D Y PATIL UNIVERSITY
NAVI MUMBAI

Subject Name: Cryptography and Network Security

Unit No:1 Unit Name: Introduction to Cryptography

Faculty Name : Dr. Pallavi Sapkale

Index

D Y PATIL RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

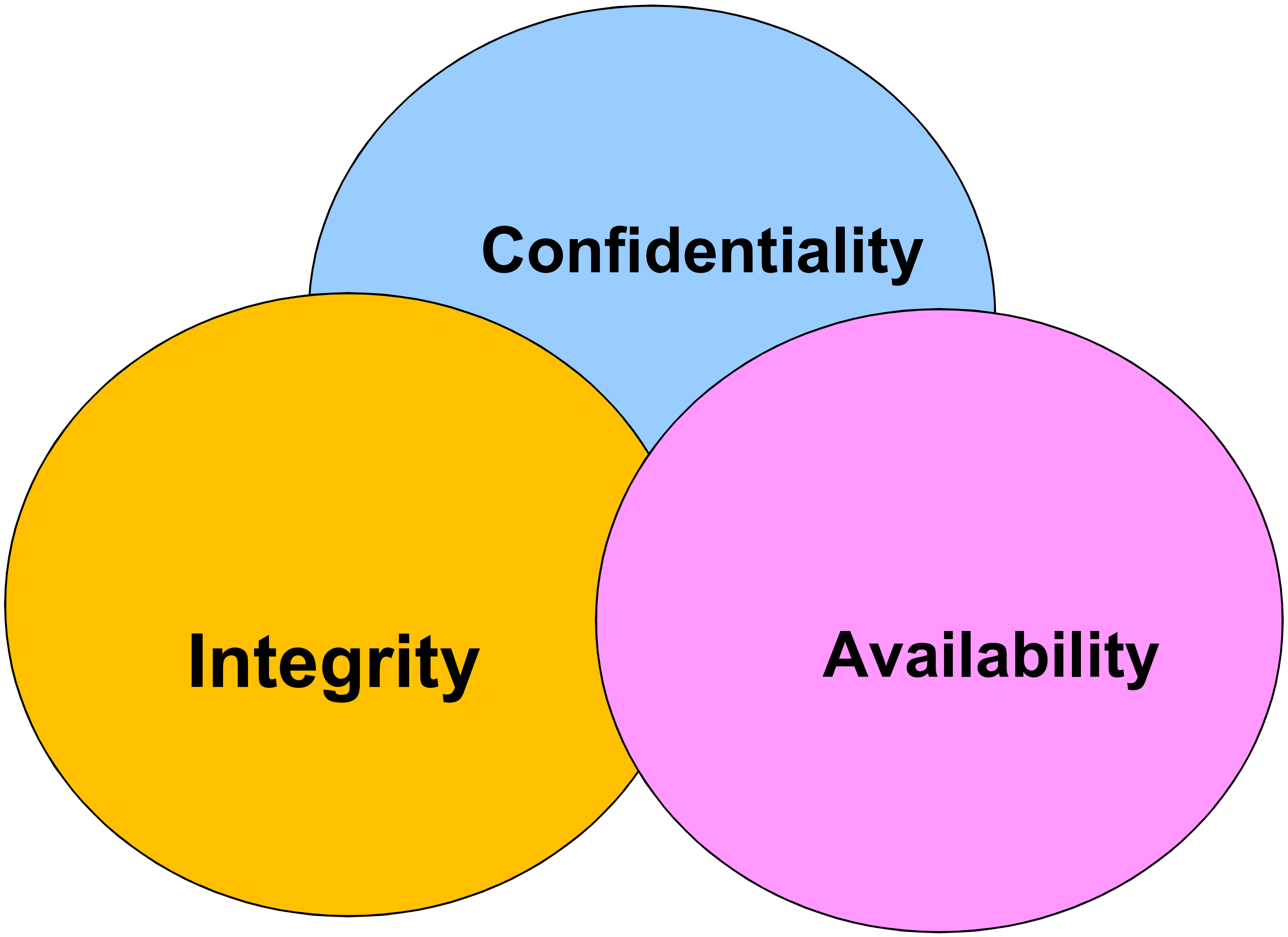
Lecture No: 1

Security Goals, Attacks, Services and Mechanisms, Techniques

Objectives

- **To define three security goals**
- **To define security attacks that threaten security goals**
- **To define security services and how they are related to the three security goals**
- **To define security mechanisms to provide security services**
- **To introduce two techniques, cryptography and steganography, to implement security mechanisms**

Security Goals



Confidentiality

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those

malicious actions that endanger the confidentiality of its information.

Hides information from Unauthorized access

Eg: Military , Industry and in banking information need to kept secret.

Integrity

Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

-protect information from unauthorized change

Eg: banking application

Availability

The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

-information need to be available to authorized user when it is required.

Eg: banking application

Security Services

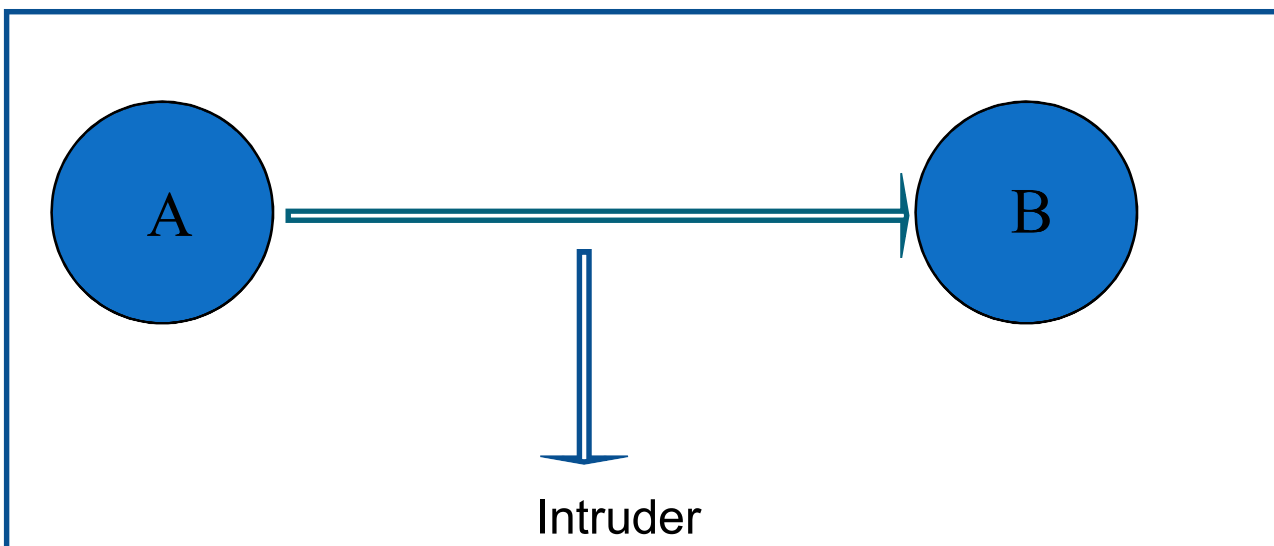
- **Confidentiality**: Protection from disclosure to unauthorized party or process
- **Authenticity**: is the identification and assurance of the origin of information
- **Integrity**: refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes
- **Non-Repudiation**: Originator cannot deny sending the message

Security Services

- **Availability** : refers to the ability to use the information or resource desired.
- **Access control** : who is allowed to access what resources, hosts, software, network connections
- **Anonymity** : hides user details

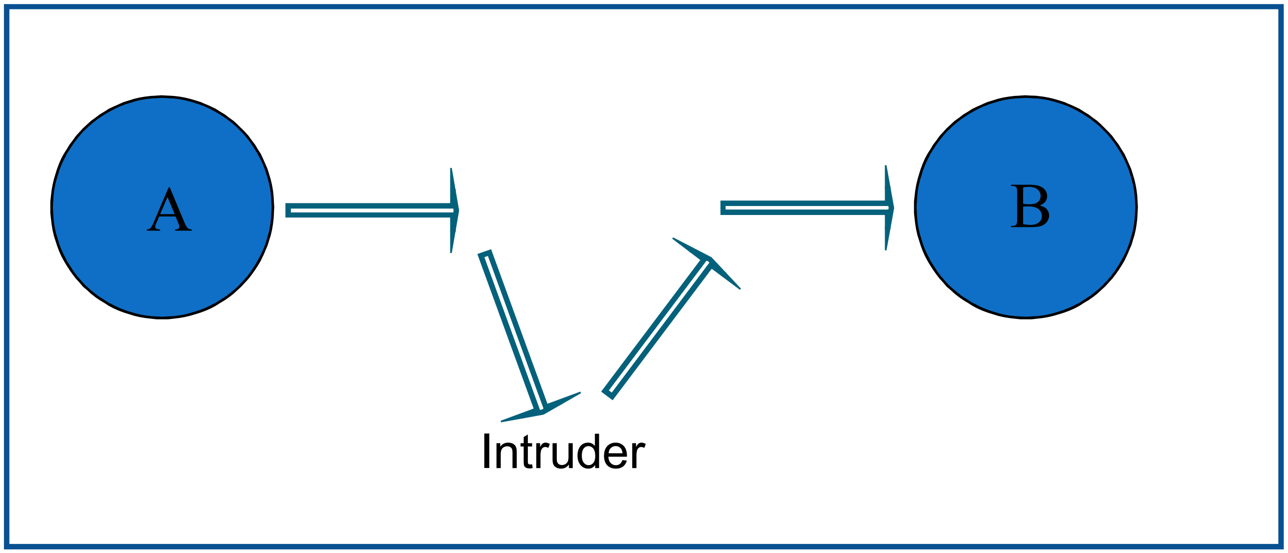
Interception

- Intruder(passive) intercepts in middle of the activity and view the message
- Attack on confidentiality



Modification

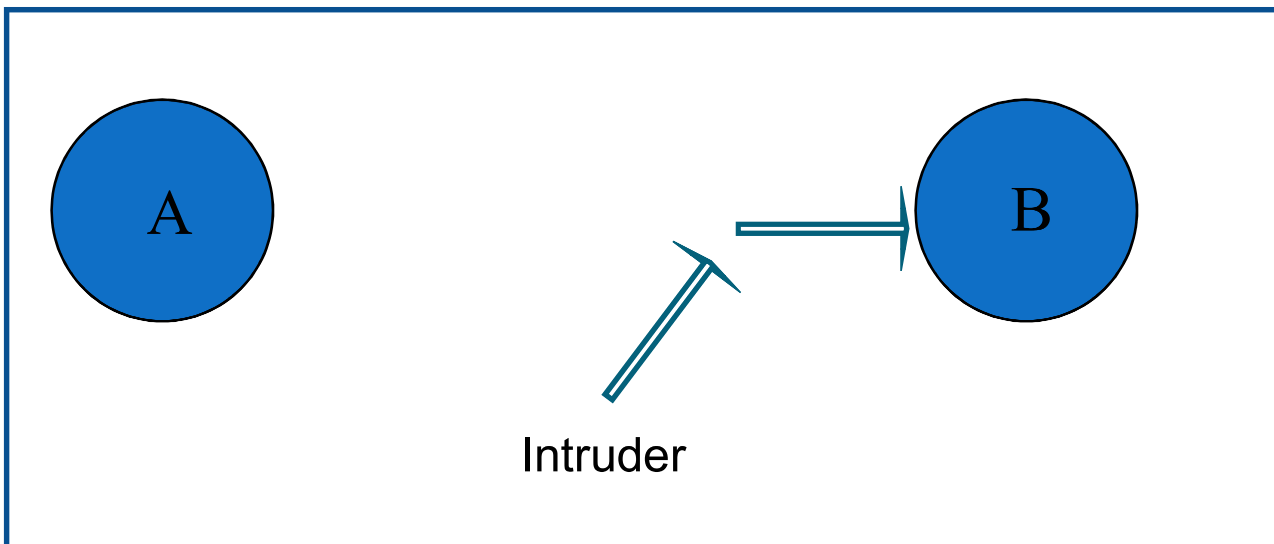
- Active intruder intercepts in middle and modifies the message
- Attack on Integrity



D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Fabrication

- Active intruder fabricates the message and send impersonating a sender
- Attack on authenticity

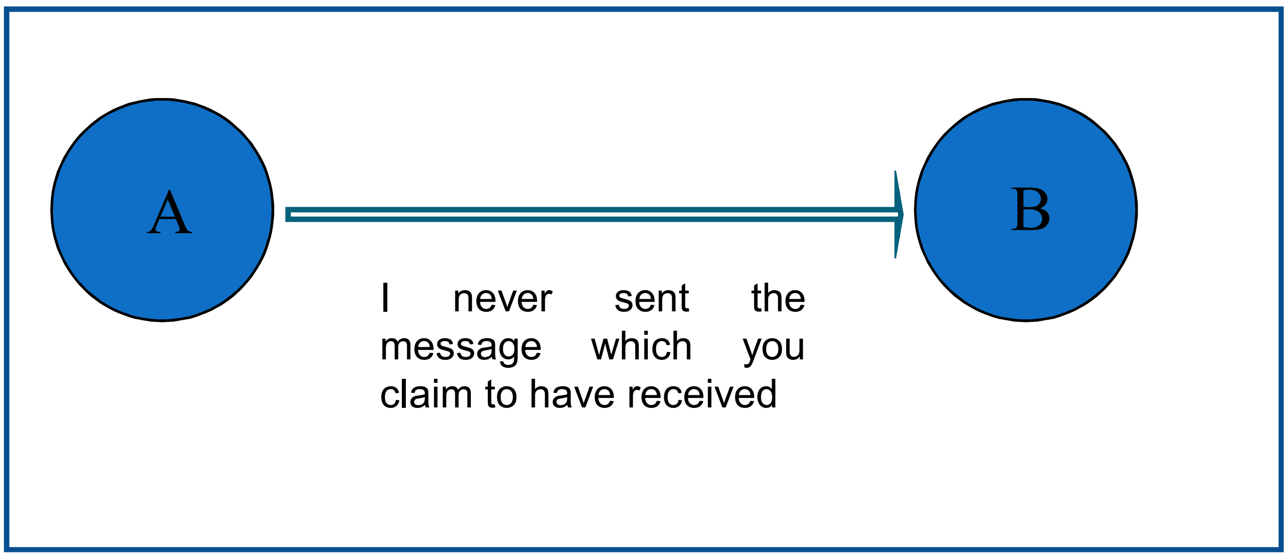


Interruption

- Active intruder intercepts in middle and stop communication
- Attack on availability

Non-Repudiation

- It does not allow the sender of a message to refuse the claim of not sending that message



ATTACKS

The three goals of security—confidentiality, integrity, and availability—can be threatened by security attacks.

Topics discussed in this section:

Attacks Threatening Confidentiality
Attacks Threatening Integrity
Attacks Threatening Availability
Passive versus Active Attacks

Security Attacks

An **attack** is any action that compromise security of information

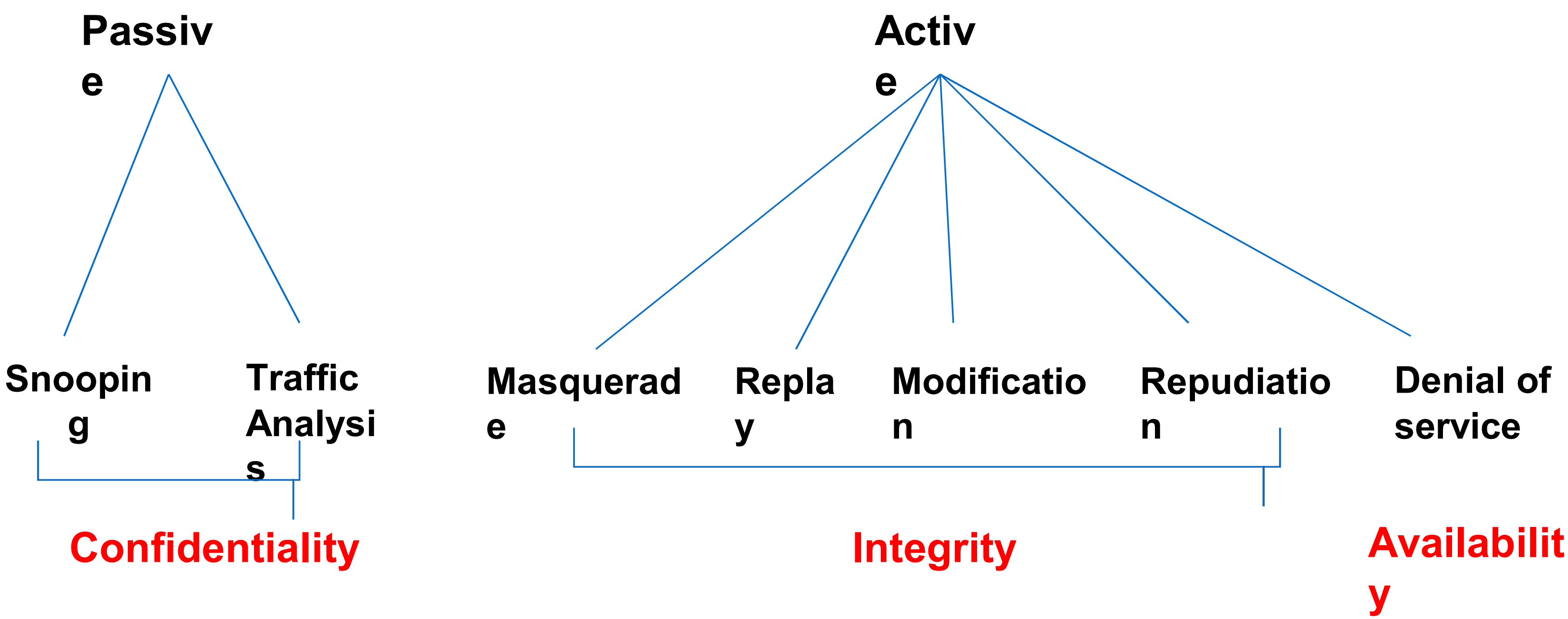
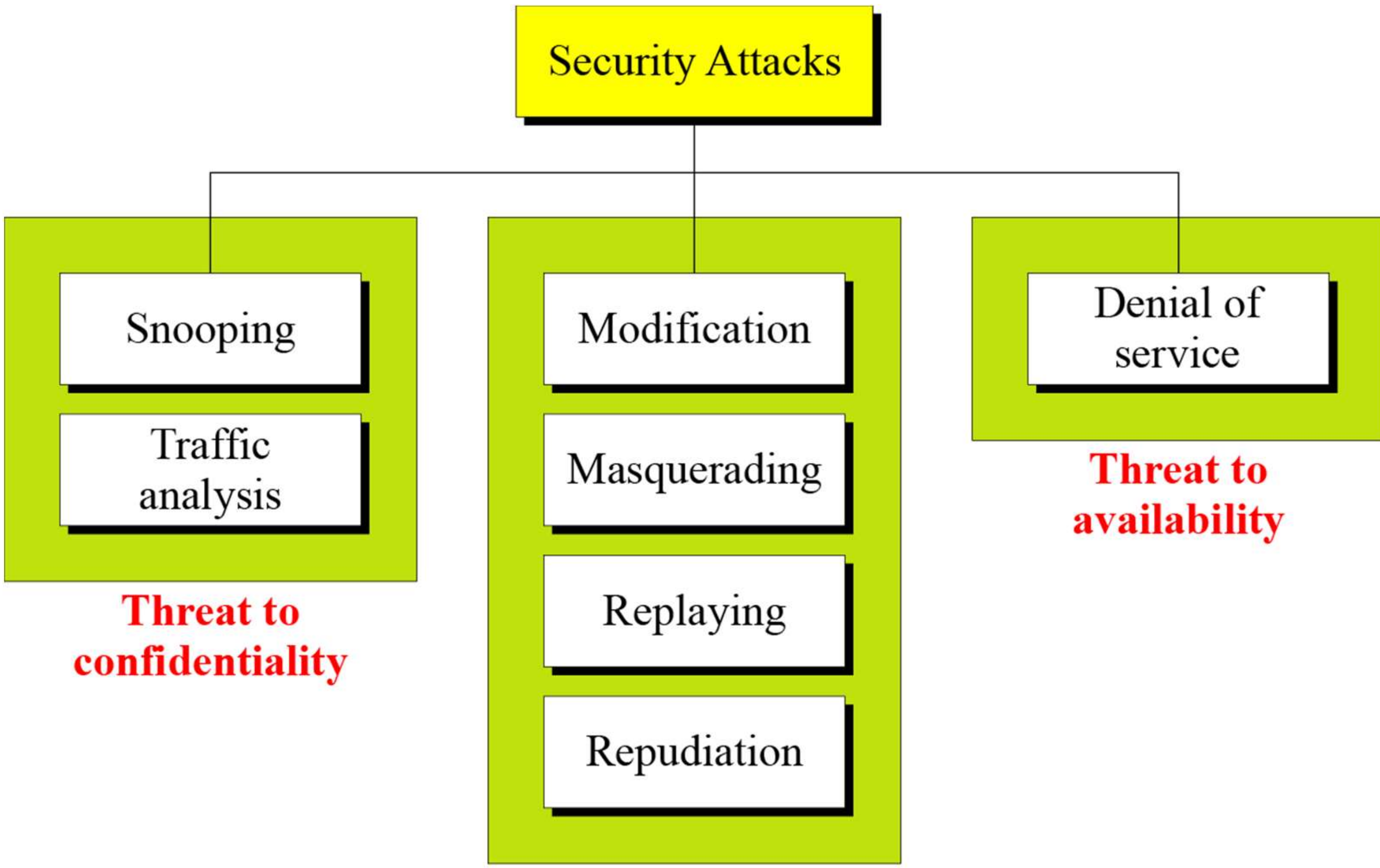
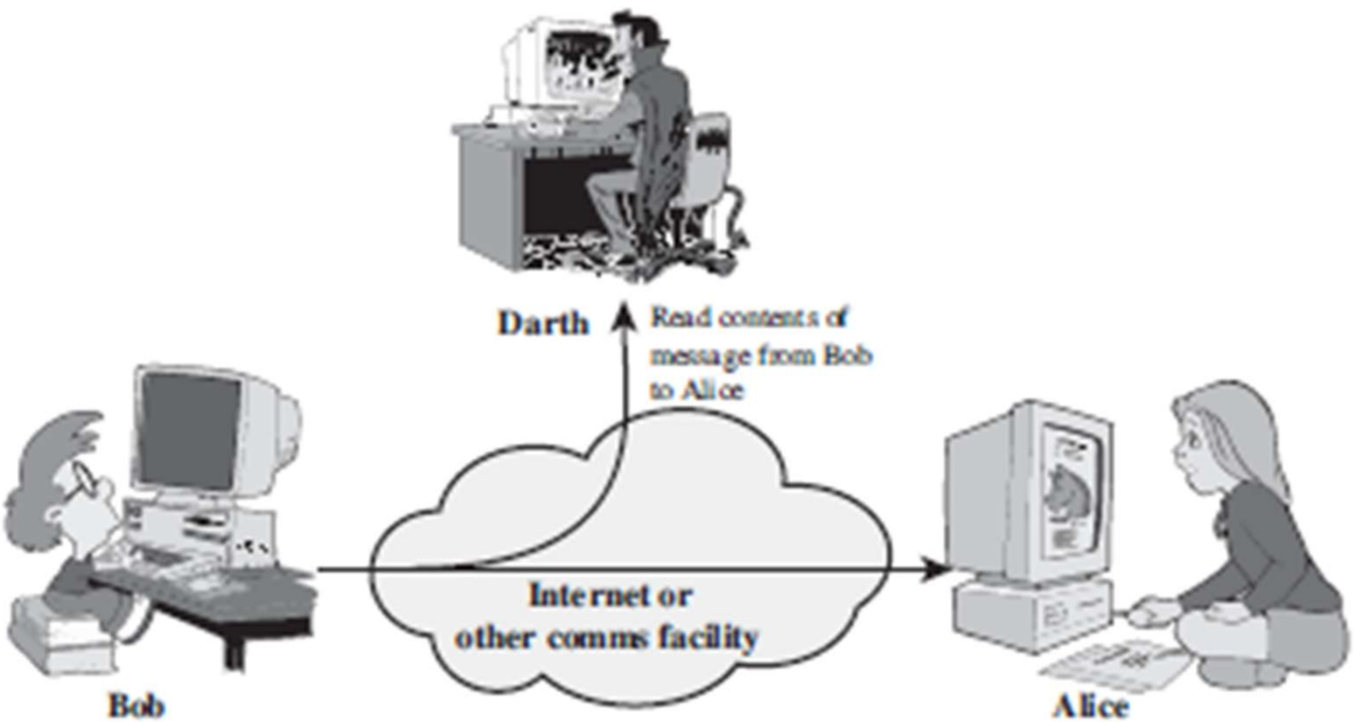


Figure 1.2 Taxonomy of attacks with relation to security goals



Attacks Threatening Confidentiality

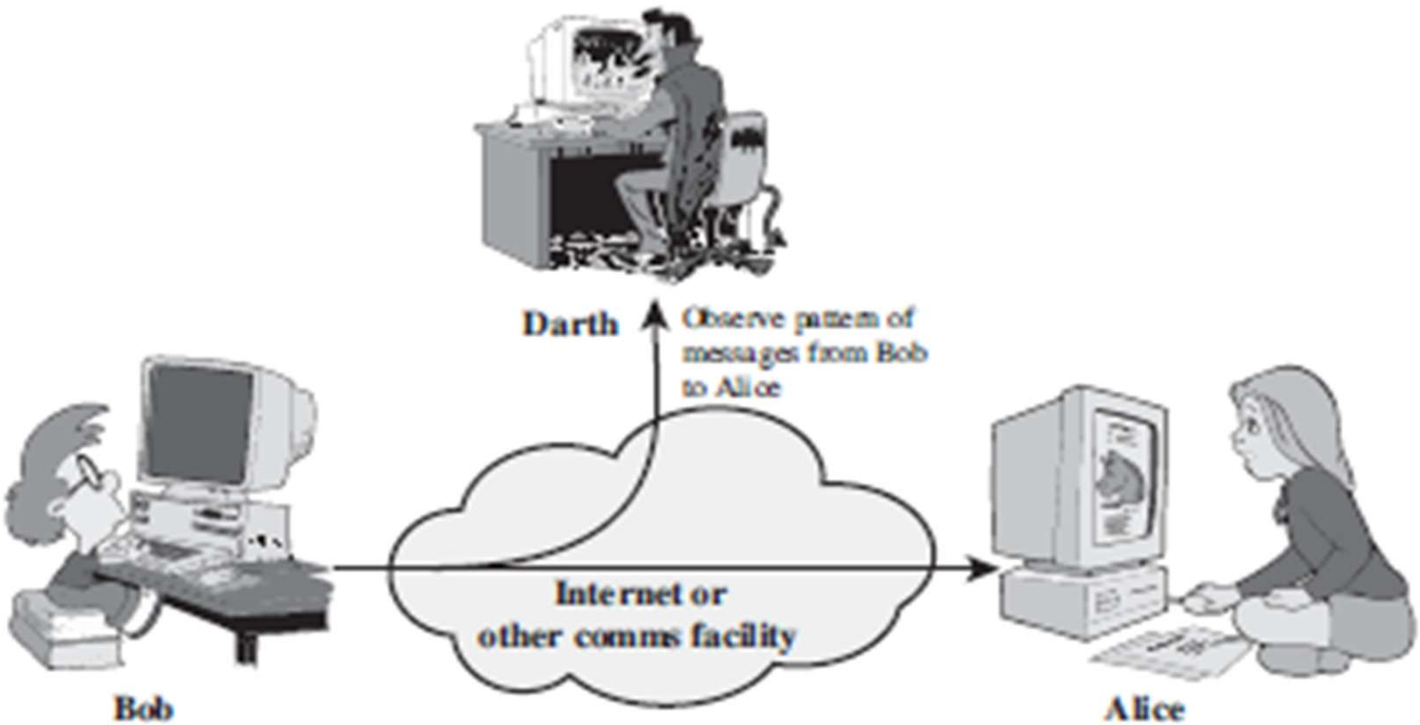
Snooping refers to unauthorized access to or interception of data.



(a) Release of message contents

Attacks Threatening Confidentiality

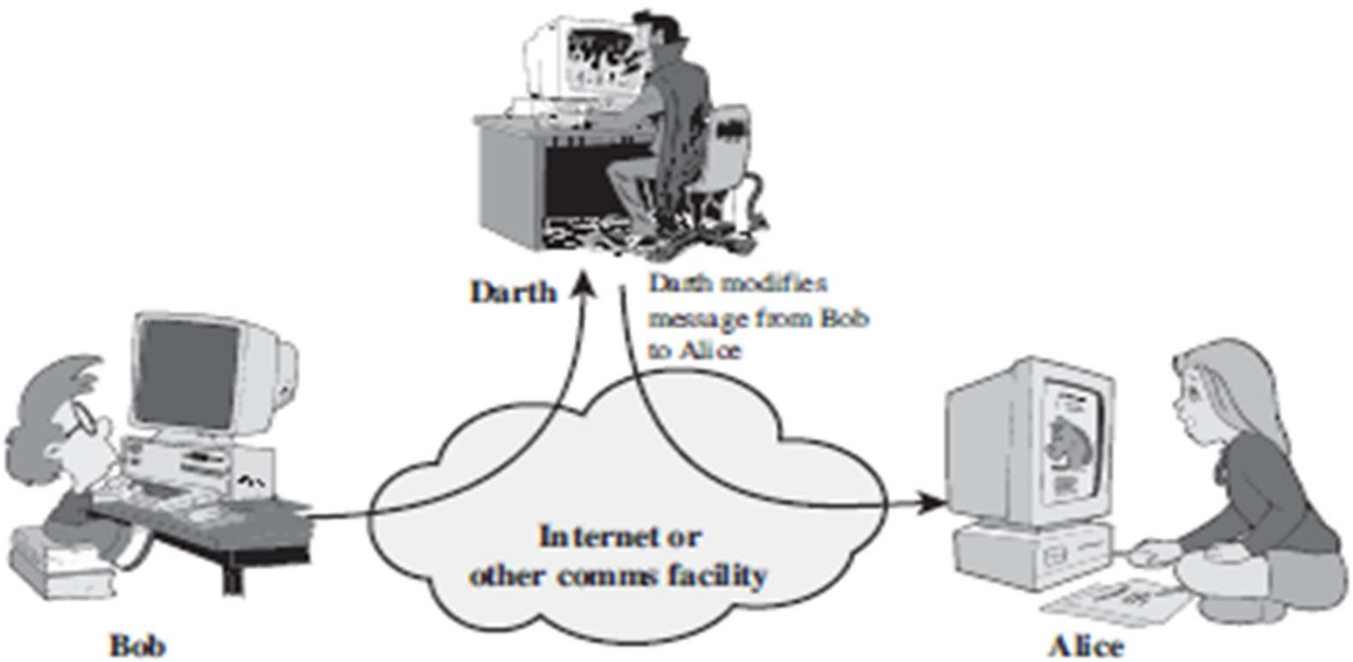
Traffic analysis refers to obtaining some other type of information by monitoring online traffic.



(b) Traffic analysis

Attacks Threatening Integrity

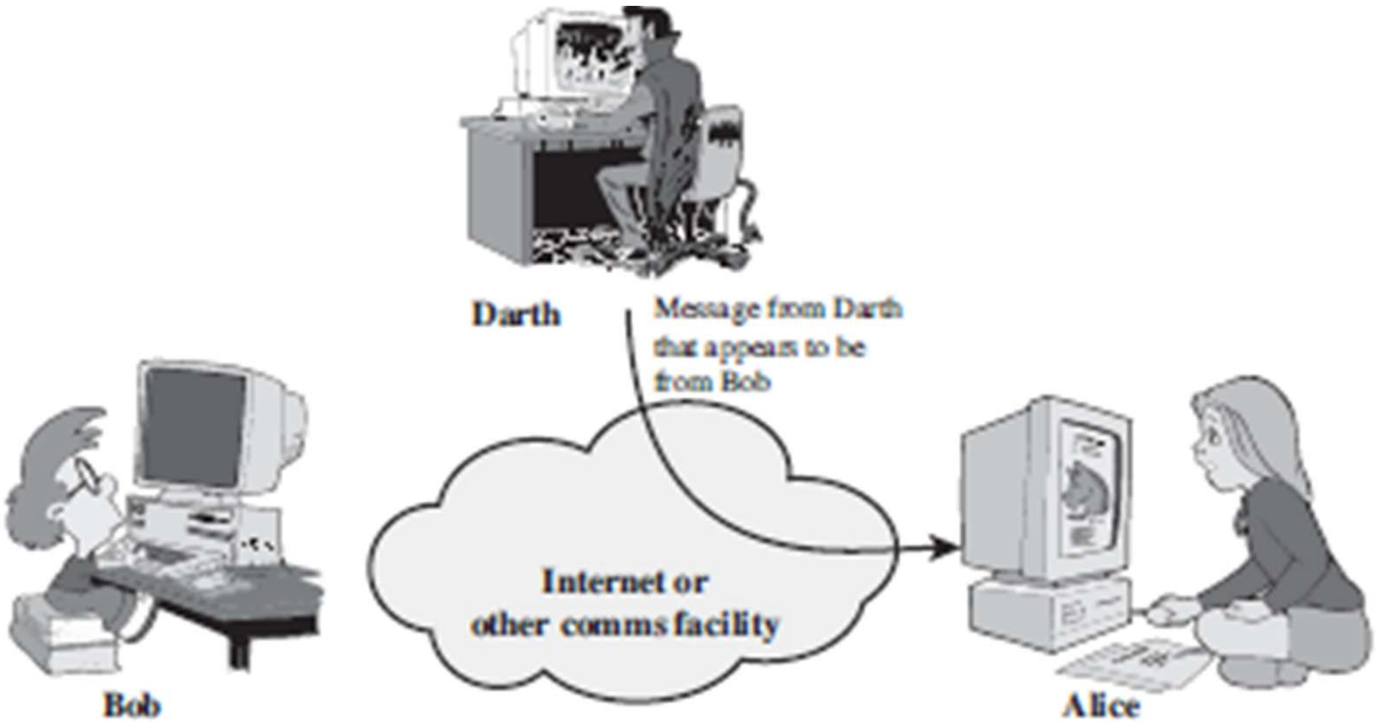
Modification means that the attacker intercepts the message and changes it.



(c) Modification of messages

1.2.2 Attacks Threatening Integrity

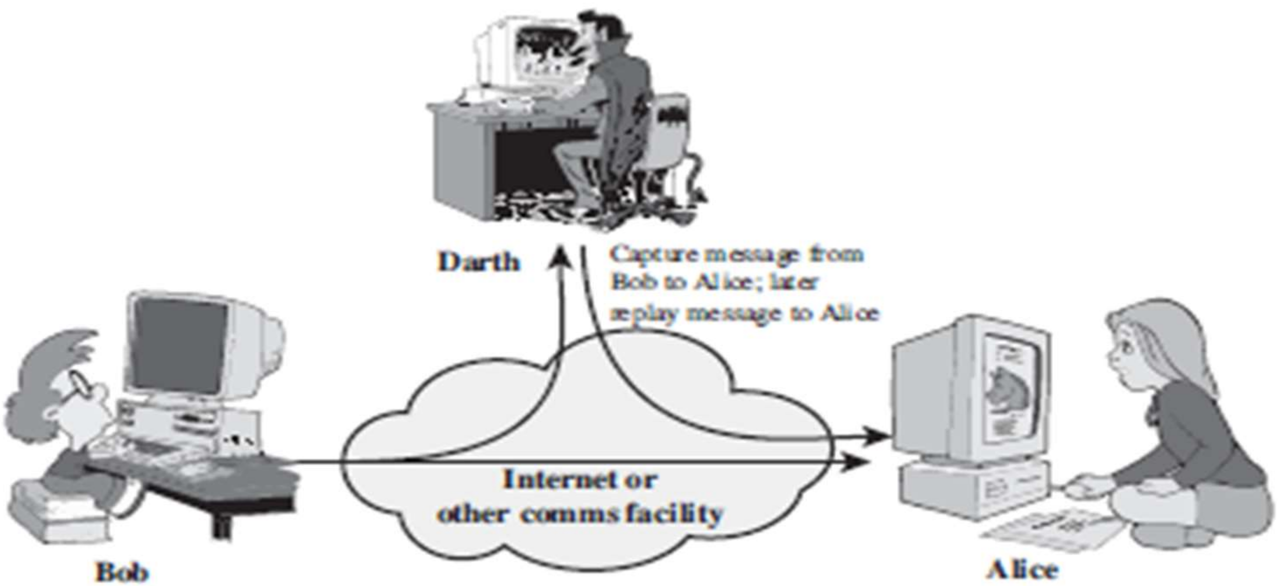
Masquerading or spoofing happens when the attacker impersonates somebody else.



(a) Masquerade

1.2.2 Attacks Threatening Integrity

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.



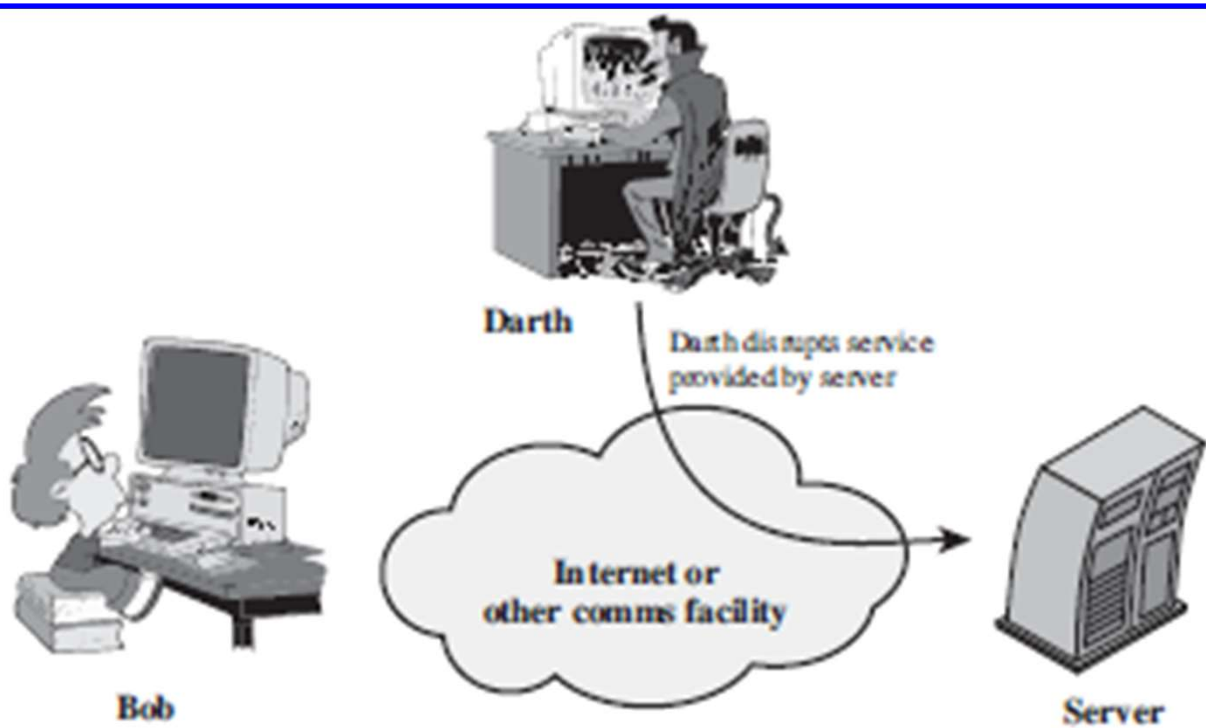
(b) Replay

1.2.2 Attacks Threatening Integrity

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

1.2.3 Attacks Threatening Availability

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.



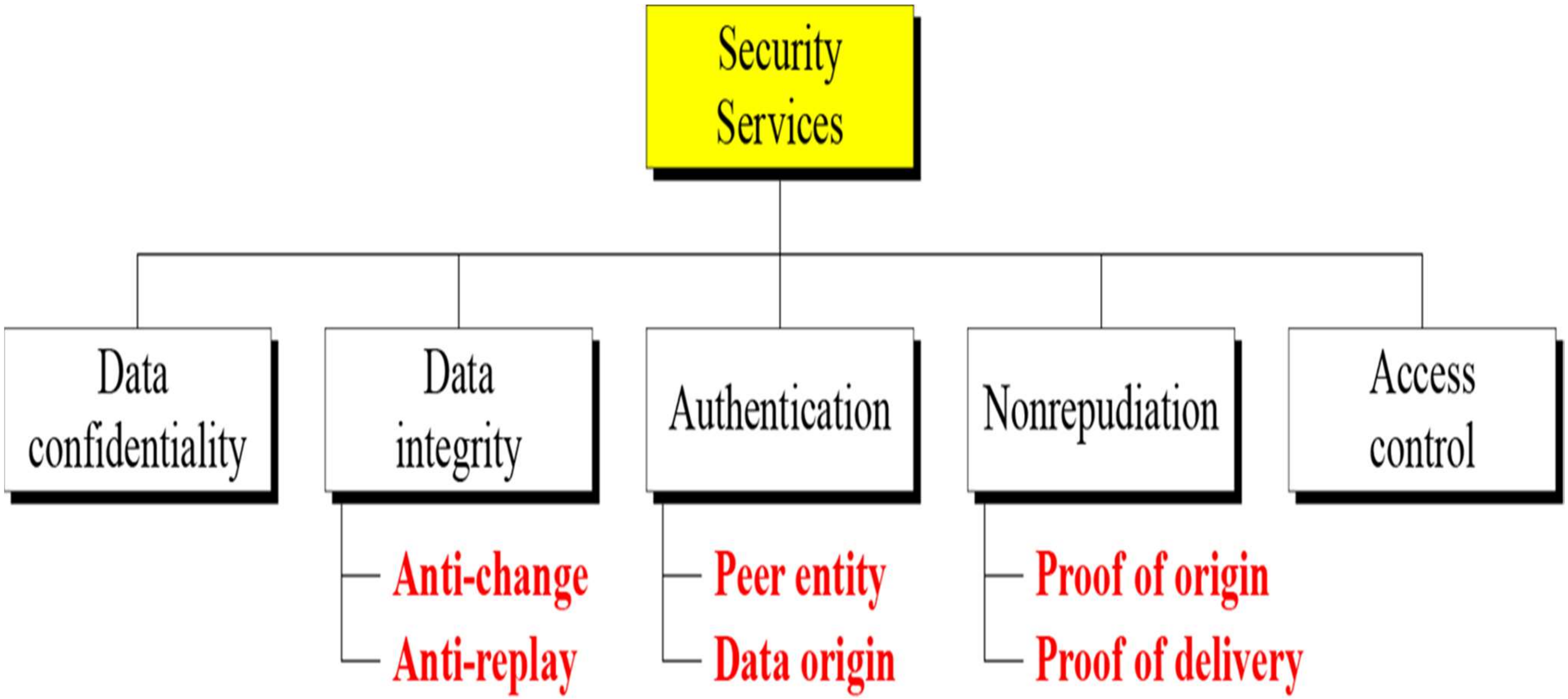
(d) Denial of service

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service..

Topics discussed in this section:

Security Services
Security Mechanism
Relation between Services and Mechanisms

Security Services



Security Mechanisms

"A method, protocol, tool, or procedure for enforcing a security policy"

- Encipherment
- Data Integrity(Hashing)
- Digital Signature
- Access control
- Authentication Exchange
- Traffic Padding
- Routing Control
- Notarization

Relation between Security Services and Security Mechanisms

Security Services	Security Mechanisms
Confidentiality	Encipherment and routing control
Integrity	Encipherment, digital signature, data integrity(Hashing)
Authentication	Encipherment, Digital signature, Authenticating Exchange
Nonrepudiation	Digital signature, Data integrity(Hashing), notarization
Access control	Access Control Mechanism

TECHNIQUES

Mechanisms discussed in the previous sections are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: cryptography and steganography.

Topics discussed in this section:

Cryptography

Steganography

Classical Security Techniques

1.Cryptography

- Symmetric Key Encipherment/Secret Key Cryptography/Private Key Cryptography
- Asymmetric Key Encipherment/ Shared Key Cryptography/ Public Key Cryptography

2. Steganography

Cryptography

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Cryptography

- Symmetric(Secret/Shared/Private key)

$$C = E_k(M)$$

$$M = D_k(C)$$

- Asymmetric(Public key)

$$C = E_{pu.k}(M)$$

$$M = D_{pr.k}(C)$$

1.4.2 Steganography

The word steganography, with origin in Greek, means "covered writing," in contrast with cryptography, which means "secret writing."

Example: covering data with text

This book is mostly about cryptography, not steganography.

□ □□ □ □ □ □ □□

0 1 0 0 0 0 1

Example: using dictionary

A	**friend**	**called**	**a**	**doctor.**
0	10010	0001	0	01001

Example: covering data under color image

0101001**1**	1011110**0**	0101010**1**
0101111**0**	1011110**0**	0110010**1**
0111111**0**	0100101**0**	0001010**1**

UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Basic Terminologies

- **Plaintext** - original message
- **Ciphertext** - coded message
- **Cipher** - algorithm for transforming plaintext to ciphertext
- **Key** - info used in cipher known only to sender/receiver
- **Encipher (encrypt)** - converting plaintext to ciphertext
- **Decipher (decrypt)** - recovering plaintext from ciphertext
- **Cryptanalysis (code breaking)** - study of principles/ methods of deciphering ciphertext without knowing key
- **Cryptology** - field of both cryptography and cryptanalysis

Requirements for Secure Conventional Encryption

- Strong encryption algorithm
  - An opponent who knows one or more ciphertexts would not be able to find the plaintexts or the key
  - Ideally, even if he knows one or more pairs of plaintext-ciphertext, he would not be able to find the key
- Sender and receiver must share the same key. Once the key is compromised, all communications using that key are readable
- Encryption algorithm is not a secret. It is impractical to decrypt the message on the basis of the ciphertext plus the knowledge of the encryption algorithm

Thank You

D Y PATIL
RAMRAO ADIK
INSTITUTE OF
TECHNOLOGY
NAVI MUMBAI

Lecture No: 2

Integer Arithmetic and Modular Arithmetic: Euclidean Algorithm

INTEGER ARITHMETIC

In integer arithmetic, we use a set and a few operations. You are familiar with this set and the corresponding operations, but they are reviewed here to create a background for modular arithmetic.

Topics discussed in this section:

- Set of Integers
- Binary Operations
- Integer Division
- Divisibility

Set of Integers

The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity (Figure 2.1).

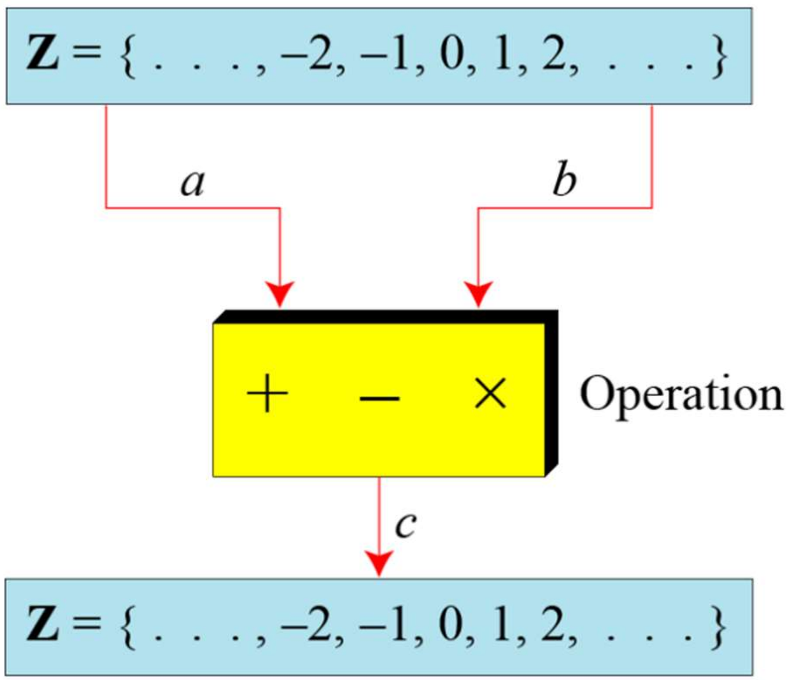
The set of integers

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

Binary Operations

We are interested in three binary operations applied to the set of integers in cryptography. A binary operation takes two inputs and creates one output.

Three binary operations for the set of integers



Example

The following shows the results of the three binary operations on two integers. Because each input can be either positive or negative, we can have four cases for each operation.

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

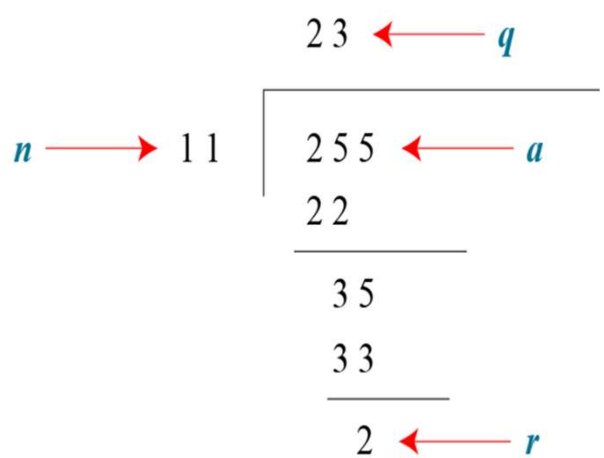
Integer Division

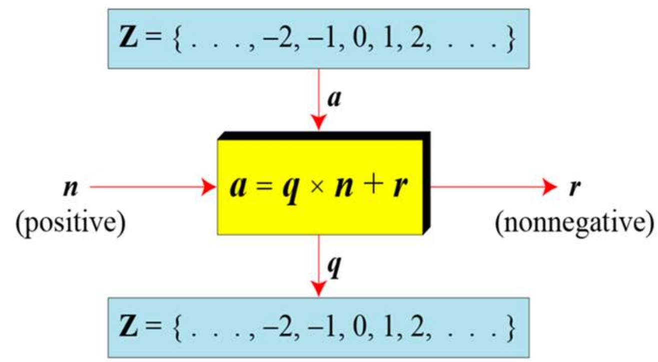
In integer arithmetic, if we divide a by n, we can get q And r .
The relationship between these four integers can be shown as

$$a = q \times n + r$$

Example

Assume that a = 255 and n = 11. We can find q = 23 and R = 2 using the division algorithm.





When we use a computer or a calculator, r and q are negative when a is negative. How can we apply the restriction that r needs to be positive? The solution is simple, we decrement the value of q by 1 and we add the value of n to r to make it positive.

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

Divisbility

If a is not zero and we let r = 0 in the division relation, we get

$$a = q \times n$$

If the remainder is zero, $a \mid n$

If the remainder is not zero, $a \nmid n$

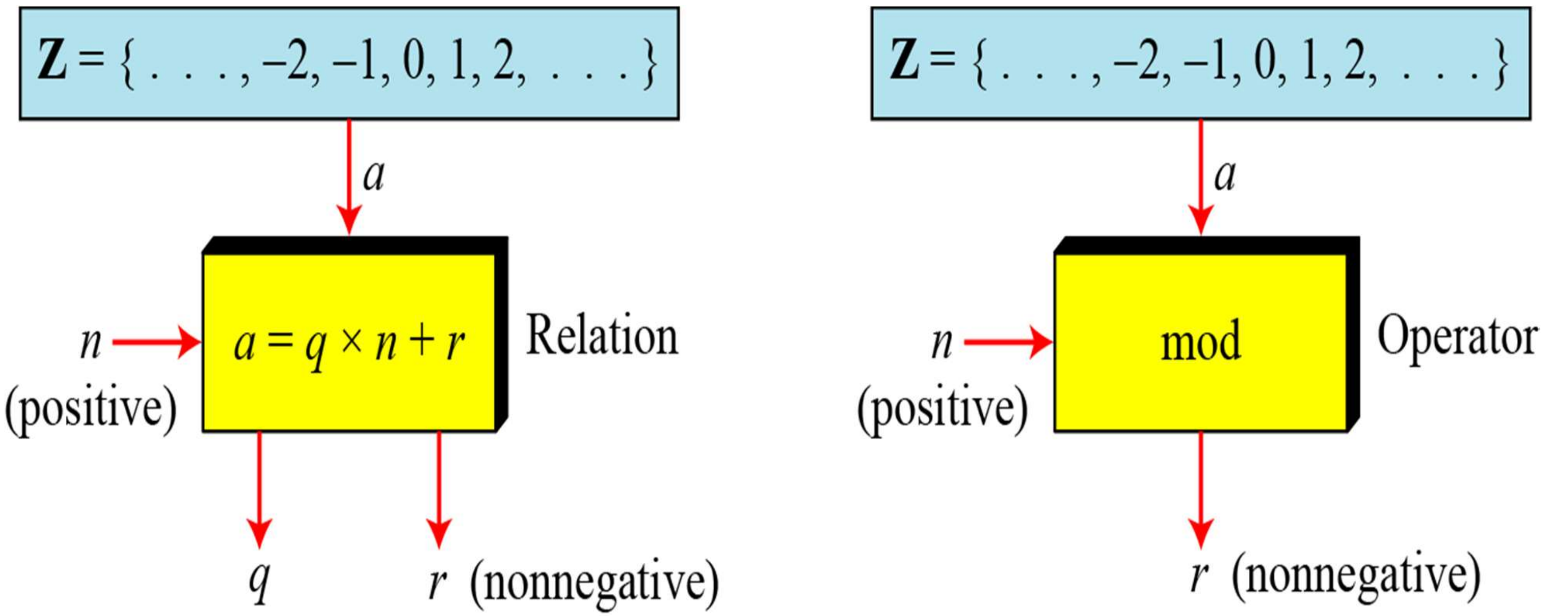
The integer 4 divides the integer 32 because 32 = 8 × 4. We show this as

$$4 \mid 32$$

The number 8 does not divide the number 42 because 42 = 5 × 8 + 2. There is a remainder, the number 2, in the equation. We show this as

$$8 \nmid 42$$

Modular Arithmetic



Modular Arithmetic

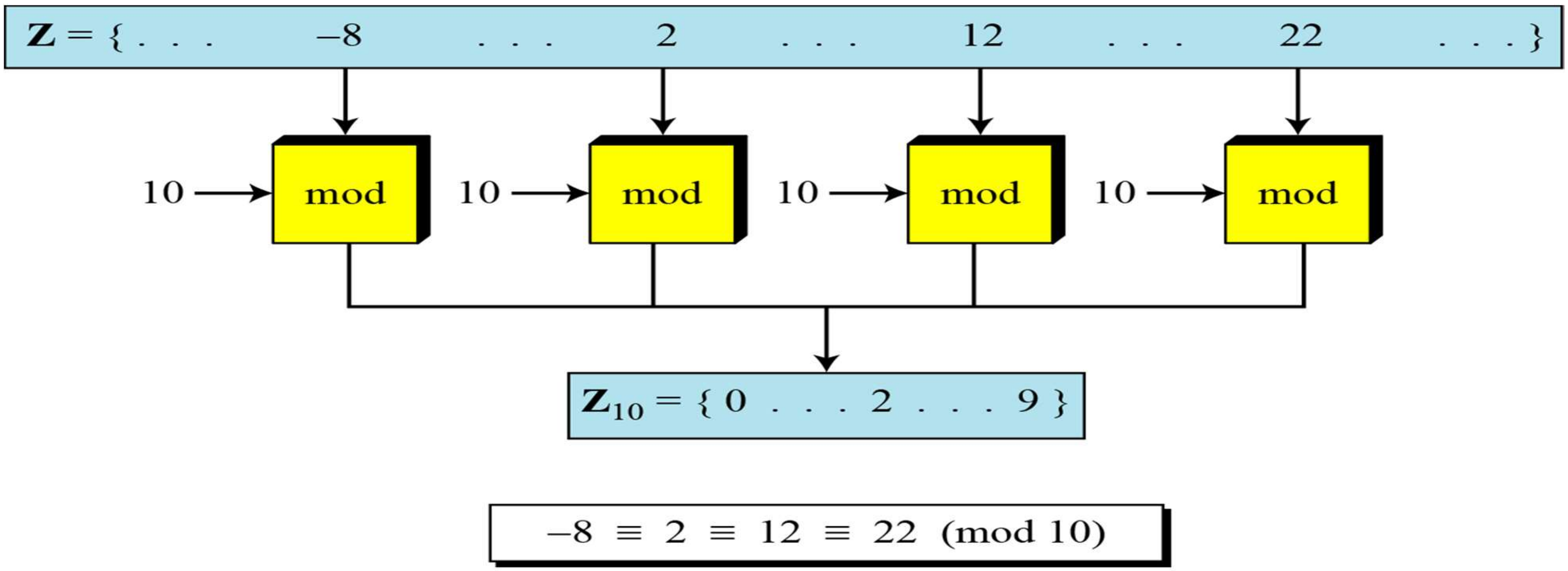
Examples:

1. 39 mod 5 = **4**
2. 98 mod 12 = **2**
3. -28 mod 11 = **-6 + 11 = 5**
4. -4 mod 10 = **- 4 + 10 = 6**

Set of Residues (Z_n) - nonnegative integers less than n

Congruence

a ≡ b (mod n) : a is said to be congruent to b modulo n if they leave same remainder when divided by n



Congruence Relationship

Properties of Modulo Operator

- $a \equiv b \bmod n$ if $n|(a-b)$
- $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$
- $a \equiv b \bmod n$ and $b \equiv c \bmod n$ implies $a \equiv c \bmod n$
- $(a \bmod n) + (b \bmod n) = (a + b) \bmod n$
- $(a \bmod n) \times (b \bmod n) = (a \times b) \bmod n$
- $(a + b) \equiv (a + c) \bmod n$ then $b \equiv c \bmod n$

Modular Exponentiation

$5^3 \bmod 7 = 5.5.5 = 125 \bmod 7 = 6$

$5^{30} \bmod 7 = ?$

$5^1 \bmod 7 = 5$

$5^2 \bmod 7 = 4$

$5^4 \bmod 7 = 4^2 \bmod 7 = 16 \bmod 7 = 2$

$5^8 \bmod 7 = 2^2 \bmod 7 = 4$

$5^{16} \bmod 7 = 4^2 \bmod 7 = 2$

$5^{30} \bmod 7 = (5^{16} .5^8 .5^4 .5^2) \bmod 7 = (2.4.2.4) \bmod 7 = 1$

Examples:

1. $9^{15} \bmod 16$
2. $60^{40} \bmod 100$

Inverses

- Additive Inverse

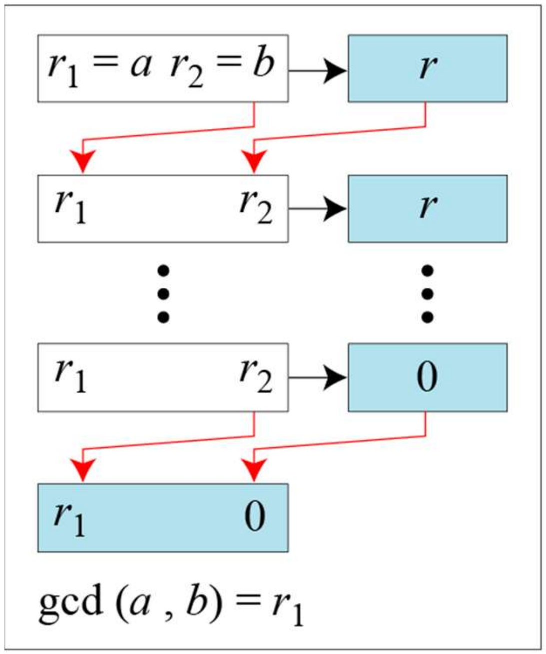
  Two numbers a and b are additive inverses of each other if $a + b \equiv 0 \pmod{n}$

- Multiplicative Inverse

  Two numbers a and b are multiplicative inverse of each other if $a \times b \equiv 1 \pmod{n}$

Note: a can have multiplicative inverse if gcd(a, n)=1

Euclidean Algorithm for GCD Calculation



a. Process

$$
\begin{array}{l}
r_1 \leftarrow a; \qquad r_2 \leftarrow b; \qquad \text{(Initialization)} \\
\text{while } (r_2 > 0) \\
\quad \{ \\
\qquad q \leftarrow r_1 / r_2; \\
\qquad r \quad \leftarrow r_1 - q \times r_2; \\
\qquad r_1 \leftarrow r_2; \quad r_2 \leftarrow r; \\
\quad \} \\
\gcd(a, b) \leftarrow r_1
\end{array}
$$

b. Algorithm

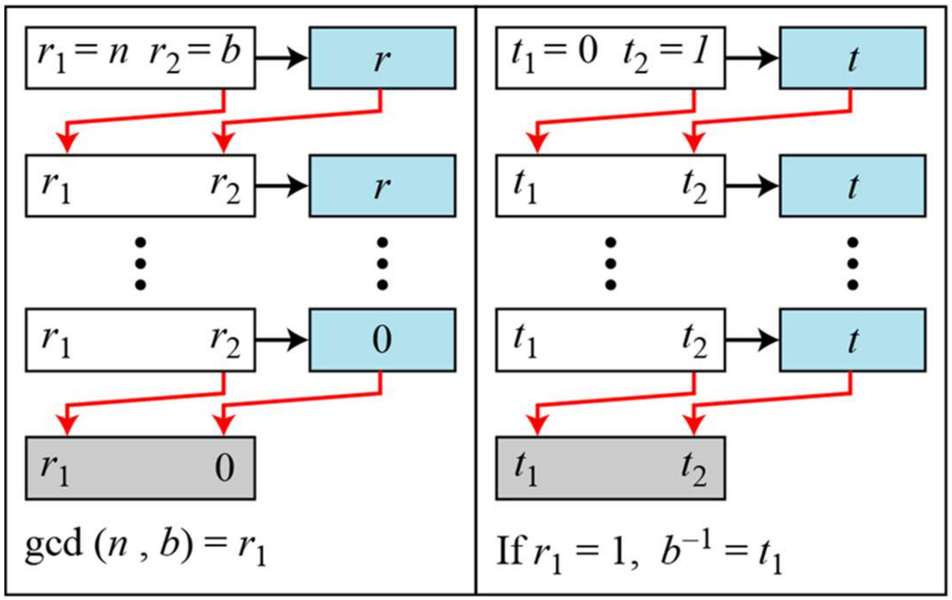
When gcd (a, b) = 1, we say that a and b are relatively prime.

Euclidean Algorithm for GCD Calculation

gcd (25, 65) = 5

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

Multiplicative Inverse using Extended Euclidean Algorithm



a. Process

```
r1 ← n;      r2 ← b;
t1 ← 0;      t2 ← 1;

while (r2 > 0)
 {
   q ← r1 / r2;

    r ← r1 − q × r2;
    r1 ← r2;     r2 ← r;

    t ← t1 − q × t2;
    t1 ← t2;     t2 ← t;

 }
   if (r1 = 1) then b^-1 ← t1
```

b. Algorithm

Example

Find multiplicative inverse of 7 in Z_{16}

q	r_1	r_2	r	t_1	t_2	t
2	16	7	2	0	1	-2
3	7	2	1	1	-2	7
2	2	1	0	-2	7	-16
	1	0		7	-16	

Multiplicative inverse of 7 in Z_{16} = 7 mod 16 = 7

Lecture No: 3

Primality Testing- Factorization, Euler‘s Totient Function, Fermat‘s and Euler‘s theorem

Primality Testing— Factorization

Primality testing is an algorithm for determining if a number is prime, while **factorization** is a computationally difficult problem for finding the prime factors of a number.

Primality Testing

Primality testing is the process of determining whether a given number n is prime or composite. There are various algorithms and techniques for primality testing, each with different efficiency and accuracy. Some common methods include:

1.TrialDivision:Checkwhether n is divisible by any integer a in the range 2 to n

Euler's Phi(totient)Function

- $\varphi(1) = 0$
- $\varphi(p)= p-1$ if p is prime
- $\varphi(m \times n)= \varphi(m) \times \varphi(n)$ if m and n are relatively prime(co-prime)
- $\varphi(p^e) = p^e - p^{e-1}$ if p is prime
- Also, if $n= p_1^{e1} \times p_2^{e2} \times \ldots . \times p_k^{ek}$ then

$$\phi(n)= (p_1^{e1} - p_1^{e1-1}) \times (p_2^{e2} - p_2^{e2-1}) \times \ldots\ldots \times (p_k^{ek} - p_k^{ek-1})$$

- Find: $\varphi(29)=$ 28 $\varphi(32)=$ 16 $\varphi(80)=$ 32

  $\varphi(108)=$ 40 $\varphi(101)=$ 100 $\varphi(240)=$ 64

D Y PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Euler's Theorem

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod{n} \; [a\ ,\ n \text{ are coprime}]}$$

- Proof:

  if $a = 3 \quad n = 10$

  $\phi(n) = \phi(10) = \phi(2 \times 5) = 4$

  $a^{\phi(n)} = 3^4 \equiv 1 \pmod{10}$

Example: Find 6^{24} mod 35

$6^{24} \bmod 35 = 6^{\phi(35)} \bmod 35 = 1$

Euler’s Theorem

To find multiplicative inverse modulo a composite If n and a are coprime, then

$$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$$

Examples:

1. 7^{-1} mod 75
2. 50^{-1} mod 23

Fermat's Theorem

First Version

$$\boxed{a^{p-1} \equiv 1 \bmod p}$$

[p is prime, a is integer such that p does not divide a]

Example: Find 6^{10} mod 11

$6^{11-1} \bmod 11 = 6^{10} \bmod 11 = 1$

Fermat's Theorem

- It can also be used to find multiplicative inverse.
- If p is prime and a is an integer such that p does not divide a, then

$$\boxed{a^{-1} \bmod p = a^{p-2} \bmod p}$$

a. $8^{-1} \bmod 17 = 8^{17-2} \bmod 17 = 8^{15} \bmod 17 = 15 \bmod 17$

b. $5^{-1} \bmod 23 = 5^{23-2} \bmod 23 = 5^{21} \bmod 23 = 14 \bmod 23$

c. $60^{-1} \bmod 101 = 60^{101-2} \bmod 101 = 60^{99} \bmod 101 = 32 \bmod 101$

d. $22^{-1} \bmod 211 = 22^{211-2} \bmod 211 = 22^{209} \bmod 211 = 48 \bmod 211$