker then provides instructions regarding how the target can regain control of their computer. The name "ransomware” is appropriate because the malware demands a ransom from the victim.

7. Password Attack

Passwords are the access verification tool of choice for most people, so figuring out a target’s password is an attractive proposition for a hacker.

LGG_1416_2023

{NOT IMPORTANT BUT INFORMATIVE: An attacker may also try to intercept network transmissions to grab passwords not encrypted by the network. They can also use social engineering, which convinces the target to input their password to solve a seemingly "important" problem. In other cases, the attacker can simply guess the user's password, particularly if they use a default password or one that is easy to remember such as "1234567."

Attackers also often use brute-force methods to guess passwords. A brute-force password hack uses basic information about the individual or their job title to try to guess their password. For example, their name, birthdate, anniversary, or other personal but easy-to-discover details can be used in different combinations to decipher their password. Information that users put on social media can also be leveraged in a brute-force password hack. What the individual does for fun, specific hobbies, names of pets, or names of children are sometimes used to form passwords, making them relatively easy to guess for brute-force attackers.

A hacker can also use a dictionary attack to ascertain a user's password. A dictionary attack is a technique that uses common words and phrases, such as those listed in a dictionary, to try and guess the target's password.

One effective method of preventing brute-force and dictionary password attacks is to set up a lock-out policy. This locks out access to devices, websites, or applications automatically after a certain number of failed attempts. With a lock-out policy, the attacker only has a few tries before they get banned from access. If you have a lockout policy in place already and discover that your account has been locked out because of too many login attempts, it is wise to change your password.

If an attacker systematically uses a brute-force or dictionary attack to guess your password, they may take note of the passwords that did not work. For example, if your password is your last name followed by your year of birth and the hacker tries putting your birth year before your last name on the final attempt, they may get it right on the next try.}

8. SQL Injection Attack

Structured Query Language (SQL) injection is a common method of taking advantage of websites that depend on databases to serve their users. Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server. The command is inserted, or "injected", into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated.

9. URL Interpretation

With URL interpretation, attackers alter and fabricate certain URL addresses and use them to gain access to the target's personal and professional data. This kind of attack is also referred to as URL poisoning. The name "URL interpretation" comes from the fact that the attacker knows the order in which a web-page's URL information needs to be entered. The attacker then "interprets" this syntax, using it to figure out how to get into areas they do not have access to.

10. DNS Spoofing

With Domain Name System (DNS) spoofing, a hacker alters DNS records to send traffic to a fake or "spoofed" website. Once on the fraudulent site, the victim may enter sensitive information that can be used or sold by the hacker. The hacker may also construct a poor-quality site with derogatory or inflammatory content to make a competitor company look bad.

To prevent DNS spoofing, make sure your DNS servers are kept up-to-date. Attackers aim to exploit vulnerabilities in DNS servers, and the most recent software versions often contain fixes that close known vulnerabilities.

11. Trojan Horses

A Trojan horse attack uses a malicious program that is hidden inside a seemingly legitimate one. When the user executes the presumably innocent program, the malware inside the Trojan can be used to open a backdoor into the system through which hackers can penetrate the computer or network. This threat gets its name from the story of the Greek soldiers who hid inside a horse to infiltrate the city of Troy and win the war. Once the "gift" was accepted and brought within the gates of Troy, the Greek soldiers jumped out and attacked. In a similar way, an unsuspecting user may welcome an innocent-looking application into their system only to usher in a hidden threat.

To prevent Trojan attacks, users should be instructed not to download or install anything unless its source can be verified. Also, NGFWs can be used to examine data packets for potential threats of Trojans.

12. Eavesdropping Attacks

Eavesdropping attacks involve the bad actor intercepting traffic as it is sent through the network. In this way, an attacker can collect usernames, passwords, and other confidential information like credit cards. Eavesdropping can be active or passive.

With active eavesdropping, the hacker inserts a piece of software within the network traffic path to collect information that the hacker analyzes for useful data. Passive eavesdropping attacks are different in that the hacker "listens in," or eavesdrops, on the transmissions, looking for useful data they can steal.

Both active and passive eavesdropping are types of MITM attacks. One of the best ways of preventing them is by encrypting your data, which prevents it from being used by a hacker, regardless of whether they use active or passive eavesdropping.

13. Birthday Attack

In a birthday attack, an attacker abuses a security feature: hash algorithms, which are used to verify the authenticity of messages. The hash algorithm is a digital signature, and the receiver of the message checks it before accepting the message as authentic. If a hacker can create a hash that is identical to what the sender has appended to their message, the hacker can simply replace the sender's message with their own. The receiving device will accept it because it has the right hash.

The name "birthday attack" refers to the birthday paradox, which is based on the fact that in a room of 23 people, there is more than a 50% chance that two of them have the same birthday. Hence, while people think their birthdays, like hashes, are unique, they are not as unique as many think.

To prevent birthday attacks, use longer hashes for verification. With each extra digit added to the hash, the odds of creating a matching one decrease significantly.

14. Malware Attack

Malware is a general term for malicious software, hence the "mal" at the start of the word. Malware infects a computer and changes how it functions, destroys data, or spies on the user or network traffic as it passes through. Malware can either spread from one device to another or remain in place, only impacting its host device.

Several of the attack methods described above can involve forms of malware, including MITM attacks, phishing, ransomware, SQL injection, Trojan horses, drive-by attacks, and XSS attacks.

In a malware attack, the software has to be installed on the target device. This requires an action on the part of the user. Therefore, in addition to using firewalls that can detect malware, users

should be educated regarding which types of software to avoid, the kinds of links they should verify before clicking, and the emails and attachments they should not engage with.

[[Qs. 1)Explain Incomplete Mediation with the help of an example. Also discuss its security implications[5M] {NOTE: comes under "non malicious program errors"}

Qs. 2)Discuss the problem of incomplete mediation with example. [3M]]]

Incomplete Mediation

- Technically, incomplete mediation means that data is exposed somewhere in the pathway between submission and acceptance
- The ultimate problem is the successful submission and acceptance of bad data
- The cause of the problem is the break, or lack of security in the pathway

Consider the example of the previous section:

http://www.somesite.com/subpage/userinput&parm1=(808)555-1212&parm2=2004Jan01

The two parameters look like a telephone number and a date. Probably the client's (user's) web browser enters those two values in their specified format for easy processing on the server's side. What would happen if parm2 were submitted as 1800Jan01? Or 1800Feb30? Or 2048Min32? Or 1Aardvark2Many?

Something would likely fail. As with buffer overflows, one possibility is that the system would fail catastrophically, with a routine's failing on a data type error as it tried to handle a month named "Min" or even a year (like 1800) which was out of range. Another possibility is that the receiving program would continue to execute but would generate a very wrong result. (For example, imagine the amount of interest due today on a billing error with a start date of 1 Jan 1800.) Then again, the processing server might have a default condition, deciding to treat 1Aardvark2Many as 3 July 1947. The possibilities are endless.

One way to address the potential problems is to try to anticipate them. For instance, the programmer in the examples above may have written code to check for correctness on the *client*'s side (that is, the user's browser). The client program can search for and screen out errors. Or, to prevent the use of nonsense data, the program can restrict choices only to valid ones. For example, the program supplying the parameters might have solicited them by using a drop-down box or choice list from which only the twelve conventional months would have been possible choices. Similarly, the year could have been tested to ensure that the value was between 1995 and 2005, and date numbers would have to have been appropriate for the months in which they occur (no 30th of February, for example). Using these verification techniques, the programmer may have felt well insulated from the possible problems a careless or malicious user could cause.

However, the program is still vulnerable. By packing the result into the return URL, the programmer left these data fields in a place accessible to (and changeable by) the user. In particular, the user could edit the URL line, change any parameter values, and resend the line. On the server side, there is no way for the server to tell if the response line came from the client's browser or as a result of the user's editing the URL directly. We say in this case that the data values are not completely mediated: The sensitive data (namely, the parameter values) are in an exposed, uncontrolled condition.

Security Implication

Incomplete mediation is easy to exploit, but it has been exercised less often than buffer overflows. Nevertheless, unchecked data values represent a serious potential vulnerability.

To demonstrate this flaw's security implications, we use a real example; only the name of the vendor has been changed to protect the guilty. Things, Inc., was a very large, international vendor of consumer products, called Objects. The company was ready to sell its Objects through a web site, using what appeared to be a standard e-commerce application. The management at Things decided to let some of its in-house developers produce the web site so that its customers could order Objects directly from the web.

To accompany the web site, Things developed a complete price list of its Objects, including pictures, descriptions, and drop-down menus for size, shape, color, scent, and any other properties. For example, a customer on the web could choose to buy 20 of part number 555A Objects. If the price of one such part were $10, the web server would correctly compute the price of the 20 parts to be $200. Then the customer could decide whether to have the Objects shipped by boat, by ground transportation, or sent electronically. If the customer were to choose boat delivery, the customer's web browser would complete a form with parameters like these:

http://www.things.com/order/final&custID=101&part=555A
&qy=20&price=10&ship=boat&shipcost=5&total=205

So far, so good; everything in the parameter passage looks correct. But this procedure leaves the parameter statement open for malicious tampering. Things should not need to pass the price of the items back to itself as an input parameter; presumably Things knows how much its Objects cost, and they are unlikely to change dramatically since the time the price was quoted a few screens earlier.

LGG_1416_2023

A malicious attacker may decide to exploit this peculiarity by supplying instead the following URL, where the price has been reduced from $205 to $25:

http://www.things.com/order/final&custID=101&part=555A
&qy=20&price=1&ship=boat&shipcost=5&total=25

Surprise! It worked. The attacker could have ordered Objects from Things in any quantity at any price. And yes, this code was running on the web site for a while before the problem was detected. From a security perspective, the most serious concern about this flaw was the length of time that it could have run undetected. Had the whole world suddenly made a rush to Things's web site and bought Objects at a fraction of their price, Things probably would have noticed. But Things is large enough that it would never have detected a few customers a day choosing prices that were similar to (but smaller than) the real price, say 30 percent off. The e-commerce division would have shown a slightly smaller profit than other divisions, but the difference probably would not have been enough to raise anyone's eyebrows; the vulnerability could have gone unnoticed for years. Fortunately Things hired a consultant to do a routine review of its code, and the consultant found the error quickly.

[[Qs. 1)Differentiate between confusion and diffusion. [2M]

Qs. 2)Describe the concept of Diffusion and confusion. [4M]]]

Ans

In cryptography, confusion and diffusion are two properties of the operation of a secure cipher. Both Confusion and Diffusion are used to stop the deduction of the secret writing key, these properties, when present, work to thwart the application of statistics and other methods of cryptanalysis.

Confusion is employed for making uninformed cipher text whereas diffusion is employed for increasing the redundancy of the plain text over the foremost part of the cipher text to make it obscure. The stream cipher solely depends on confusion, where else, diffusion is employed by both stream and block cipher.

Features	Confusion	Diffusion

LGG_1416_2023

Definition	**It is a cryptography technique utilized to create vague ciphertext.**	**It is employed to generate cryptic plain texts.**
Achieved through	**It is achieved via the substitution technique.**	**It is achieved via the transposition technique.**
Seeks to	**The relationship between the ciphertext statistics and the encryption key value is complicated.**	**The plain text's statistical structure is dispersed into the ciphertext's long-range statistics.**
Used by	**It utilizes only block cipher.**	**It utilizes both stream and block cipher.**
Modifications	**If one bit in secret is changed, most bits in the cipher text will be changed.**	**If one image within the plain text changes, most images within the cipher text will also change.**
Resultant	**Vagueness is increased**	**Redundancy is increased**
Relations	**It conceals the relation between the key and the ciphertext.**	**It conceals the relation between the plaintext and the ciphertext.**

LGG_1416_2023

{Note: Question on vulnerability

[[Qs. 1)Describe hardware vulnerabilities in detail. [4M]

Qs. 2)Describe software vulnerabilities in detail. [4M]

Qs. 3)List different types of vulnerabilities ? Explain software vulnerability. [4M]

Qs. 4)Explain vulnerability scanner. How is it used to improve security? [2M]]] }

Answer. 1,2,3)

Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving, the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

1. Hardware Vulnerability:

A hardware vulnerability is a weakness which can be used to attack the system hardware physically or remotely.
For examples:

1. **Old version of systems or devices**
2. **Unprotected storage**
3. **Unencrypted devices, etc.**

2. Software Vulnerability:

A software error in development or configuration such as the execution of it can violate the security policy. For examples:

1. **Lack of input validation**
2. **Unverified uploads**
3. **Cross-site scripting**
4. **Unencrypted data, etc.**

3. Network Vulnerability:

A weakness happens in a network which can be hardware or software.

For examples:

1. Unprotected communication
2. Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
3. Social engineering attacks
4. Misconfigured firewalls

4. Procedural Vulnerability:

A weakness happen in an organization operational methods.

For examples:

1. Password procedure – Password should follow the standard password policy.
2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

Answer. 4)

A vulnerability scanner is a software designed for testing applications or computers for vulnerabilities. It identifies and creates a directory for each process connected to the system(eg. firewalls, servers, networks, etc). Vulnerabilities are identified from misconfigurations and flawed programming within a given network. The probability of risks in a system is identified by the vulnerabilities present.

Working of Vulnerability Scanning

The vulnerability scanning works on a three-step procedure. They are as follows:

- Vulnerabilities Identification
- Analysis of the risk possessed by vulnerabilities found
- Operations against the identifies Vulnerability

LGG_1416_2023

{ONLY ONE}

Qs. 1)Describe how Access List is used to protect general objects in a system. Discuss its limitations[4M]

Answer. 1)

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd, and so on.
2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.
3. There is an implicit denial at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

Advantages of ACL –

- **Improve network performance.**
- **Provides security as the administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.**
- **Provides control over the traffic as it can permit or deny according to the need of the network.**

Limitation of Access-list: ??????

LGG_1416_2023

Qs. 2)Describe how directory approach is used to protect general objects in a system. Discuss its limitations [4M]

Answer. 2)

The directory approach, also known as the access control list (ACL) approach, is a method used to protect general objects within a system in information security. It involves the use of a directory or a list that specifies the access permissions for different users or groups of users on specific objects.

In this approach, each object in the system has an associated access control list that defines the access rights for various users or groups. The access control list typically includes entries that specify the permissions, such as read, write, execute, delete, or modify, that are granted or denied to different entities.

When a user requests access to an object, the system checks the access control list to determine whether the user's access rights match the permissions specified in the list. If the user's permissions align with the access control list, access is granted; otherwise, it is denied.

The directory approach offers several advantages in protecting general objects within a system:

1. Granular Control: It provides a fine-grained level of control over access permissions. Each user or group can have specific privileges assigned to them, allowing for precise control over who can perform what actions on an object.

2. Flexibility: The access control lists can be easily modified to adjust the permissions as needed. It allows for dynamic changes in access rights without requiring significant changes to the underlying system.

3. Scalability: The directory approach can scale well as the number of objects and users increases. It can handle a large number of objects and effectively manage access control for different entities.

However, the directory approach has limitations that can impact information security:

1. Complexity: Managing access control lists for numerous objects and users can become complex and difficult to administer, especially in large-scale systems. It requires careful planning and maintenance to ensure that access permissions are correctly assigned and updated.

2. Inefficient Handling of Dynamic Environments: The directory approach may struggle to handle dynamic environments where the access requirements change frequently. As access control lists

need to be updated manually, it can lead to delays in granting or revoking access permissions in real-time.

3. Potential for Misconfigurations: Human errors or misconfigurations can lead to unintended access rights being granted or denied. Inaccurate access control lists can result in unauthorized access or data breaches.

4. Lack of Contextual Information: The directory approach primarily focuses on access permissions without considering contextual factors such as time, location, or user behavior. This may limit the ability to implement more sophisticated security measures, such as adaptive access control.

Qs. 3)Discuss various methods of file protection. [4M]

Answer. 3)

File protection is an essential component of modern operating systems, ensuring that files are secured from unauthorized access, alteration, or deletion. In this context, there are several types of file protection mechanisms used in operating systems to provide robust data security.

- **File Permissions** – File permissions are a basic form of file protection that controls access to files by setting permissions for users and groups. File permissions allow the system administrator to assign specific access rights to users and groups, which can include read, write, and execute privileges. These access rights can be assigned at the file or directory level, allowing users and groups to access specific files or directories as needed. File permissions can be modified by the system administrator at any time to adjust access privileges, which helps to prevent unauthorized access.
- **Encryption** – Encryption is the process of converting plain text into ciphertext to protect files from unauthorized access. Encrypted files can only be accessed by authorized users who have the correct encryption key to decrypt them. Encryption is widely used to secure sensitive data such as financial information, personal data, and other confidential information. In an operating system, encryption can be applied to individual files or entire directories, providing an extra layer of protection against unauthorized access.
- **Access Control Lists (ACLs)** – Access control lists (ACLs) are lists of permissions attached to files and directories that define which users or groups have access to them and what actions

they can perform on them. ACLs can be more granular than file permissions, allowing the system administrator to specify exactly which users or groups can access specific files or directories. ACLs can also be used to grant or deny specific permissions, such as read, write, or execute privileges, to individual users or groups.

- **Auditing and Logging** – Auditing and logging are mechanisms used to track and monitor file access, changes, and deletions. It involves creating a record of all file access and changes, including who accessed the file, what actions were performed, and when they were performed. Auditing and logging can help to detect and prevent unauthorized access and can also provide an audit trail for compliance purposes.
- **Physical File Security** – Physical file security involves protecting files from physical damage or theft. It includes measures such as file storage and access control, backup and recovery, and physical security best practices. Physical file security is essential for ensuring the integrity and availability of critical data, as well as compliance with regulatory requirements.

Qs. 4)Write short notes on the following:[4M]

(a) Replay Attack

(b) Security Goals

(c) Asymmetric key cryptography

(d) Substitution ciphers

Answer. 4)

(a) Replay Attack:

A replay attack is a type of network attack in which an attacker captures a valid network transmission and then retransmit it later. The main objective is to trick the system into accepting the retransmission of the data as a legitimate one.

(b) Security Goals:

LGG_1416_2023

The Three Security Goals are Confidentiality, Integrity and Availability.

(c) Asymmetric key cryptography:{alearady exlained}

(d) Substitution ciphers:

A substitution cipher is a method of encrypting in which units of plaintext are replaced withthe ciphertext, in a defined manner, with the help of a key; the "units" may be single letters, pairs of letters, triplets of letters, mixtures of the above, and so forth.

Qs. 5)Define the following

Symmetric and Asymmetric encryption [2M]

Answer. 5)

Symmetric Key Encryption:

In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

Asymmetric Key Encryption:

Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different key to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.

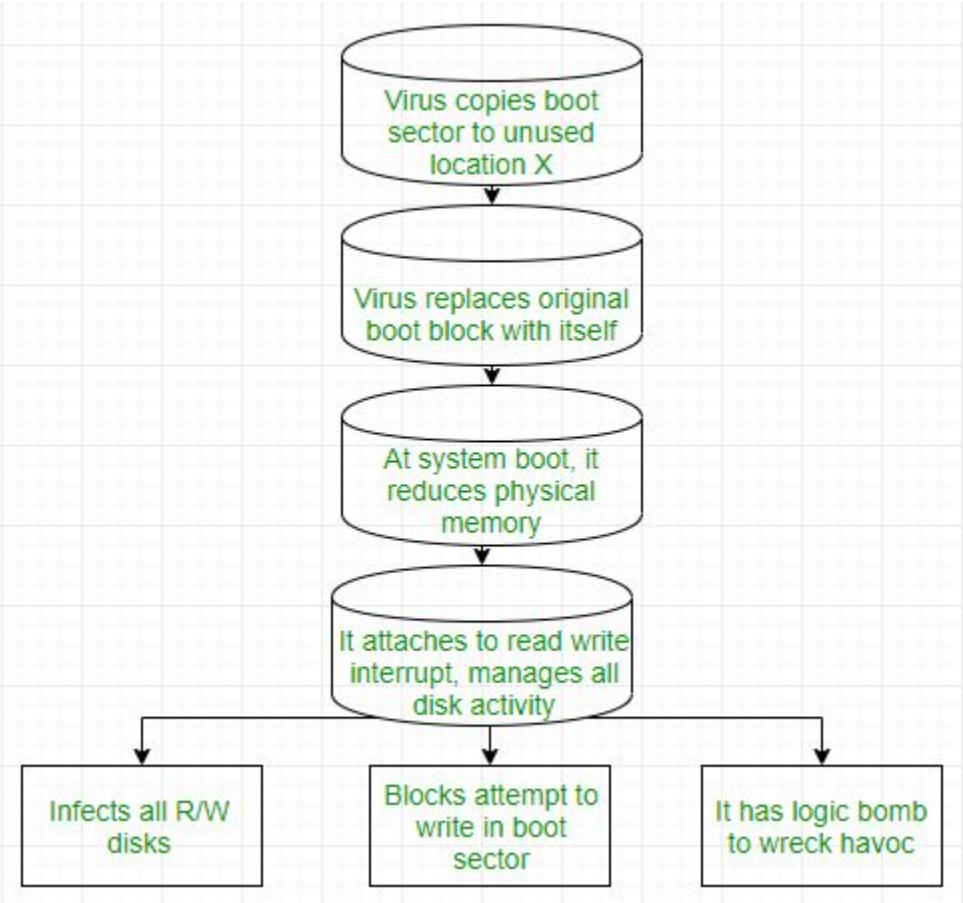
Qs. 6)Write short notes on the following: [5M]

(a) Boot sector virus

Answer. 6)

- Boot sector Virus:
  It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as

memory viruses as they do not infect the file systems.



Qs. 8)How to achieve memory and address protection using base/bound register method? [5M]

Answer. 26)

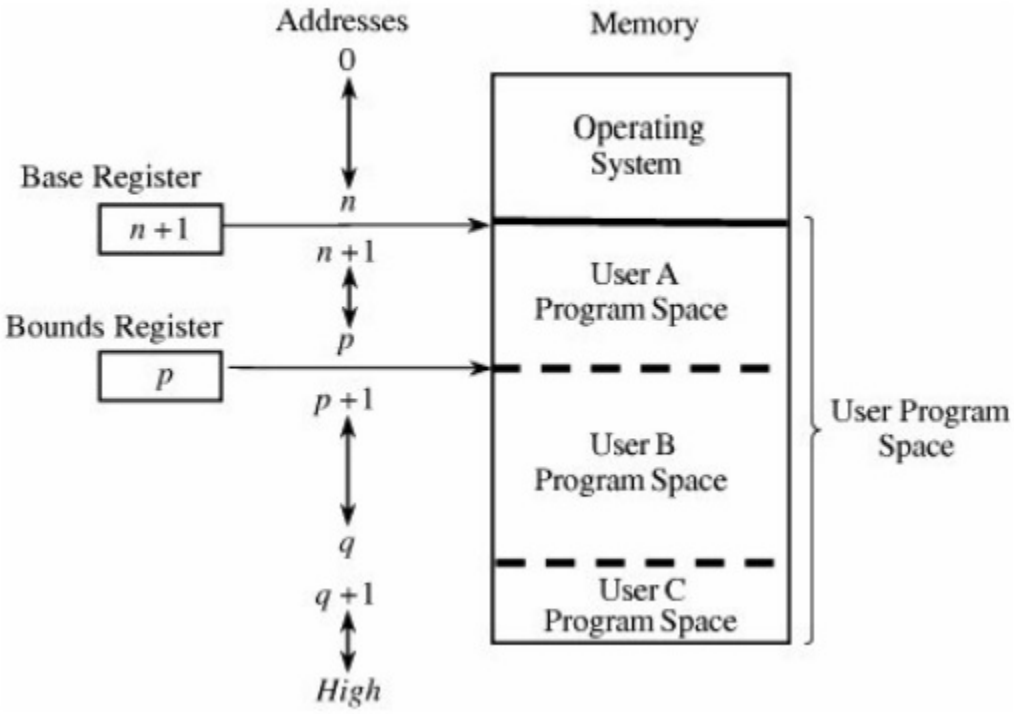
The most obvious problem of multiprogramming is preventing one program from affecting the data and programs in the memory space of other users. Fortunately, protection can be built into the hardware mechanisms that control efficient use of memory, so solid protection can be provided at essentially no additional cost.

LGG_1416_2023

Base/Bounds Registers

Fence registers provide a lower bound (a starting address) but not an upper one. An upper bound can be useful in knowing how much space is allotted and in checking for overflows into "forbidden" areas. To overcome this difficulty, a second register is often added, as shown in Figure 4-3. The second register, called a bounds register, is an upper address limit, in the same way that a base or fence register is a lower address limit. Each program address is forced to be above the base address because the contents of the base register are added to the address; each address is also checked to ensure that it is below the bounds address. In this way, a program's addresses are neatly confined to the space between the base and the bounds registers.

Figure 4-3. Pair of Base/Bounds Registers.



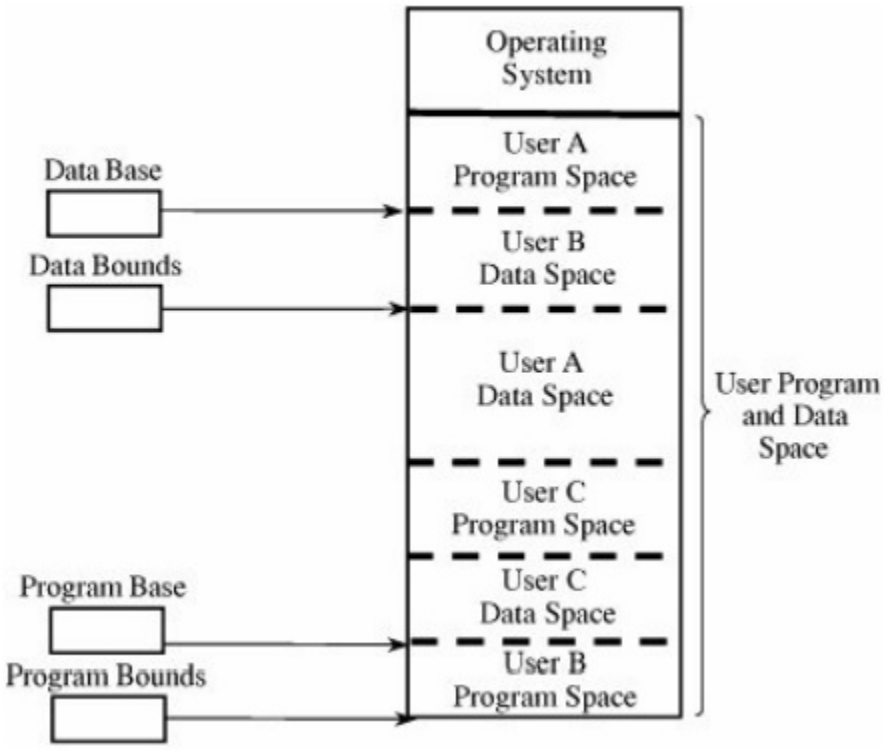
This technique protects a program's addresses from modification by another user. When execution changes from one user's program to another's, the operating system must change the contents of the base and

bounds registers to reflect the true address space for that user. This change is part of the general preparation, called a context switch, that the operating system must perform when transferring control from one user to another.

With a pair of base/bounds registers, a user is perfectly protected from outside users, or, more correctly, outside users are protected from errors in any other user's program. Erroneous addresses inside a user's address space can still affect that program because the base/bounds checking guarantees only that each address is inside the user's address space. For example, a user error might occur when a subscript is out of range or an undefined variable generates an address reference within the user's space but, unfortunately, inside the executable instructions of the user's program. In this manner, a user can accidentally store data on top of instructions. Such an error can let a user inadvertently destroy a program, but (fortunately) only the user's own program.

We can solve this overwriting problem by using another pair of base/bounds registers, one for the instructions (code) of the program and a second for the data space. Then, only instruction fetches (instructions to be executed) are relocated and checked with the first register pair, and only data accesses (operands of instructions) are relocated and checked with the second register pair. The use of two pairs of base/bounds registers is shown in Figure 4-4. Although two pairs of registers do not prevent all program errors, they limit the effect of data-manipulating instructions to the data space. The pairs of registers offer another more important advantage: the ability to split a program into two pieces that can be relocated separately.

Figure 4-4. Two Pairs of Base/Bounds Registers.



Qs. 9)What are the various ways for the control of access of general objects? Explain directory method in detail. [5M]

Answer. 26)

Control of Access to General Objects

Protecting memory is a specific case of the more general problem of protecting objects. As multiprogramming has developed, the numbers and kinds of objects shared have also increased. Here are some examples of the kinds of objects for which protection is desirable:

- **memory**
- **a file or data set on an auxiliary storage device**

- an executing program in memory
- a directory of files
- a hardware device
- a data structure, such as a stack
- a table of the operating system
- instructions, especially privileged instructions
- passwords and the user authentication mechanism
- the protection mechanism itself

The memory protection mechanism can be fairly simple because every memory access is guaranteed to go through certain points in the hardware. With more general objects, the number of points of access may be larger, a central authority through which all accesses pass may be lacking, and the kind of access may not simply be limited to read, write, or execute.

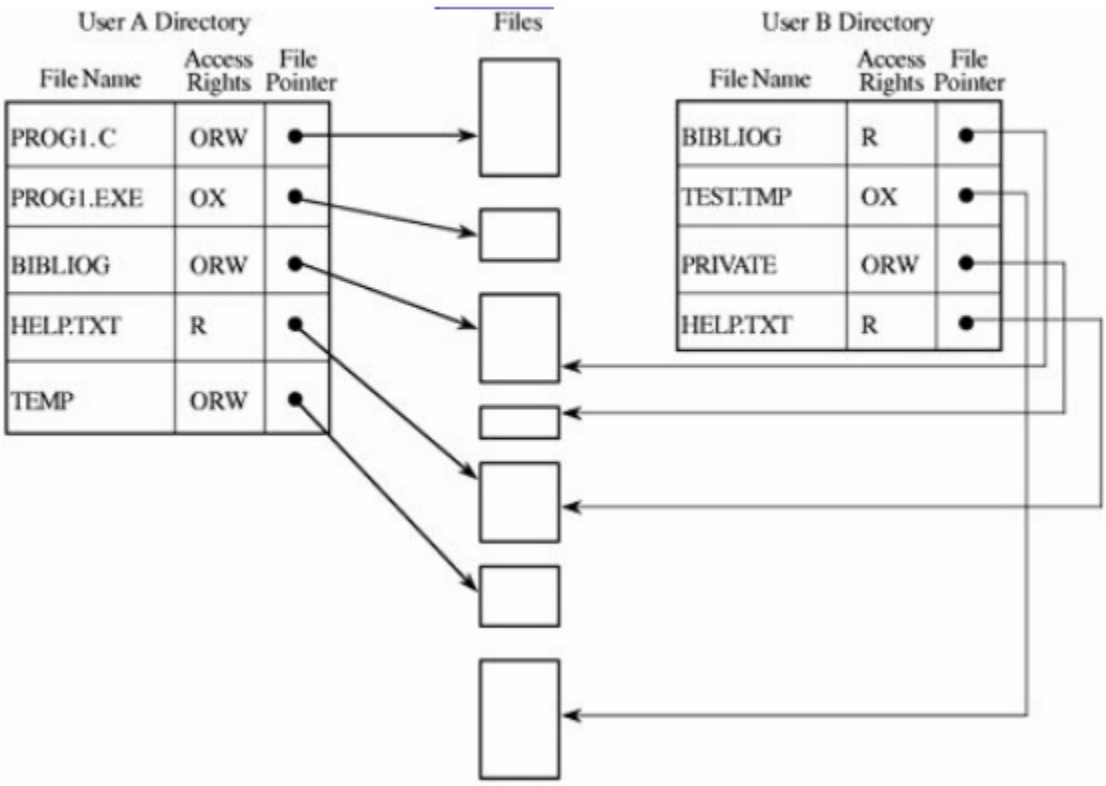
Furthermore, all accesses to memory occur through a program, so we can refer to the program or the programmer as the accessing agent.

Directory

One simple way to protect an object is to use a mechanism that works like a file directory. Imagine we are trying to protect files (the set of objects) from users of a computing system (the set of subjects). Every file has a unique owner who possesses "control" access rights (including the rights to declare who has what access) and to revoke access to any person at any time. Each user has a file directory, which lists all the files to which that user has access.

Clearly, no user can be allowed to write in the file directory because that would be a way to forge access to a file. Therefore, the operating system must maintain all file directories, under commands from the owners of files. The obvious rights to files are the common read, write, and execute familiar on many shared systems. Furthermore, another right, owner, is possessed by the owner, permitting that user to grant and revoke access rights. Figure 4-10 shows an example of a file directory.

Figure 4-10. Directory Access.



This approach is easy to implement because it uses one list per user, naming all the objects that user is allowed to access. However, several difficulties can arise. First, the list becomes too large if many shared objects, such as libraries of subprograms or a common table of users, are accessible to all users. The directory of each user must have one entry for each such shared object, even if the user has no intention of accessing the object. Deletion must be reflected in all directories.

A second difficulty is revocation of access. If owner A has passed to user B the right to read file F, an entry for F is made in the directory for B. This granting of access implies a level of trust between A and B. If A later questions that trust, A may want to revoke the access right of B. The operating system can respond easily to the single request to delete the right of B to access F because that action involves deleting one entry from a specific directory. But if A wants to remove the rights of everyone to access F, the operating system must search each individual directory for the entry F, an activity that can be time consuming on a large system. For example, large timesharing systems or networks of smaller systems can easily have 5,000 to 10,000 active

accounts. Moreover, B may have passed the access right for F to another user, so A may not know that F's access exists and should be revoked. This problem is particularly serious in a network.

Qs. 10)How to handle the problem of failure of a computing system in the middle of modifying data? Also give an example. [10M]

Answer. 10)

Handling the problem of failure of a computing system in the middle of modifying data is a critical aspect of information security. To address this issue, several measures can be taken:

1. Transaction Logging: Use transaction logging mechanisms to record all modifications made to the data. This involves keeping a log of each change made to the data, including the old and new values, timestamps, and any other relevant information. In the event of a system failure, the log can be used to recover and restore the data to its previous consistent state.

2. Atomic Transactions: Implement atomic transactions, which ensure that a series of modifications to the data are treated as a single unit of work. Atomicity guarantees that either all the modifications in a transaction are applied successfully, or none of them are applied at all. If a failure occurs during the modification process, the entire transaction can be rolled back, undoing any changes made so far.

3. Write-Ahead Logging: Use write-ahead logging (WAL) techniques, where changes are recorded in the log before being applied to the actual data. This ensures that the log is updated first, and then the data is modified. In case of a failure, the changes can be replayed from the log to restore the data to a consistent state.

4. Checkpointing: Periodically create checkpoints by saving the current state of the data and associated metadata. Checkpoints serve as recovery points that can be used to restore the data to

a known good state in case of a failure. If a failure occurs, the system can be restarted from the most recent checkpoint and replay the logged transactions to bring the data up to date.

Example:

Consider a database management system handling financial transactions. When a user transfers funds from one account to another, the system must ensure the consistency and integrity of the data, even in the event of a failure. Suppose a system failure occurs during the transfer process. By implementing transaction logging, the database records the transaction details, including the source account, destination account, and the amount being transferred. Upon recovery, the system can examine the log, identify the incomplete transaction, and roll it back to restore the original balances of the accounts involved.

Qs. 11)Distinguish between diagrams and trigrams giving suitable examples. Why are these used ? [3M]

Answer. 11)

1. Diagrams: Diagrams are graphical representations that depict the relationships between different components or entities within a system. They are visual tools used to illustrate concepts, processes, architectures, or data flows. Diagrams provide a clear and concise way to communicate complex information and help in understanding the structure and functionality of a system. In information security, diagrams are commonly used to represent network topologies, system architectures, threat models, and data flows.

Example:

A network diagram is a type of diagram that represents the interconnections between various devices, such as computers, servers, routers, and switches, within a network. It illustrates the physical and logical layout of the network, including the connections, IP addresses, and routing paths. Network diagrams are crucial in information security to identify potential vulnerabilities, plan security measures, and understand the flow of data within the network.

2. Trigrams: Trigrams, on the other hand, refer to a concept related to the analysis of text or data patterns. Trigrams are sequences of three consecutive elements, which can be characters, words, or any other units of analysis. In the context of information security, trigrams are often used in the field of cryptography and data analysis.

Example:

In the field of cryptography, trigrams can be used in frequency analysis, which is a technique to determine the frequency of occurrence of letters, characters, or combinations of characters in a text. By analyzing the frequency of trigrams, one can identify patterns and make statistical inferences to break or analyze the encryption scheme. For example, in English text, the trigram "the" is quite common, and its frequency can be used to deduce certain properties of the encrypted text.

Qs. 12)Differentiate between masquerading and replay attacks.[3M]

Answer. 12)

Masquerading (or *impersonation*; the two terms are equivalent)

A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.

Masquerade attacks can be perpetrated using stolen passwords and logons, by locating gaps in programs, or by finding a way around the authentication process,

Replay attack is a network attack in which a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and re transmit it.

Thus, a "replay attack" is often a specific kind of impersonation; or you can consider replay attacks to be a *tool* used to implement an impersonation attack.

Suppose node S want to send some data to R. For this S has to prove his identity to R. This way S sends his password to R for identification. At that time, an attacker an intercept the password of S and a presenting itself as S, when asked for the proof of identity. A sends S password read from the last session, which R accepts

LGG_1416_2023

Qs. 13)Define Trap door and its use.[3M]

Answer. 26)

Trap Door:

- **A trap door is kind of a secret entry point into a program that allows anyone to gain access to any system without going through the usual security access procedures.**
- **Another definition of a trap door is it is a method of bypassing normal authentication methods. Therefore it is also known as a back door.**
- **Trap Doors are quite difficult to detect and also in order to find them the programmers or the developers have to go through the components of the system.**
- **Programmers use Trap door legally to debug and test programs. Trap doors turn to threats when any dishonest programmers gain illegal access.**
- **Program development and software update activities should be the first focus of security measures. The operating system that controls the trap doors is difficult to implement.**

Qs. 14)What is the role of proxy server in the information security?[3M]

Answer. 26)

Proxy server refers to a server that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources. There are different types of proxy servers available that are put into use according to the purpose of a request made by the clients to the servers. The basic purpose of Proxy servers is to protect the direct connection of Internet clients and internet resources. The proxy server also prevents the identification of the client's IP address when the client makes any request is made to any other servers.

- **Internet Client and Internet resources: For internet clients, Proxy servers also act as a shield for an internal network against the request coming from a client to access the**

data stored on the server. It makes the original IP address of the node remains hidden while accessing data from that server.

- Protects true host identity: In this method, outgoing traffic appears to come from the proxy server rather than internet navigation. It must be configured to the specific application such as HTTPs or FTP. For example, organizations can use a proxy to observe the traffic of its employees to get the work efficiently done. It can also be used to keep a check on any kind of highly confidential data leakage. Some can also use it to increase their websites rank.

Qs. 15)What is sensitive data? List the factors that can make data sensitive. [5M]

Answer. 26)

Sensitive data is confidential information that must be kept safe and out of reach from all outsiders unless they have permission to access it. Access to sensitive data should be limited through sufficient data security and information security practices designed to prevent data leaks and data breaches.

Several factors can make data sensitive.

- **Inherently sensitive.** The value itself may be so revealing that it is sensitive. Examples are the locations of defensive missiles or the median income of barbers in a town with only one barber.

- **From a sensitive source.** The source of the data may indicate a need for confidentiality. An example is information from an informer whose identity would be compromised if the information were disclosed.

- **Declared sensitive.** The database administrator or the owner of the data may have declared the data to be sensitive. Examples are classified military data or the name of the anonymous donor of a piece of art.

- **Part of a sensitive attribute or a sensitive record.** In a database, an entire attribute or record may be classified as sensitive. Examples are the salary attribute of a personnel database or a record describing a secret space mission.

- **Sensitive in relation to previously disclosed information.** Some data become sensitive in the presence of other data. For example, the longitude coordinate of a secret gold mine reveals little, but the longitude coordinate in conjunction with the latitude coordinate pinpoints the mine.

Qs. 16)What do you understand by capability lists? Explain the advantage of capability lists over access control list. [3+2M]

Answer. 26)

Capability Lists:

Capability lists can be created by splitting the access matrix row-wise. A capability list is a subject-wise list that specifies the list of rights the subject has for every object. Thus, the capability list of a user or a process or domain is a list of rights that it has on the various objects. A capability consists of two fields-object descriptor access rights. An object descriptor is an identifier for an object and access right indicates various operations such as read, write execute, etc. granted to an object. A capability can be given as a pair (x, r) where x is the name of an object and r is a set of privileges or rights.

LGG_1416_2023

Sr. No	Access Control Lists	Capability Lists
1.	It is defined object-wise (resources).	It is defined subject-wise (users, processes, and procedures).
2.	It lists the various subjects along with the rights of an object.	It lists the various objects along with the rights permitted on them for a subject.
3.	Each object (resource) has a list of pairs of the form <subject, access rights>	Each subject (user, process procedure) has a list of pairs of the form <object, access rights>
4.	It would be tedious to have separate listings for each object (user), therefore, they are grouped into classes. For example, in UNIX, there are three classes self, group, and anybody else.	Here capabilities are the names of the objects. The objects not referred to in at capability list cannot be ever named.

5.	The default is: Everyone should be able to access a file.	The default is: No one should be able to access a file unless they have been given a capability.
6.	Access lists are simple and are used in almost all file systems.	Capabilities are used in systems that need to be very secure as they prohibit sharing of information unless access is given to a subject.

Qs. 17)Explain Syndrome Decoding. [2M]

Answer. 26)

Syndrome decoding is a highly efficient method of decoding a linear code over a noisy channel, i.e. one on which errors are made. In essence, syndrome decoding is minimum distance decoding using a reduced lookup table. This is allowed by the linearity of the code.

Qs. 18)Define network footprinting and network fingerprinting? How are these two related? [3M]

Answer. 18)

1. Network Footprinting: Network footprinting, is the process of collecting information about a target network. It involves gathering data related to network topology, system architecture, IP addresses, domain names, registered network services, and other publicly available information. Network footprinting aims to create a blueprint or map of the target network to understand its structure, potential vulnerabilities, and attack surfaces. This information can be used by attackers

to plan their intrusion attempts or by security professionals to assess the network's security posture and identify potential weaknesses.

2. Network Fingerprinting: Network fingerprinting, is the technique of identifying the operating system or software running on a target system or device. It involves analyzing network traffic patterns, packet responses, and other characteristics unique to different operating systems or applications. By examining these characteristics, network fingerprinting tools or methods attempt to determine the specific OS or software version in use. This information is valuable for attackers to exploit vulnerabilities specific to a particular OS version or for defenders to understand the composition of their network and identify potential security risks.

Relationship between Network Footprinting and Network Fingerprinting:

Network footprinting and network fingerprinting are complementary techniques used in the reconnaissance phase of an attack or security assessment. Network footprinting provides an overall understanding of the target network's structure, while network fingerprinting focuses on identifying the specific operating systems or software versions in use.

During network footprinting, the gathered information can be used to identify potential targets for further analysis or exploitation. Network fingerprinting techniques can then be employed to identify the specific operating systems on these targets, enabling attackers or defenders to tailor their attacks or defenses accordingly.

Qs. 19)Define minimum weight of the code.[1M]

Answer. 26)

A linear [n,k] code C over F is a k-dimensional vector subspace of Fn. The elements of C are called codewords and the weight wt(x) of a codeword x is the number of non-zero coordinates in x. The minimum weight of C is defined as min{wt(x): | $0 \neq x$ in C}.

Qs. 20)Describe linear block code. Explain the difference between hamming distance and hamming weight. (Parameters of hamming code)[3M]

LGG_1416_2023

Answer. 26)

Linear block code is a type of error-correcting code in which the actual information bits are linearly combined with the parity check bits so as to generate a linear codeword that is transmitted through the channel. Another major type of error-correcting code is convolution code.

In the linear block code technique, the complete message is divided into blocks and these blocks are combined with redundant bits so as to deal with error detection and correction.

Hamming Distance

Hamming distance is a metric for comparing two binary data strings. While comparing two binary strings of equal length, Hamming distance is the number of bit positions in which the two bits are different.

The Hamming distance between two strings, a and b is denoted as d(a,b).

It is used for error detection or error correction when data is transmitted over computer networks. It is also using in coding theory for comparing equal length data words.

Qs. 21)Define congruence and compare with equality[2M]

Answer. 21)

In the context of information security, congruence and equality are two distinct concepts that are often used to describe different relationships.

1. Congruence:

Congruence refers to two entities being equivalent or having the same characteristics while allowing for variations in representation or format. In information security, congruence is often used when comparing cryptographic keys, hash values, or digital signatures. Two entities can be considered congruent if they fulfill the same function or provide the same level of security, even if their underlying structure or representation differs.

For example, in symmetric key cryptography, two keys can be considered congruent if they produce the same result when used for encryption or decryption, even if they are represented in

different formats or generated using different algorithms. Similarly, in digital signatures, congruence may refer to different representations of the same signed message or document.

2. Equality:

Equality, on the other hand, refers to two entities being identical in all respects, with no variation or difference between them. In information security, equality is often used to compare data elements, such as passwords, cryptographic hashes, or encrypted data. If two entities are equal, they have the exact same value or characteristics, without any variations.

For example, in password-based authentication, when a user enters their password, it is compared with the stored password hash. If the entered password hash is equal to the stored hash, the authentication is successful. In this case, equality is necessary because any variation in the password hash would indicate a mismatch and potentially compromise security.

In summary, congruence allows for variations in representation or format while still considering two entities equivalent, whereas equality requires exact identity or matching values between two entities. Both concepts are relevant in information security, but their usage depends on the specific context and the properties being compared.

Qs. 22)Explain modulo operator along with its application. Also define residue classes with an example. [2M]

Answer. 22)

The modulo operator, denoted by the symbol "%", is a mathematical operation that calculates the remainder of a division operation. In other words, it returns the remainder when one number is divided by another. The modulo operator is commonly used in computer programming and mathematics.The modulo operator is defined as follows: if we have two integers, a and b, where b is not zero, then the result of a modulo b is the remainder when a is divided by b. It can be represented as:

a % b = r

where "a" is the dividend, "b" is the divisor, and "r" is the remainder.

The modulo operator finds various applications in programming and mathematics, including:

LGG_1416_2023

1. Finding remainders: It can be used to determine if a number is even or odd by checking if it is divisible by 2. If a number modulo 2 equals 0, it is even; otherwise, it is odd.

2. Hash functions: Modulo arithmetic is frequently used in hash functions to map large input sets to smaller output sets. It helps distribute data uniformly across a fixed number of buckets or slots.

In cryptography, residue classes play a significant role in public-key cryptography systems such as RSA.Residue classes, also known as congruence classes, are sets of integers that have the same remainder when divided by a fixed modulus. For example, let's consider the modulus 7. The residue class [2] would contain all integers that leave a remainder of 2 when divided by 7: {...-12, -5, 2, 9, 16...}.In information security, residue classes are utilized in the RSA algorithm. RSA encryption and decryption involve modular exponentiation, where the modulo operation is applied to large numbers. The residue classes ensure that the results of these operations remain within a certain range, making the algorithm secure and efficient.

For example, when encrypting a message using RSA, the message is converted into an integer, raised to a specific power, and then taken modulo the product of two large prime numbers. The residue class resulting from this modulo operation forms the encrypted message, making it challenging for an adversary to decipher the original message without the corresponding private key.

Qs. 23)Differentiate between the following: [2M]

(a) Public key and Private key.

Answer. 26)

S.NO	Private Key	Public Key

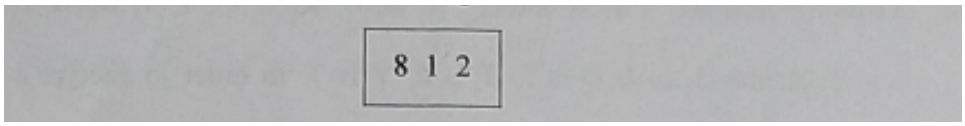
1.	The private key is faster than the public key.	It is slower than a private key.
2.	In this, the same key (secret key) and algorithm are used to encrypt and decrypt the message.	In public-key cryptography, two keys are used, one key is used for encryption, and the other is used for decryption.
3.	In private key cryptography, the key is kept a secret.	In public-key cryptography, one of the two keys is kept a secret.
4.	The private key is Symmetrical because there is only one key that is called a secret key.	The public key is Asymmetrical because there are two types of keys: private and public keys.
5.	In this cryptography, the sender and receiver need to share the same key.	In this cryptography, the sender and receiver do not need to share the same key.

6.	In this cryptography, the key is private.	In this cryptography, the public key can be public and a private key is private.
7.	It is an efficient technology.	It is an inefficient technology.
8.	It is used for large amounts of text.	It is used for only short messages.
9.	There is the possibility of losing the key that renders the systems void.	There is less possibility of key loss, as the key is held publicly.
10.	The private key is to be shared between two parties.	The public key can be used by anyone.
11.	The Performance testing checks the reliability, scalability, and speed of the system.	The Load testing checks the sustainability of the system.

12.	The private key is used in algorithms such as AES 128, AES 192 and AES 256.	The public key is used in algorithms such as RSA, DSA, etc.
13.	The private key is kept secret.	The public key is widely distributed.
14.	It is used to protect disk drives and other data storage devices.	It is used to secure web sessions and emails.
15.	The recipient's private key decrypts the message.	The recipient's public key encrypts the message.
16.	If the private key is the locking key, then the system can be used to verify documents sent by the holder of the private key.	If the public key is the locking key, then it can be used to send private communication.

Qs. 24)(a)Show the P-Box for the following table:

LGG_1416_2023



(b) A message has 2000 bits. It is supposed to be encrypted using a block cipher of 64 bits, find the size of padding and the number of blocks. [3+2M]

Answer. 26)

(b) Since the block size of the cipher is 64 bits, we'll need to divide the message into multiple blocks of that size. The number of blocks required can be calculated by dividing the message size by the block size:

Number of Blocks = Message Size / Block Size

= 2000 bits / 64 bits

= 31.25

Since the number of blocks cannot be a fraction, we round up to the nearest whole number. Therefore, we'll need 32 blocks to encrypt the entire message.

Now, let's calculate the size of the padding. Padding is added to the message to fill up any remaining space in the last block. In this case, the last block will not be completely filled since the message size is not evenly divisible by the block size.

Padding Size = Block Size - (Message Size % Block Size)

= 64 bits - (2000 bits % 64 bits)

= 64 bits - 32 bits

= 32 bits

Therefore, we'll need a padding size of 32 bits to fill the remaining space in the last block.

In summary, for a message size of 2000 bits and a block size of 64 bits, we'll need 32 blocks and a padding size of 32 bits.

LGG_1416_2023

Qs. 25) (a)Give a list of possible items, which could be stored on a smart card, for authentication and encryption of connections.

A smart card is a safe place to store valuable information such as private keys, account numbers, passwords, or personal information. It's also a secure place to perform processes that one doesn't want to be exposed to the world, for example, performing a public key or private key encryption.

(b) How are those items stored on the smart card? [2+1M]

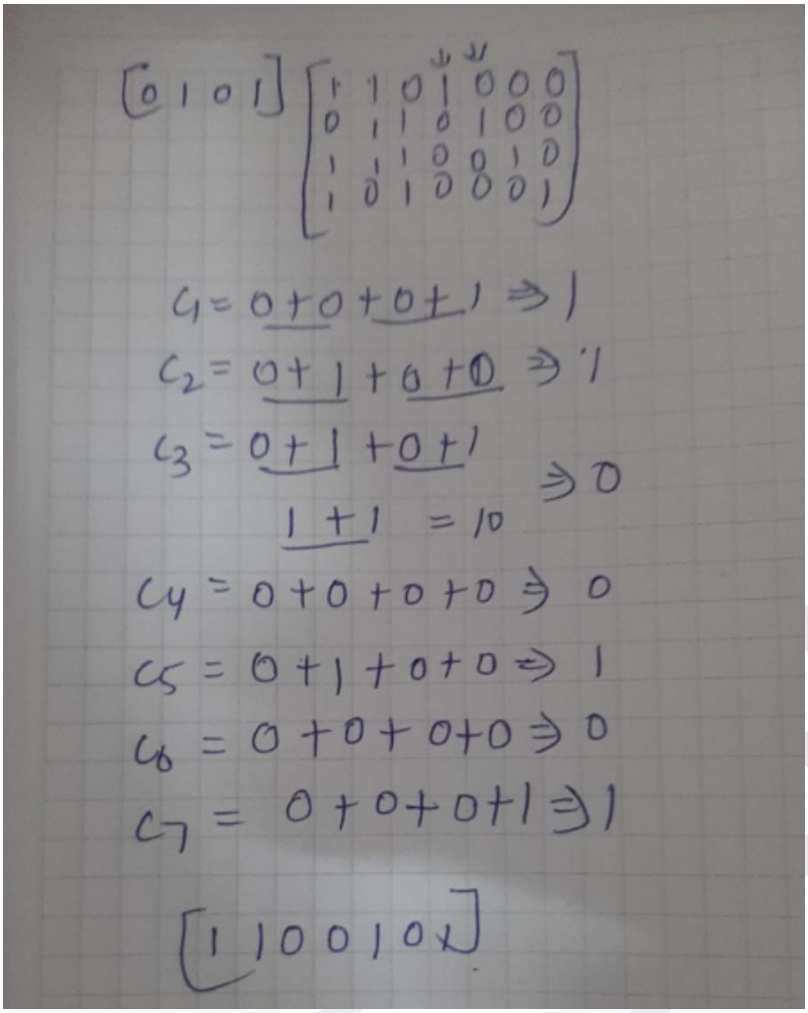
Answer. 26)

Qs.26) Given the following Generator matrix, what will be the encoded message for the word (0101)?

$$G = \begin{bmatrix} g_0 \\ g_1 \\ g_3 \\ g_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

V=u.G =0110100+1010001=1100101 [3M]

Answer. 26) multiply (0101) with G.



Qs. 27)Differentiate between law and ethics. [3M]

Answer. 27)

BASIS FOR COMPARISON	LAW	ETHICS

Meaning	**The law refers to a systematic body of rules that governs the whole society and the actions of its individual members.**	**Ethics is a branch of moral philosophy that guides people about the basic human conduct.**
What is it?	**Set of rules and regulations**	**Set of guidelines**
Governed By	**Government**	**Individual, Legal and Professional norms**
Expression	**Expressed and published in writing.**	**They are abstract.**
Violation	**Violation of law is not permissible which may result in punishment like imprisonment or fine or both.**	**There is no punishment for violation of ethics.**
Objective	**Law is created with an intent to maintain social order and peace in the society and provide protection to all the citizens.**	**Ethics are made to help people to decide what is right or wrong and how to act.**
Binding	**Law has a legal binding.**	**Ethics do not have a binding nature.**

Qs. 28)Write short note on Eavesdropping and Wiretapping [5M]

Answer. 28)

Eavesdropping

It is the act of intercepting communications between two points.

In the digital world, eavesdropping takes the form of sniffing for data in what is called network eavesdropping. A specialized program is used to sniff and record packets of data communications from a network and then subsequently listened to or read using cryptographic tools for analysis and decryption.

For example,

- **Voice over IP (VoIP) calls made using IP-based communication can be picked up and recorded using protocol analyzers and then converted to audio files using other specialized software.**
- **Data sniffing is easily done on a local network that uses a HUB since all communications are sent to all the ports (non-recipients just drop the data) and a sniffer will simply accept all of the incoming data.**
- **This goes the same for wireless networking where data is broadcast so even non-recipients can receive the data if they have the proper tools.**
- **Hacking into devices such as IP phones is also done in order to eavesdrop on the owner of the phone by remotely activating the speaker phone function.Devices with microphones including laptops and cellphones also can be hacked to remotely activate their microphones and discreetly send data to the attacker.**

Wiretapping:

It is also known as wire tapping or telephone tapping, is the monitoring of telephone and Internet-based conversations by a third party, often by covert means.

- **Legal wiretapping by a government agency is also called lawful interception.**
- **Passive wiretapping: monitors or records the traffic, while**
- **active wiretapping: alters or otherwise affects it.**

Qs. 29)List the different layers of an organization where security must be implemented to protect its operations. [3M]

Answer. 29)

A successful organization should have the following multiple layers of security in place to protect its operations:

- **physical security**
- **personal security**
- **operations security**
- **communications security**
- **network security**
- **information security.**

Qs. 30)Assume a hacker hacks into a network, copies a few files, defaces the Web page, and steals credit card numbers, how many different threat categories does this attack fall into? [2M]

Answer. 30)

These are the threats categories which fall under this attack:

1. **data breach**
2. **Unauthorized access**
3. **SQL injection**
4. **Cross-site scripting (XSS)**
5. **DNS hijacking**
6. **Malware infection**
7. **phishing**

Qs. 31)What measures can individuals take to protect against shoulder surfing? [1M]

Answer. 31)

A shoulder Surfing Attack is a social engineering technique where an attacker simply looks over someone's shoulder to get confidential information. It could be as simple as when a person is entering their PIN in an ATM or when a person is entering the username and password to their social media account/Internet Banking etc.

LGG_1416_2023

These are the following measures can individuals take to protect against shoulder surfing:

1. Enable 2-factor authentication

Always enable 2-factor authentication, like an OTP, approval on your mobile device, or usage of Microsoft/Google authenticator apps.

2. Get Physical Obstacle/Shield

While entering a password or an ATM PIN, try to hide it with your body so it is not visible to the person standing behind you. If an OTP, or credit card details must be communicated over the phone, make sure you move away to a place where nobody can listen to the conversations.

3. Never login to shared devices

Never login to any of your accounts using public computers like in airports, train stations, libraries or it could be a display device in an electronic gadget store. Confidential information can be stolen.

4. Never use public Wi-Fi

It is advised not to use public unprotected Wi-Fi networks to log in to any personal accounts like social media, banks, and shopping sites. The traffic can always be monitored especially when the Wi-Fi connection uses the weakest protocol WEP.

5. Privacy shield

Use privacy filters/shields on laptops and smartphones where the display on the screens can be seen in only one direction.

6. Stop using the same passwords

Many of them use the same password for multiple accounts. Doing so can risk other accounts being compromised as well. Always try to use a different password for different accounts.

7. Use alternative methods

Wherever it is possible utilize biometric authentications like a fingerprint and face recognition to log in to laptops, smartphones, and applications.

8. Use password managers

Using password manager applications, one does not have to create a password, the password manager creates a lengthy random string and stores it. When a password is required, one does not have to type any password as the password manager logs in for you. one does not have to create a password, the password manager creates a random lengthy string and stores it. When a password is required, one does not have to type any password as the password manager logs in for you.

Qs. 32)Differentiate between Honeynet, Honeypot and Padded cell systems. [3M]

Answer. 32)

Honeypot	**Honeynet**	**Padded cell system**
• A honeypot is a system that is designed to lure in attackers and then track or monitor their activities. • Honeypots can be used	• A honeynet is formed when many honeypot systems are linked together on a network segment. • A honeynet can be used	• A padded cell is a tightened honeypot that works in unison with the traditional Intrusion Detection and Prevention System(IDPS)

for a variety of purposes, including research, detection, and prevention of attacks. • Honeypots are supplied with sophisticated detectors and incident recorders. These features help identify attempted system access and collect data on the behavior of the potential attacker. • low cost, low maintenance	for the same purposes as a single honeypot, but it has the added benefit of being able to track attacks across multiple systems. • high cost, high maintenance	• Padded cells, like honeypots, are well-equipped and provide a unique opportunity for a target company to watch an attacker's operations. • high cost, high maintenance

Qs. 33)What are the properties of cryptographic hash function? Name any two hash functions.[5M]

Answer. 33)

A cryptographic hash function is a mathematical function used in cryptography. Typical hash functions take inputs of variable lengths to return outputs of a fixed length.

In particular, cryptographic hash functions exhibit these three properties:

- They are "collision-free." This means that no two input hashes should map to the same output hash.
- They can be hidden. It should be difficult to guess the input value for a hash function from its output.
- They should be puzzle-friendly. It should be difficult to select an input that provides a predefined output. Thus, the input should be selected from a distribution that's as wide as possible.

Hash Functions:

1. MurmurHash: MurmurHash is a fast and efficient non-cryptographic hash function designed for use in hash tables and other data structures. It is not suitable for security purposes as it is vulnerable to collision attacks.
2. BLAKE2: BLAKE2 is a cryptographic hash function designed to be fast and secure. It is an improvement over the popular SHA-3 algorithm and is widely used in applications that require high-speed hashing, such as cryptocurrency mining.
3. Argon2: Argon2 is a memory-hard password hashing function designed to be resistant to brute-force attacks. It is widely used for password storage and is recommended by the Password Hashing Competition. The main goal of Argon2 is to make it difficult for attackers to crack passwords by using techniques such as brute force attacks or dictionary attacks. It achieves this by using a computationally-intensive algorithm that makes it difficult for attackers to perform large numbers of password guesses in a short amount of time.

Qs. 34)Which policies would you suggest to be adopted by organizations to protect privacy of its users.[5M]

Answer. 34)

To protect its users an organization can adopt the following policies.

1. **Firewalls**—utilities that enable you to monitor and filter network traffic. You can use firewalls to ensure that only authorized users are allowed to access or transfer data.
2. **Authentication and authorization**—controls that help you verify credentials and assure that user privileges are applied correctly.
3. **Encryption**—alters data content according to an algorithm that can only be reversed with the right encryption key. Encryption protects your data from unauthorized access even if data is stolen by making it unreadable.
4. **Endpoint protection**—protects gateways to your network, including ports, routers, and connected devices. Endpoint protection software typically enables you to monitor your network perimeter and to filter traffic as needed.

5. **Data erasure**—limits liability by deleting data that is no longer needed. This can be done after data is processed and analyzed or periodically when data is no longer relevant. Erasing unnecessary data is a requirement of many compliance regulations, such as GDPR.
6. **Disaster recovery**—a set of practices and technologies that determine how an organization deals with a disaster, such as a cyber attack, natural disaster, or large-scale equipment failure. The disaster recovery process typically involves setting up a remote disaster recovery site with copies of protected systems, and switching operations to those systems in case of disaster.
7. **Data discovery**—a first step in data protection, this involves discovering which data sets exist in the organization, which of them are business critical and which contains sensitive data that might be subject to compliance regulations.
8. **Data loss prevention (DLP)**—a set of strategies and tools that you can use to prevent data from being stolen, lost, or accidentally deleted. Data loss prevention solutions often include several tools to protect against and recover from data loss.
9. **Storage with built-in data protection**—modern storage equipment provides built-in disk clustering and redundancy
10. **Backup**—creates copies of data and stores them separately, making it possible to restore the data later in case of loss or modification. Backups are a critical strategy for ensuring business continuity when original data is lost, destroyed, or damaged, either accidentally or maliciously.
11. **Snapshots**—a snapshot is similar to a backup, but it is a complete image of a protected system, including data and system files. A snapshot can be used to restore an entire system to a specific point in time.
12. **Replication**—a technique for copying data on an ongoing basis from a protected system to another location. This provides a living, up-to-date copy of the data, allowing not only recovery but also immediate failover to the copy if the primary system goes down.

Qs. 35)Explain the modification and fabrication security attacks with the help of an example each.[5M]

Answer. 35)

Modification:

Modification is an attack against the integrity of the information. Basically there is three types of modifications.

- **Change: Change existing information. The information is already existed but incorrect. Change attacks can be targeted at sensitive information or public information.**
- **Insertion: When an insertion attack is made, information that did not previously exist is added. This attack may be mounted against historical information or information that is yet to be acted upon.**
- **Deletion : Removal of existing information.**

Examples of Modification attacks include:

- **Modifying the contents of messages in the network.**
- **Changing information stored in data files.**
- **Altering programs so they perform differently.**
- **Reconfiguring system hardware or network topologies.**

Mitigate the attack :

- **Introduction of intrusion detection systems (IDS) which could look for different signatures which represent an attack.**
- **Using Encryption mechanisms**
- **Traffic padding**
- **Keeping backups**
- **Use messaging techniques such as checksums, sequence numbers, digests, authentication codes**

Fabrication:

A fabrication attack creates illegitimate information, processes, communications or other data within a system.

Often, fabricated data is inserted right alongside authentic data. When a known system is compromised, attackers may use fabrication techniques to gain trust, create a false trail, collect data for illicit use, spawn malicious or extraneous processes. In addition, fabricated data may reduce confidence in genuine data with the affected system.

Examples of Fabrication attacks include:

- SQL Injection
- Route Injection
- User / Credential Counterfeiting
- Log / Audit Trail Falsification
- Email Spoofing

Mitigate the attack :

- Use of Authentication and authorization mechanisms
- Using Firewalls
- Use Digital Signatures - Digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Qs. 36)Define Risk and Risk Leverage. List the basic steps of Risk Analysis.[5M]

Answer. 36)

Risk:

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

(i) the adverse impacts that would arise if the circumstance or event

occurs.

(ii) the likelihood of occurrence.

Risk leverage: **{***YE MENE KHUD SE LIKHA HE AGAR TUM KHI PADOGE TO ISKO UPDATE KAR DENA***}**

This is the process by which one gets to know about the type of risk they will face in a particular event.

Risk Analysis:

Risk analysis defines the review of risks related to the specific action or event. Risk analysis is used in information technology, projects, security issues and some other events where risks can be analyzed based on a quantitative and qualitative basis.

There are some steps followed by a risk analysis process are as follows –

Establish the Risk Assessment Team – The risk assessment team will be answerable for the collection, analysis, and documenting of the assessment results to management.

Set the scope of the Project – The assessment team should recognize at the outset the goals of the assessment project, department, or functional events to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be inspected and operations to be checked.

Identify assets covered by the Assessment – Assets can involve, but are not defined to, personnel, hardware, software, data (such as classification of sensitivity and criticality), facilities and current controls that security those assets. It is the key to recognize all assets related to the assessment project determined in the scope.

Categorize Potential Losses – It can identify the losses that can result from some type of damage to an asset. Losses can result from physical damage, denial of service, alteration, unauthorized access or disclosure. Losses can be intangible, including the loss of the organizations' credibility.

Identify Threats and Vulnerabilities – A threat is an event, procedures, activity, or process that exploits a vulnerability to attack an asset. It involves natural threats, accidental threats, human accidental threats, and human malicious threats. These can involve power failure, biological contamination or hazardous chemical spills, acts

of features, or hardware/software failure, data elimination or loss of integrity, sabotage, or theft or vandalism.

Vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be recognized by addressing the following in the data collection process such as physical security, environment, system security, communications security, personnel security, plans, policies, processes, management, support, etc.

Identify existing Controls – Controls are safeguards that decrease the probability that a threat will exploit a vulnerability to strongly attack an asset. It can recognize those safeguards that are currently executed, and determine their effectiveness in the context of the current analysis.

Analyze the Data – In this step, all the collected data will be used to decide the actual risks to the assets under consideration. A method to analyze data contains preparing a record of assets and displaying corresponding threats, type of loss and vulnerability. Analysis of this data should contains an assessment of the possible frequency of the potential fall.

Qs. 37)List various threats to Email. Also list out the four main requirements to secure Email. (5M)

Answer. 37)

1. Malware Delivery via Spam

Malware is one of the most serious yet common threats that are commonly delivered through emails. This technique is especially successful at targeting employees within organizations. By sending spam mail impersonating legitimate senders such as customers, partners, or suppliers, victims are easily tricked into downloading rogue files that contain malware. Most of the time, the victims do not realize that they are installing malware onto their computers because signs of intrusion do not occur right away. The attackers can silently take control of the victim's computer, then sneak through the corporate IT network to spread the malware into nearby systems until

eventually, the entire IT infrastructure becomes infected, a process that can take days or even months. During this time, it would be lucky if the organization discovers the malware at the early stages. Yet, oftentimes, the intrusion is only detected after significant parts of the IT system have already been compromised, with servers encrypted and sensitive data leaked.

2. Credential Theft via Phishing Emails

Phishing emails are very similar to spam, except that they are more customized and more often than not used to deceive victims into giving up sensitive information directly. For example, attackers could somehow acquire a list of customer data from a financial institution, possibly leaked from a previous data breach. The list may contain the customers' names, email addresses, bank account numbers, and perhaps other personal information. The attackers then may use such a list to craft highly convincing spear-phishing emails to lure the victims into clicking a fake link that requires them to fill in their online banking login credentials. Similar attacks can be done to company employees by tricking them into giving out credentials for corporate admin accounts.

3. Business Email Compromise

Business email compromise (BEC) is a highly sophisticated type of spear phishing that targets high-ranking employees at the targeted organization, hence also commonly referred to as "CEO fraud". Different from other phishing attacks, in a BEC attack, the attackers invest a lot of time to study the victim's habits and behaviors, and gain information on the recent events they are involved in from their social media activities. After gaining all the information, a highly realistic email would be sent to the victim. For instance, after knowing that the victim is recently involved in negotiating a partnership opportunity with a particular person at a particular company. The

email would impersonate that person with details of the negotiation while sending a carbon copy of the email to a manager at the finance department to transfer funds into their account as an upfront deposit. With such specific details and accurate email addresses, it is almost impossible for the victim to notice any flaw. Thus BEC is commonly used to steal money and trade secrets.

4. Malicious Bot and DDoS Attacks

Just like how a traditional DDoS attack crashes the victim's web server, attackers can use hijacked botnets to send out a massive amount of emails to a targeted organization, causing the email server to crash from system overload. DDoS attacks on web servers are more common in B2C businesses as they rely on their websites for generating sales, while DDoS attacks on email servers tend to target B2B businesses because a large portion of their sales is conducted via email communication.

5. Authentication Attacks on Email Servers

Sometimes, the email inbox itself can become the target of attackers. In this case, attackers would try to launch authentication attacks on the email servers by using brute force, credential stuffing, and other methods to break over authentication and gain access to the email server. This would grant the attackers access to all the email messages and attachments stored in the server.

6. Vulnerabilities in Email Servers

LGG_1416_2023

Recently, four zero-day vulnerabilities found in Microsoft Exchange Server were exploited by alleged Chinese state-sponsored hackers. This was later discovered to have compromised over 30,000 servers affecting more than 100,000 organizations worldwide, leaking millions of emails. Indeed, a compromise of the email server is a catastrophic event not only due to the exposure of email messages, but also because hackers can easily infect nearby IT systems by traveling through the internal network.

Four main requirements to secure Email:

- Learn to inspect message headers.
- Avoid Clicking on Links or Downloading Attachments
- Update Your DMARC Records With the Domain Registrar
- Make Use of SMTP SSL/TLS Ports
- Use Restrictive Mail Relay Options

Qs. 38)Discuss various types of threats. [5M]

Answer. 38)

Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm objects or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses etc. Many users believe that malware, viruses, worms, bots are all the same things. But they are not the same, only similarity is that they all are malicious software that behaves differently.

Malware is a combination of 2 terms- Malicious and Software. So Malware basically means malicious software that can be an intrusive program code or anything that is designed to perform malicious operations on a system. Malware can be divided in 2 categories:

1. Infection Methods
2. Malware Actions

Malware on the basis of Infection Method are following:

1. **Virus – They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.**
2. **Worms – Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.**
3. **Trojan – The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.**

   Their purpose is to conceal themselves inside the software that seem legitimate and when that software is executed they will do their task of either stealing information or any other purpose for which they are designed.

   They often provide backdoor gateway for malicious programs or malevolent users to enter your system and steal your valuable data without your knowledge and permission. Examples include FTP Trojans, Proxy Trojans, Remote Access Trojans etc.

4. **Bots –: can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet.**

LGG_1416_2023

Malware on the basis of Actions:

1. **Adware** – Adware is not exactly malicious but they do breach privacy of the users. They display ads on a computer's desktop or inside individual programs. They come attached with free-to-use software, thus main source of revenue for such developers. They monitor your interests and display relevant ads. An attacker can embed malicious code inside the software and adware can monitor your system activities and can even compromise your machine.
2. **Spyware** – It is a program or we can say software that monitors your activities on computer and reveal collected information to an interested party. Spyware are generally dropped by Trojans, viruses or worms. Once dropped they install themselves and sits silently to avoid detection.

   One of the most common example of spyware is KEYLOGGER. The basic job of keylogger is to record user keystrokes with timestamp. Thus capturing interesting information like username, passwords, credit card details etc.
3. **Ransomware** – It is type of malware that will either encrypt your files or will lock your computer making it inaccessible either partially or wholly. Then a screen will be displayed asking for money i.e. ransom in exchange.
4. **Scareware** – It masquerades as a tool to help fix your system but when the software is executed it will infect your system or completely destroy it. The software will display a message to frighten you and force to take some action like pay them to fix your system.
5. **Rootkits** – are designed to gain root access or we can say administrative privileges in the user system. Once gained the root access, the exploiter can do anything from stealing private files to private data.
6. **Zombies** – They work similar to Spyware. Infection mechanism is same but they don't spy and steal information rather they wait for the command from hackers.

- **Theft of intellectual property means violation of intellectual property rights like copyrights, patents etc.**
- **Identity theft means to act someone else to obtain a person's personal information or to access vital information they have like accessing the computer or social media account of a person by login into the account by using their login credentials.**
- **Theft of equipment and information is increasing these days due to the mobile nature of devices and increasing information capacity.**
- **Sabotage means destroying a company's website to cause loss of confidence on part of its customer.**
- **Information extortion means theft of company's property or information to receive payment in exchange. For example ransomware may lock victims file making them inaccessible thus forcing victims to make payment in exchange. Only after payment the victim's files will be unlocked.**

These are the old generation attacks that continue these days also with advancement every year. Apart from these there are many other threats. Below is the brief description of these new generation threats.

- **Technology with weak security – With the advancement in technology, with every passing day a new gadget is being released in the market. But very few are fully secured and follow Information Security principles. Since the market is very competitive Security factor is compromised to make devices more up to date. This leads to theft of data/ information from the devices**
- **Social media attacks – In this cyber criminals identify and infect a cluster of websites that persons of a particular organization visit, to steal information.**
- **Mobile Malware –There is a saying when there is connectivity to the Internet there will be danger to Security. Same goes for Mobile phones where gaming applications are designed to lure customer to download the game and unintentionally they will install malware or virus on the device.**

- **Outdated Security Software – With new threats emerging everyday, updation in security software is a prerequisite to have a fully secured environment.**
- **Corporate data on personal devices – These days every organization follows a rule BYOD. BYOD means Bring your own device like Laptops, Tablets to the workplace. Clearly BYOD pose a serious threat to security of data but due to productivity issues organizations are arguing to adopt this.**
- **Social Engineering – is the art of manipulating people so that they give up their confidential information like bank account details, password etc. These criminals can trick you into giving your private and confidential information or they will gain your trust to get access to your computer to install a malicious software- that will give them control of your computer. For example email or message from your friend, that was probably not sent by your friend. Criminal can access your friends device and then by accessing the contact list, he can send infected email and message to all contacts. Since the message/ email is from a known person recipient will definitely check the link or attachment in the message, thus unintentionally infecting the computer.**