Lecture Notes

**B.Tech. (CSE) Seventh Semester**

**CRYPTOGRAPHY AND NETWORK SECURITY**

**Code: EURCS 721** **Category: CE**

**Credits: 4** **Hours: 4 per week**

**Department: CSE**

**Unit-I**

Introduction to Cryptography: Introduction To Security: Attacks, Services & Mechanisms, Security, Attacks, Security Services. Conventional Encryption: Classical Techniques, Conventional Encryption Model, and Steganography, Classical Encryption Techniques. Modern Techniques: Simplified DES, Block Cipher Principles, DES Standard, DES Strength, Differential & Linear Cryptanalysis, Block Cipher Design Principles, Block Cipher ModesOf Operation.

**Unit-II**

Conventional Encryption Algorithms: Triples DES, Blowfish, International Data Encryption Algorithm, RCS, CAST-128, RC2 Placement & Encryption Function, Key Distribution, Random Number Generation, Placement Of Encryption Function.

**Unit-III**

Public Key Encryption: Public-Key Cryptography: Principles of Public-Key Cryptosystems, RSA Algorithm, Key Management, Fermat's & Euler's Theorm, Primality, The Chinese Remainder Theorem.

**Unit-IV**

Hash Functions: Message Authentication & Hash Functions: Authentication Requirements, Authentication Functions, Message Authentication Codes, Hash Functions, Birthday Attacks, Security Of Hash Function & MACS, MD5 Message Digest Algorithm, Secure Hash Algorithm (SHA), Digital Signatures: Digital Signatures, Authentication Protocol, Digital Signature Standard (DSS), Proof Of Digital Signature Algorithm.

**Unit-V**

Network & System Security: Authentication Applications: Kerberos X.509, Directory Authentication Service, Electronic Mail Security, Pretty Good Privacy (PGP), S / Mime, Security: Architecture, Authentication Header, Encapsulating Security Payloads, Combining Security Associations, Key Management, Web Security: Secure Socket Layer & Transport Layer Security, Secure Electronic Transaction (Set), System Security: Intruders, Viruses, Firewall Design Principles, Trusted Systems.

**Lecture 1**

**The OSI Security Architecture**

To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. This is difficult enough in a centralized data processing environment; with the use of local and wide area networks, the problems are compounded.

ITU-T Recommendation X.800, *Security Architecture for OSI*, defines such a systematic approach. The OSI security architecture is useful to managers as a way of organizing the task of providing security. Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms.

For our purposes, the OSI security architecture provides a useful, if abstract, overview of many of the concepts that this book deals with. The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as follows:

* **Security attack:** Any action that compromises the security of information owned by anorganization.
* **Security mechanism:** A process (or a device incorporating such a process) that is designed todetect, prevent, or recover from a security attack.
* **Security service:** A processing or communication service that enhances the security of the dataprocessing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

**Lecture 2**

**Security Attacks**

A useful means of classifying security attacks, used both in X.800 and RFC 2828, is in terms of *passive* *attacks* and *active attacks*. A passive attack attempts to learn or make use of information from thesystem but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

**Passive Attacks**

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents and traffic analysis.

The **release of message contents** is easily understood. 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.

**Active Attacks**

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A **masquerade** takes place when one entity pretends to be a different entity.

A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

**Authentication**

The authentication service is concerned with assuring that a communication is authentic. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Two specific authentication services are defined in X.800:

* **Peer entity authentication:** Provides for the corroboration of the identity of a peer entity in anassociation. It is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.
* **Data origin authentication:** Provides for the corroboration of the source of a data unit. It doesnot provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior interactions between the communicating entities.

**Access Control**

In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

**Data Confidentiality**

Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. For example, when a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection. Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message. These refinements are less useful than the broad approach and may even be more complex and expensive to implement.

The other aspect of confidentiality is the protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility.

**Data Integrity**

As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection.

A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering, or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service. On the other hand, a connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only.

**Nonrepudiation**

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

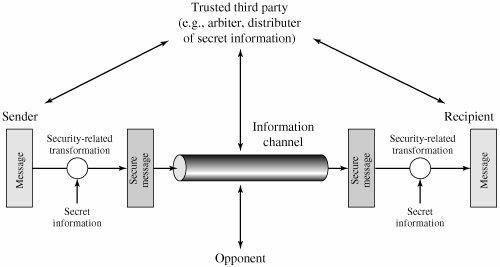
**Availability Service**

Both X.800 and RFC 2828 define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them). A variety of attacks can result in the loss of or reduction in availability. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption, whereas others require some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

**Lecture 3**

**A Model for Network Security**

A model for much of what we will be discussing is captured, in very general terms, in. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the *principals* in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.



Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

**Network Access Security Model**

