SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Chennai-600119

COURSE CODE:SCS1316

COURSE NAME : NETWORK SECURITY

Topics To be Covered In This Video Lecture

- Course Introduction
- Course Objectives
- Course Outcomes
- Detailed Curriculum
- Recommended Text Books/ Reference Books
- Unit I – Introduction (followed by detailed explanation of Individual Sub Sections)

Course Introduction

- What is Network Security?
- Need for Network Security
- Concepts of Cryptography
- Concepts of Internet Security
- Concepts of Computer Security
- How to Provide Network Security
- Issues / Challenges faced by Network Security Engineer

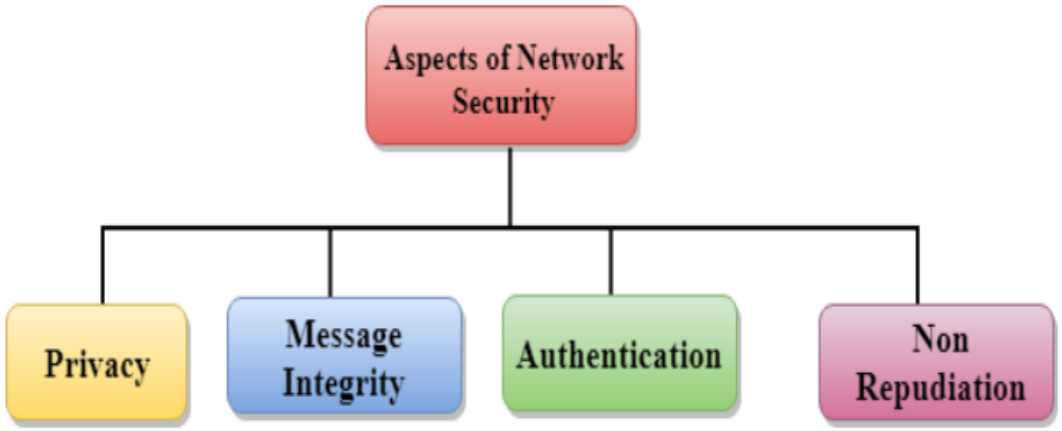


Image Adopted from: https://www.javatpoint.com/computer-network-security

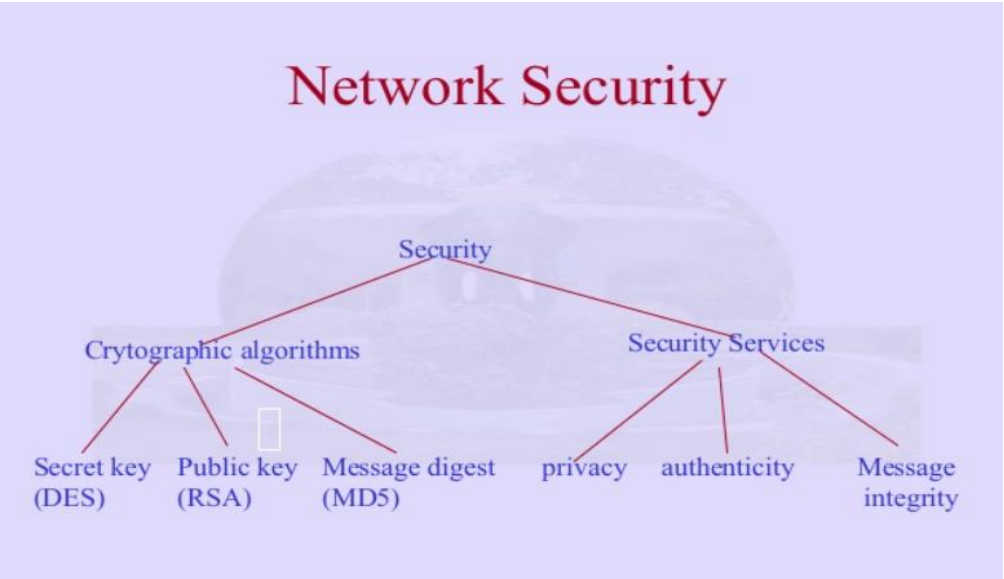


Image Adopted from :
https://www.slideshare.net/UmangGupta5/lecture43-network-security

Course Objectives

- To impart knowledge on basics of computer network security
- To understand different types of vulnerabilities, threats and attacks
- To get familiarize in basic number theory and cryptography related to network security issues
- To acquaint details about security functions and data security
- To acquire in-depth details required to ensure safe transfer of data in internet.

Course Outcomes

On completion of the course, student will be able to

- Describe the essential basics of Network security
- Classify different types of vulnerabilities, threats and attacks
- Encrypt and decrypt using basic cryptographic algorithms
- Demonstrate and analyze various security system procedures for internet security
- Describe the behavior of computer system security using Firewalls
- Appraise and report on advances in intrusion detection systems and antivirus software

SCS1316 – NETWORK SECURITY

Detailed Syllabus

UNIT 1- NETWORK SECURITY AND NUMBER THEORY BASICS

Network security- Examples of security violations-Computer security concepts – confidentiality – Integrity – Availability - Accountability, Challenges of computer security- Hacking-Vulnerability threats-attacks-passive attacks-types-Active attacks-types-Denial of service attacks-Model for network security. Modular arithmetic- Addition-Inverse divisibility-prime numbers-Euler's theorem-Fermat's theorem

UNIT 2- CRYPTOGRAPHY BASICS

Terminologies- Cryptography- Classification- based on operation, number of keys used, Processing- Crypt analysis –Types-Classical Encryption- Stream cipher, Substitution Cipher, Ceaser Cipher, Brute Force attack, Vignere Cipher-One time pad, Transposition Cipher -Simple row column Transfer, Play Fair Cipher, 2X2 Hill cipher- Rail fence Cipher-Block Cipher-Modes of operation,–DES- -AES-RSA algorithm

SCS1316 – NETWORK SECURITY

Detailed Syllabus

UNIT 3- SECURITY FUNCTIONS AND DATA SECURITY

Public Key Crypto system- Diffie-Helmann Key Exchange- Key management Techniques-Hash Functions- Requirements-Hash Algorithm-MD5,SHA_1-Message Authentication Code (MAC)- HMAC Digital Signature-User Authentication-Kerbroes-X.509 Certificates,X.509 Formats, Public Key Infrastructure- PKIX Architecture-Model-Management Functions

UNIT 4- INTERNET SECURITY

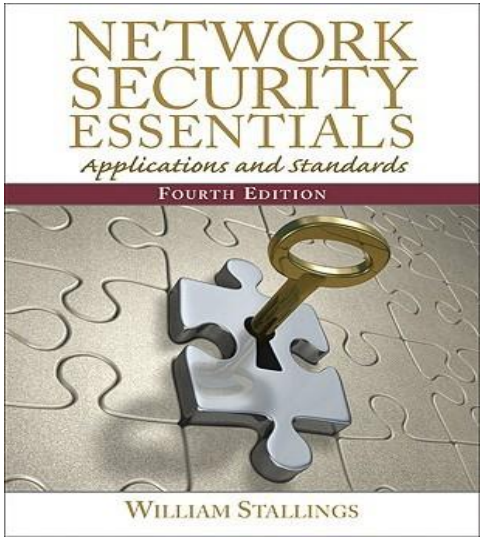
Email Security-PGP-S/MIME- Secured Electronic Transaction-IP Security Overview-IPSec Documents-IPSec Services, IPSec Architecture, IP Traffic Processing-Encapsulating Security Payload-Internet key Exchange- Firewalls- Stateful Packet Inspection- Application Gateways/Proxies- Hybrid Systems

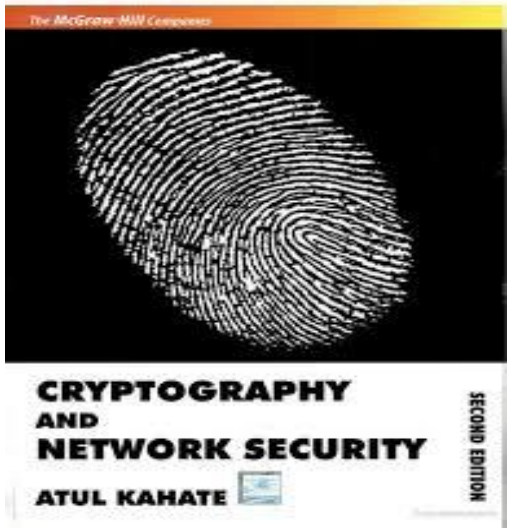
UNIT 5- COMPUTER SYSTEM SECURITY

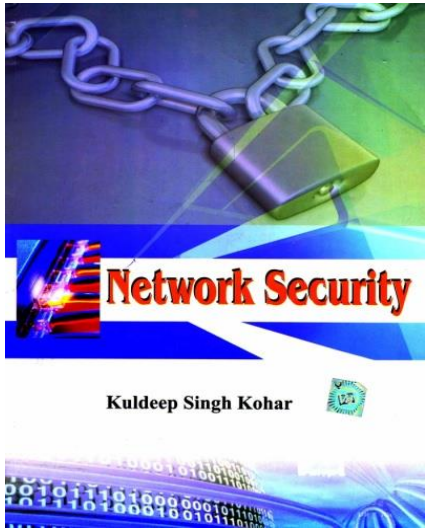
Malicious Software- Types-Backdoor-Worms-Logic bomb- Trojan Horses-Viruses - Classifications- Virus Kits-Email Viruses-Antivirus Approach-Distributed Denial of Service Attacks-Counter Measures-Intrusion Detection System (IDS),Network Based IDS-Host based IDS- Steps involved in deploying IDS

Reference Text books

1. Willliam Stallings, " Network Security Essentials"4th Edition Copyright © 2011 Pearson education, Inc., publishing as [Prentice Hall],
2. Atul Khahate, "Cryptography and network security",3rd Edition, Copyright © 2013 TMH Publishing
3. Kuldeep Singh Kohar", Network Security", revised reprint 2011.Vayu Education of India, New Delhi







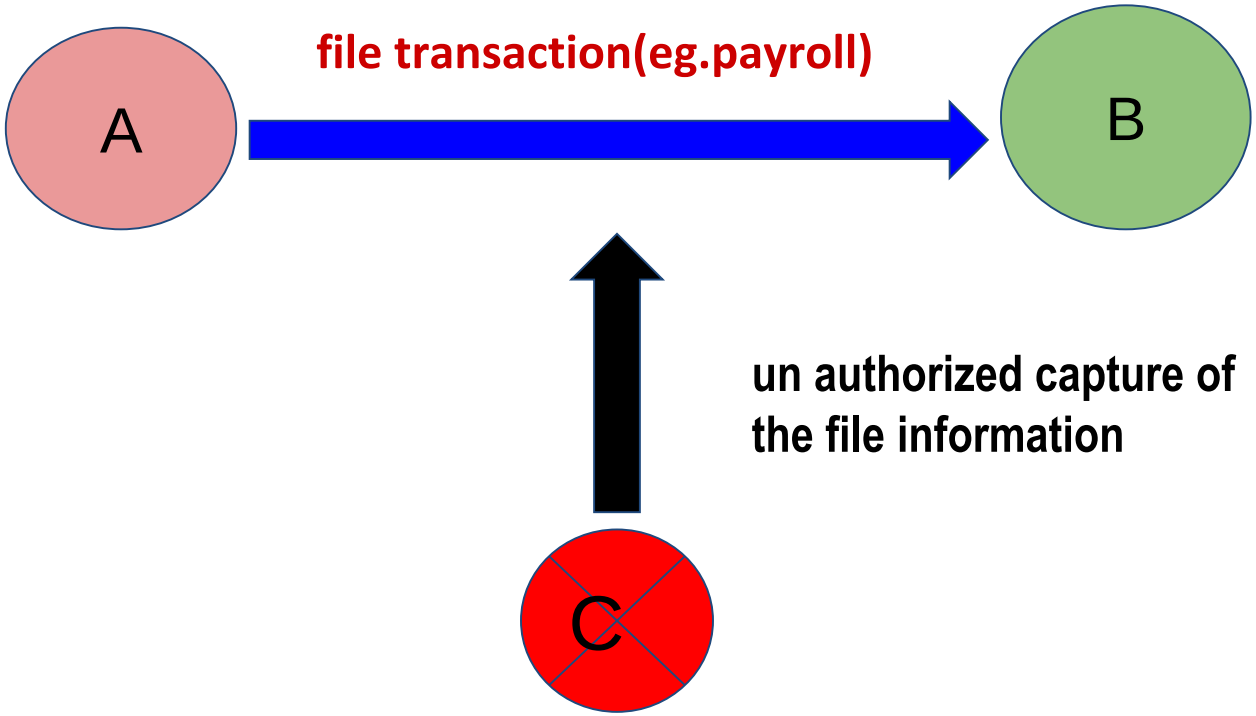
UNIT-1 NETWORK SECURITY AND NUMBER THEORY

Network security- Examples of security violations-Computer security concepts – confidentiality – Integrity – Availability - Accountability, Challenges of computer security-Hacking-Vulnerability threats-attacks-passive attacks-types-Active attacks-types-Denial of service attacks-Model for network security. Modular arithmetic- Addition-Inverse divisibility-prime numbers-Euler's theorem-Fermat's theorem

Need of Security

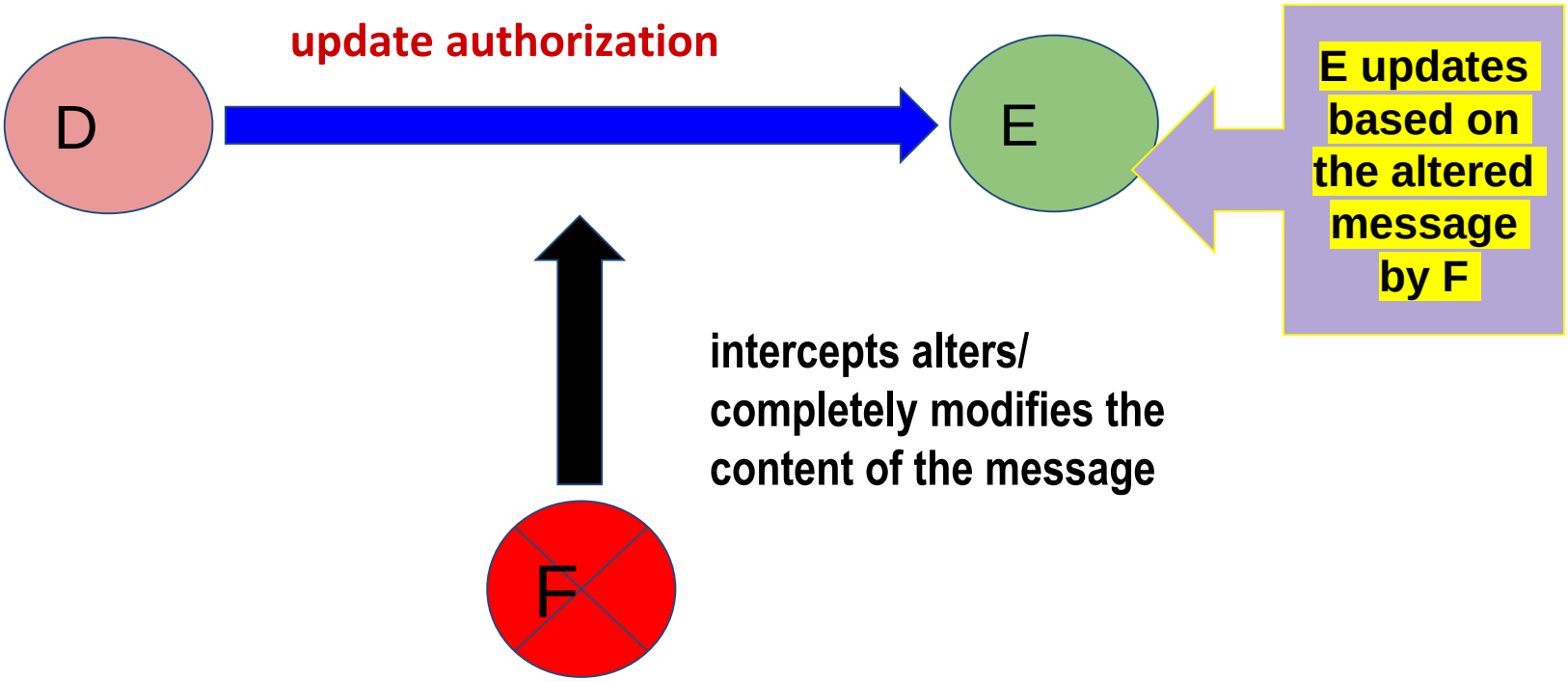
- Information Security requirements have changed in recent times
- Traditionally provided by physical and administrative mechanisms
- Computer requires automated tools to protect files and other stored information
- Use of networks and communications links require measures to protect data during transmission
- Keeping information secure from modification and unauthorized access

Examples of security violations



- User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.

Cont'd...



A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

Definitions

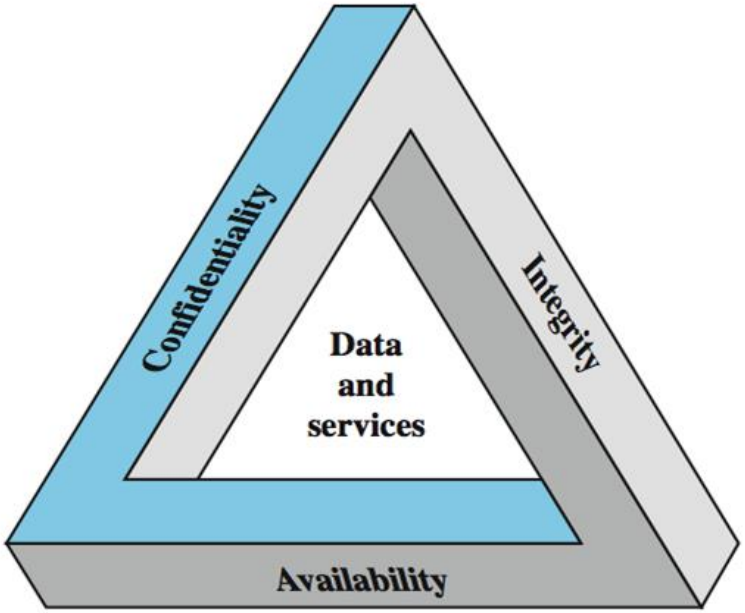
- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

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)

Key Security Concepts

Three key objectives that are at the heart of computer security



Often referred to as the **CIA triad**

Takes care of the fundamental security objectives for both data and for information and computing services

CIA Triad - Continued

- **Confidentiality** (covers both data confidentiality and privacy): preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity** (covers both data and system integrity): Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

CIA Triad - Continued

- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Additional Concepts

- 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.
- Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Computer Security Challenges

- Not simple – easy to get it wrong
- Must consider potential attacks
- Procedures used counter-intuitive
- Involve algorithms and secret info
- Must decide where to deploy mechanisms
- Battle of wits between attacker / admin
- Not perceived to be of benefit until it fails
- Requires regular monitoring it is a process, not an event
- Security is still too often an afterthought
- Many users / security administrators view strong security as an impediment to efficient and user-friendly operation

Aspects of Security

- 3 aspects of information security
  - security attack
  - security mechanism
  - security service

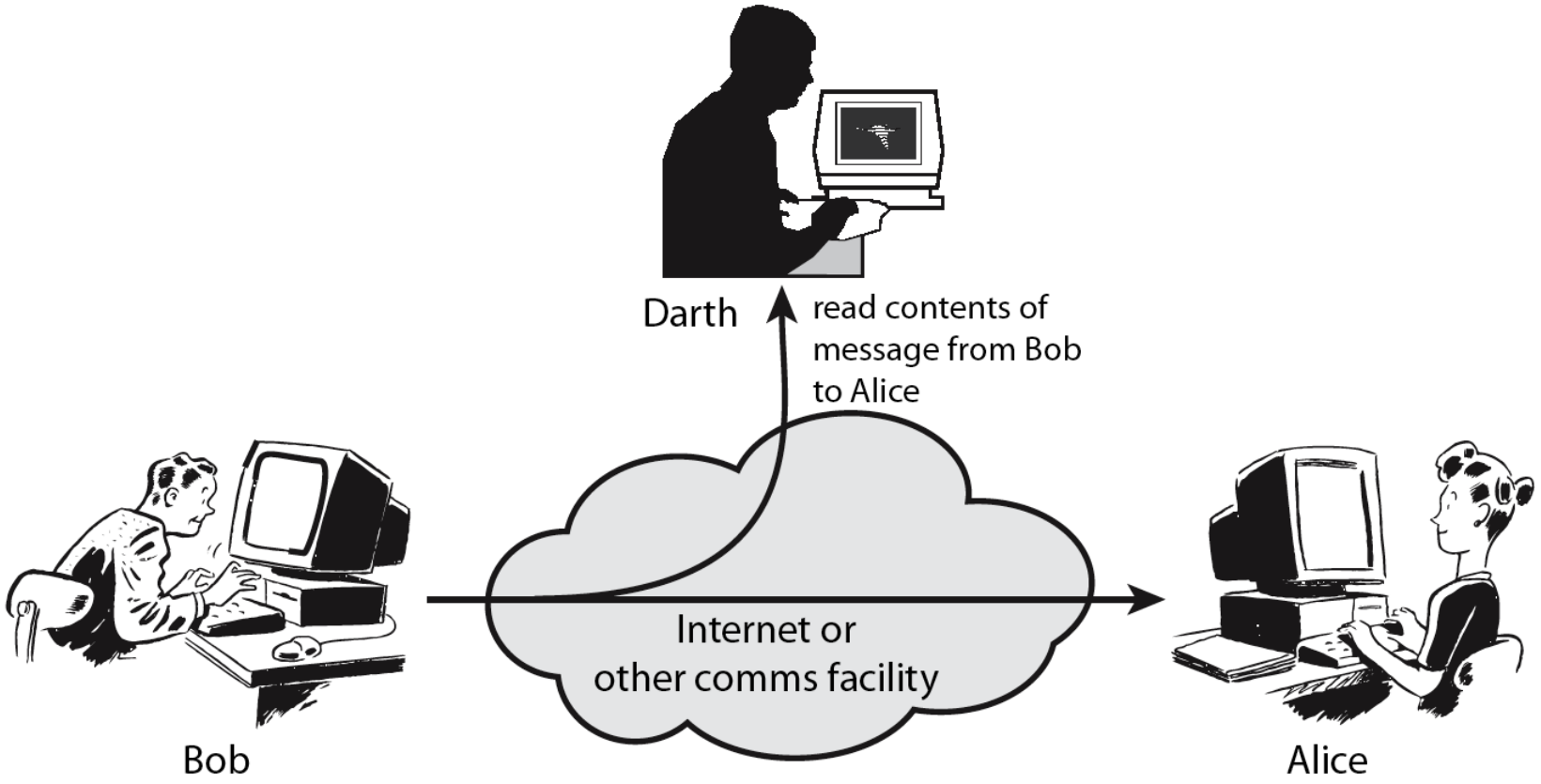
Security Attack's

- **Attack** - Any action that compromises the security of information owned by an organization
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- Often threat & attack used to mean same thing
- Have a wide range of attacks

Types of attacks

- Passive Attacks
- Active Attacks

Passive Attacks



Passive Attacks

- Eavesdropping on or monitoring of the transmissions between the transmitter and the destinations
- The aim of the intruder is to obtain the information that is being transmitted on the network

Types of Passive Attacks:

a) **Release of message contents**
b) **Traffic Analysis**

Note: A passive attack attempts to acquire or make use of information which is being transmitted through the network but does not Damages the system resources

Release of Message

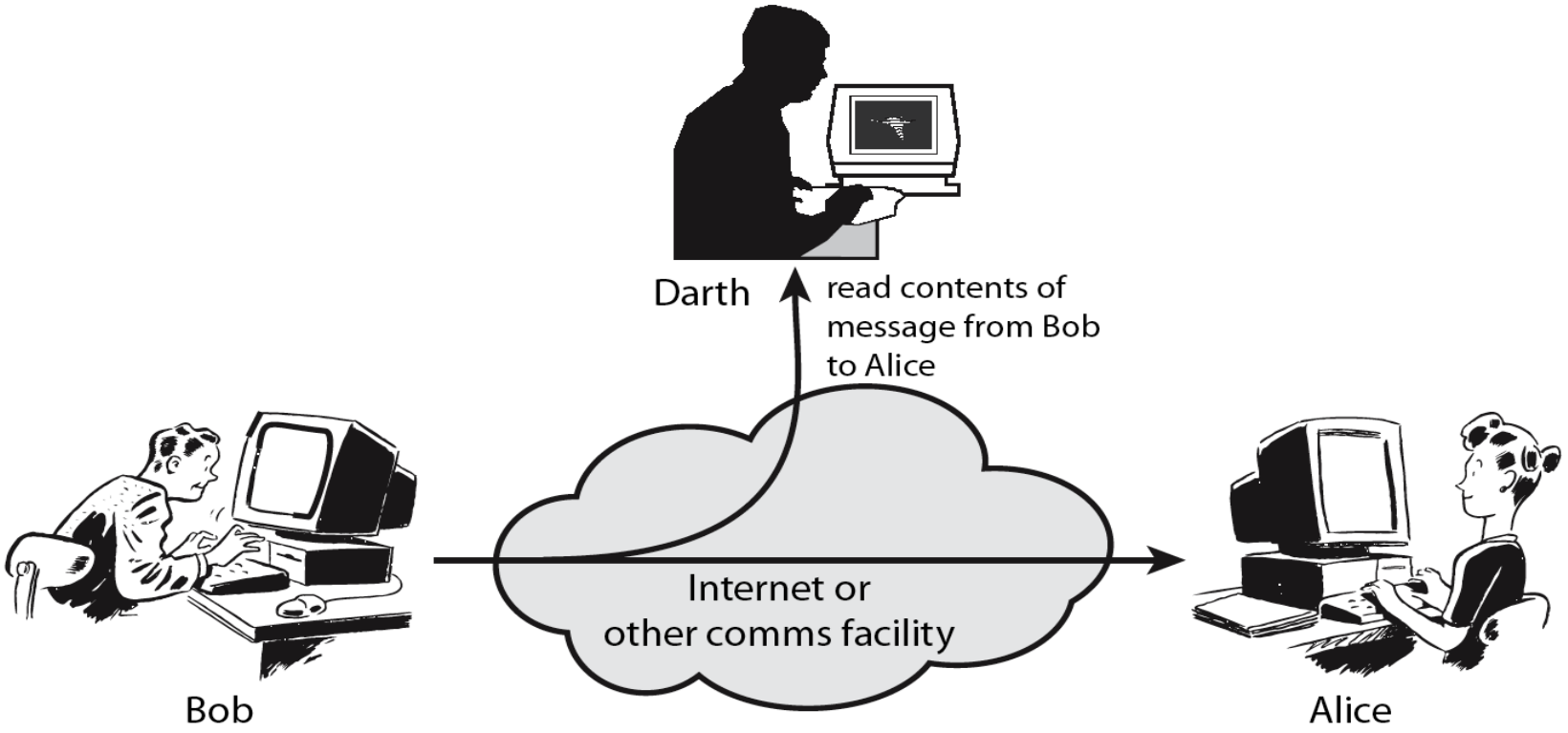
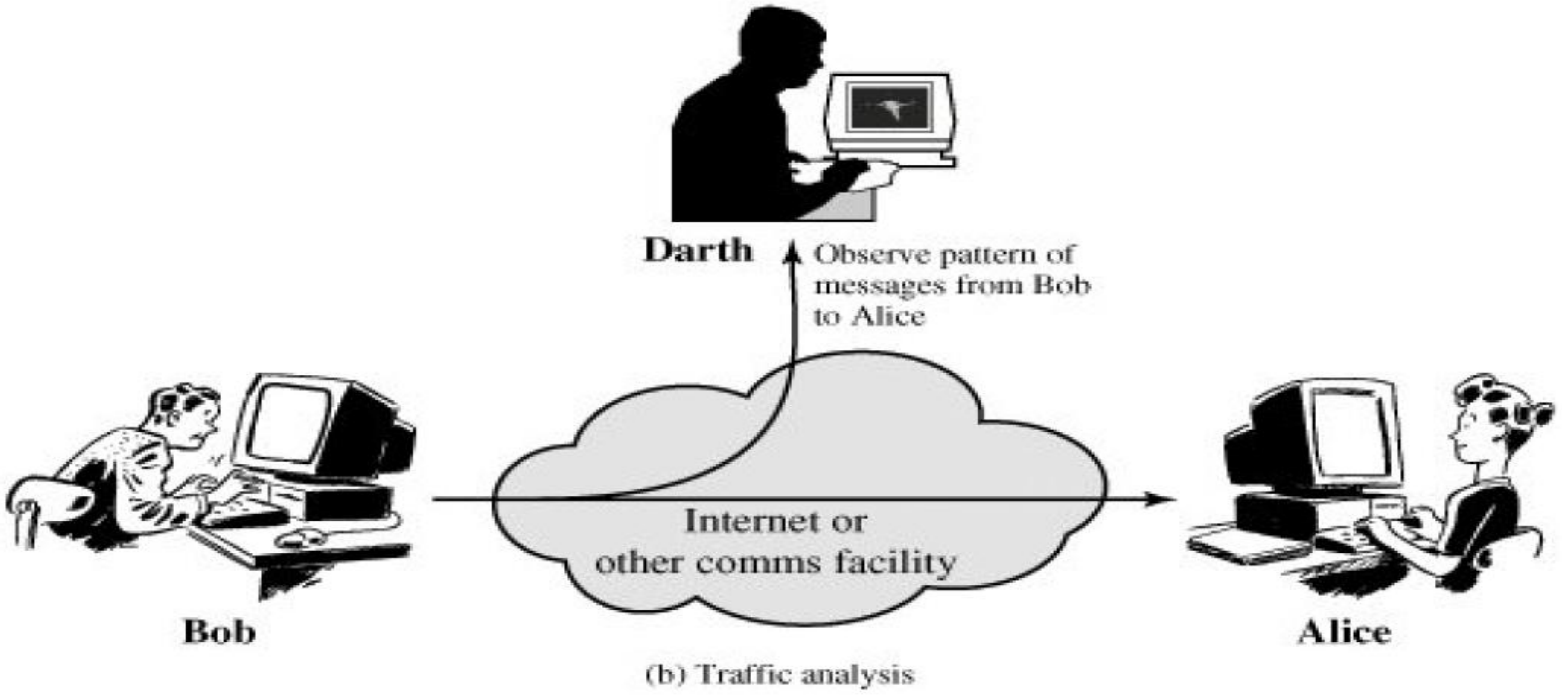


Image Adopted from:Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings-PHI publications

- Darth – the Intruder eavesdrops or monitors the data which is transmitted from Bob to Alice. He discovers the information but is not altering it or withholding it. Just reads the contents.

Traffic Analysis



(b) Traffic analysis

Image Adopted from:Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings-PHI publications

- The opponent can determine the location and identity of
- Source and destination hosts
- Could observe the frequency and length of messages being transmitted
- This analysis helps the unauthorized person in guessing the nature of the communication that was taking place

Active Attacks

- **Active Attacks:**

Involves in the Modification/Alteration/Tampering of the message or in the creation of a false message

Types of Active Attacks:

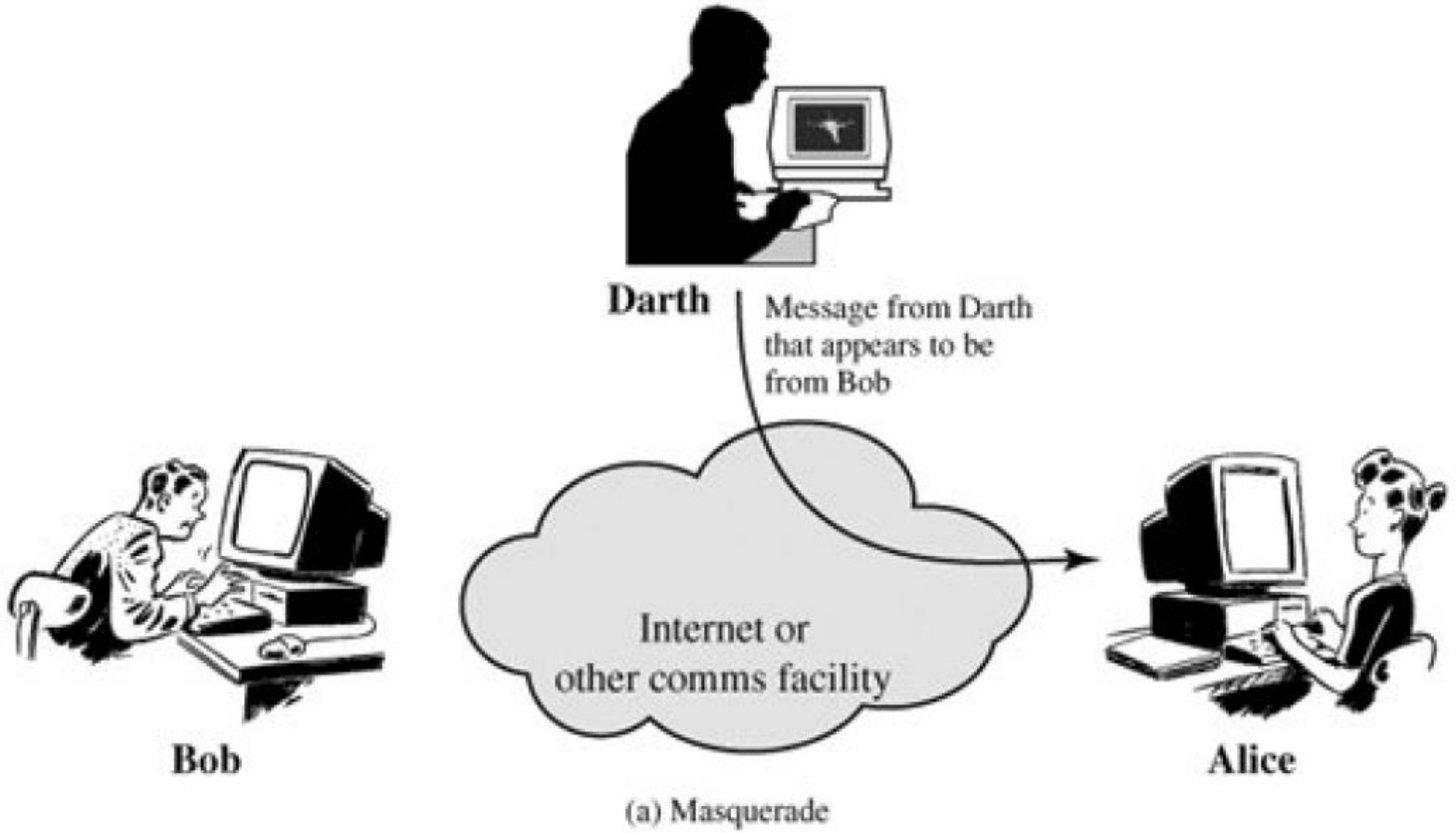
(A) Masquerade

(B) Replay

(C) Modification of Messages

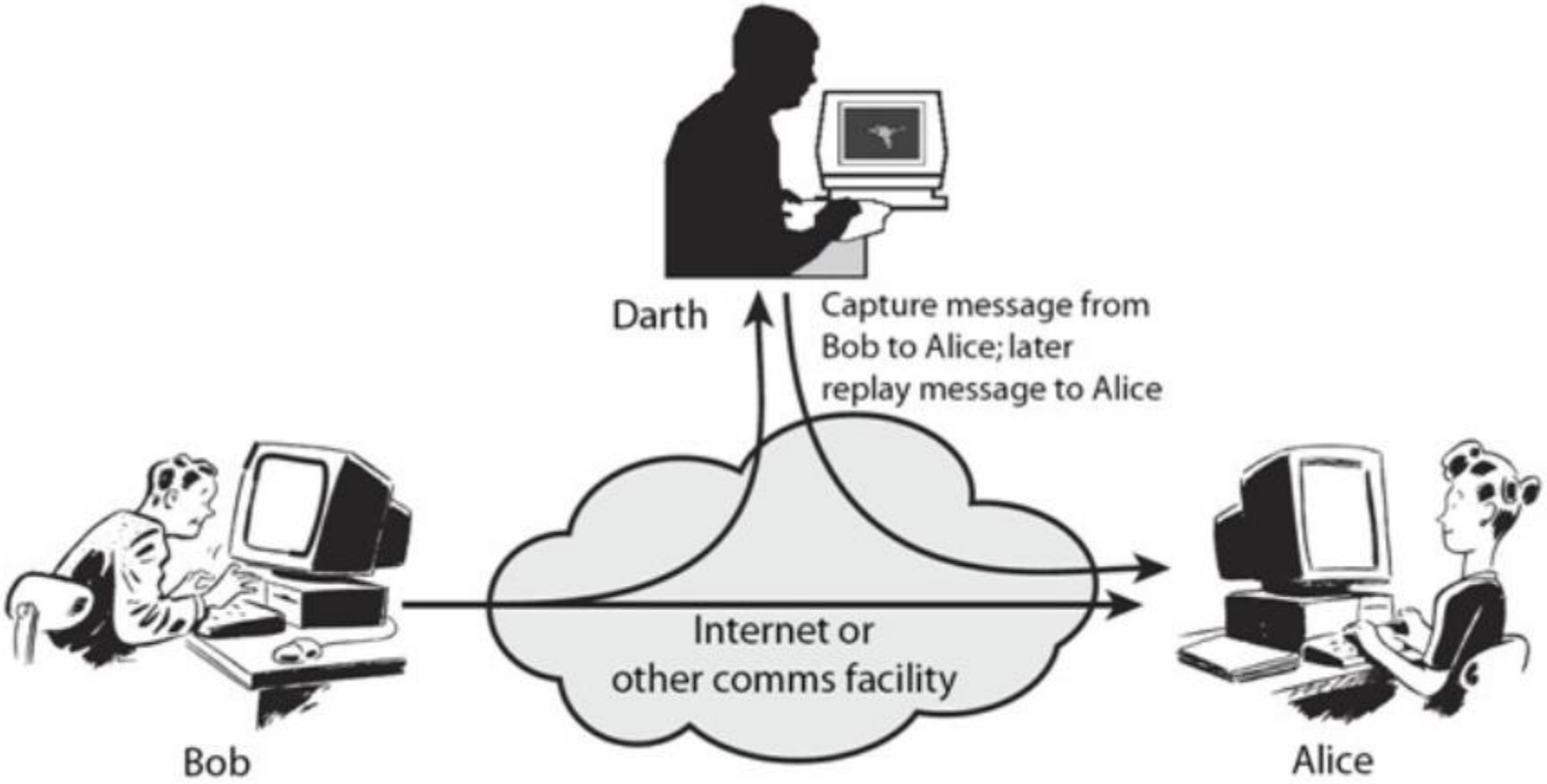
(D) Denial of Service (DoS)

Masquerade

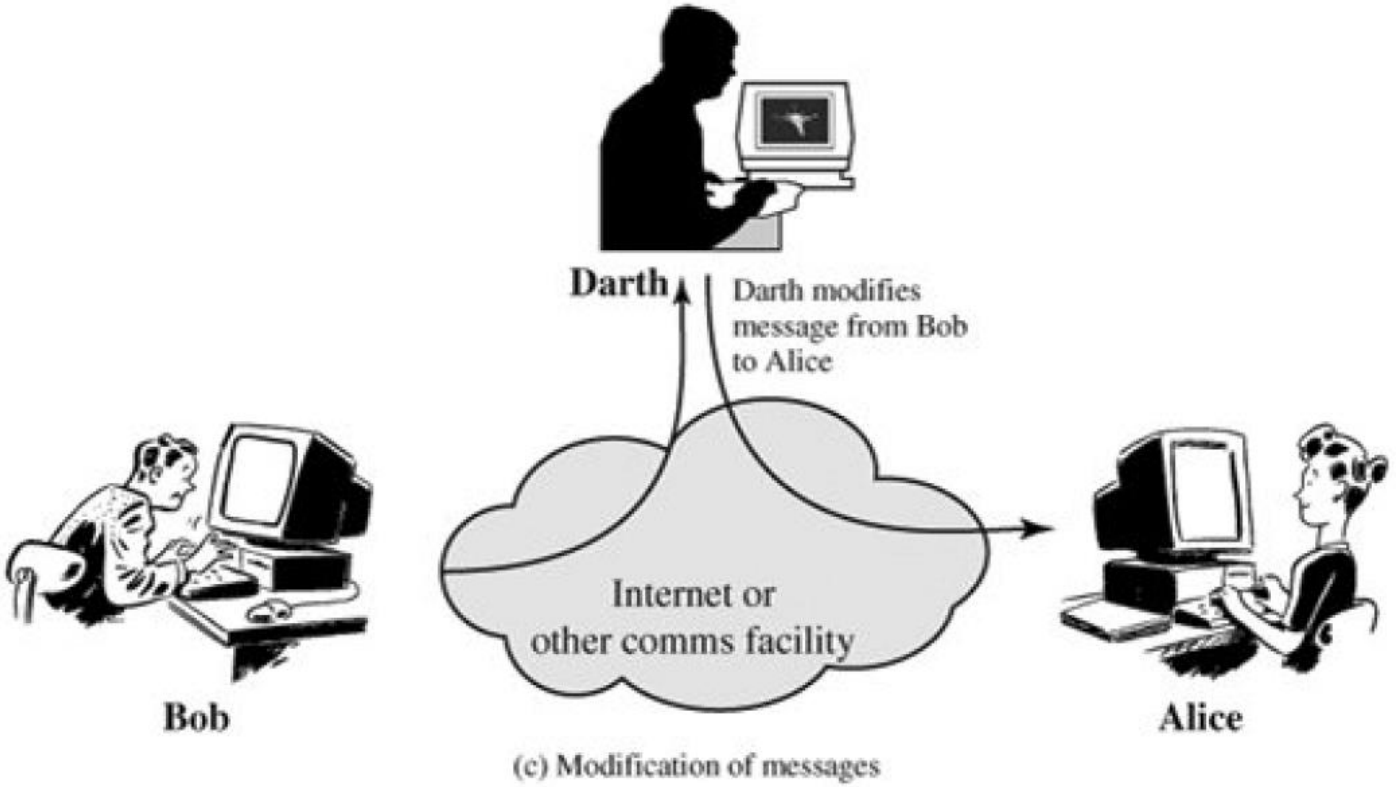


(a) Masquerade

Replay

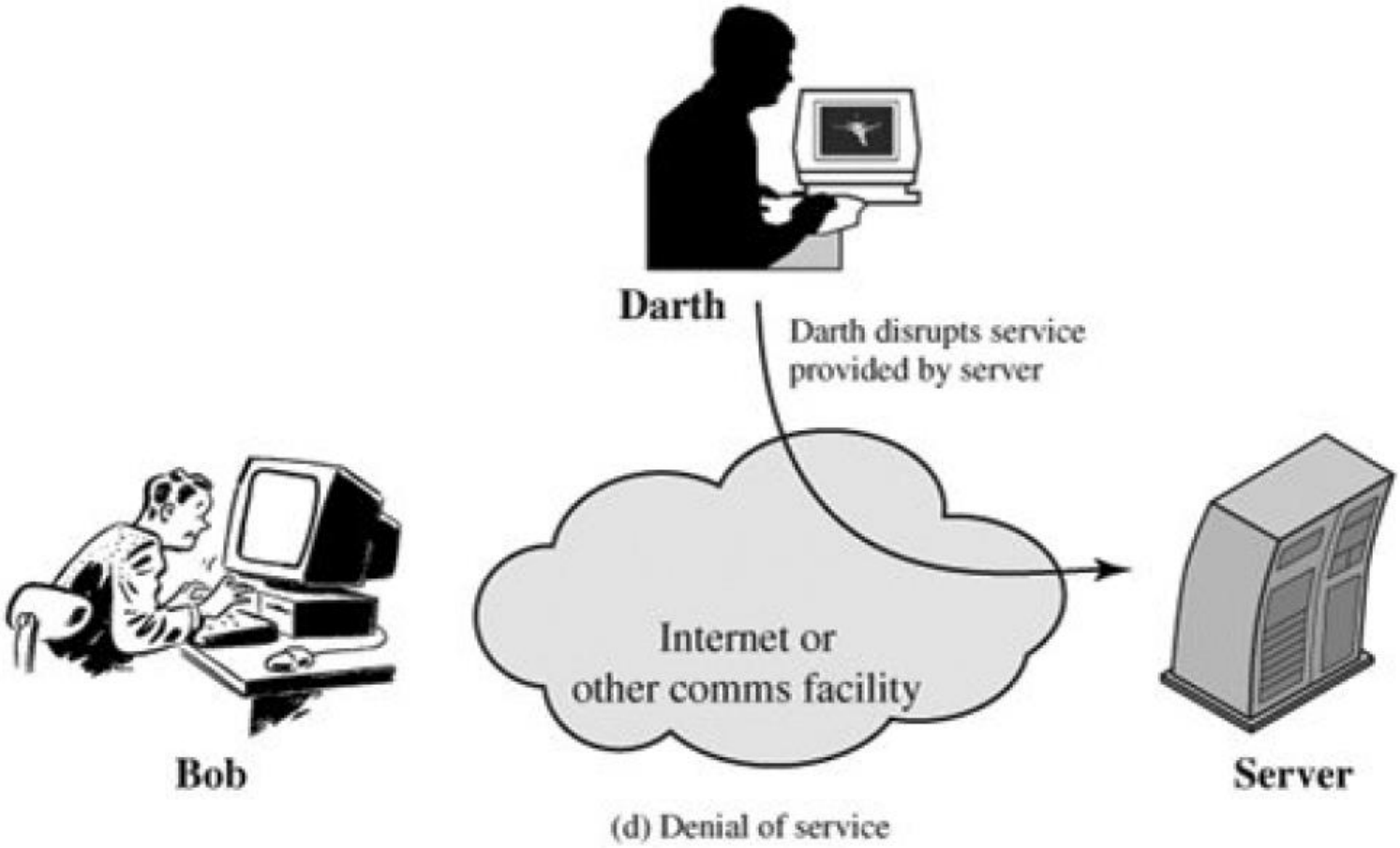

Darth
Capture message from
Bob to Alice; later
replay message to Alice
Internet or
other comms facility
Bob
Alice

Modification of Message



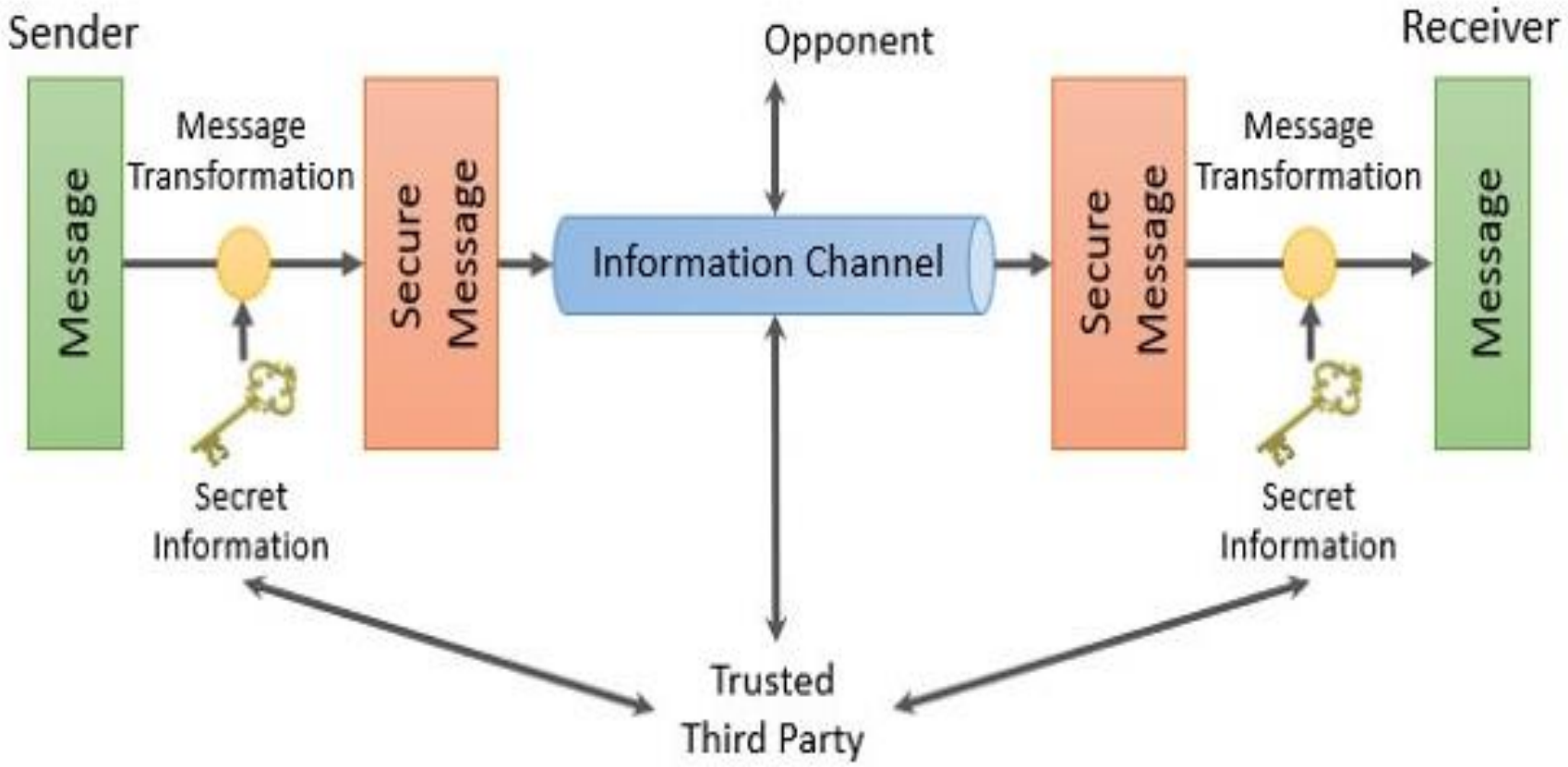
(c) Modification of messages

Denial of Service



(d) Denial of service

Network Security Model



Contd..,

- For a message to be sent or receive there must be a sender and a receiver.
- Both the sender and receiver must also be mutually agreeing to the sharing of the message.
- Now, the transmission of a message from sender to receiver needs a medium i.e. **Information channel** which is an **Internet** service.

Contd..,

- A logical route is defined through the network (Internet), from sender to the receiver and using the communication protocols both the sender and the receiver established communication.
- Security of the message over the network is important when the message has some confidential or authentic information which has a threat from an opponent present at the information channel.

Components

Any security service would have the three components

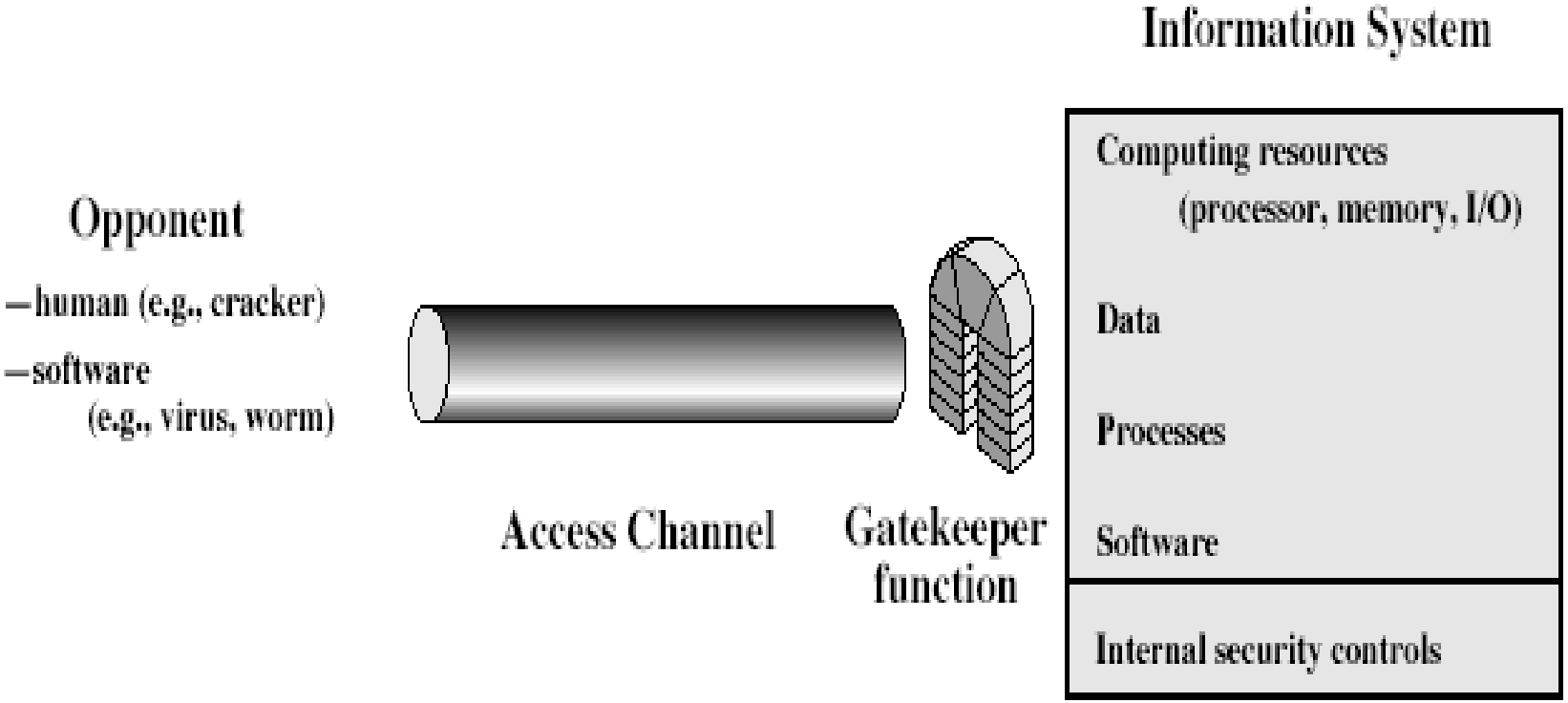
- **Transformation**
- **Sharing**
- **Trusted third party**

- **Transformation** of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the **encryption** of the message.
- **Sharing** of the secret information between sender and receiver.
- The **encryption key** which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

Cont'd…

- There must be a **trusted third party** which should take the responsibility of **distributing the secret information** (key) to both the communicating parties and also prevent it from any opponent.
- A third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

Model for Network Access Security



Cont'd…

- Using this model requires us to
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorized users access designated information or resources
- Trusted computer systems may be useful to help implement this model

Basic tasks in designing security service

This general model shows that there are four basic tasks in designing a particular security service:

- Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.
- Generate the secret information to be used with the algorithm.
- Develop methods for the distribution and sharing of the secret information.
- Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Prime Numbers

- **Prime numbers** are the positive integers having only two factors, 1 and the integer itself

For example,

Factors of 6 are 1,2,3 and 6, which are four factors in total.

But factors of 7 are only 1 and 7, totally two

Hence, 7 is a prime number but 6 is not, instead it is a composite number.

**Always remember that 1 is neither prime nor composite

- Another way of defining Prime Number is - **It is a positive number or integer, which is not a product of any other two positive integers.**

Relative Prime Numbers

- The numbers ‘a’ & ‘b’ are said to be Relative Prime numbers if ‘a’ & ‘b’ does not have a common factor

  i.e., GCD(a, b)= 1

  GCD – Greatest Common Divisor

For example,

Assume a=15 & b = 28

Factors of 15 are 1,3,5

Factors of 28 are 1,2,4,7,14

GCD is the largest number that divides both of them.

In this case 1 is the common divisor

So GCD (15,28) = 1 ,Hence 15 & 28 are relatively Prime numbers

Practice Problem: Find GCD of 36 and 60

MODULAR ARITHMETIC

The quotient remainder theorem

- To **prove some properties** about **modular arithmetic** we often make use of the **quotient remainder theorem**.
- It is a simple idea that comes directly from long division.

The quotient remainder theorem says:

Given **any** integer **A**, and **a positive** integer **B**, there exist **unique integers Q and R** such that

A= B * Q + R **where 0 ≤ R < B**

Where A - DIVIDEND

B - DIVISOR /MODULUS

Q - QUOTIENT &

R - REMINDER/ RESIDUE

A mod B = R

EXAMPLES

A mod B = R

A = 13, B = 5

13 = **5** * 2 + **3**

13 mod **5** = **3**

A = 8, B = 4

8 = **4** * 2 + **0**

8 mod **4** = **0**

A = 7, B = 2

7 = **2** * 3 + **1**

7 mod **2** = **1**

A = -16, B = 26

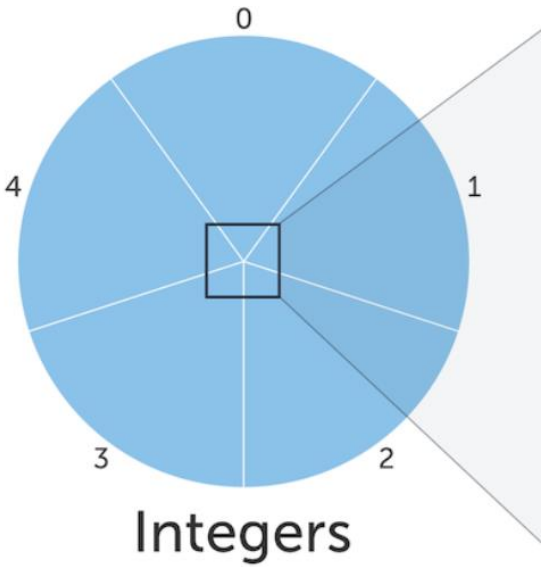
-16 = **26** * -1 + **10**

-16 mod **26** = **10**

Congruence Modulo

$$A \equiv B (\mathrm{mod}\ C)$$

This says that A is congruent to B modulo C



26 mod 5=1

1 mod 5 =1

6 mod 5=1

11 mod 5 =1

16 mod 5 =1

21 mod 5 =1

Same Equivalence class

Cont'd...

1. $\equiv$ is the symbol for congruence, which means the values A and B are in the same **equivalence class**.

2. $(\mathrm{mod}\ C)$ tells us what **operation** we applied to A and B.

3. when we have both of these, we call "$\equiv$" **congruence modulo** C.

Cont'd...

Example:

e.g. $26 \equiv 11 \pmod 5$

$26 \bmod 5 = 1$ so it is in the equivalence class for 1,

$11 \bmod 5 = 1$ so it is in the equivalence class for 1, as well.

Properties

MODULAR ADDITION

$$(A + B) \bmod C = (A \bmod C + B \bmod C) \bmod C$$

Example:

Let **A=14, B=17, C=5**

Let's verify: **(A + B) mod C = (A mod C + B mod C) mod C**

LHS = Left Hand Side of the Equation

RHS = Right Hand Side of the Equation

Contd.,

LHS = **(A + B) mod C**

LHS = (**14 + 17**) mod 5

LHS = **31** mod 5

LHS = 1

RHS = (A mod C + B mod C) mod C

RHS = (**14 mod 5 + 17 mod 5**) mod 5

RHS = (**4 + 2**) mod 5

RHS = 1

LHS = RHS = 1 Hence Proved

Modular Subtraction

- **(A - B) mod C = (A mod C - B mod C) mod C**

Example: Prove **(7-4) mod11 = (7 mod 11 – 4 mod 11) mod 11**

LHS : 7 – 4 mod 11

= 3 mod 11 = 2

RHS : (7 mod 11 – 4 mod 11) mod 11 This can be Written as

(7-4 mod 11) mod 11

(3 mod 11) mod 11

3 mod 11 = 2

Since LHS = RHS / Hence Proved

Modular Multiplication

- **[(A mod C) * (B mod C)] mod C = (A * B) mod C**

Example: Let A= 4, B= 7, C= 6

LHS : [(A mod C)*(B mod C)] mod C
= [(4 mod 6)*(7 mod 6)] mod 6
= [4 * 1] mod 6
= 4 mod 6 = 4

RHS : (A*B) Mod C
= (4*7) mod 6
= 28 mod 6
= 4
LHS = RHS / Hence proved

Inverse Modular Arithmetic

1. $7^{-1} \bmod 160$

$160 = 22 \times 7 + 6$ | $6 = 160 - (22 \times 7)$

$7 = 1 \times 6 + 1$ | $1 = 7 - (1 \times 6)$

$1 = 7 - (1 \times 6)$

$= 7 - (1 \times (160 - (22 \times 7))$ for 6 substitute

$= 7 - (1 \times (160 - (22 \times 7))$

$= 1x7 - 1x160 + 22x7$ (Taking 7 as common so (1+22)7)

$= 23\ (7) - 1x160$

$7^{-1} \bmod 160 = 23$

Contd.,

Solve : $23^{-1} \bmod 26$

$26 = 1 \times 23 + 3$	$3 = 26 - (1 \times 23)$
$23 = 7 \times 3 + 2$	$2 = 23 - (7 \times 3)$
$3 = 1 \times 2 + 1$ stop	$1 = 3 - (1 \times 2)$

$1 = 3 - (1 \times 2)$

$= 3 - (1 \times (23 - (7 \times 3)))$

$= 3 - (1 \times 23) + (7 \times 3)$

$= 1 \times 3 - (1 \times 23) + (7 \times 3)$

$= 8 \times 3 - 1 \times 23$

$= 8 \times (26 - (1 \times 23)) - (1 \times 23)$

$= 26 \times 8 - 9 (23)$

$-9 + 26 = 17$ (for negative number add the divisor from the problem)

$23^{-1} \bmod 26 = 17$

Euler's Totient Function

- Euler's Totient function is also known as PHI function (φ(n)) or ϕ(n)

Euler's Totient function for any given number 'n' is defined as the Total count of the numbers which are relatively Prime to 'n' and are less than 'n'.

Example 1:

Assume 'n' = 10

Consider the numbers which are lesser than n(in this case 10).Then the Relative Prime numbers for 10 are 1,3,7,9.

Hence φ(n)) or ϕ(n) = 4 (Since Relative Prime for 10 is 1,3,7,9) (Total 4 Numbers).

Euler's Totient Function

❖ **If the given number 'n' is a Prime number then, ϕ(p) = P-1**

Example 2:

Consider n=7 (Since 7 is a prime number Euler's Totient function φ(7) = 7-1 = 6.

Example 3: n=13. Find φ(13).

φ(13) = ?

Example 4: n= 11. Find φ(11).

Example 5: (non prime number)

n = 14. Find φ(14) = ?

Hint: Count of Relative Prime numbers for 14.

Euler's Theorem

- **Euler's Theorem states** that , If 'p' & 'q' are two prime numbers such that p ≠ q & n =pq ,Then ϕ(n) =(p-1)*(q-1).

Example 1:

Assume 'p' = 2 & 'q' = 5

n = pq

= 2*5

= 10

So ϕ(10) = (2-1)*(5-1)

= 4

Example 2:

Consider p=7 & q= 11 , n= 7*11= 77 .Find φ(77).

φ(77) = (7-1)*(11-1) =6*10 =60

Fermat's Theorem

- Fermat's Theorem/ Fermat's Little Theorem States that if 'P' is a Prime number and 'a' is a Positive Integer which is not Divisible by 'P' then

$$a^{P-1} = 1 \bmod P$$

Example: Let a = 3 and P = 7

$$\mathbf{a^{P-1} = 1 \bmod P}$$

$$3^{7-1} = 1 \bmod 7 = 3^6 \bmod 7$$

$$(3^2)^3 \bmod 7 = (9 \bmod 7)^3$$

$$= (2 \bmod 7)^3$$

$$= 2^3 \bmod 7 = 8 \bmod 7 = 1$$

Hence proved.

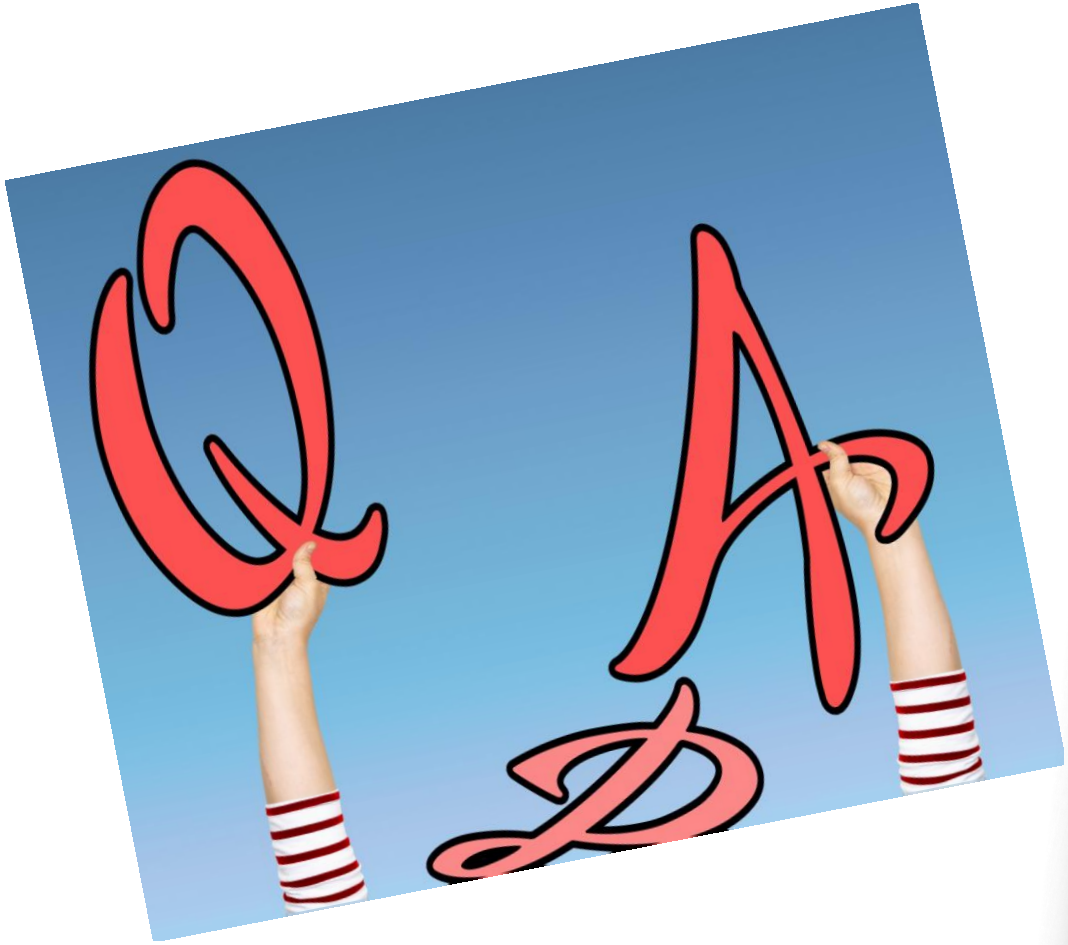
Fermat's Theorem

Practice Problems:

1. Prove Fermat's Theorem .Consider a=2, P= 5

$$a^{P-1} = 1 \bmod P$$

2. Prove Fermat's Theorem Using a=3, P= 7


Q
A


THANK
YOU