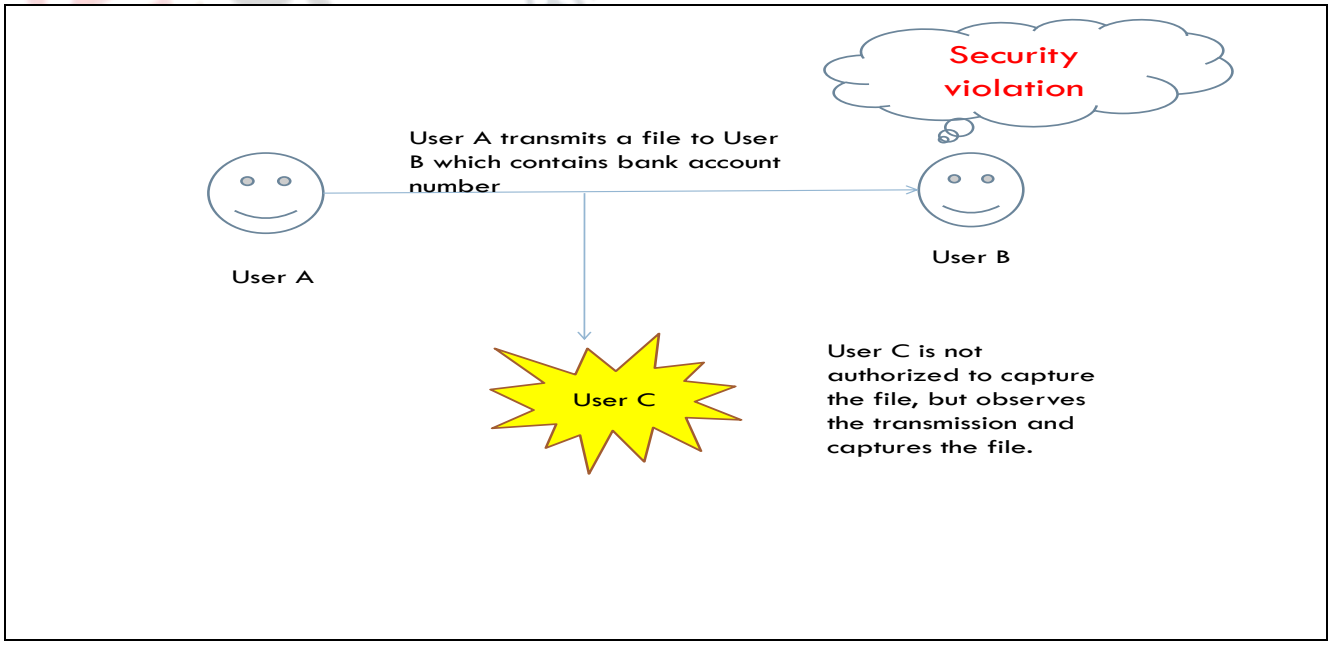
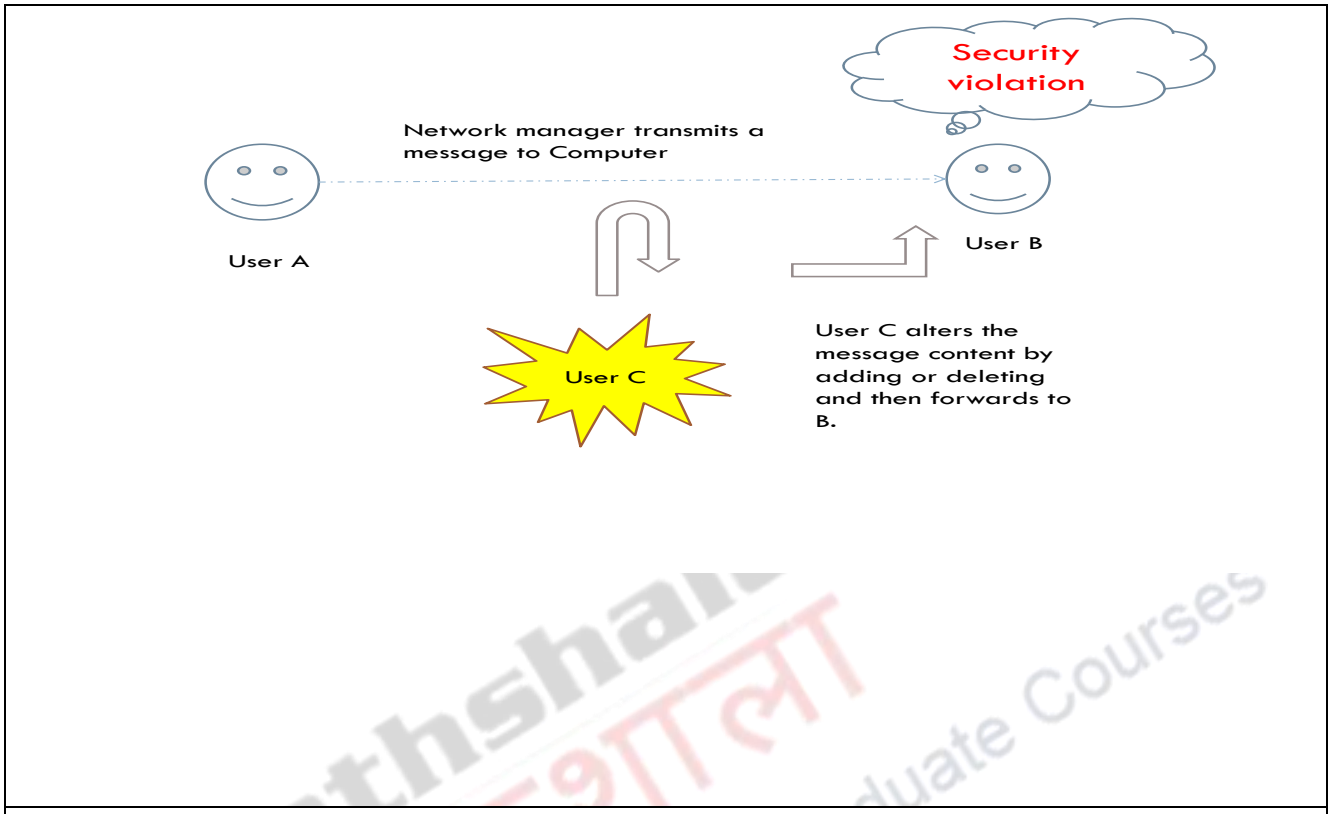
Module 1: Introduction to cryptography, key principles of security, security mechanisms, security services, threat, attack, the information systems security engineering process.

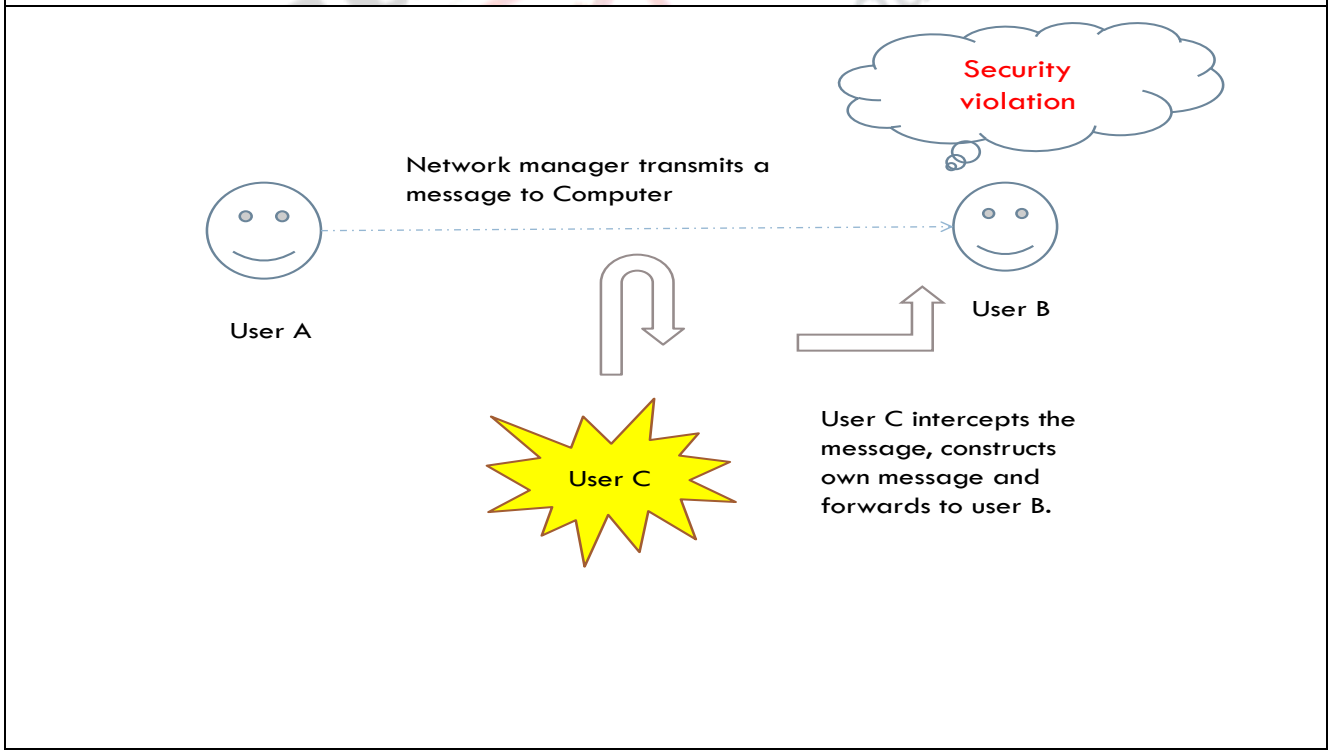
Types of security :

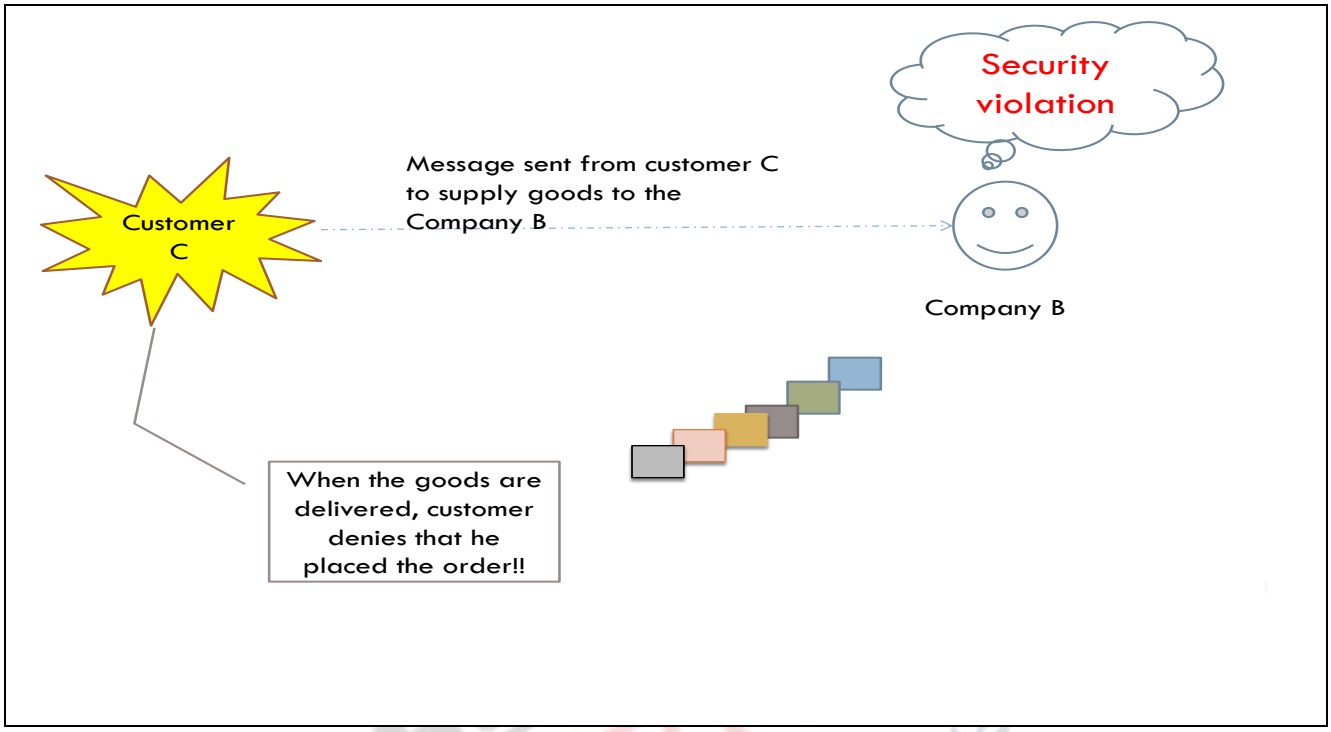
Information Security	Protecting information (physical or digital) from unauthorized access, use, disclosure, disruption, modification or destruction.
Computer Security	To protect files and other information stored on the computer. Computer may be time shared or part of public telephone network, data network or the internet.
Network Security	To protect data, when data is transmitted between computer to computer.

Security Violation :




Security violation
Network manager transmits a message to Computer
User A
User B
User C
User C alters the message content by adding or deleting and then forwards to B.


Security violation
Network manager transmits a message to Computer
User A
User B
User C
User C intercepts the message, constructs own message and forwards to user B.



The OSI Security Architecture:

The International Telecommunication Union(ITU) Telecommunication Standardization Sector(ITU-T) develops standards relating to open systems interconnection(OSI). OSI security architecture was developed in the context of the OSI protocol architecture.

The OSI Security Architecture:

1. **Security attack:** If information owned by an organization is compromised by any action, it is called security attack.
2. **Security mechanism:** Security mechanism is a process that is designed to detect, prevent or recover from a security attack.
3. **Security service:** Security service is used to mitigate security attack by using one or more security mechanism.

Security Policy: An Information Technology (IT) Security Policy identifies the rules and procedures for all who are accessing and using an organization's IT assets and resources.

Vulnerabilities, Threats, Attacks(RFC 2828):

- A vulnerability is a weakness in the security system.

- A threat is a potential cause of an incident, that may result in harm of systems and organization.
- An attack is an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Example of Attack(Password Guessing):

Password :
The attacker tries to guess the password.

Security Attacks:

- **Passive attack:** The attacker collects the information or make use of collected information but do not modify any resources so system resources are not affected.
- **Active attack:** The attacker changes or actions are altered.

Types of Passive Attacks:

- Release of message content.
- Traffic analysis.

Types of Active Attacks:

- Masquerade
- Replay
- Modification of messages
- Denial of service

Security Services(X.800):

- **Authentication**

  The parties exchanging information are truly the same parties that they claim to be.
- **Access control**

  Unauthorized persons can not use the resources.
- **Confidentiality**

  Unauthorized disclosure of data is not done.
- **Integrity**

  Data received is same as sent by an authorized person. No modification done.
- **Nonrepudiation**

Sender or receiver cannot deny that the message was sent and was received.

Security Mechanisms:

Encipherment	Use mathematical algorithm . The data is transformed from one form to another by using algorithm and key, which is difficult to understand.
Digital signature	Appended data so that the receiver can identify and verify the source.
Access control	Mechanisms that enforce access rights to resources.
Data Integrity	Mechanisms to assure the integrity of data.
Authentication Exchange	Mechanism to ensure identity by exchanging information.
Traffic padding	To get rid of traffic analysis, some bits are inserted into data.
Routing Control	In case of security threat, secure routing path is selected.
Notarization	For data exchange, trusted third party is used.

Cryptography :

- Original message is called plaintext.
- Coded message is called ciphertext.
- Process of converting plaintext to ciphertext is known as enciphering or encryption.
- Retrieving plaintext from the ciphertext is deciphering or decryption.
- Schemes used for encryption – decryption is called cryptography.
- Cryptanalysis is about breaking the code.

Encryption algorithms – Symmetric Encryption:

- C=E(K,P) Where C is the ciphertext, P is the plaintext, E is Encryption algorithm and K is the key.
- P=D(K,C) Where P is plaintext, C is ciphertext, D is decryption algorithm and K is the key.
- Encryption and Decryption keys are same. So this form is called symmetric encryption.

Encryption algorithms – Asymmetric Encryption:

- C=E(K_E,P) Where C is the ciphertext, P is the plaintext, E is Encryption algorithm and K_E is the encryption key.
- P=D(K_D,C) Where P is plaintext, C is ciphertext, D is decryption algorithm and K_D is the decryption key.
- Encryption and Decryption keys are different. So this form is called Asymmetric encryption.

Characteristics of cryptographic systems:

1. The type of operations used for transforming plaintext to ciphertext.
   - Substitution
   - transposition
2. The number of keys used.
3. The method in which processing of plaintext is done.
   - Block cipher
   - Stream cipher

Cryptanalysis:

Cryptanalysis is to recover the key by attacking the encryption system instead of recovering the plaintext or ciphertext.

- Two general approaches to attack a conventional encryption scheme.
  - Cryptanalysis: derive plaintext or key by relying on nature of algorithm and some knowledge of general characteristics of plaintext or sample plaintext-ciphertext pair.
  - Brute-force attack: The attacker tries all possible keys on ciphertext until plaintext is obtained.

Cryptanalytic attack: These types of attacks depend on amount of information known.

[1] Cryptography and Network Security Principles and Practices – William Stallings.

Type of Attack	Known to cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext
Known plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key.
Chosen plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key.
Chosen ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.
Chosen text	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key. • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key.

Probable word attack:

- An electronic funds transfer message has a standardized header or banner. This is an example of known plaintext.
- If an attacker is after some specific information, parts of the message is known. This is called probable word attack.

- Source code developed by Company Z includes copyright statement in some standardized position.

An Encryption scheme is called **unconditionally secure**, if the ciphertext generated by the scheme does not have enough information so that it can uniquely determine the corresponding plaintext, even though much of the ciphertext is available.

An Encryption scheme is **computationally secure**, if one of the following criteria is met.

1. The cost of breaking the cipher exceeds the value of the encrypted information.
2. The time required to break the cipher exceeds the useful lifetime of the information.

Brute force attack: This attack includes trying all possible keys to obtain plaintext from the ciphertext such that plaintext is modifiable.