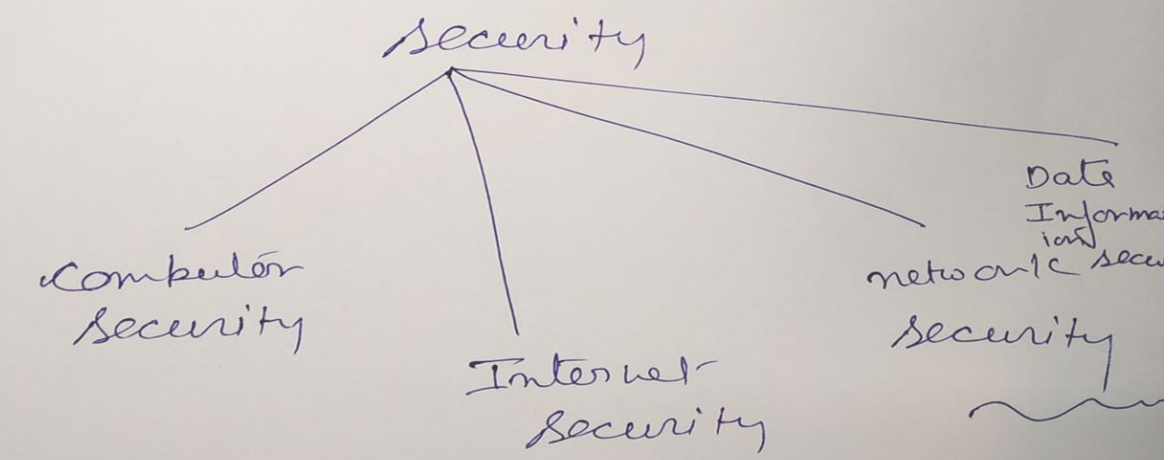
NETWORK SECURITY
DITS-512
INTRODUCTION

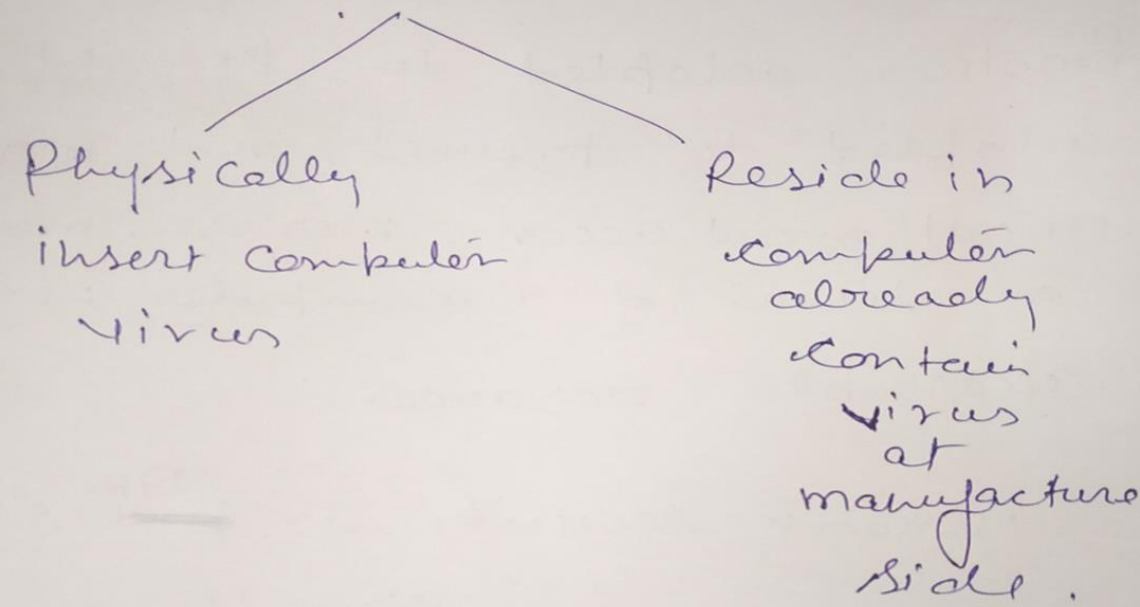
Network Security

→ Network security consists of the policies and practices adopted to prevent and practices adopted to prevent and monitor unauthorized access, misuse, modification or denial of a computer network. Network accessible resources.

→ Network security is ~~kind~~ Type of security



→ There are no clear boundries b/w these two form of security

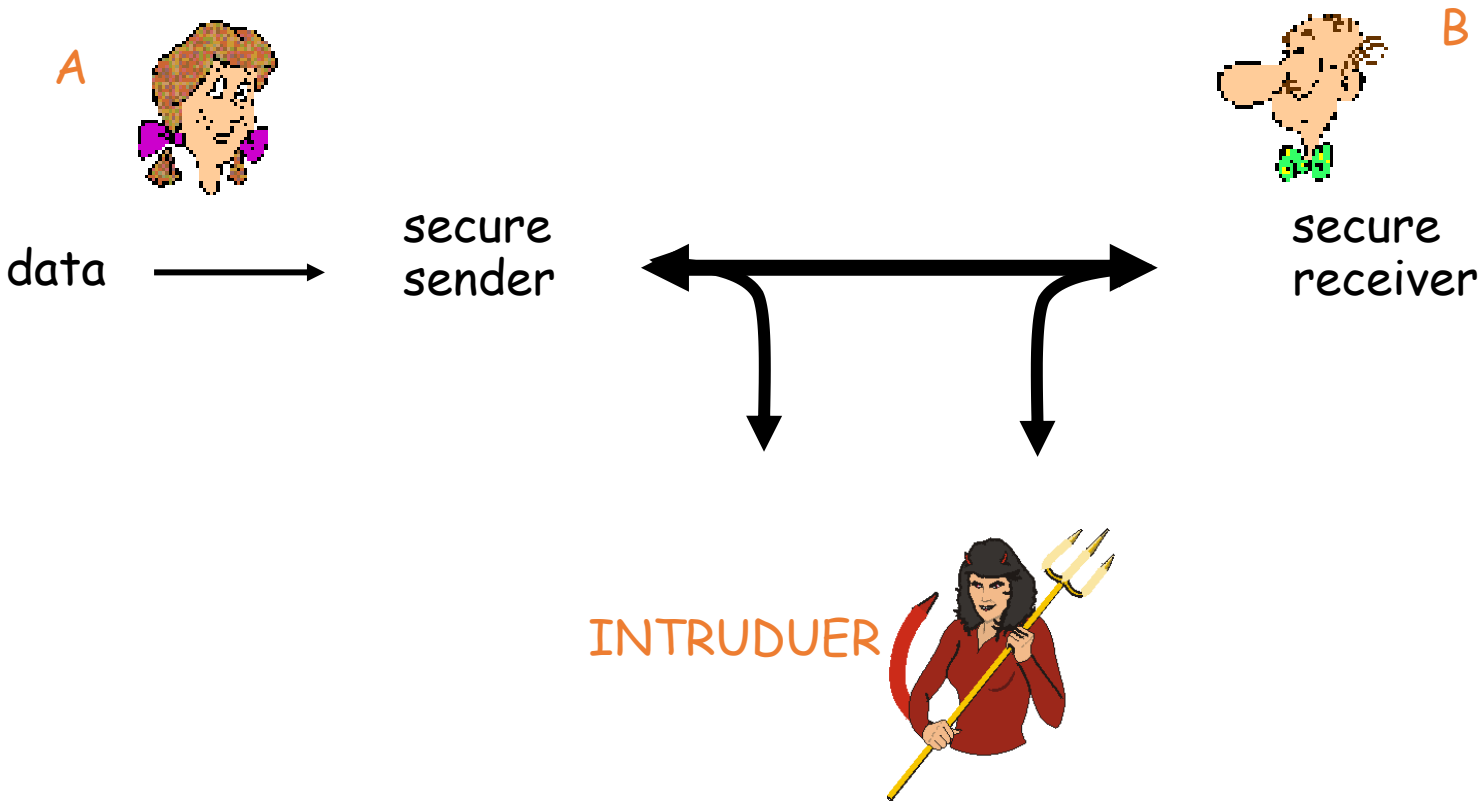


→ Now a days information is an asset that has value like any other asset

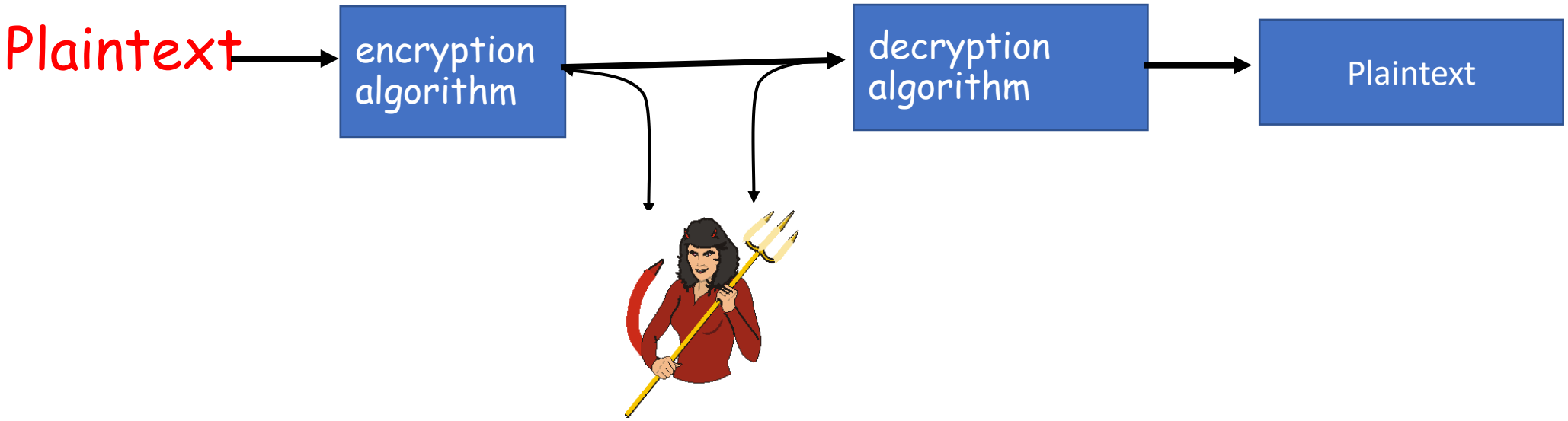
→ information needs to be secure from attacks

A Sends data to B

- well-known in network security world
- B, A want to communicate “securely”
- Intruder may intercept, delete, add messages



The language of cryptography



- Issues
  - What is a good symmetric encryption scheme?
  - What is the complexity of encrypting/decrypting?
  - What is the size of the ciphertext, relative to the plaintext?

OSI security architecture

- The OSI security architecture provides a systematic framework for defining security attacks mechanism and services.
- Security attacks are classified as either passive attacks which include unauthorised reading of message of file and traffic analysis and active attack such as modification of message and denial of service .
- Security mechanism any process that is designed to detect, prevent or recover from security attack.
- Security Services include Authentication, access control, data confidentiality, Data integrity, Non repudation & availability.

Network layer:->

•In this layer , the security framework uses firewall, for packet inspection which are entering & leaving network.
•Router using access control lists filters IP packets preventing unused traffic.
•VPNs protect information by encrypting it and sending it through encrypted tunnels through network or internet.

Transport Layer:->

•At this level, we use secure socket layer(SSL) & Transport Layer Security(TLS)

➔ ***SSL :-*** It is able to provide security service for any TCP based application protocol like FTP, HTTP, TELNET etc.
It is based on connected oriented & reliable services.
Eg- Handshake

➔ ***TLS:-*** It aims to enhance the security services by additional security properties for transport layer.
It is based on Internet terminology where the application layer is directly on top of the transport layer.
Eg:- Message Authentication.

- **Security features at Various layers of OSI model**

- **Physical layer:->**
- **At this layer , the security framework protects the cable plant ,the wiring & telecommunication infrastructure.**

- **The physical layer is to protect physical hardware in network area, server & system.**

- **Protecting the physical layer entries(entry point), alarms on entrances & access of data centers.**

- **Data Link Layer:->**
- **At this layer , the security framework protects the system with number of technologies.**

- **Network intrusion detection system watch traffic flowing over the wires, leaking for bit stream patterns that could indicate attacks on malicious content.**

- **Host intrusion detection system monitor bit streams entering the host machine at neywork interface** card(NIC) level, also looking for suspicious patterns

- Session Layer:->
  - In this, the security from work uses a number of techniques & tools to protect system.
-
  - Some of the policies for system management such as Hardening the OS, keeping batch level & OS revisions up to date.

- Presentation & Application Layer:->

  - The security framework utilizes user account management to control access to network system & applications.

  - Virus scanning application to scan hard drive & system memory for malicious code, update scan engines, & virus signature are used.

  - For security we use some protocol like SMTP, secure electrical transaction over HTTP.