CSE-4743 || **Computer Security** || Mid Note

By- **Sorowar Mahabub**, C201032 & **Main Uddin**, C201091

(Sir class e poranor shomoi bolsilo **concept ta bujte kono kichu specific babe memorize korte mana korse**, er mane scenario type question thakbe. Memorize na kore reading pore jinish ta ki sheta bujar try korle better) - Main

Segment-1 (10 Marks)

Definition Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

CIA Triad: (aim is to prevent attackers/hackers from some services) **(Must read** from previous – Search below**)**

Example of CIA Triad: Bank services.

- ✓ Account information: If customer send money (though phone/app) to his bank account or for transaction. The information will must be known bank services and customer or whom the money is sent, not by others. This is ensured by confidentiality by encrypted the message.
- ✓ If a customer send money to others though that bank or for transaction through bank, the received information must be same which sent. This is ensured by integrity for not to modify the message.
- ✓ If customer want to access into that banking server, hacker shouldn't disrupt it. This is ensured by Availability it will let access those who are authorized.

Two other significant security concepts:

- □ **Authenticity:** It's validating source or origin of data and other file transfer through proof or identity. This is important because its ensures that the message (email, payment, transaction etc.) was not corrupted or intercepted during transmission.
- □ **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. Use for fault detection.

OSI Security Architecture: (Security Attack, Security Mechanism, Security Services**)**

The OSI security architecture focuses on security attacks, mechanisms, and services.

1. **Security Attack:** 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 try to access the message/ content/ data being shared by the sender and receiver by keeping a close watch on the transmission. Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption. ***Two types of passive attacks are the release*** of (i) **message contents** and (ii) **traffic analysis**.

   (i) Message content: A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

   (ii) Traffic Analysis: Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption.

   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.

2. **Security Mechanism:** A process that is designed to detect, prevent, or recover from a security attack. Security Mechanisms are also responsible for protecting a system, network, or device against unauthorized access or other security threats.

   a) **Specific Security Mechanism:**

   - **Encipherment (Encryption):** It involves the use of algorithms to transform data into a form that can only be read by someone with the appropriate decryption key. Encryption can be used to protect data it is transmitted over a network, or to protect data when it is stored on a device.

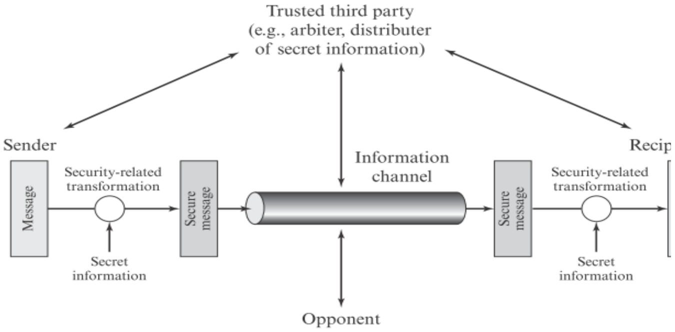
- **Digital Signature:** It is a security mechanism that involves the use of cryptographic techniques to create a unique, verifiable identifier for a digital document or message, which can be used to ensure the authenticity and integrity of the document or message.
- **Access Control**: A variety of mechanism that fulfil the access right to resources. User -> Access control -> file.
- **Data Integrity:** It is used to assure the integrity of data.

b) Pervasive Security Mechanism:

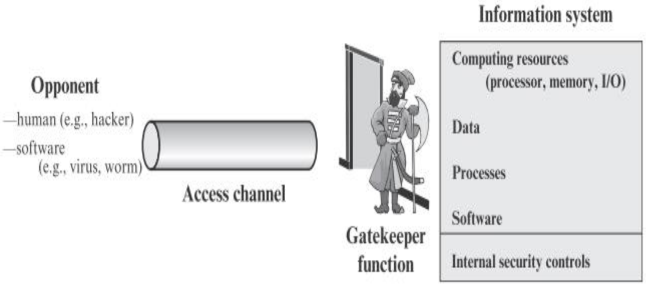
- **Trusted Functionality:** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
- **Security Label:** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
- **Event Detection:** Detection of security-relevant events.
- **Security Audit Trail:** Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
- **Security Recovery:** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

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.
   - **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 change 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.

Model for Network Security:



Network Access Security Model:



Segment-3 (10 Marks)

Euclidean Algorithm: One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. Two integers are **relatively prime** (or coprime) if there is no integer greater than one that divides them both (that is, their greatest common divisor is one).

Greatest Common Divisor:

More formally, the positive integer c is said to be the greatest common divisor of a and b if

1. c is a divisor of a and of b.
2. any divisor of a and b is a divisor of c.

An equivalent definition is the following:

$$\gcd(a, b) = \max[k, \text{such that } k \mid a \text{ and } k \mid b]$$

Because we require that the greatest common divisor be positive, $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$. In general, $\gcd(a, b) = \gcd(|a|, |b|)$.

$$\boxed{\gcd(60, 24) = \gcd(60, -24) = 12}$$

This flowchart given below may come in exam:

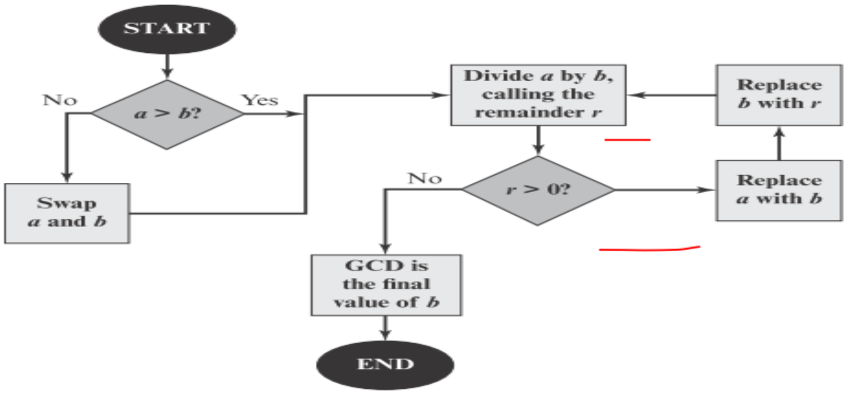


Figure 2.2 Euclidean Algorithm

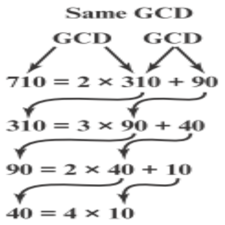
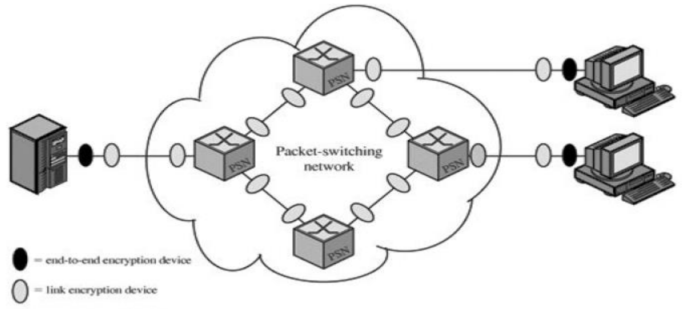


Figure 2.3 Euclidean Algorithm Example: gcd(710, 310)

Imp. Placement of Encryption Function: If encryption is to be used to counter attacks on confidentiality, we need to decide what to encrypt and where the encryption function should be located. To begin, this section examines the potential locations of security attacks and then looks at the two major approaches to encryption placement: **link** and **end to end**.



Link Encryption, End to End Encryption, Using both link and end to end encryption: See Prev Sol (below)

Key Distribution: The strength of any cryptographic system rests with the key distribution technique, a term that refers to the means of delivering a key to two parties who wish to exchange data, without allowing others to see the key.

For two parties A and B, key distribution can be achieved in a number of ways, as follows:

□ A can select a key and physically deliver it to B.

□ A third party can select the key and physically deliver it to A and B.

□ If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key.

□ If A and B each has an encrypted connection to a third-party C, C can deliver a key on the encrypted links to A and B.

Key Distribution Center (KDC):

The use of a key distribution center is based on the use of a hierarchy of keys. At a minimum, two levels of keys are used (Figure 7.8). Communication between end systems is encrypted using a temporary key, often referred to as a session key. ***Typically,*** the session key is used for the duration of a logical connection, such as a frame relay connection or transport connection, and then discarded. Each session key is obtained from the key distribution center. Accordingly, session keys are transmitted in encrypted form, using a master key that is shared by the key distribution center and an end system or user.

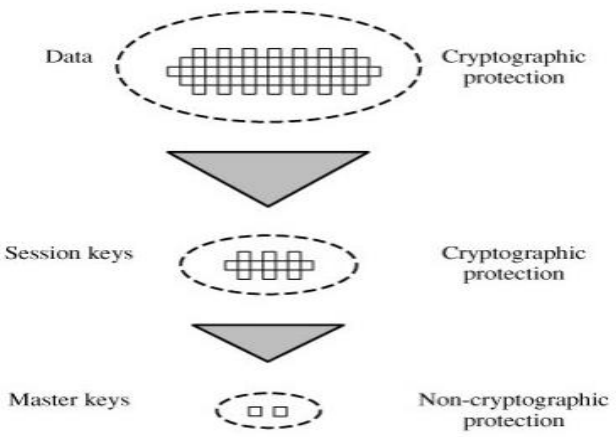
For each end system or user, there is a unique master key that it shares with the key distribution center. Of course, these master keys must be distributed in some fashion. However, the scale of the problem is vastly reduced.

If there are N entities that wish to communicate in pairs, then, as was mentioned, as many as-

$$\frac{\mathbf{N(N-1)}}{\mathbf{2}}$$

session keys are needed at any one time. However, only N master keys are required, one for each entity.

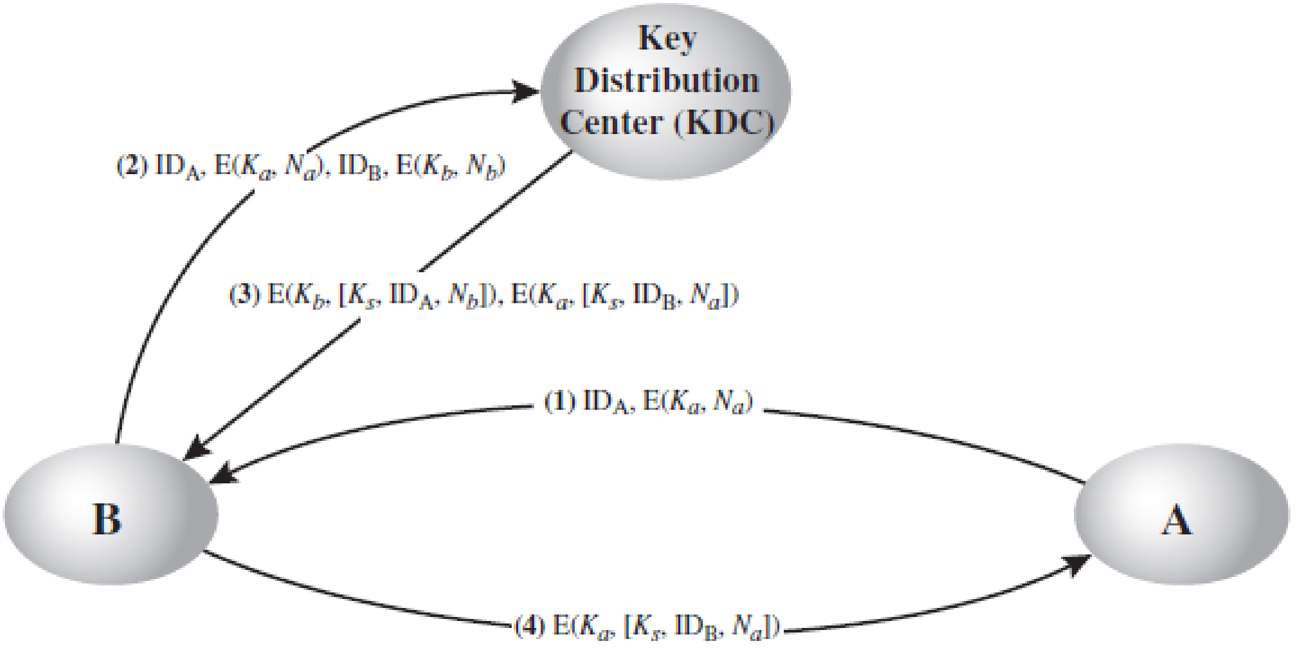
Figure 7.8. The Use of a Key Hierarchy



A Key Distribution Scenario:

Just figure ta draw kore then mon moto explain kore dile hoe jabe, figure tate muloto bujaise A, B ke access korar jonno kibabe KDC theke key ta nise. Eikhne kon step theke kon steps jacche ta number die bujai dise.

- Main


Key Distribution Center (KDC)
(2) ID_A, $E(K_a, N_a)$, ID_B, $E(K_b, N_b)$
(3) $E(K_b, [K_s, \text{ID}_A, N_b])$, $E(K_a, [K_s, \text{ID}_B, N_a])$
(1) ID_A, $E(K_a, N_a)$
B
A
(4) $E(K_a, [K_s, \text{ID}_B, N_a])$

Groups, Rings and Fields: *(Possibility to come in exam less than 50%, And it's not in the syllabus however sir taught us in class. Concept is very big if you want learn then watch this video link is given below, this video is enough to understands)*

Resource Link: https://youtu.be/oBL-Cb5GxA0

Autumn- 2022

1(a) Explain how the password are stored nowadays. Give example of tradeoffs between usability and security considering "authentication".

Nowadays, passwords are typically stored using a process called "***hashing***" and "***salting***." **Hashing** is a one-way cryptographic function that takes an input (such as a password) and converts it into a fixed-length string of characters, which is often referred to as a hash value or hash code. **Salting** involves adding a random value, known as a salt, to the password before hashing. This adds an extra layer of security by making it much more difficult for attackers to use precomputed tables (rainbow tables) to crack passwords.

Here's how the process works:

1.Hashing: When a user creates a password during registration, the system generates a unique salt for that user. The user's password and the salt are combined and then hashed. The resulting hash value is stored in the system's database.

2.Verification: When the user attempts to log in, the system retrieves the stored salt and applies the same hashing function to the entered password and salt. The resulting hash is compared to the stored hash. If they match, the password is valid, and the user is granted access.

Example of Trade-offs between Usability and Security:

1. Usability vs. Length and Complexity:

- Usability: Users tend to prefer simple and easy-to-remember passwords.
- Security: Longer and more complex passwords are generally more secure.
- Trade-off: Stricter password complexity requirements might discourage users from creating strong passwords or lead them to write down their passwords, which could compromise security.

2.Usability vs. Multi-Factor Authentication (MFA):

- Usability: Single-factor authentication (password-only) is simpler and quicker for users.
- Security: Multi-factor authentication adds an extra layer of security by requiring users to provide multiple forms of verification (e.g., password + SMS code or fingerprint).
- Trade-off: While MFA enhances security, it might require additional steps for users during login, potentially affecting the overall user experience.

3. Usability vs. Password Recovery:

- Usability: Easy password recovery methods (such as security questions) can make it convenient for users to regain access to their accounts.
- Security: Weak or easily guessable security questions could expose vulnerabilities to attackers.
- Trade-off: Stronger security questions or alternative methods of account recovery might be more secure but could be more challenging for users to remember or use effectively.

4. Usability vs. Password Storage Method:

- Usability: Storing passwords in plaintext (unencrypted) would allow for easy retrieval and management.
- Security: Storing passwords in plaintext is highly insecure, as any breach would expose user passwords.
- Trade-off: Hashing and salting passwords provide much higher security, but they require additional computational resources and more complex management.

Balancing usability and security are a continuous challenge in authentication systems. Striking the right balance ensures that users can access their accounts conveniently while maintaining a strong defense against unauthorized access.

1(b) Software and system security is all about managing risk. Do you agree with this statement? why?

Yes, I agree with the statement. Software and system security revolves around managing risk because:

1. Threat Landscape: The digital world is rife with threats like cyberattacks, data breaches, and malware. Managing risk involves identifying these threats, assessing their potential impact, and implementing countermeasures to minimize vulnerabilities.

2. Vulnerabilities Abound: Software and systems often have inherent vulnerabilities that can be exploited by attackers. Managing risk means recognizing these weaknesses, understanding their implications, and taking steps to mitigate or eliminate them.

3. Resource Optimization: Resources are limited. Managing risk helps allocate resources effectively by prioritizing security efforts where they are most needed, based on the likelihood and potential impact of threats.

4. Adaptive Approach: Threats and technologies evolve. Risk management fosters an adaptive approach, ensuring security measures stay up to date and effective against emerging threats.

5. Usability Consideration: Striking a balance between security and usability is vital. Risk management helps find the right compromise, ensuring security measures don't hinder functionality or user experience.

6. Regulatory Compliance: Many industries have regulatory requirements for security. Managing risk ensures compliance by identifying and addressing security gaps.

7. Business Continuity: Cyber incidents can disrupt operations. By managing risk, organizations safeguard against potential downtime and financial losses.

8. Holistic View: Risk management involves assessing technical, procedural, and human factors. This holistic approach strengthens security at multiple levels.

In summary, managing risk in software and system security is an essential approach that ensures proactive identification and mitigation of potential threats and vulnerabilities, allowing organizations to make informed decisions and maintain a strong security posture.

Calculate ALE (annualized loss expectancy) for each case. Consider probability of small ATM fraud is five times higher than that of large ATM fraud. (Answer in ***Bold with italic*** format)

Loss type	**Amount**	**Incidence**	**ALE**
SWIFT* fraud	Tk. 20,000,000	0.005	20,000,000×0.005= ***10000***
ATM fraud (large)	Tk. 250,000	0.10	250,000×0.10= ***25000***
ATM fraud (small)	Tk. 20,000	(0.10×5= ***0.5***)	20,000×0.5= ***10000***
Teller theft	Tk. 3,240	300	3,240×300= ***972000***

Au'22 || Sp'22 2(a) Explain the CIA triad with necessary examples? what is it significance?

The CIA triad is a widely used information security model that can guide an organization's efforts and policies aimed at keeping its data secure. The model has nothing to do with the U.S. Central Intelligence Agency; rather, the initials stand for the three principles on which infosec rests: Confidentiality, Integrity, and Availability.

Confidentiality: Only authorized users and processes should be able to access or modify data. ***For example****, a bank ATM can offer users access to bank balances and other information only after they have entered their PIN.*

Integrity: Data should be maintained in a correct state and nobody should be able to improperly modify it, either accidentally or maliciously. ***For example,*** *data encryption is one method to assure confidentiality so that unauthorized users cannot retrieve or access the data to which they do not have permission access.*

Availability: Authorized users should be able to access data whenever they need to do so. ***For example,*** *a hospital's electronic health record system must be available 24/7 so that doctors can access patient records whenever they need them.*

Significance of the CIA Triad:

1. Comprehensive Security: The CIA triad provides a holistic framework for addressing various aspects of security, ensuring that a well-rounded approach is taken to protect information and systems.

2. Risk Management: By considering the three components, organizations can identify vulnerabilities and potential threats, allowing them to prioritize security measures based on the risks associated with each component.

3. Balancing Trade-offs: The triad helps in striking a balance between security, usability, and convenience. Organizations can evaluate trade-offs between confidentiality, integrity, and availability based on their specific needs and priorities.

4. Legal and Regulatory Compliance: Many industries are subject to legal and regulatory requirements that mandate protection of sensitive information. Adhering to the CIA triad principles helps organizations meet these compliance standards.

5. Trust and Reputation: Implementing strong security measures based on the CIA triad enhances user trust and confidence in the organization's ability to protect their data and maintain service availability.

6. Mitigating Cyberattacks: The principles of the CIA triad help in mitigating various types of cyberattacks, including data breaches, unauthorized access, tampering, and denial-of-service attacks.

2(b) Write down an algorithm (i.e., *pseudocode*) to cryptanalyze a transposition cipher. You can consider a suitable ciphertext example if required.

A simple algorithm in pseudocode to cryptanalyze a transposition cipher. We'll use a basic columnar transposition cipher as an example.

Let's assume, **Ciphertext: EEATNISDTESOREARHTOLC** and **Key: 35241**

Here, The key "35241" indicates that the columns of the original plaintext should be rearranged in that order.

Pseudocode:

```
function decrypt_transposition(ciphertext, key):
    num_columns = length(key)
    num_rows = ceil(length(ciphertext) / num_columns)
    matrix = create_empty_matrix(num_rows, num_columns)
    result = ""
    index = 0
    for column in key:
        for row = 1 to num_rows:
            if index < length(ciphertext):
                matrix[row][column] = ciphertext[index]
                index = index + 1

    for row = 1 to num_rows:
        for column = 1 to num_columns:
            if matrix[row][column] is not empty:
                result = result + matrix[row][column]
    return result

ciphertext = "EEATNISDTESOREARHTOLC"
key = "35241"
plaintext = decrypt_transposition(ciphertext, key)
print("Plaintext:", plaintext)
```

This algorithm decrypts the columnar transposition cipher by arranging the columns according to the given key and then reading the rows in order to recover the original plaintext.

For the given example, using the key "35241", the algorithm would output: ***Plaintext: THISMESSAGEISCLEAR***

2(b-or) Analyze and explain the strength of a one-time pad with any suitable plaintext and ciphertext example.

The one-time pad is a type of encryption technique known for its theoretical strength and security. It operates by using a random and secret key that is as long as the plaintext message. The key is never reused, making it difficult for attackers to decipher the original message even if they have access to the encrypted text.

Let's consider a specific example to further illustrate the strength of the one-time pad encryption.

Plaintext: ATTACK **Key:** QWERT **Ciphertext:** QNVWXM

In this example, we'll walk through how the one-time pad encryption process works and highlight its strengths.

1. Key-Length Security: The key used in the one-time pad must be as long as the plaintext. In our case, the key "*QWERT*" is as long as the plaintext "*ATTACK*."

2. Encryption Process: Each letter in the plaintext is shifted by the corresponding letter in the key using modular arithmetic. **For example**, the letter **'A' is shifted by 'Q,' 'T' is shifted by 'W,'** and so on. This produces the ciphertext "*QNVWXM*."

3. Perfect Secrecy: One of the key strengths of the one-time pad is its perfect secrecy. Even if an attacker knows the ciphertext ("*QNVWXM*"), without the original key ("*QWERT*"), they cannot deduce the original plaintext ("*ATTACK*"). This is because every possible plaintext corresponds to an equally likely set of keys, making it impossible for the attacker to narrow down a specific solution.

4. Key Reuse Mitigation: To further emphasize the strength of one-time pad, consider what would happen if the same key were reused for a different message. Let's say the key "*QWERT*" is reused for a new plaintext "*HELLO*." The result would be:

Plaintext: HELLO **Key:** QWERT
Ciphertext: XIGGO

Now, even though the key is the same as before, the ciphertext "*XIGGO*" bears no resemblance to the previous ciphertext "*QNVWXM*." This demonstrates that even a minor change in the plaintext leads to a completely different ciphertext, ensuring that patterns cannot be exploited.

5. Unpredictability: The randomness of the key ensures that the relationship between the plaintext and the ciphertext is entirely unpredictable. Without knowledge of the key, an attacker cannot discern any patterns or correlations.

In summary, the strength of the one-time pad lies in its perfect secrecy, information-theoretic security, and the fact that it can produce ciphertexts that are statistically indistinguishable from random noise, making it a robust and theoretically unbreakable encryption technique when used properly.

3(a) Describe how communication is secured using end-to-end encryption.

End-to-end encryption is a security mechanism that ensures that the data exchanged between two parties remains confidential and cannot be accessed by any intermediary, including service providers, hackers, or even the platform facilitating the communication. This type of encryption provides a high level of privacy and security for sensitive information shared between users. *Here's how end-to-end encryption works and its key components:*

1. Encryption Key Generation:

- ✓ Each user involved in the communication generates a pair of cryptographic keys: a public key and a private key.
- ✓ The public key is shared openly, while the private key is kept secret and known only to the user.

2. Message Encryption:

- ✓ When User A wants to send a message to User B, User A's device retrieves User B's public key from a trusted source (e.g., a key server or through the application itself).
- ✓ User A's device then encrypts the message using User B's public key. Only User B's private key can decrypt this message.

3. Secure Transmission:

- ✓ The encrypted message is transmitted over a network, such as the internet, to User B's device.
- ✓ Even if someone intercepts the message while it's in transit, they cannot decipher its contents without User B's private key.

4. Message Decryption:

- ✓ Upon receiving the encrypted message, User B's device uses its private key to decrypt the message.
- ✓ The decrypted message is then made accessible to User B.

5. Ensuring Authenticity:

To ensure that the message hasn't been tampered with during transit, digital signatures can be used. User A can sign the message with their private key, and User B can verify the signature using User A's public key.

End-to-end encryption provides several benefits:
Confidentiality: Only the intended recipient can decrypt and read the message, ensuring that no one else, including service providers, hackers, or unauthorized individuals, can access the content.
Privacy: Even the service provider facilitating the communication doesn't have access to the content of the messages, enhancing user privacy.
Data Security: The encryption process safeguards data from breaches or data leaks that might occur on the communication platform's servers.
Trustworthiness: Users have greater confidence that their conversations are secure and private, fostering trust in the communication platform.
Mitigation against Man-in-the-Middle Attacks: Since the communication is encrypted end-to-end, attackers attempting to intercept messages between the sender and recipient cannot decipher the content.

Popular messaging apps like *Signal*, *WhatsApp*, and *Telegram* implement end-to-end encryption to ensure the security and privacy of their users' conversations. However, while end-to-end encryption provides strong protection, it's essential for users to also consider the security of their devices and the potential for compromised endpoints, as these factors can still impact the overall security of the communication.

3(a-or) Explain congruence with an example. Show the additive and multiplicative inverses for modulo 7 arithmetic.

Congruence is a mathematical relationship that involves integers and modular arithmetic. Two integers are said to be congruent modulo a certain number (called the modulus) if their difference is evenly divisible by that modulus. In mathematical notation, if we have integers a, b, and a modulus n (where n > 0), we say that "a is congruent to b modulo n," written as: **a ≡ b (mod n)**

Here's an example to illustrate congruence: Let's consider congruence modulo 5:
✓17 ≡ 2 (mod 5) because 17 - 2 = 15, and 15 is divisible by 5.
✓34 ≡ 4 (mod 5) because 34 - 4 = 30, and 30 is divisible by 5.

Now, let's discuss **additive and multiplicative inverses in modulo 7 arithmetic:**

Additive Inverse: For a given integer a in modulo n arithmetic, its additive inverse is another integer b such that a + b is congruent to 0 modulo n. In other words, b is the number that, when added to a, results in a multiple of n.
In modulo 7 arithmetic:
✓The add. inverse of 3 is 4, because 3 + 4 ≡ 0 (mod 7).
✓The add. inverse of 5 is 2, because 5 + 2 ≡ 0 (mod 7).

Multiplicative Inverse: For a given integer a in modulo n arithmetic, its multiplicative inverse is another integer b such that a * b is congruent to 1 modulo n. In other words, b is the number that, when multiplied by a, gives a result that leaves a remainder of 1 when divided by n.
In modulo 7 arithmetic:
✓The mul. inverse of 3 is 5, because 3 * 5 ≡ 1 (mod 7).
✓The mul. inverse of 4 is 2, because 4 * 2 ≡ 1 (mod 7).

It's important to note that not all integers have additive or multiplicative inverses in every modulus. For example, in modulo 7 arithmetic, there is no additive inverse for 0, and not all numbers have multiplicative inverses.

3(b) Describe briefly the logical and physical access control methods >> ***Answer in below in Sp-22.***

Spring 2022

1a) What is risk management? How can an organization manage the risk?

Risk management is the process of identifying, assessing, and mitigating risks that could potentially affect an organization's ability to achieve its objectives. Risks are uncertainties that can have positive or negative effects on an organization's projects, operations, or overall success. Effective risk management involves systematically evaluating these risks and taking actions to minimize their impact.

Here's a general overview of how an organization can manage risks:

1. **Risk Identification:** The first step is to identify and document all potential risks that could impact the organization. This involves looking at internal and external factors that could lead to disruptions, financial losses, legal issues, reputation damage, and so on.
2. **Risk Assessment:** Once risks are identified, they need to be assessed in terms of their potential impact and likelihood. This helps prioritize which risks need more immediate attention and resources.

3. **Risk Analysis:** For each identified risk, a more detailed analysis is conducted to understand its root causes, potential consequences, and possible scenarios. This helps in developing a better understanding of the risks and how they might interact with each other.
4. **Risk Mitigation Strategies:** Based on the analysis, organizations develop strategies to mitigate the identified risks. These strategies can include risk avoidance (eliminating activities that pose a risk), risk reduction (implementing safeguards to reduce the impact or likelihood of the risk), risk transfer (using insurance or contracts to shift the risk to another party), and risk acceptance (deciding to bear the risk if its impact is deemed acceptable).
5. **Implementation of Controls:** Organizations put in place controls, processes, and procedures to execute the chosen risk mitigation strategies. This could involve revising business processes, adopting new technologies, training employees, etc.
6. **Monitoring and Review:** Risk management is an ongoing process. Organizations continuously monitor the effectiveness of the implemented controls and regularly review the risk landscape to identify emerging risks or changes in existing risks.
7. **Communication and Reporting:** Effective risk management involves clear communication within the organization. Relevant stakeholders need to be informed about the risks, mitigation strategies, and progress. Reporting mechanisms should be established to keep everyone informed about the risk management efforts.
8. **Adaptation and Learning:** Organizations should be adaptable and open to learning from their risk management efforts. If a risk materializes despite mitigation efforts, a post-incident analysis should be conducted to understand why the risk occurred and how the organization can improve its risk management strategies in the future.
9. **Crisis Management Planning:** Despite all efforts, some risks might still materialize. Organizations should have crisis management plans in place to respond effectively to unexpected events and minimize their impact.

Remember that risk management is not a one-time activity but an ongoing process that requires attention and adaptation as the organization's environment and circumstances change. Different industries and organizations might have specific methodologies and tools tailored to their unique risks and challenges.

1b) Describe a network security model for your IT infrastructure and explain the roles of different entities in the model.

One commonly used network security model is the "***Defense in Depth***" model. This approach involves layering various security measures throughout your network to create multiple lines of defense against potential threats. Here's an overview of the model and the roles of different entities within it:

1. **Perimeter Defense:** The outermost layer of defense is the perimeter of your network. This is where you establish boundaries between your internal network and the external world, typically using firewalls, intrusion prevention systems (IPS), and intrusion detection systems (IDS). These entities monitor incoming and outgoing traffic, filtering out potentially malicious or unauthorized activity.
   - **Firewalls:** Control incoming/outgoing traffic based on rules.
   - **Intrusion Prevention Systems (IPS):** Block known attack patterns.
   - **Intrusion Detection Systems (IDS):** Alert on suspicious activity.
2. **Network Segmentation:** This involves dividing your internal network into smaller segments or zones, each with its own set of security controls. Even if an attacker breaches the perimeter, they'll face additional layers of security when attempting to move within the network.
   - **VLANs:** Divide network into segments for isolation.
   - **Network Access Control (NAC):** Ensure authorized access.
3. **Access Control:** This layer manages user and device access to different parts of the network. It ensures that only authorized individuals can access sensitive resources.
   - **Authentication Systems:** Verify user/device identity.

- **Authorization Systems:** Grant appropriate access.

4. **Access Control:** This layer manages user and device access to different parts of the network. It ensures that only authorized individuals can access sensitive resources.
   - Antivirus/ endpoints from threats.
   - Endpoint Detection and Response (EDR): Monitor/respond to endpoint issues.
   - Mobile Device Management (MDM): Secure mobile devices.
   - Antimalware: Protect
5. **Data Security:** This layer ensures the confidentiality, integrity, and availability of sensitive data.

Encryption: Safeguard data using encryption methods.

- **Data Loss Prevention (DLP):** Prevent unauthorized data transfers.
- **Backup and Recovery:** Regularly backup and restore critical data.

6. **Monitoring and Incident Response:** Constantly monitoring the network for signs of suspicious activity is essential. If a breach occurs, an effective incident response plan should be in place to mitigate the damage.
   - **Security Information and Event Management (SIEM):** Analyze security data.
   - **Incident Response Team:** Manage and coordinate breach responses.

2a) CIA >> previously solved

2b) Write down the steps of cryptanalysis for a transposition cipher, along with an example.

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

a) 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.

b) Width of the rows and the permutation of the columns are usually defined by a keyword.

c) 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".

d) Any spare spaces are filled with nulls or left blank or placed by a character (Example: _).

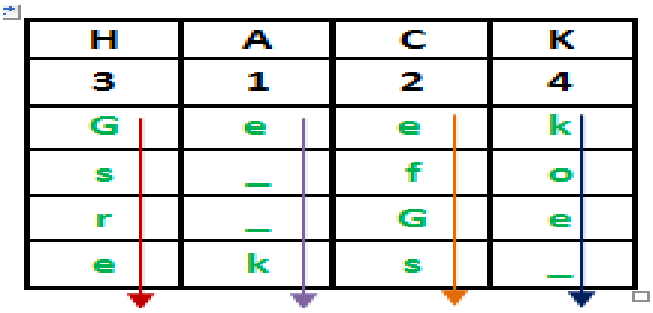
e) Finally, the message is read off in columns, in the order specified by the keyword.

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_ _k efGs Gsre koe_

Decryption:

a) To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.

b) Then, write the message out in columns again, then re-order the columns by reforming the key word.

2b) **or->** For a Shift cipher (Csesar cipher), find the cipher text for plaintext letter x with a shift value of k=3. Show modular operations in depth both for encrypting and decryption

Sure, let's go through both the encryption and decryption processes of a Caesar cipher with a shift value of k=3. In a Caesar cipher, each letter in the plaintext is shifted by a fixed amount to produce the ciphertext. The shift is done modulo the number of letters in the alphabet (26 for the English alphabet).

Encryption:

We want to encrypt the plaintext letter "X" with a shift value of 3.

1. Find the position of the letter "X" in the alphabet: X = 24.
2. Apply the shift: (24 + 3) % 26 = 1.
3. The resulting position is 1, which corresponds to the letter "A".

So, for the letter "X", the ciphertext is "A".

Decryption:

Now let's decrypt the ciphertext letter "A" back to the original plaintext letter "X" using the same shift value of 3.

1. Find the position of the letter "A" in the alphabet: A = 1.
2. Apply the reverse shift: (1 - 3) % 26 = 24. (***26-24***)
3. The resulting position is 24, which corresponds to the letter "X".

So, for the letter "A", the original plaintext is "X".

In the modulo operation, when shifting beyond the end of the alphabet, the remainder wraps around to the beginning. This ensures that the shifted letters stay within the range of the alphabet.

3a) Why we need both End to end and link encryption?

Both end-to-end and link encryption play distinct yet complementary roles in ensuring a robust and comprehensive approach to data security in communication networks.

End-to-end encryption focuses on securing the content of the communication itself. It guarantees that only the intended sender and recipient can access and understand the data, regardless of how many intermediaries it passes through. This is critical in safeguarding sensitive information from unauthorized access, ensuring data privacy, and maintaining the integrity of the content. Even if a malicious entity gains access to the communication path, they would be unable to decipher the encrypted content without the appropriate decryption keys. ***For example,*** Alice wants to send Bob an encrypted message. She uses Bob's public key to encrypt her message to him. Then, when Bob receives the message, he uses his private key on his device to decrypt the message from Alice.

On the other hand, link encryption addresses the security of the communication path itself. It involves encrypting data at each hop or network segment, protecting it from potential threats within the network. Link encryption guards against insider attacks, unauthorized interception, and tampering during transit between network devices. This layer of protection ensures that data remains secure as it traverses various points within the network infrastructure.

By combining both end-to-end and link encryption, organizations achieve a defense-in-depth strategy. End-to-end encryption ensures data confidentiality and integrity from sender to receiver, even if data is intercepted along the way. Meanwhile, link encryption fortifies the communication path, safeguarding data at each stage of its journey. This layered approach mitigates the risks associated with breaches, eavesdropping, and insider threats, creating a comprehensive security posture that is crucial in today's interconnected and data-driven digital landscape.

Au'22 || Sp'22 3a) or-> Describe briefly the logical and physical access control methods

Logical Access Control: Logical access control refers to the use of digital or software-based mechanisms to restrict and manage users' access to computer systems, networks, and digital resources. It focuses on ensuring that the right individuals have appropriate access privileges to digital assets. Some common methods include:

- **Username and Password:** The most basic form of access control, requiring users to provide unique usernames and passwords to authenticate themselves.
- **Multi-Factor Authentication (MFA):** Involves using multiple factors like passwords, biometrics, smart cards, or tokens to enhance security by requiring multiple proofs of identity.
- **Role-Based Access Control (RBAC):** Assigns access rights based on predefined roles, ensuring that users only have access to resources relevant to their job functions.
- **Attribute-Based Access Control (ABAC):** Grants access based on user attributes and resource properties, allowing more granular control over permissions.
- **Single Sign-On (SSO):** Allows users to access multiple systems with a single set of credentials, simplifying authentication while maintaining security.

Physical Access Control: Physical access control involves mechanisms and procedures designed to restrict entry to physical spaces, ensuring that only authorized individuals can enter specific areas. It's commonly used to protect buildings, rooms, and facilities. Some methods include:

- **Key-Based Access:** Traditional method where authorized individuals use physical keys to access restricted areas.

- **Smart Cards and Proximity Cards:** Users present a card to a card reader, and access is granted if the card's information matches the authorized data.
- **Biometric Authentication:** Uses physical characteristics like fingerprints, retinal scans, or facial recognition to grant access based on unique biological traits.
- **Access Control Lists (ACLs):** Lists individuals or groups authorized to enter a specific area and the times they are allowed access.
- **Security Guards:** Human personnel monitor access points, verifying identities and controlling entry to restricted areas.

Both logical and physical access control methods are crucial components of overall security strategies, ensuring that digital assets and physical spaces are protected from unauthorized access. They work together to provide comprehensive protection against various forms of threats and risks.

3b) Find the GCD of (450,120). How to find whether two numbers are co-prime?

To find the Greatest Common Divisor (GCD) of 450 and 120, we can use the Euclidean algorithm:

1. Divide the larger number (450) by the smaller number (120).
2. Find the remainder (450 % 120 = 90).
3. Replace the larger number (450) with the smaller number (120) and the smaller number (120) with the remainder (90).
4. Repeat steps 1-3 until the remainder becomes 0.
5. The last non-zero remainder is the GCD (90 in this case).

Using the Euclidean algorithm:

- 450 % 120 = 90
- 120 % 90 = 30
- 90 % 30 = 0

Since the remainder has become 0, the GCD is the last non-zero remainder, which is 30.

Two numbers are said to be coprime (or relatively prime) if their greatest common divisor (GCD) is 1. In other words, they don't share any common factors other than 1. To determine whether two numbers are coprime:

1. Calculate the GCD of the two numbers using the Euclidean algorithm.
2. If the GCD is 1, the numbers are coprime; if the GCD is greater than 1, they are not coprime.

In our case, the GCD of 450 and 120 is 30, which is not 1. Therefore, 450 and 120 are not coprime.

This is all about Segment 01 & 03 + Previous Solve of Autumn-2021 & Spring-2022

Segment- 02 will be available here >> **Click Me**