OVERVIEW OF CRYPTOGRAPHY

R. Saravanan

Senior Professor

School of Information Tech and Engineering

VIT UNIVERSITY

Overview of Cryptography

- **Cryptography** – *design & analysis* of math techniques for *secure communication* of data in the *presence of adversaries* over an *insecure Channel*.
- Cryptography involves techniques to *secure the data/systems from illegitimate users.*
- **Legitimate Users**: Sender & Receiver.
- **Illegitimate Users**: Eavesdropper, Adversary, opponent, unauthorized person.

AIM of Cryptography

- **Securing data / systems from adversaries**
  - **Change** the data **from meaningful**/intelligible form **to meaningless**/unintelligible form by **scrambling** (transforming) it; called as **Encryption**.
  - Protecting the data by **hiding** it in the **multimedia** data such as **images, audio, video**; called as **Steganography** (not a part of cryptography).

Some Terminology

- **plaintext -** original message. – small letters
- **ciphertext -** encoded message – capital letters
- **key -** info used to generate ciphertext and it is known only to sender/receiver
- **encipher (encryption) -** converting plaintext to ciphertext
- **decipher (decryption) -** recovering plaintext from ciphertext
- **Cryptography** ={ algorithms used for encryption, decryption and message digest generation}
- **Cryptanalysis**: Techniques used for breaking the cipher text without knowing the key.
- **Cryptology** = Cryptography + Cryptanalysis.

Network Security

- **Aim:**
  - To *Secure the data transmissions* in the network
  - To *protect the data and systems* from the attacks by adversaries *through the network*.
- **Techniques adopted**:
  - Encryption, steganography, hashing, intrusion detection & prevention, antivirus and antispyware, firewalls etc.

Security Goals

- **Confidentiality-** only authorized user can access. Eg., *Confidential letters* should be opened by only the addressee
- **Data integrity -** Protecting data from unauthorized changes **Eg**. Modification in Mark statement to be done by University authorities only. Bank a/c balance to be updated by bank authorities only.
- **Data Availability** – Information to be available whenever it is required. Eg. Accessibility of the a/c while withdrawing money from ATM.

Security Attacks

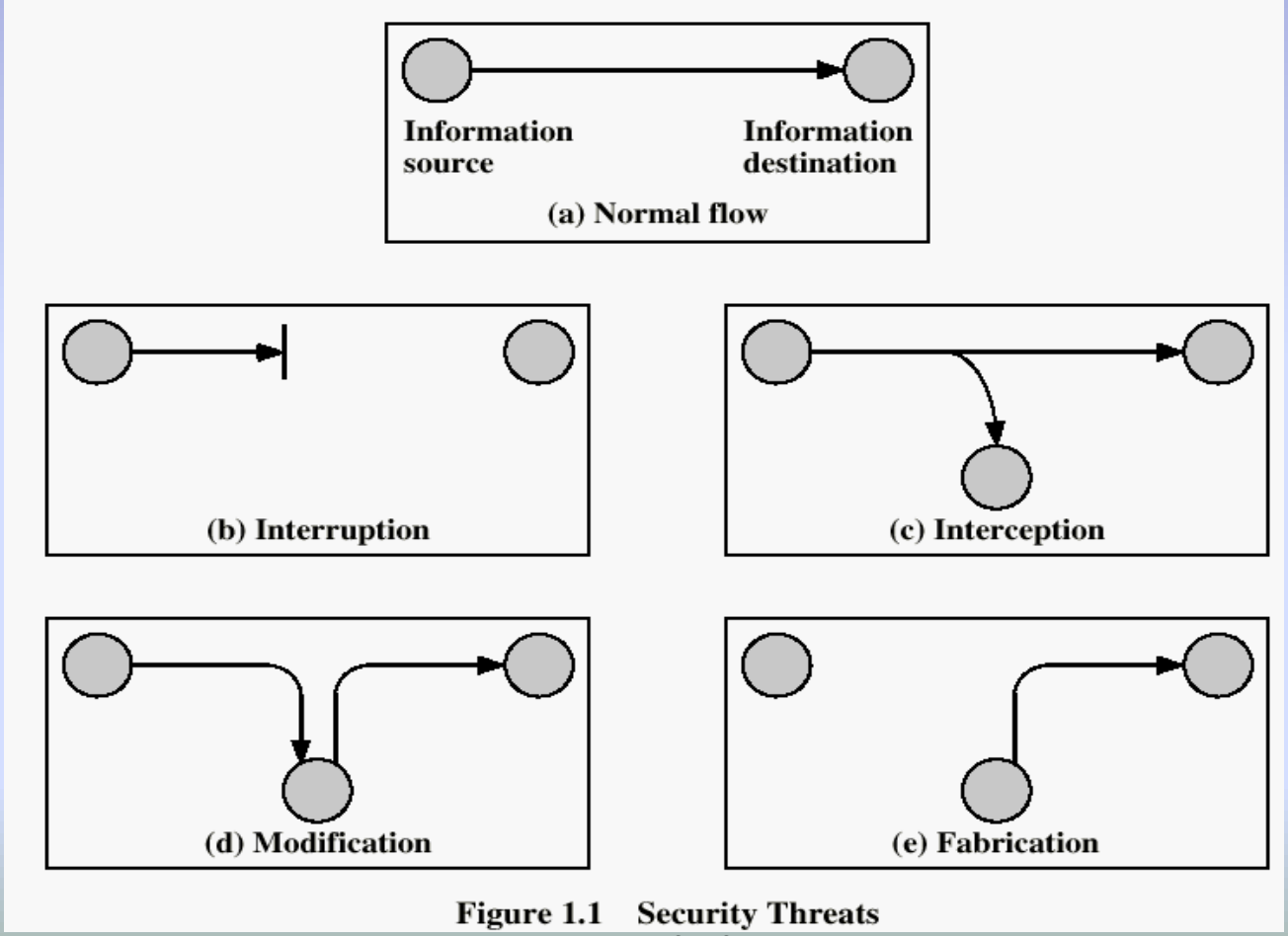


Figure 1.1 Security Threats

Attacks & Preventions

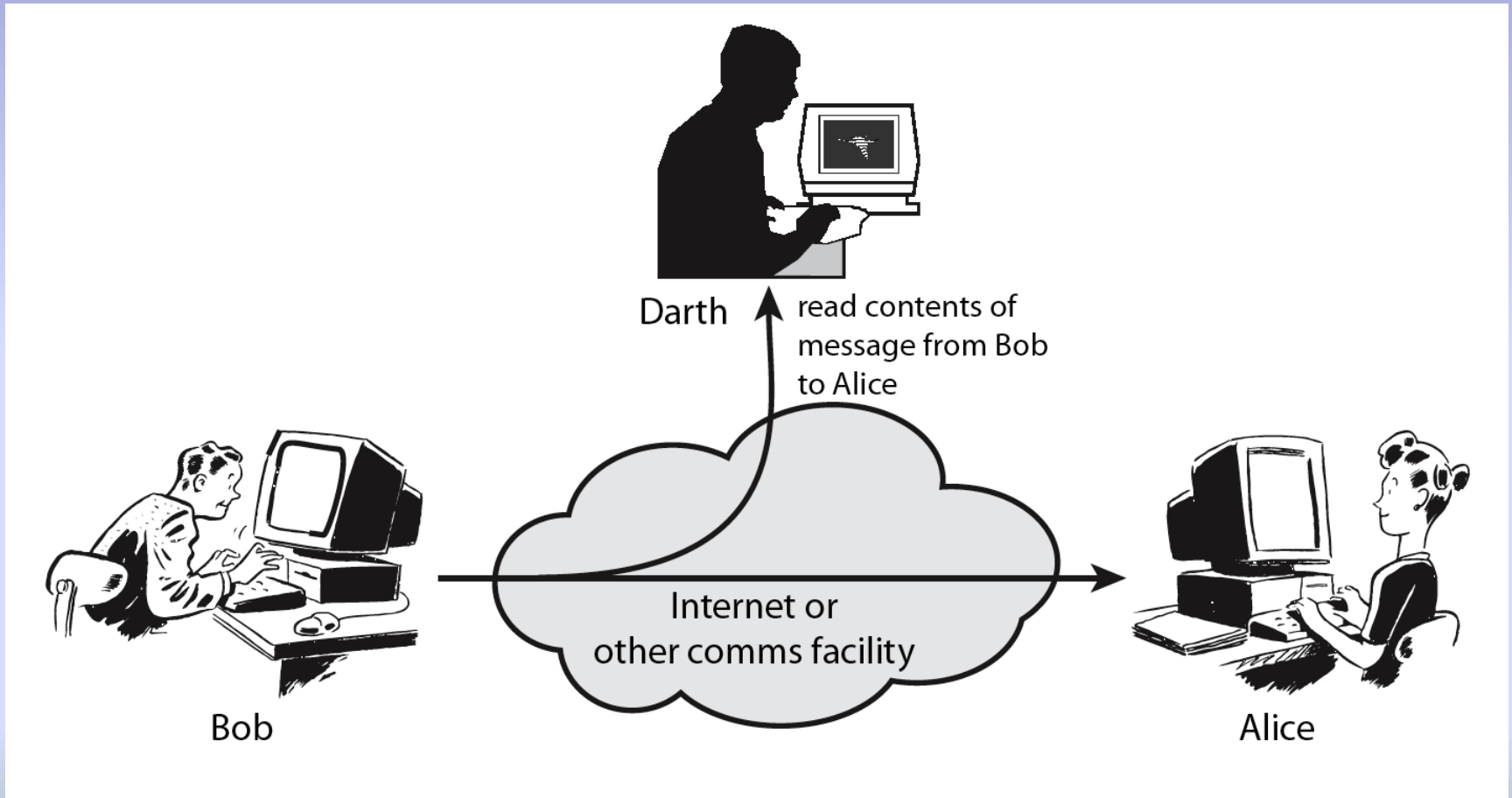
- Attacks on Confidentiality.
  - **Snooping** – Unauthorized access / interception of data. **Eg**. Intercepting credit card details in online transactions.
  - **Traffic Analysis** – Monitoring the traffic in the network. Using it, guessing the sender, receiver, nature of transaction etc.
- Prevention: Encryption.

- **Attacks on Data integrity**
  - **Modification** (content, sequence, timing (delay)) → deletion, insertion & replacement- Prevention: Use Hashing
  - **Masquerade** – impersonation. Use Digital signature.
  - **Replay** – Copy the data when it is transmitted in the n/w and retransmit it. Eg. When a user sends to a bank: "Make payment to Merchant XYZ". The merchant retransmits a copy of it to get the payment second time also.
  - **Repudiation** (source / destination) – Source sends data and says that it didn't send. Destination receives and says that it didn't receive.
- **Attack on Availability**: Denial of Service, Data deletion by virus

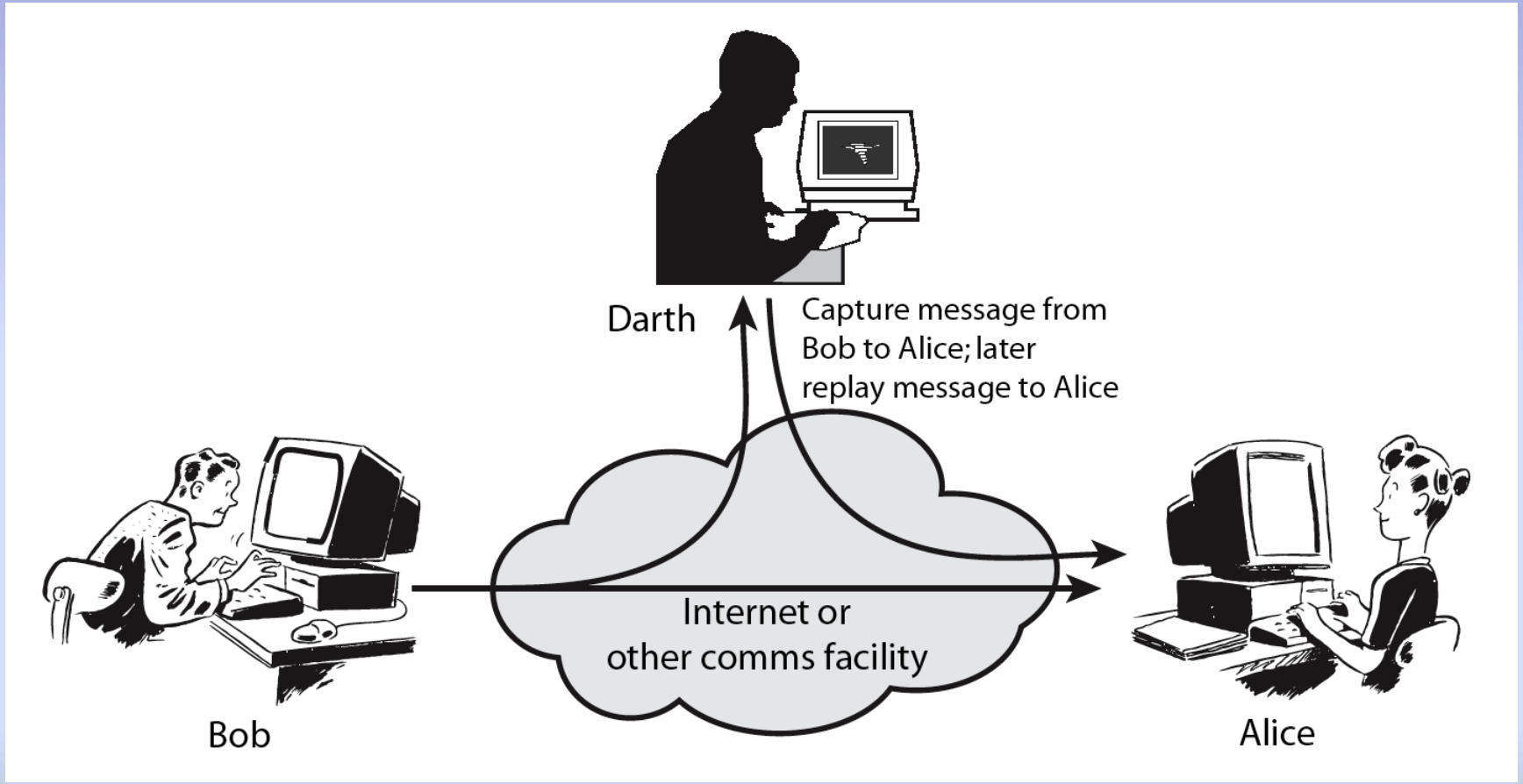
Types of Attacks

- **Passive Attack-** it *neither modifies* the data *nor harms* the systems but *affects the sender/receiver* Eg. Snooping, traffic analysis
- **Active Attack**. Eg. Modification, repudiation etc.

Passive Attacks



Active Attacks



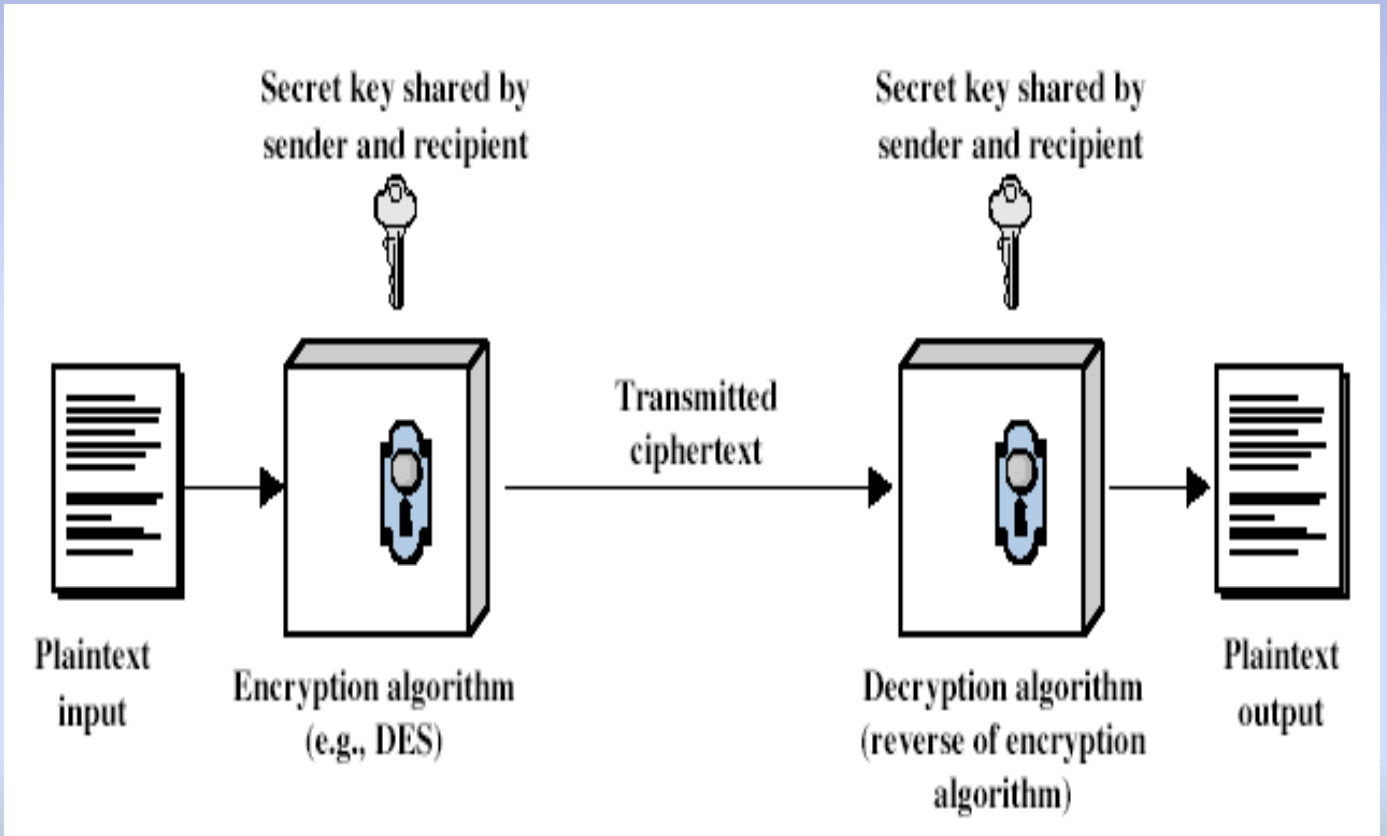
Cryptanalyst

- Assume that **Adversary is powerful** & has all capabilities and **resources** to perform all kinds of attack.
- He knows communication protocols and cryptographic techniques deployed.
- Only the key (secret data) is unknown (kept secret)

Types of Cryptosystems

- **Secret Key** Cryptosystem (Symmetric key, conventional, single key)
- **Public key** Cryptosystem (Asymmetric key, Two Key)
- **Hybrid** Cryptosystem (uses both systems)

Secret Key Cryptosystem



Secret Key Cryptography

- **Operations:** substitutions and Permutations
- Based on **Feistel cipher** network mostly
- **Ex :** Skipjack, Triple DES, AES, IDEA, Blowfish (twofish, threefish), RC4 etc.
- **Strength analysis**: Avalenche effect. Amount of confusion and diffusion
  - A small change in either key or PT results in major changes in CT
- **Attacks:** Brute force, cipher text only, Known plain text, chosen plain text, chosen cipher text etc.

Substitution

- **Substitution** – substitute one letter for another. i.e, replace one symbol by another
  - **Mono-alphabetic substitution** – Each letter is replaced by a unique letter. Eg., if ‘t’ is replaced by ‘u’ at one place, then ‘t’ will be replaced by same latter ‘u’ everywhere.
  - **Poly-alphabetic substitution** – Each letter is replaced by any one letter in a set depending on the context. Eg., if ‘t’ is replaced by ‘u’ at one place, then ‘t’ will not be replaced by same latter ‘u’ everywhere; but it will be replaced by some other letter in the same set.
  - **Example: *Mono-alphabetic substitution*** . text → UFYU (substitute by it successor) – intelligible form→ unintelligible form
  - **Example: *Poly-alphabetic substitution***. test → LKZS. Here t is replaced by L at one place and t is replaced by S at another place. (playfair cipher)

Permutation

- **Permutation (transposition)** – interchange the symbols. i.e. permute the symbols i.e., rearrange the symbols i.e., change the order of the symbols.
  - **Example:** Test →etst (1234 is rearranged as 2134)

Symmetric Key Algorithms.

- Shift Cipher
- Substitution Cipher
- Affine Cipher
- Hill Cipher
- Vigenere Cipher
- DES - Data Encryption Standard
- AES – Advanced Encryption Standard …