GITAM
DEEMED TO BE UNIVERSITY

Course Code : CSEN2071

Course Title : Cryptography and Network Security

Class :3/4 B.Tech CSE

Semester : 6th

Sections : J and N

PPT : Unit-I

K. Venkateswarlu
Assistant Professor
Dept of CSE,GIT,GITAM

GITAM
DEEMED TO BE UNIVERSITY

Introduction to Cryptography and Network Security

GITAM
DEEMED TO BE UNIVERSITY

Index

- History and usage
- Why do we need to study cryptography
- What is a cryptography and network security title
- How does cryptography work: Example
- Cryptanalysis: Example
- Security Attacks
- Security Services
- Security Mechanisms
- Model for Network Security
- Model for Network Access Security

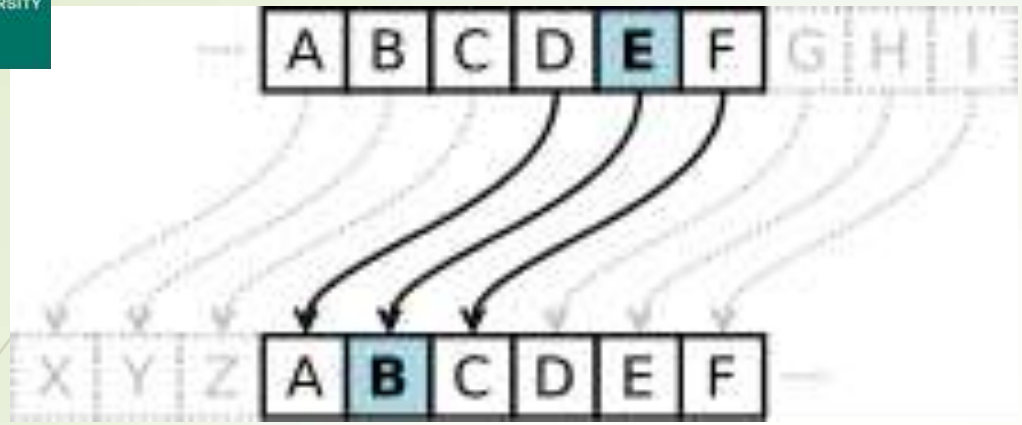
History and usage

- **Julius Caesar-**12 July 100 BC – 15 March 44 BC) was a Roman Empire.
- While Caesar's was the first recorded use of this scheme substitution ciphers.
- a **Caesar cipher**, also known as a **Caesar's cipher**, the **shift cipher**, **Caesar's Code** or **Caesar Shift**, is one of the simplest and most widely-known encryption techniques
- used it with a shift of three to protect messages of military significance

Example:

Plaintext : department of cse

Cipher Text: GHSDUWPHQW RI FVH



- Substitution type ciphers, this Caesar cipher is the simplest to solve, since there are only 25 possible combinations.

- This type of cipher is implemented on a wheel device. A disk or wheel has the alphabet printed on it and then a movable smaller disk or wheel with the same alphabet printed on it is mounted forming an inner wheel. The inner wheel then can be rotated so that any letter on one wheel can be aligned with any letter on the other wheel.

GITAM
DEEMED TO BE UNIVERSITY

- This course develops a basic understanding of the algorithms used to protect users data in online.
- **Cryptography** is a method to encrypt and decrypt the data. Sometimes **we need** to send or receive the data in encrypted format. ... So it is the most preferred method to store secret data.
- **Studying cryptography** leads to better carrier in defense and as a computer specialist.

What is a cryptography and network security title ?

- The **word** '**crypto**' **comes** from the Greek **word**
- kruptós, **meaning** 'hidden' or 'secret'.

- The English suffix -**graphy** means a "field of study" or related to "writing", and is an anglicization of the French -graphie inherited from the Latin -graphia, which is a transliterated direct borrowing from Greek.

- **cryptography == secret writing**

GITAM
DEEMED TO BE UNIVERSITY

- A **network** is a collection of computers, servers, mainframes, **network** devices, peripherals, or other devices connected to one another to allow the sharing of data. An example of a **network** is the Internet, which connects millions of people all over the world.

- **Network security** is a broad term that covers a multitude of technologies, devices and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer **networks** and data using both software and hardware technologies.

Cryptography and Network Security

- **Organized into three broad categories:**

- **1.Cryptology:** The two main branches of cryptology are
- **cryptography:** The Science & art of creating secret codes.
- **Cryptanalysis:** The Science & art of breaking those codes.

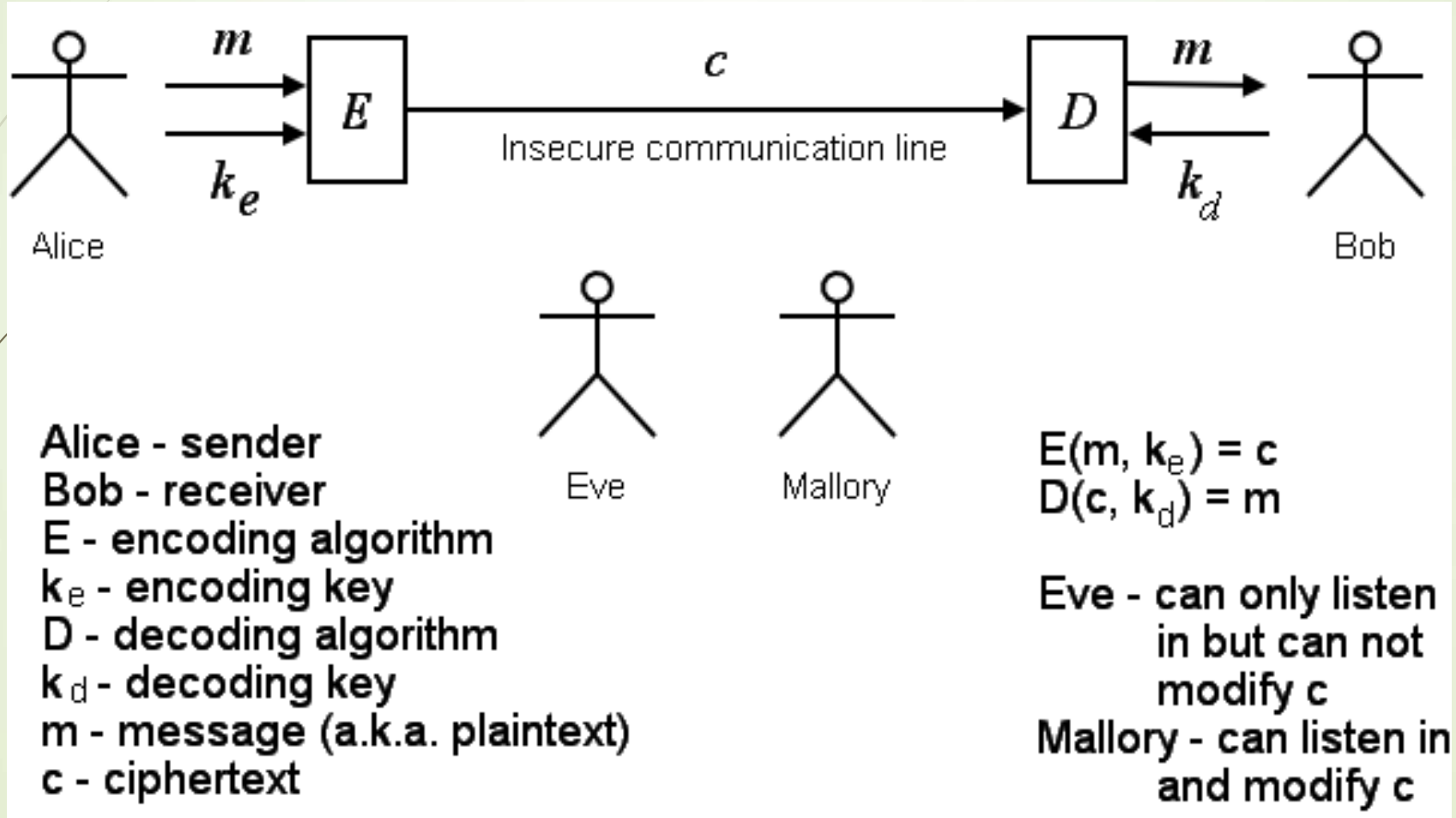
- **2.Network security:** the use of cryptographic algorithms in network protocols and network applications.

- **3.Computer security:** The security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses). Typically, the computer to be secured is attached to a network and the bulk of the threats arise from the network.

How does cryptography work

- A Cryptographic algorithm or Cipher is a mathematical function used in the Encryption & Decryption process.
- Cryptographic algorithm works in combination with
- **1.Key**
- **2.Word/Text/Message**
- **3.Number**
- To encrypt the plain text to different cipher text
- To decrypt the cipher text to plain text
- **The security of the encryption data is dependent on two things**
- **1. The strength of cryptographic algorithm**
- **2. The Secrecy of the key**
- A cryptographic algorithm plus all possible keys and all the protocols that make it work comprise a **CRYPTOSYSTEM**

Cryptography: Example



GITAM
DEEMED TO BE UNIVERSITY

Cryptographic Algorithms & Protocol can be grouped in to four main areas.

1. **1.Symmetric Encryption :** one **key** (a secret **key**) is used to both **encrypt** and **decrypt**
2. **2.Asymmetric Encryption:** is a form of encryption where keys come in pairs. one key encrypts, only the other can decrypt.
3. **3.Data Integrity Algorithms:** to protect block of data such as message from alterations .
4. **4.Authentication Protocols:** This are schemas based on the use of cryptographic algorithms designed to authenticate the identity of entities.

Classical Encryption Techniques

Substitution Techniques

1. Caesar Cipher
2. Monoalphabetic Ciphers
3. Playfair Cipher
4. Hill Cipher
5. Polyalphabetic Ciphers
6. One-Time Pad

Transposition Techniques

1. Rail Fence Technique
2. Rotor Machines

GITAM
DEEMED TO BE UNIVERSITY

Advanced Encryption Techniques

Symmetric encryption algorithms

1. Data Encryption Standard (DES)
2. Advanced Encryption Standard (AES)
3. IDEA (International Data Encryption Algorithm)
4. Blowfish (Drop-in replacement for DES or IDEA)
5. RC4 (Rivest Cipher 4)
6. RC5 (Rivest Cipher 5)
7. RC6 (Rivest Cipher 6)

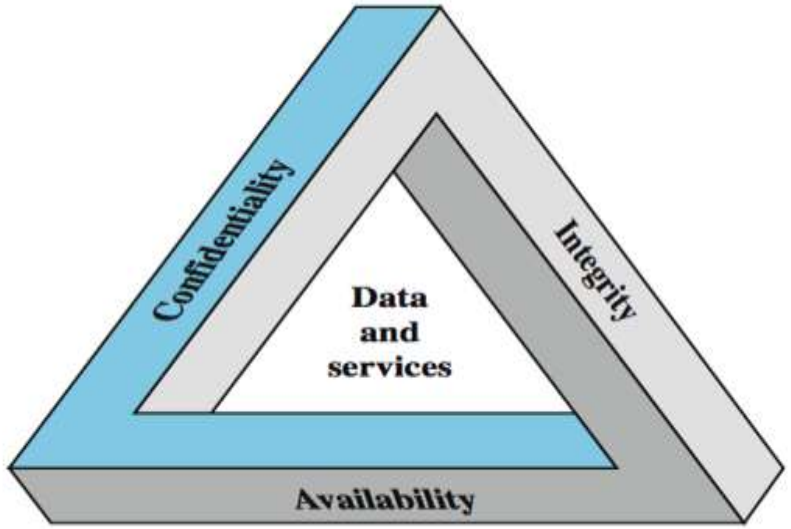
Asymmetric encryption algorithms

1. Diffie-Hellman algorithm
2. RSA (Rivest–Shamir–Adleman) algorithm
3. Elliptic-curve cryptography (ECC)
4. ElGamal encryption algorithm
5. Digital Signature Algorithm

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:



1.Confidentiality:(covers both data confidentiality and privacy): Unavailable to unauthorized persons.
2.Integrity: (covers both data and system integrity): Avoid unauthorized manipulation and change | Access into only in a authorized manner.
3.Availability: Services is provided to authorized persons.
* Additional concepts are needed for providing complete security
4.Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
5.Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

1. Low: The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
2. Moderate: The loss could be expected to have a serious adverse effect on organizational operations, assets, or individuals
3. High: The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

CRYPTANALYSIS

1. Typically, the objective of attacking an encryption system is to recover the key in use rather then simply to recover the plaintext of a single cipher text.
2. There are two general approaches to attacking a conventional encryption scheme:
3. **1. Cryptanalysis:** Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext ciphertext pairs.
4. **2.Brute-force attack:** The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Cryptanalysis: Example

Caesar Cipher:

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

P	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Example:

Plain Text	m	e	e	t
Cipher Text	P	H	H	W

0	1	2	3	4	5	6	7	8
a	b	c	d	e	f	g	h	i
26	25	24	23	22	21	20	19	18

9	10	11	12	13	14	15	16	17
j	k	l	m	n	o	p	q	r
17	16	15	14	13	12	11	10	9

18	19	20	21	22	23	24	25
s	t	u	v	w	x	y	z
8	7	6	5	4	3	2	1

Encryption:

C=E (K, P)=(P+K)mod 26

m: C=(12+3)mod 26=11 =P

e: C=(4+3)mod 26=19 =H

e: C=(4+3)mod 26=19 =H

t: C=(19+3)mod 26=4 =W

Plain Text: m e e t

Cipher Text: P H HW

Decryption:

P=D(K,C)=(C-K)mod 26

P: P=(15-3)mod 26=14 =m

H: P=(7-3)mod 26=22 =e

H: P=(7-3)mod 26=22 =e

W: P=(22-3)mod 26=7 =t

Cipher Text: P H HW

Plain Text: m e e t

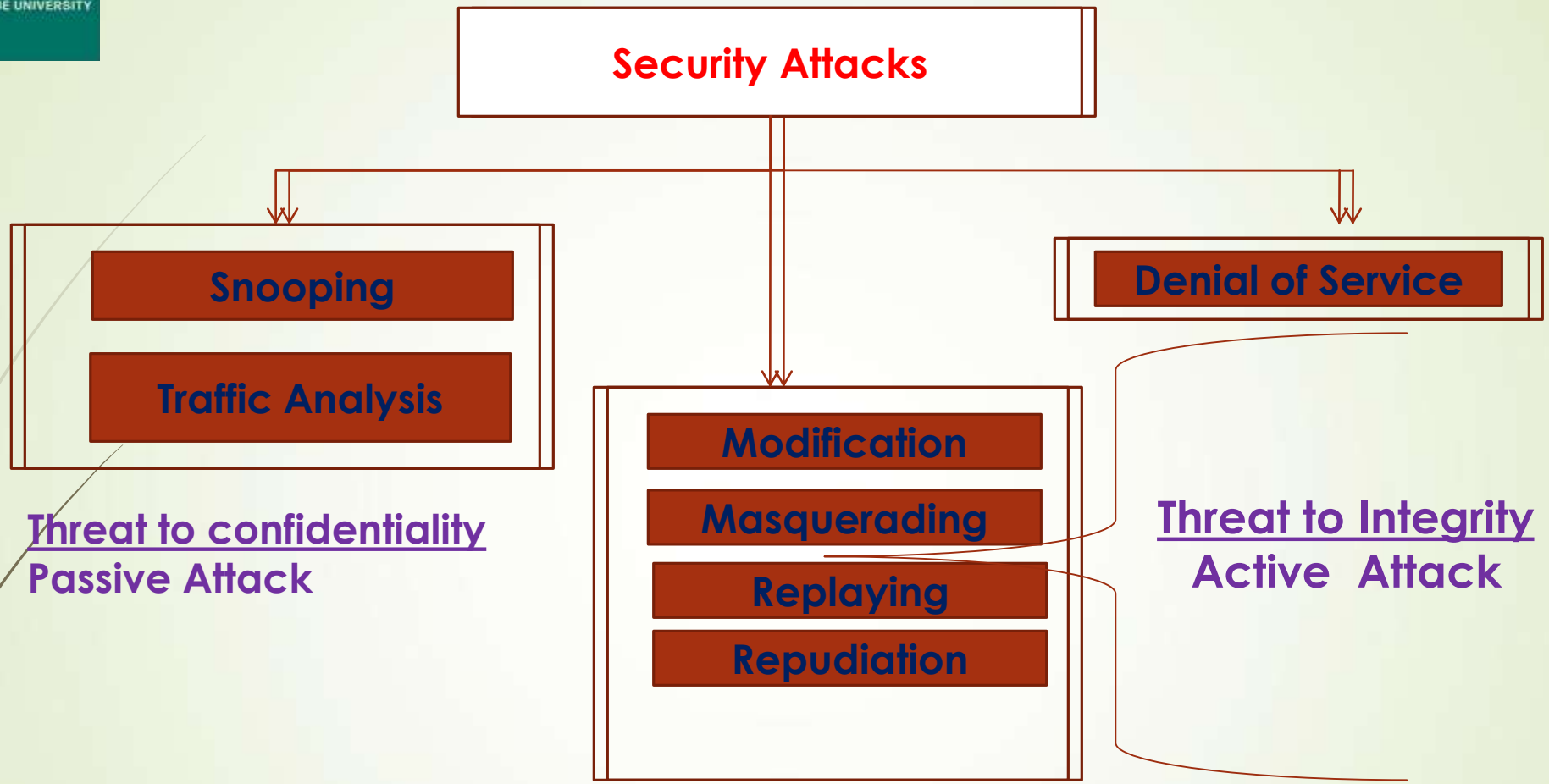
Brute-Force Cryptanalysis of Caesar Cipher

- If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: Simply try all the 25 possible keys
- shows the results of applying this strategy to the example cipher text. In this case, the plaintext leaps out as occupying the third line.

key	P	H	H	W
1	o	g	g	v
2	n	f	f	u
3	m	e	e	t
..	..	..	..	..

Security Attacks

1. **Security attacks can be classified in two**
2. **1.Passive attack :**A passive attack attempts to learn or make use of information from the system but does not affect system resources.
3. a. Release of message contents
4. b. Traffic analysis
5. **2. Active attack :**An active attack attempts to alter system resources or affect their operation.
6. a. Masquerade
7. b. Replay
8. c. Modification of message contents
9. d. Denial of service(DOS)


Security Attacks
Snooping
Traffic Analysis
Modification
Masquerading
Replaying
Repudiation
Denial of Service
Threat to confidentiality
Passive Attack
Threat to Integrity
Active Attack

Security Attacks

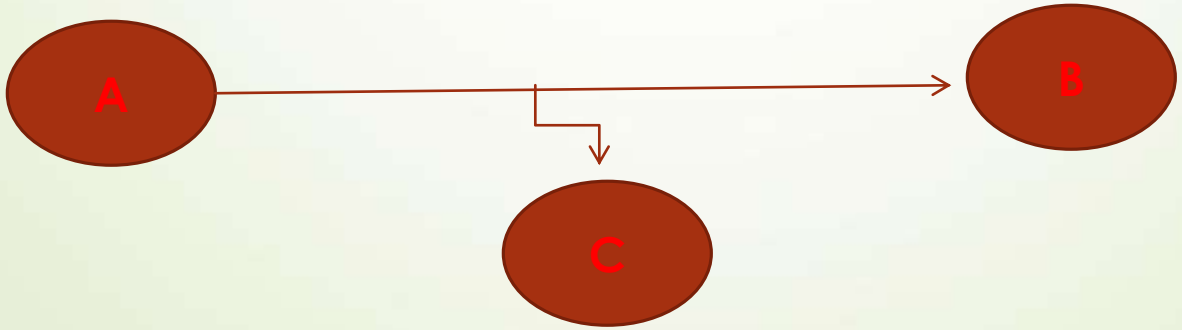
The type of security attacks are

1.Normal flow of data:

Information Source Information Destination

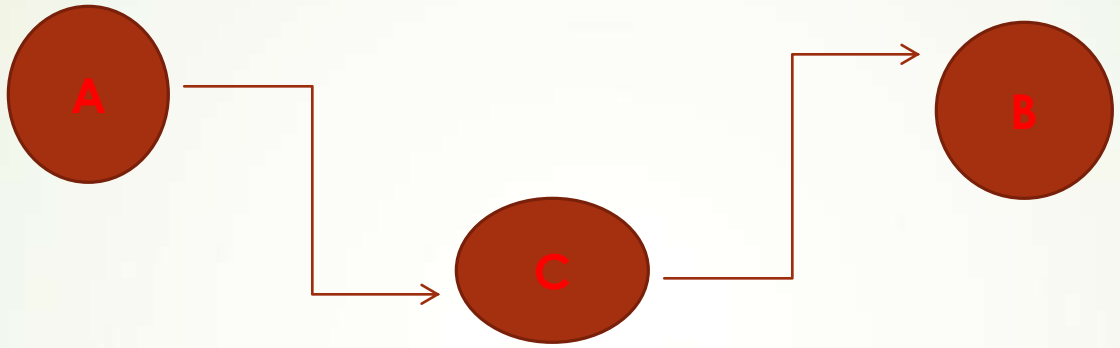
2.Interruption(break , disconnection , pause):attack on availability

3. Interception(capture , involvement):attack on confidentiality

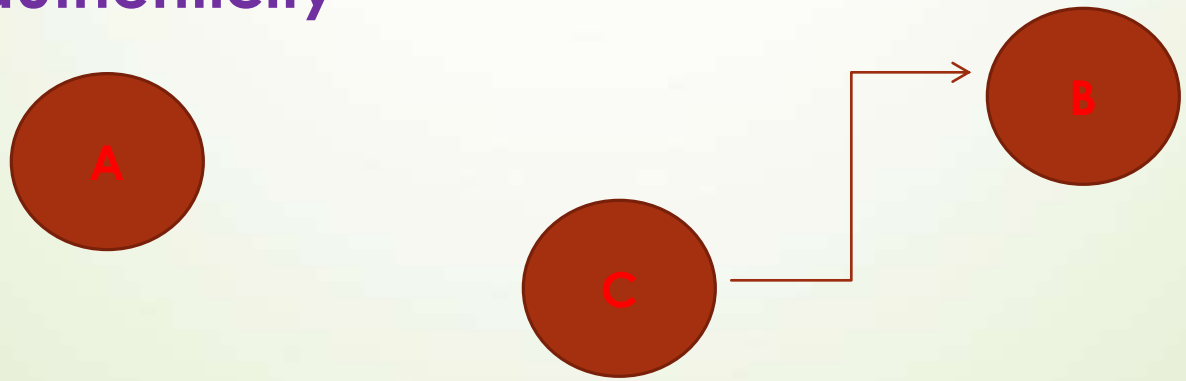


GITAM
DEEMED TO BE UNIVERSITY

4.Modification(alter , change): attack on integrity

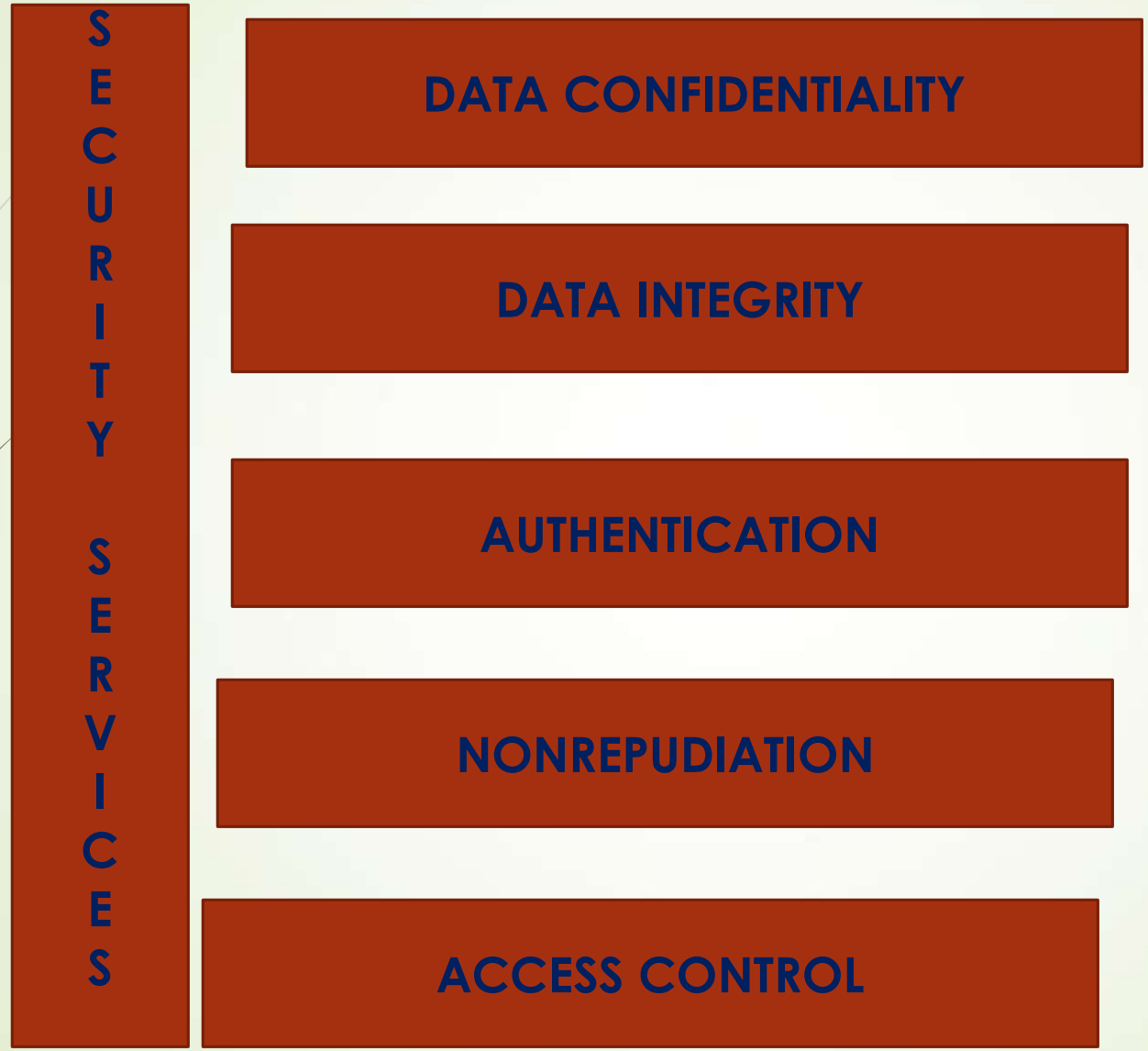


5.Fabrication(create, build, produce, construct): attack on authenticity



GITAM
DEEMED TO BE UNIVERSITY

Security Services



Security Services

1.DATA CONFIDENTIALITY: The protection of data from unauthorized disclosure.

a. Connection Confidentiality(The protection of all user data on a connection)

b. Connectionless Confidentiality(The protection of all user data in a single data block)

c. Selective-Field Confidentiality(The confidentiality of selected fields within the user data on a connection or in a single data block)

d. Traffic Flow Confidentiality(The protection of the information that might be derived from observation of traffic flows.)

Security Services

2. DATA INTEGRITY: The protection of data from an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

a. Connection Integrity with Recovery(all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted)

b. Connection Integrity without Recovery(As above, but provides only detection without recovery.)

c. Selective-Field Connection Integrity(within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.)

d. Connectionless Integrity(take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.)

e. Selective-Field Connectionless takes the form of determination of whether the selected fields have been modified.)

3.AUTHENTICATION: The assurance that the communicating entity is the one that it claims to be.

a. Peer Entity Authentication(Used in association with a logical connection to provide confidence in the identity of the entities connected.)

b. Data Origin Authentication(In a connectionless transfer, provides assurance that the source of received data is as claimed)

4. NONREPUDIATION: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

a. Nonrepudiation, Origin (Proof that the message was sent by the specified party.)

b. Nonrepudiation, Destination (Proof that the message was received by the specified party.)

5.ACCESS CONTROL : The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

GITAM
DEEMED TO BE UNIVERSITY

Security Mechanisms

SPECIFIC SECURITY MECHANISMS

- Encipherment
- Digital Signature
- Access Control
- Data Integrity
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

1. Encipherment: The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
2. Digital Signature: Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).
3. Access Control: A variety of mechanisms that enforce access rights to resources.
4. Data Integrity :A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

5. Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

6. Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

7. Routing Control: Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

8. Notarization: The use of a trusted third party to assure certain properties of a data exchange.

GITAM
DEEMED TO BE UNIVERSITY

PERVASIVE SECURITY MECHANISMS

- Trusted Functionality
- Security Label
- Event Detection
- Security Audit Trail
- Security Recovery

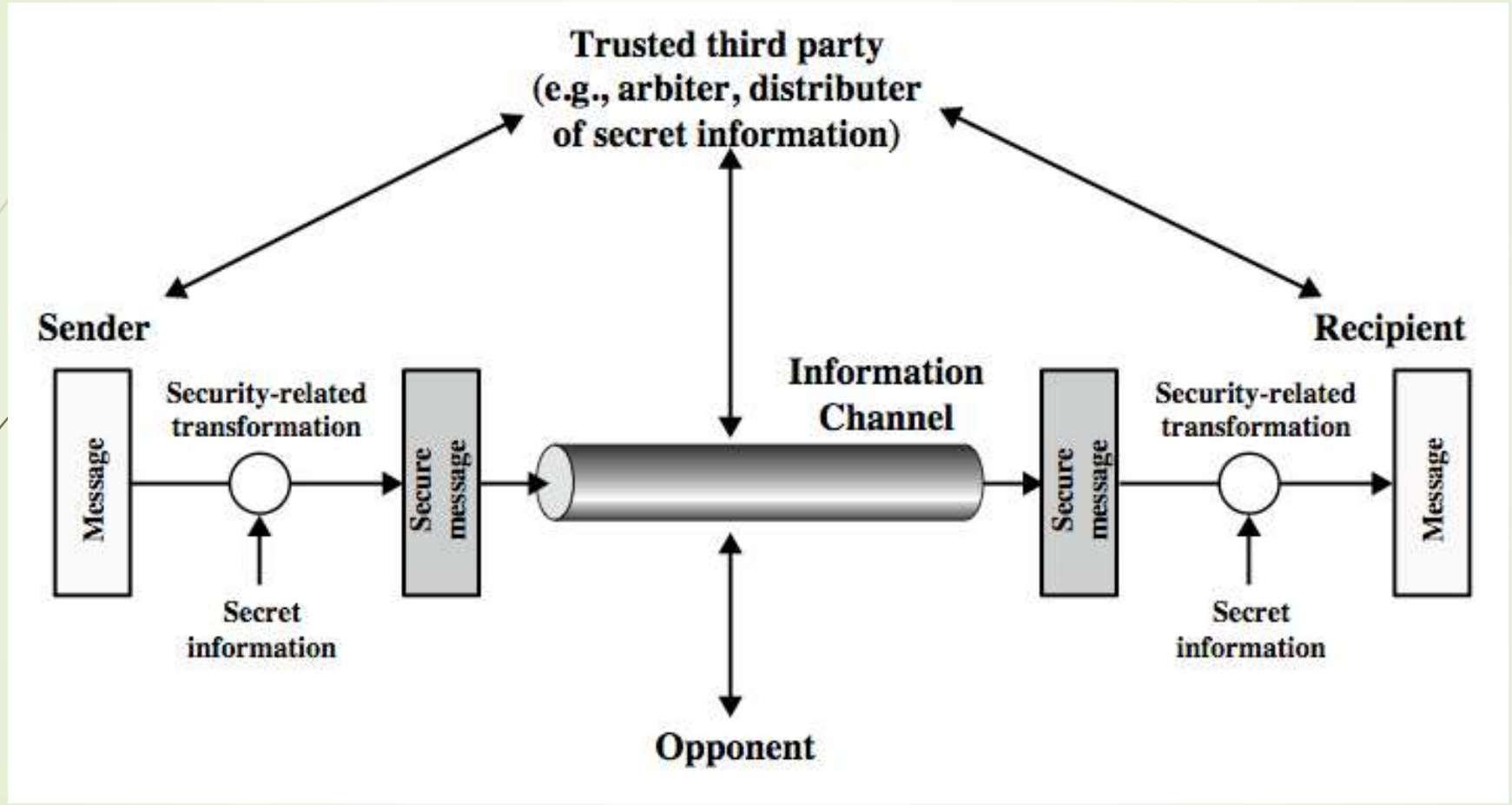
PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

1. Trusted Functionality: That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
2. Security Label: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
3. Event Detection: Detection of security-relevant events.
4. 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.
5. Security Recovery: Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Model for Network Security

- 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.


Trusted third party
(e.g., arbiter, distributer
of secret information)
Sender
Recipient
Message
Security-related
transformation
Secure
message
Information
Channel
Secure
message
Security-related
transformation
Message
Secret
information
Secret
information
Opponent

GITAM
DEEMED TO BE UNIVERSITY

Using this model requires us to:

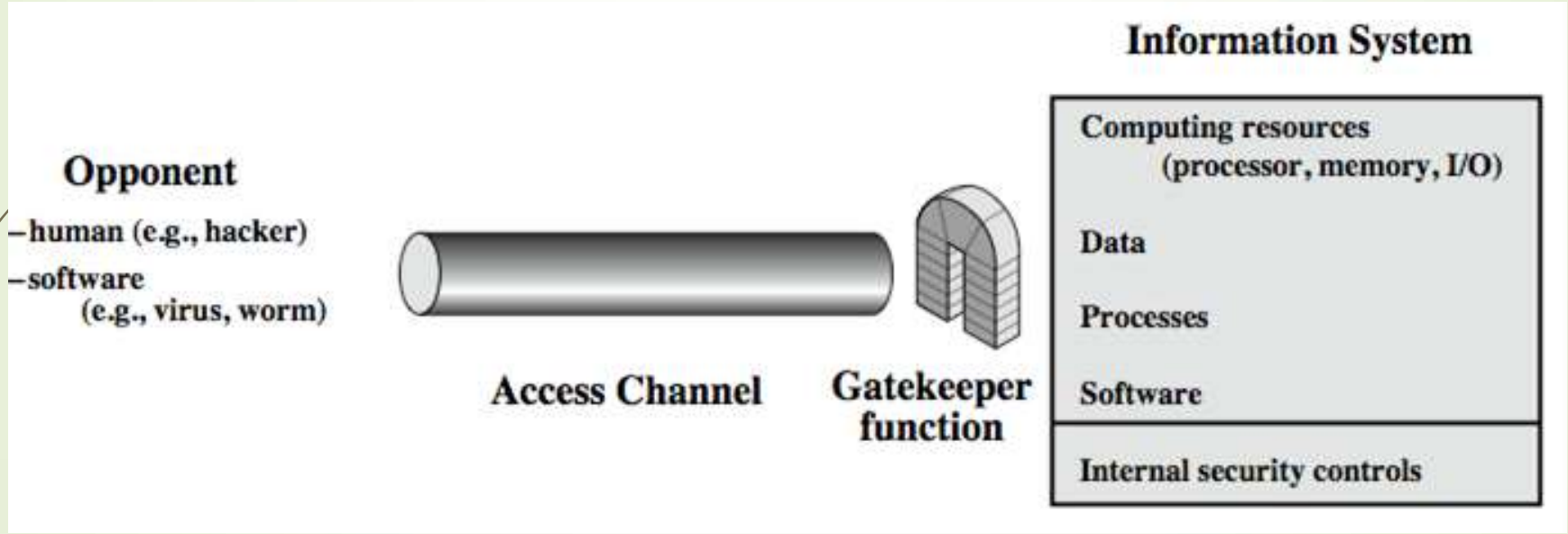
1. Design a suitable algorithm for the security transformation

2. Generate the secret information (keys) used by the algorithm

3. Develop methods to distribute and share the secret information

4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Using this model requires us to:

1. 1.select appropriate gatekeeper functions to identify users
2. 2.implement security controls to ensure only authorized users access designated information or resources

Note that model does not include:

1. 1.monitoring of system for successful penetration
2. 2.monitoring of authorized users for misuse
3. 3.audit logging for forensic uses, etc.

References

- **Text Book:**
- 1. William Stallings. Cryptography and Network Security — Principles and Practice, 7/e. Pearson Education,2017.
- **References:**
- 1. Behrouz A Fourozen and Debdeep Mukhopadhyaya, Cryptography and Network Security, 3/e, McGraW Hill, 2015.
- 2. Atul Kahate, Cryptography and Network Security, 4/e, McGraW Hill, 2019.
- 3. Introduction to Cryptography, Buchmann, Springer.
- 4. Applied Cryptography. 2nd Edition, Bruce Schneier, J ohnwiley & Sons.
- Introduction to Computer Networks and Cybersecurity Hardcover by Chwan-Hwa (J ohn) Wu ,J.David Irwin .CRC press.

GITAM
DEEMED TO BE UNIVERSITY