RAMAIAH
Institute of Technology

M.S. Ramaiah Institute of Technology
(Autonomous Institute, Affiliated to VTU)
Department of Computer Science and Engineering

Course Name: Cryptography and Network Security

Course Code - CSE643

Credits - 3:0:0

UNIT -1

Term: March 2022 – July 2022

Prepared by: Dr. Sangeetha. V
Assistant Professor

RAMAIAH
Institute of Technology

OUTLINE

Introduction: (TextBook1 - Chapter 1)

- Security Goals
- Attacks
- Services and Mechanism
- Techniques

Mathematics of Cryptography: (TextBook1 - Chapter 2)

- Integer Arithmetic
- Modular Arithmetic
- Matrices
- Linear Congruence

Security Goals

- **Security** refers to the methods and tools to defend an organization's digital assets.
- The goal of IT security is to protect these assets, devices and services from being disrupted, stolen or exploited by unauthorized users, otherwise known as Threats.
- These threats can be external or internal and malicious in both origin and nature.

Security Goals

All information security measures try to address at least one of three goals as shown in Figure:

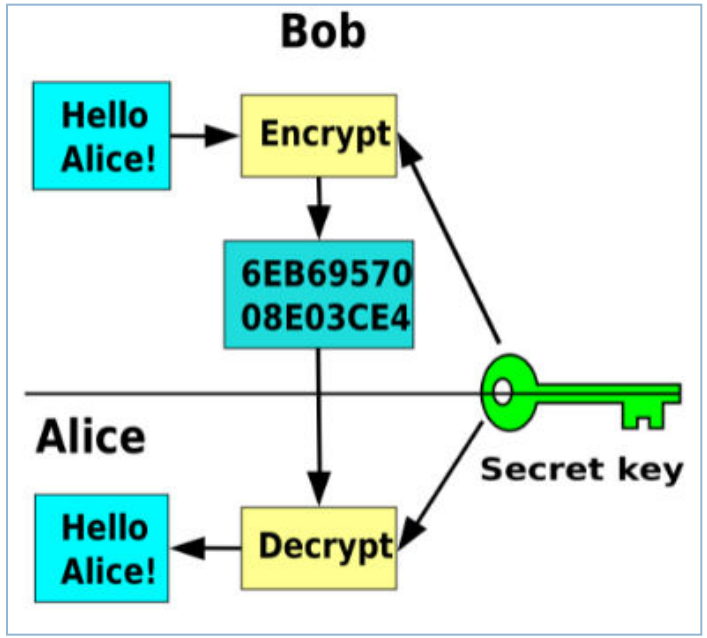
- Protect the Confidentiality of data
- Preserve the Integrity of data
- Promote the Availability of data for authorized use

Taxonomy of security goals

RAMAIAH Institute of Technology

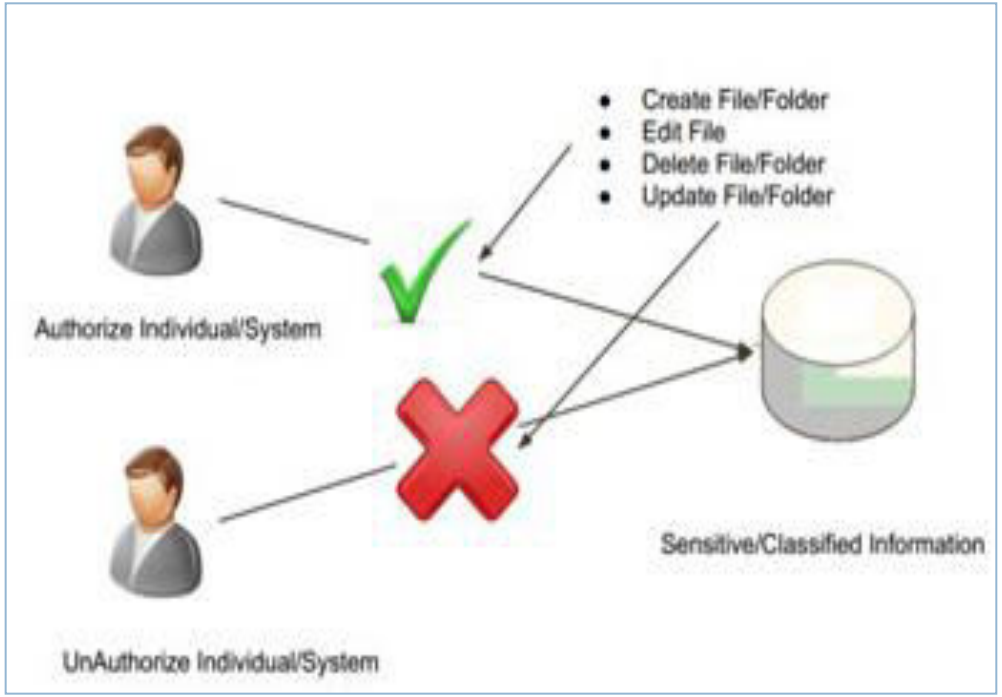
Security Goals

- **Confidentiality** is probably the most common aspect of information security. We need to protect confidential information.
- An organization needs to guard against those malicious actions that endanger the confidentiality of its information.
- Confidentiality is the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.
- Example : Banking, Military, Industry



Security Goals

- Information needs to be changed constantly.
- **Integrity** means changes need to be done only by authorized entities and through authorized mechanisms.
- Example : In Bank, when customer deposit or withdraw, balance of account need to be changed

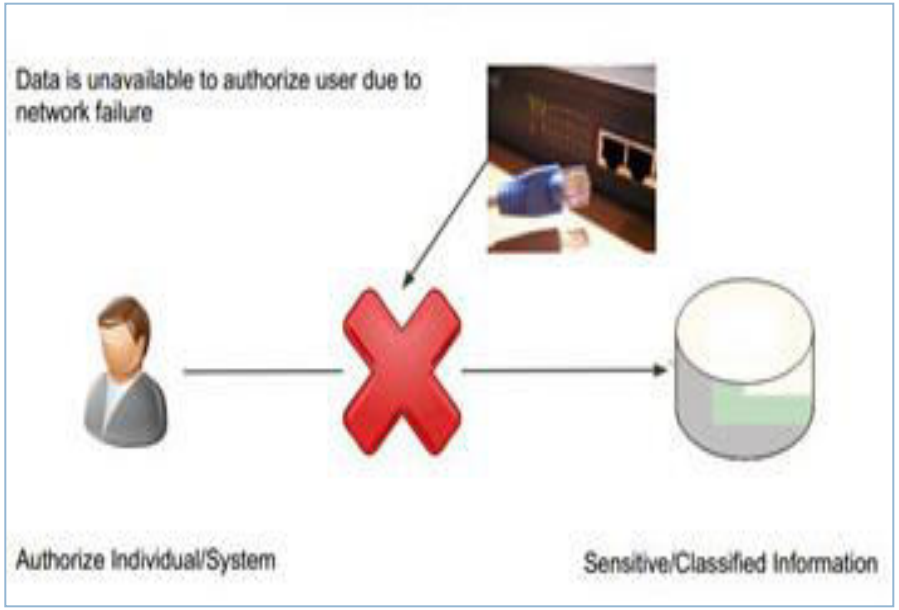


RAMAIAH Institute of Technology

Security Goals

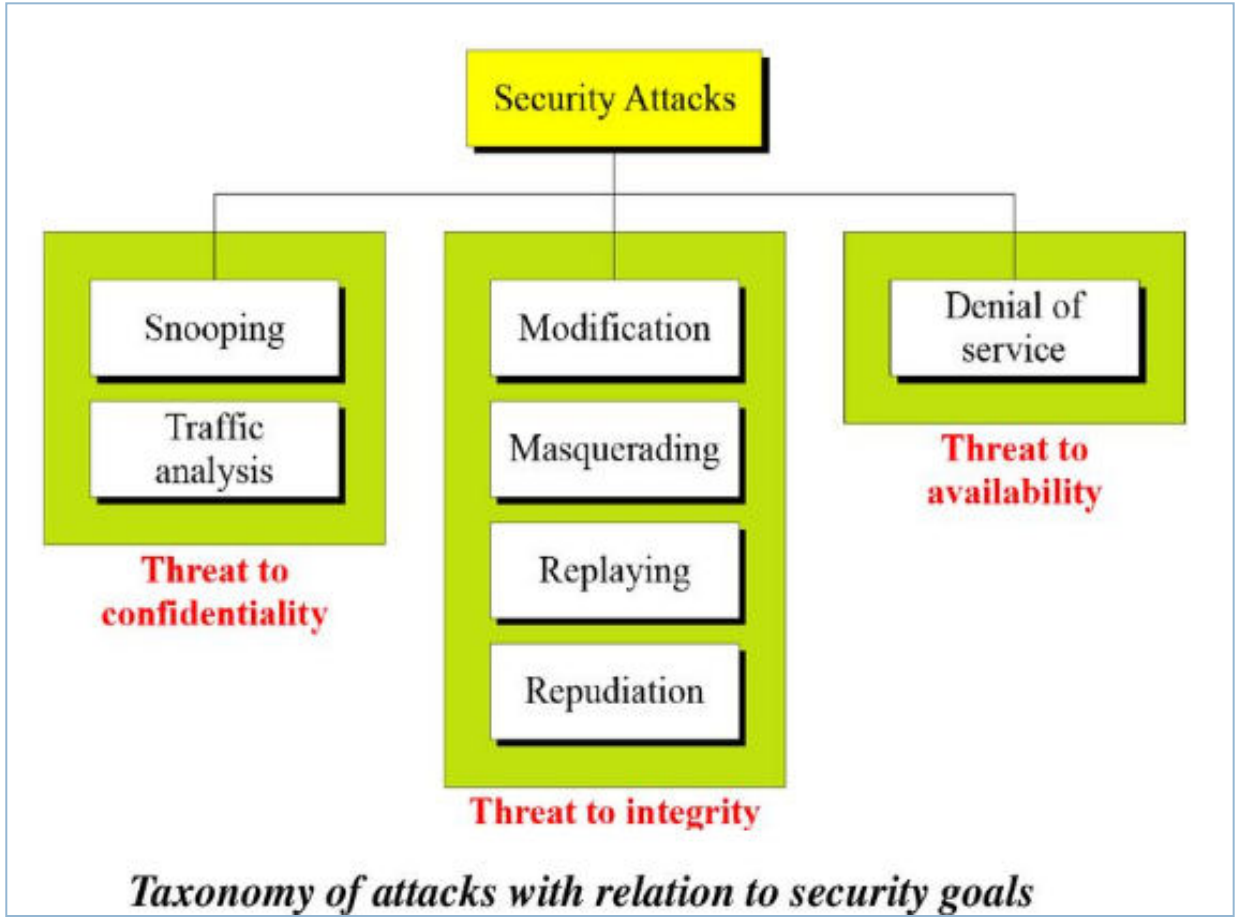
- The information created and stored by an organization needs to be available to authorized entities.
- Information needs to be constantly changed, which means it must be accessible to authorized entities.
- **Availability** is the property in which information is accessible and modifiable by authorized entities.

Example : Imagine what would happen to a bank if the customers could not access their accounts for transactions.



Attacks

- The three goals of security - confidentiality, integrity, and availability can be threatened by security attacks.
- We can divide them into 3 groups related to security goals



Taxonomy of attacks with relation to security goals

Attacks

- An attack is an threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission.
- It happens to both individuals and organizations.

Attacks

Attacks Threatening Confidentiality

1. **Snooping** refers to unauthorized access to or interception of data.

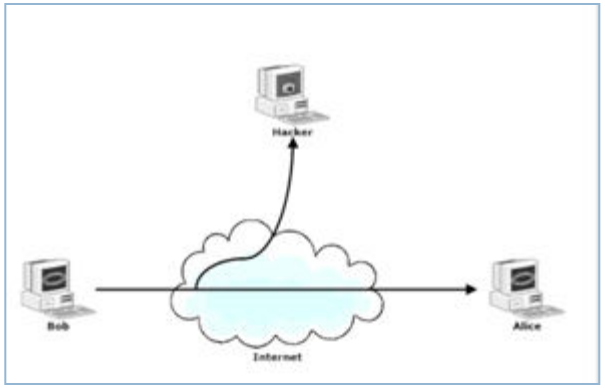
   Example : File transferred through internet may contain confidential information.

Attacks

Attacks Threatening Confidentiality

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

   Example : File transferred through internet

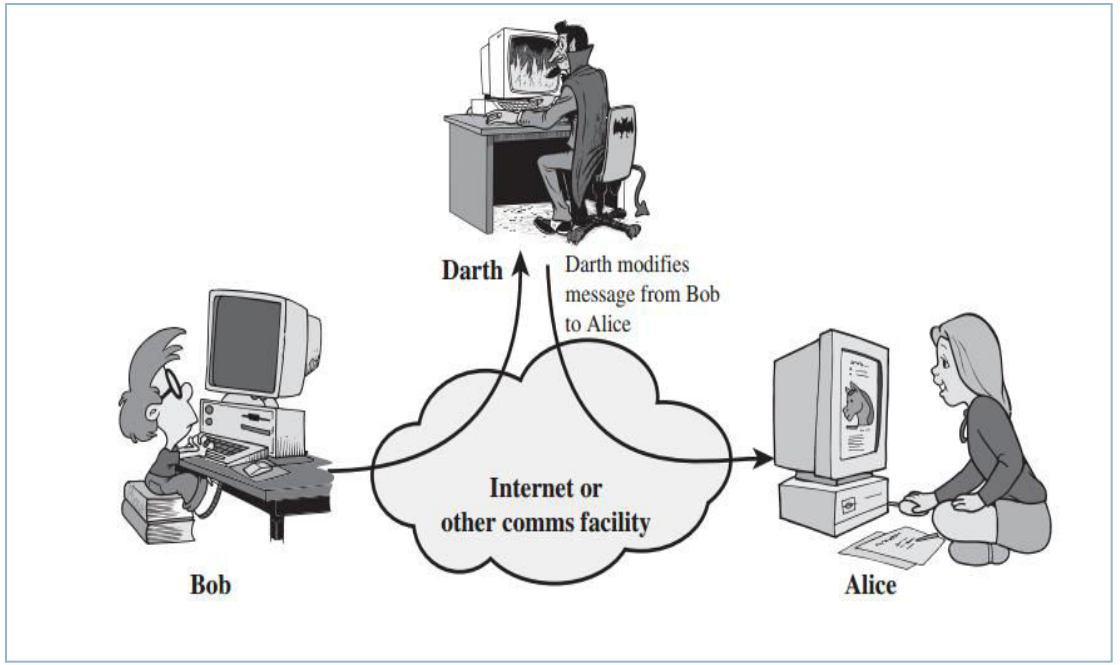


Attacks

Attacks Threatening Integrity

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

   Example: Customer send a message to bank to do some transaction.

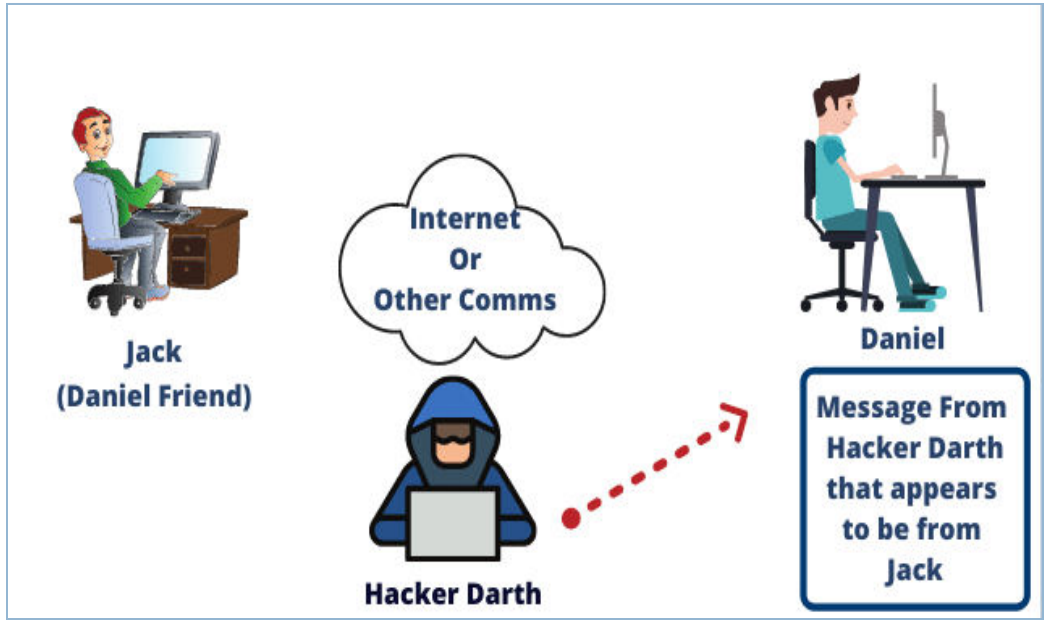


Attacks

Attacks Threatening Integrity

2. **Masquerading or spoofing** happens when the attacker impersonates somebody else.

   Example: Attacker can steal the pin of a bank customer and pretend that he/she is customer

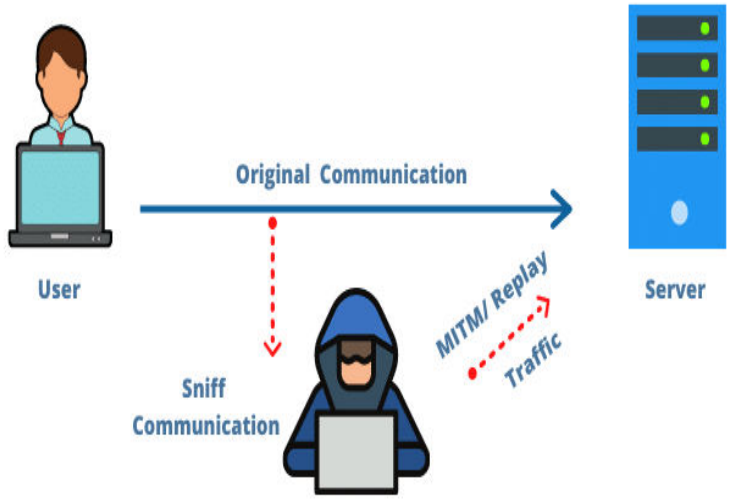


Attacks

Attacks Threatening Integrity

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

Example: Customer sends a request to her bank to ask for payment.

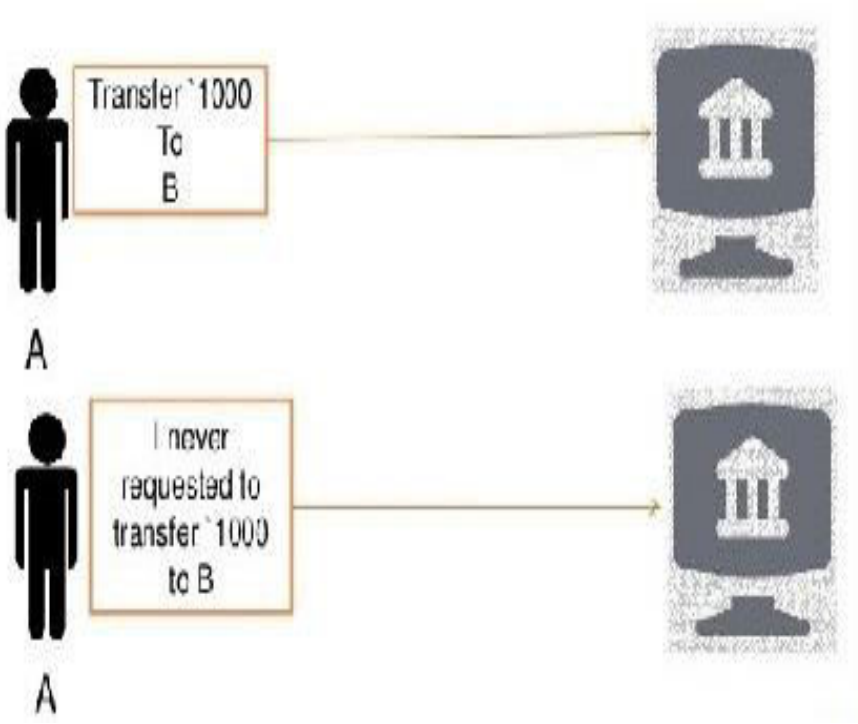


Attacks

Attacks Threatening Integrity

4. **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.

Example: Denial by the sender would be a bank customer asking her bank to send money to third party



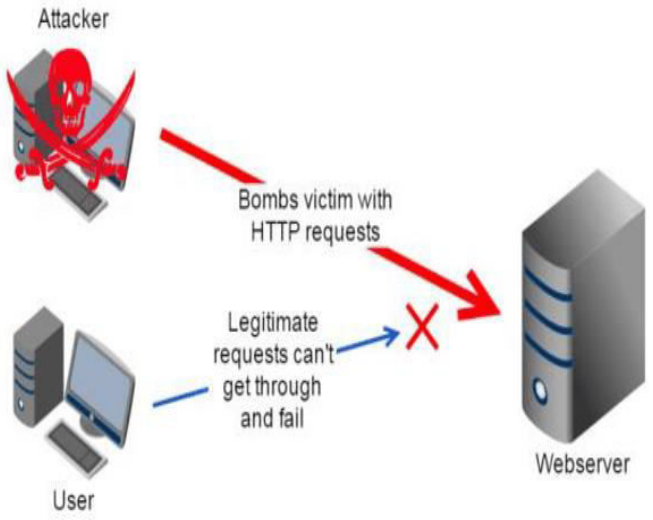
Attacks

Attacks Threatening Availability

1. **Denial of service (DoS)** attacks may slow down or totally interrupt the service of a system.

   The attacker can use several strategies to achieve this.

   - Send bogus request to a server, so that the server crashes because of heavy load.
   - Attacker intercept request from client, causing client to resend many times and overload the server.
   - Attacker intercept server response and delete, so that client believe server is not responding



Attacks

Passive Attacks

- Attackers goal is just to obtain information.
- Attack does not modify data or harm the system. The system continues with normal operation.
- However, attack may harm the sender or receiver of the message
- Attacks Threatening Confidentiality – Snooping and Traffic analysis are passive attacks

Attacks

Active Attacks

- Active attack may change the data or harm the system.
- Attacks Threatening Integrity and Availability are active attacks
- These type of attacks are easy to detect, than to prevent

Attacks

Passive versus Active Attacks

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Categorization of passive and active attacks

OSI Security Architecture

- Security Attacks
- Security Services
- Security Mechanisms

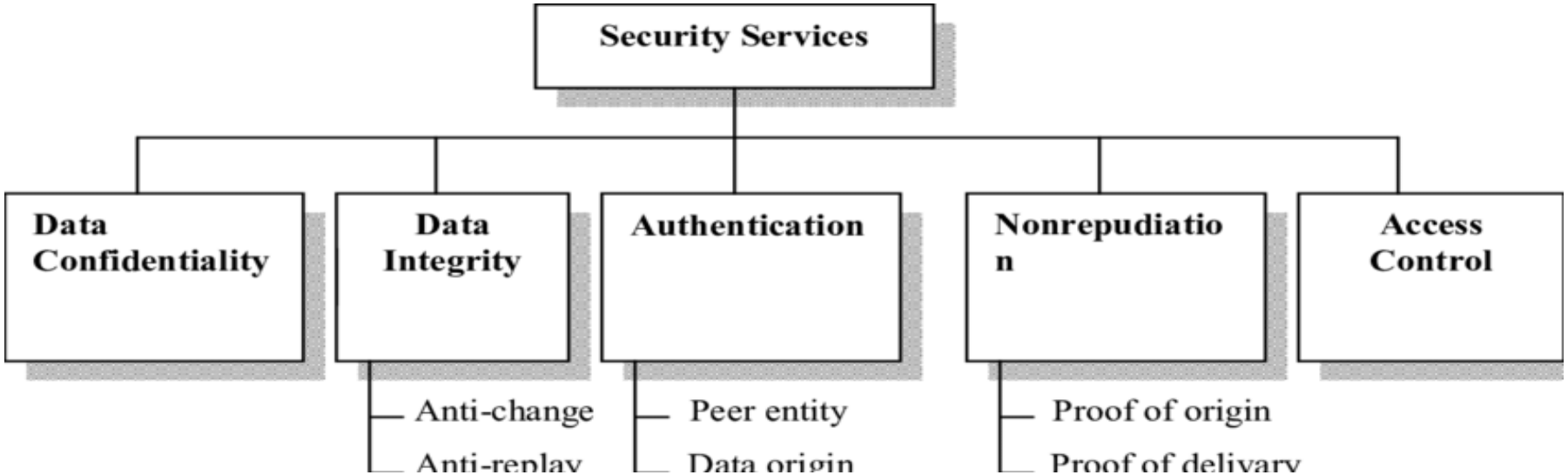
Services and Mechanisms

- **ITU-T (International Telecommunication Union-Telecommunication Standardization Sector)** provides security services and security mechanisms.
- **Security services are the communication service that is provided by a system to give a specific kind of protection to system resources.**
- Security service implement security policies and are implemented by security mechanisms

Services and Mechanisms

Security Services

Figure shows the taxonomy of the five common services.



Services and Mechanisms

Security Services

1.Data Confidentiality

Data Confidentiality deals with protecting against the disclosure of information by ensuring that the data is limited to those authorized user.

Represent the data in such a way that its semantics remain accessible only to those who possess some critical information.

Services and Mechanisms

Security Services

2.Data Integrity

Data integrity is a technique when sent message is delivered to receiver as the same.

Services and Mechanisms

Security Services

3.Authentication

- Authentication is the act of validating that users are whom they claim to be.
- Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.
- Passwords, One-time pins, Biometrics

Example :

- Logging into your computer system at the office
- Checking your account balance on your bank website

Services and Mechanisms

Security Services

4. Nonrepudiation

Non-repudiation is the assurance that someone cannot deny the validity of something.

Services and Mechanisms

Security Services

5. Access control

Access control is a security technique that regulates who or what can view or use resources in a computing environment.

Example:

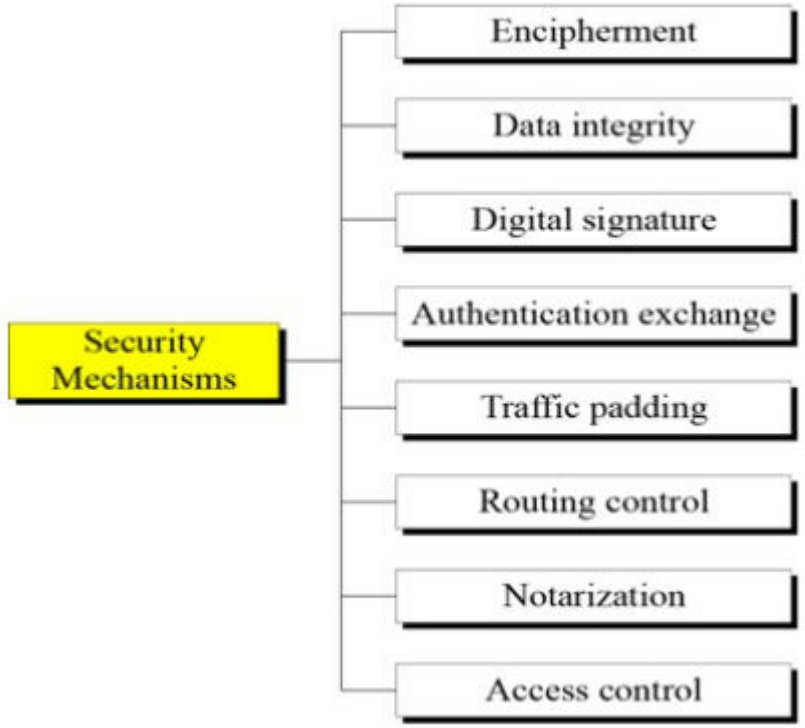
Banking Manager will have more privilege to access resource than others

Services and Mechanisms

Security Mechanisms

ITU-T(X.800) Standard recommends security mechanisms to provide security services.

Figure shows the taxonomy of these mechanisms.



Services and Mechanisms

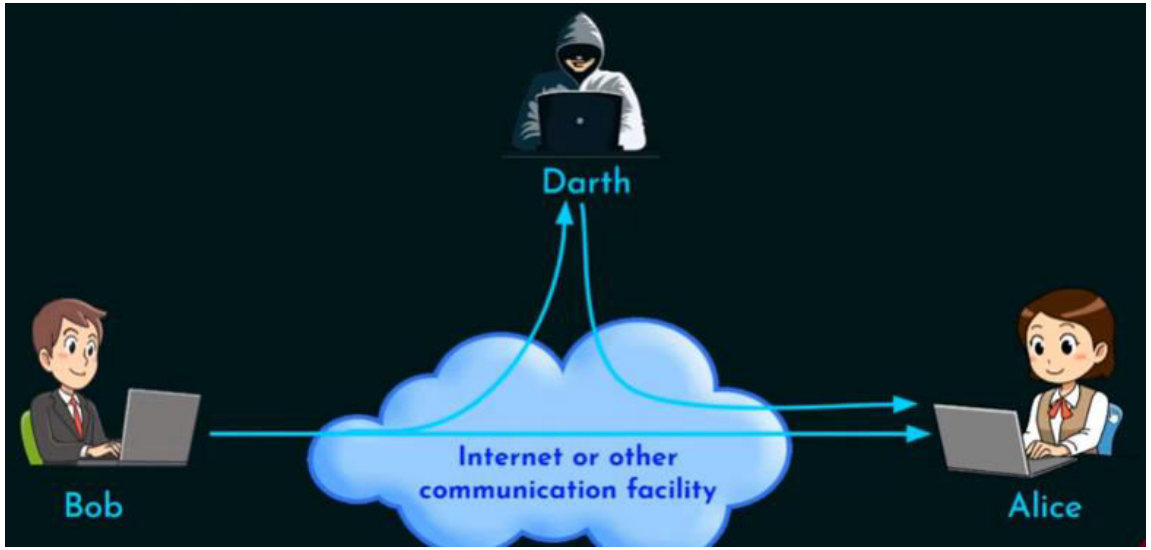
Security Mechanisms

1. **Encipherment** – Hiding or covering data can provide confidentiality. 2 techniques are Cryptography and Steganography
2. **Data Integrity** – Data integrity mechanism appends to the data a short check value that has been created by a specific process from the data itself.
3. **Digital Signature** – Sender can electronically sign the data and the receiver can electronically verify the signature.
4. **Authentication exchange –** Two entities exchange some message to prove their identity to each other.

Services and Mechanisms

Security Mechanisms

5.Traffic Padding – Inserting some bogus data into the traffic to thwart the adversary's attempt to use the traffic analysis.



Services and Mechanisms

Security Mechanisms

6.Routing control – Selecting and continuously changing different available routes between the sender and receiver to prevent the opponent from evaesdropping on a particular route.

7.Notarization – Selecting a third party to control the communication between two entities.

8.Access control – Uses method to prove that a user has access right to the data or resources owned by a system**.**

Services and Mechanisms

Relation between Services and Mechanisms

Relation between security services and mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Techniques

The actual implementation of security goals needs some help from mathematics.

Two techniques are prevalent today:

1. Cryptography
2. Steganography

Techniques

Cryptography

Cryptography is a word with Greek origins, means "**secret writing**"

- Symmetric key Encipherment
- Asymmetric key Encipherment
- Hashing

Techniques

- Plaint text - original message
- Cipher text - encrypted or coded message
- Cryptographic algorithm(cipher) is a mathematical function which uses plaintext as the input and produces ciphertext as the output and vice versa.
- Encryption - convert from plaintext to ciphertext (enciphering)
- Decryption - restore the plaintext from ciphertext (deciphering)

Techniques

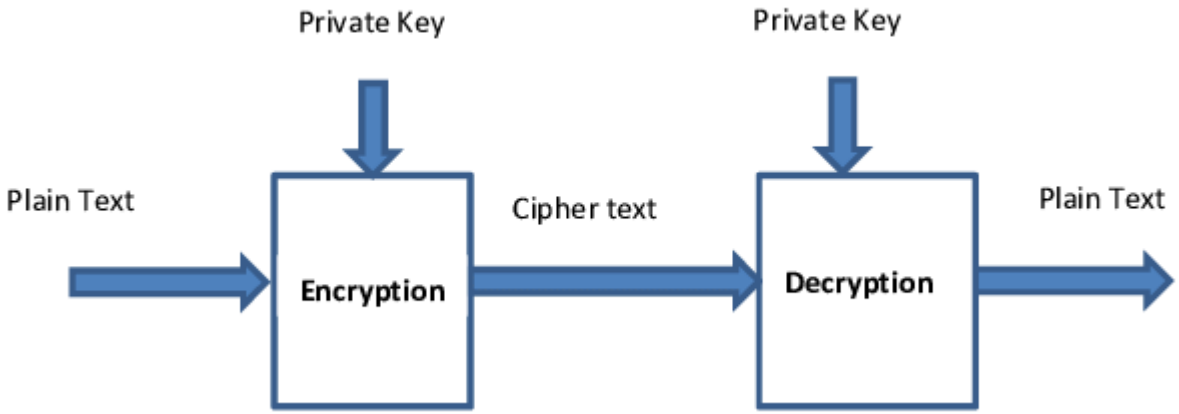
- Key - is a string of characters used within an encryption algorithm for altering data so that it appears random.
- The length of a key is normally expressed in bits.
- A longer key makes it more difficult to crack the encrypted data; however, a longer key results in longer time periods to perform encryption and decryption processes.

Techniques

Secret key : is a piece of information that is used to decrypt and encrypt messages.

Private key : (secret key) is used for encryption and decryption.

In this key is symmetric because the only key is copy or share by another party to decrypt the cipher text.

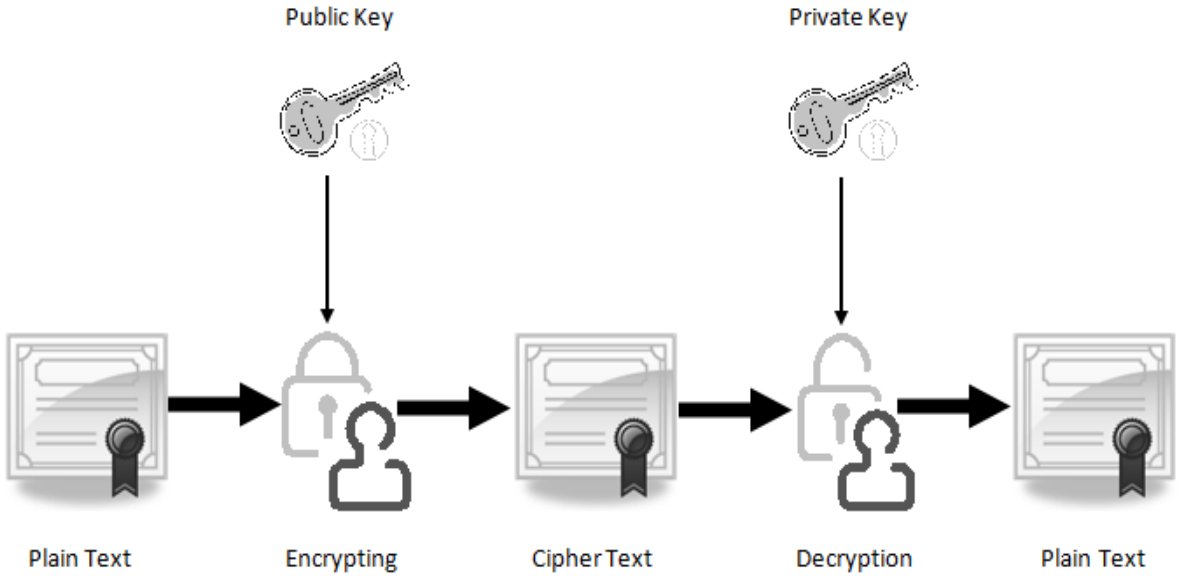


Techniques

Public key :

Two keys are used

One key is used for encryption



And another key is used for decryption.

One key (public key) is used for encrypt the plain text to convert it into cipher text and another key (private key) is used by receiver to decrypt the cipher text to read the message.

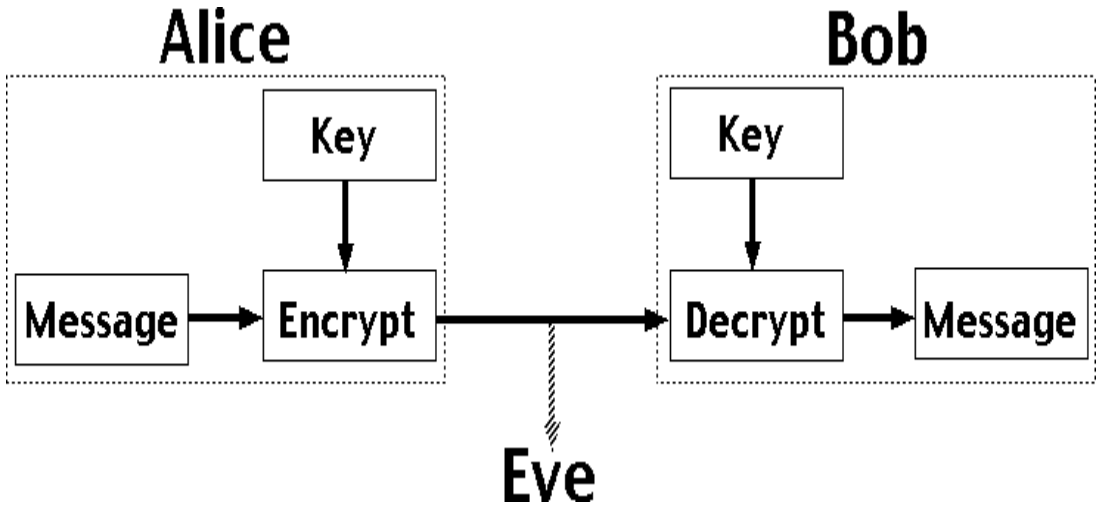
Techniques

- Symmetric key Encipherment

  Alice send a message to Bob ,over an insecure channel with the assumption that an adversary, say Eve, cannot understand the contents of the message by simply eavesdropping over the channel.

  Alice encrypts the message using an encryption algorithm.

  Bob decrypts the message using a decryption algorithm.



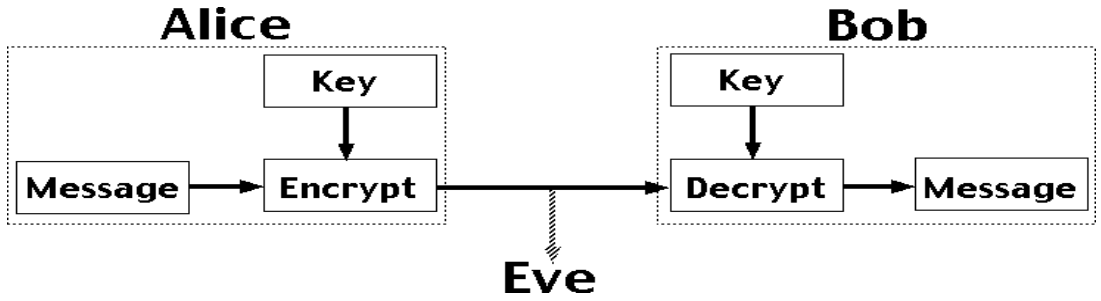
Techniques

- Symmetric key Encipherment

  Symmetric-key encipherment uses a single secret key for both encryption and decryption.

  In symmetric-key enciphering, Alice puts the message in a box and locks the box using the shared secret key.

  Bob unlocks the box with the same key and takes out the messages.



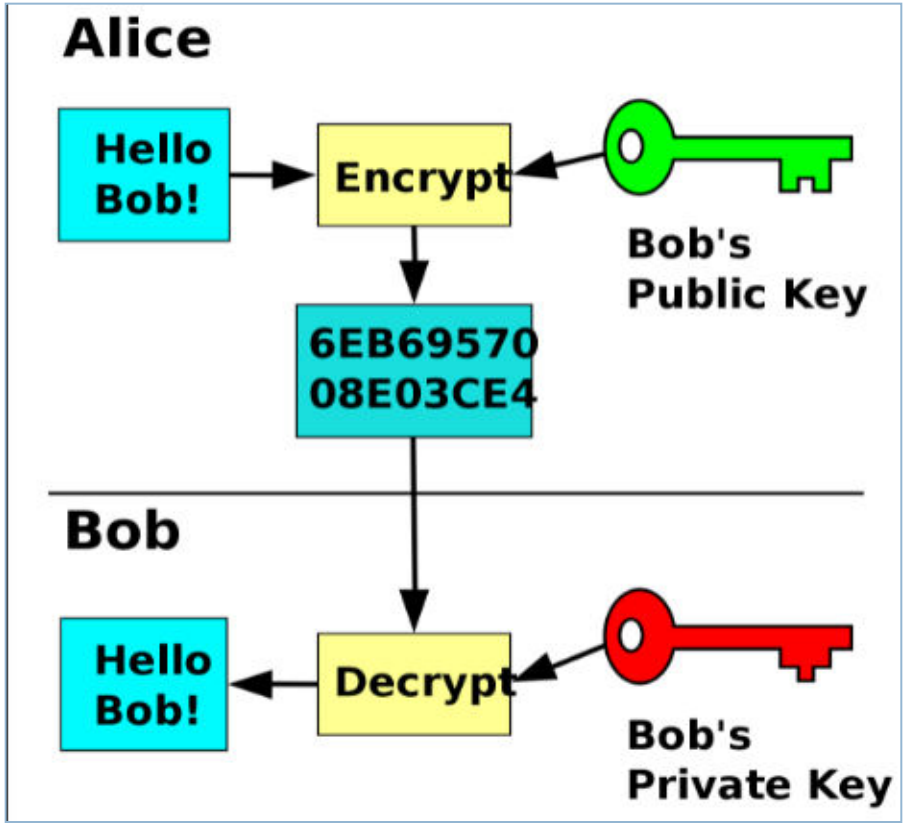
Techniques

Asymmetric key Encipherment

Two keys are used public key and private key.

To send a secure message to Bob, Alice firsts encrypts the message using Bob's public key.

To decrypts the message, Bob uses his own private key



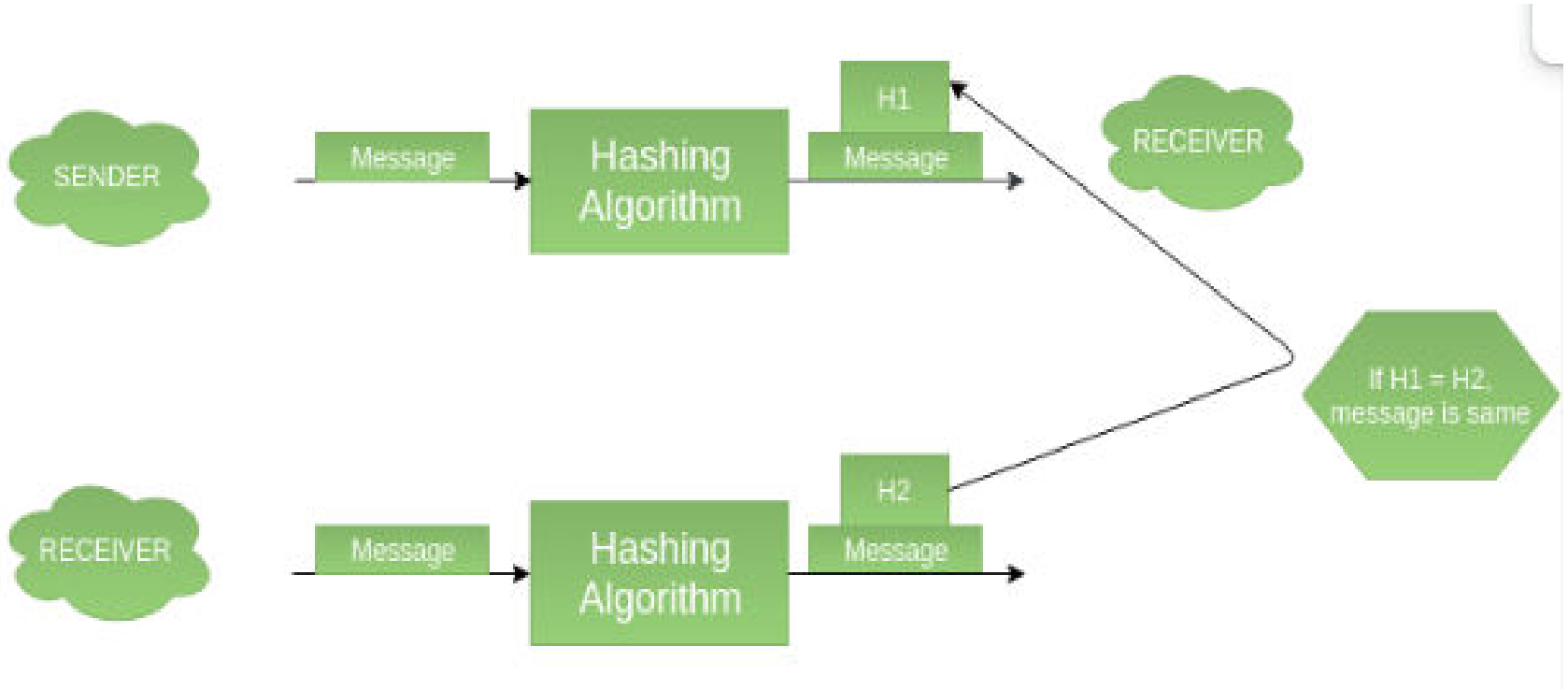
Techniques

Hashing

- A fixed-length message digest is created out of a variable- length message.
- The digest is normally much smaller than the message.
- Hashing is used to provide check values, provides data integrity.

Techniques

Hashing



Techniques

Steganography

The main idea behind steganography is to hide the existence of data in any medium like audio, video, image, etc.

Steganography in Greek means “covered writing”

- Historical use
- Modern use
  - Text cover
  - Image cover

Techniques

Steganography - Historical use

- China war – Messages were written on thin pieces of silk and rolled into a small ball and swallowed by the messenger.
- Rome and Greece – Messages were carved on pieces of wood, that were dipped into wax to cover the writing.

Techniques

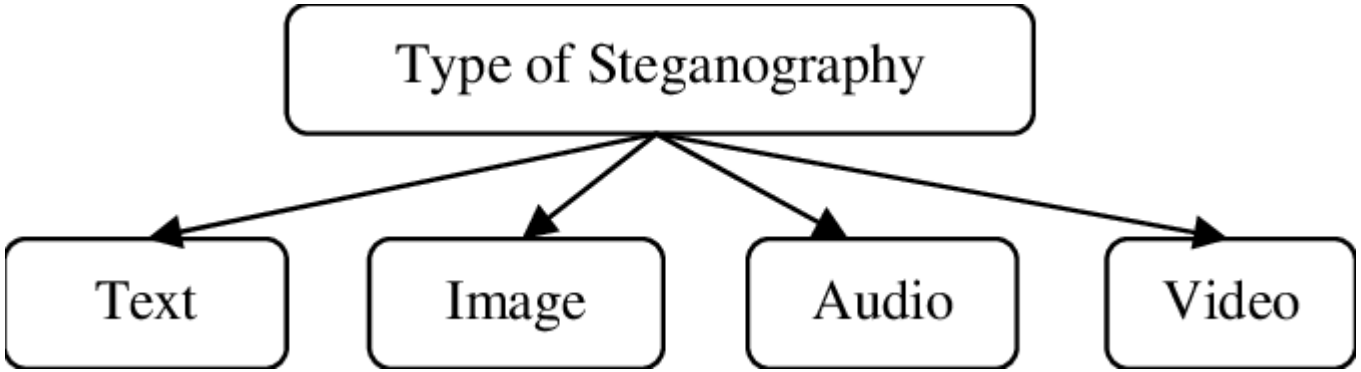
Steganography - Historical use

- Invisible inks(Onion juice/Ammonia salts) used to write secret messages, when heated with another substance, secret message are exposed.
- Some letters in an innocuous message might be overwritten in a pencil lead that is visible when exposed to light at an angle.

Techniques

Steganography – Modern use

Different forms of data can be digitized



Techniques

Steganography – Modern use – Text cover

- The cover of secret data can be text.
- Several ways to insert binary data into an text
- Example : single space – 0

  double space - 1

Techniques

Steganography – Modern use – Text cover

- The cover of secret data can be text.
- Several ways to insert binary data into an text
- Example : single space – 0

  double space - 1

Techniques

Steganography – Modern use – Text cover

- The cover of secret data can be text.
- Several ways to insert binary data into an text
- Example 1: single space – 0

  double space – 1

Message: 'A', convert to ASCII = 65

8-bit message: 0100 0001

This book is mostly about cryptography, not steganography.

□ □□□ □ □ □ □□

0 1 0 0 0 0 1

Techniques

Steganography – Modern use – Text cover

Example 2:

Use dictionary of words organized according to their grammatical usages.

- Consider a Dictionary contains 2 articles ,8 verbs , 32 nouns, 4 prepositions
- Use sentences with pattern article-noun-verb-article-noun

Techniques

Steganography – Modern use – Text cover

Example 2:

Secret data = Hi ➔ 01001000 01001001

- **Secret binary data is divided into 16-bit chunks.**
- **First bit of binary data can be represented for an article**

  0 – a

  1 – the

- **Next 5 bits can be represented by a noun**
- **Next 4 bits can be represented by a verb**
- **next bit by the second article**
- **last 5 bits by another noun**

article	noun	verb	article	noun
A	friend	called	a	doctor.
0	10010	0001	0	01001

Techniques

Steganography – Modern use – Image cover

- Secret data can also be covered under a color image.
- Image made of pixels(24 bits – 3 bytes) (red,green,blue)

Techniques

Steganography – Modern use – Image cover

- LSB(least significant bit)

  To hide binary data in image, keep or change least significant bit

  If binary data is 0 , keep the bit

  If binary data is 1, change the bit to 1

Secret data = M

01010011	10111100	01010101
01011110	10111100	01100101
01111110	01001010	00010101

Techniques

Steganography – Modern use – Image cover

- LSB(least significant bit)

50	90	75
125	200	5
25	95	180

Convert pixel value to 8-bit:

50	: 0001 1010
90	: 0101 1010
75	: 0101 0011
125	: 0111 1101
200	: 1100 1000
5	: 0000 0101
25	: 0001 1001
95	: 0101 1111
180	: 1011 0100

Message: 'A', convert to ASCII = 65

8-bit message: 0100 0001

Embed bit message to cover:

50	: 0001 101**0**
90	: 0101 101**1**
75	: 0101 001**0**
125	: 0111 110**0**
200	: 1100 100**0**
5	: 0000 010**0**
25	: 0001 100**0**
95	: 0101 111**1**
180	: 1011 0100

50	**91**	75
124	200	**4**
24	95	180

Techniques

Steganography – Modern use – Other cover

- Secret data can also be covered using audio and video

Integer Arithmetic

- In integer arithmetic, we use a set and a few operations.
- Are use to create a background for modular arithmetic.
  a. Set of Integers
  b. Binary Operations
  c. Integer Division
  d. Divisibility

Integer Arithmetic

Set of Integers

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

The set of integers

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

Integer Arithmetic

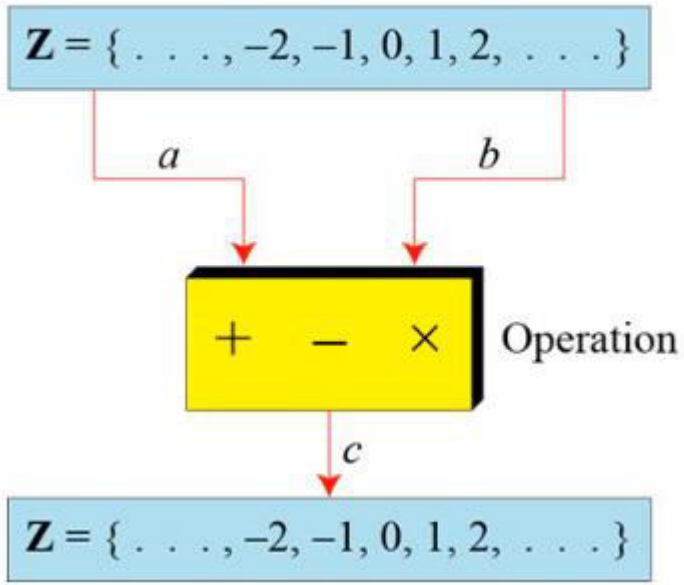
Binary Operations

In cryptography, three binary operations applied to the set of integers.

A binary operation takes two inputs and creates one output.

Figure shows three binary operations for the set of integers

Three binary operations for the set of integers



Integer Arithmetic

Binary Operations

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 Arithmetic

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

a is dividend

q is quotient

n is divisor

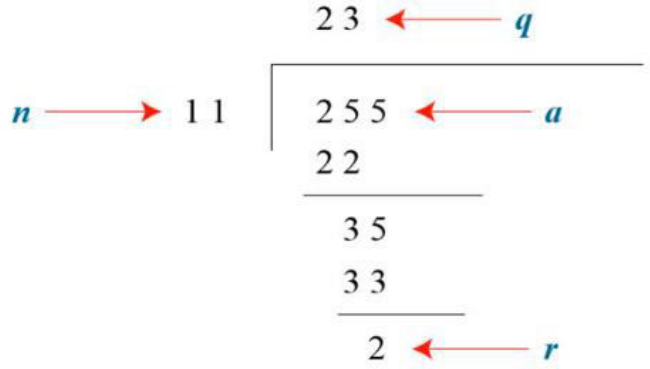
r is remainder

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

Operator / for quotient and % for Remainder

Example finding the quotient and the remainder

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



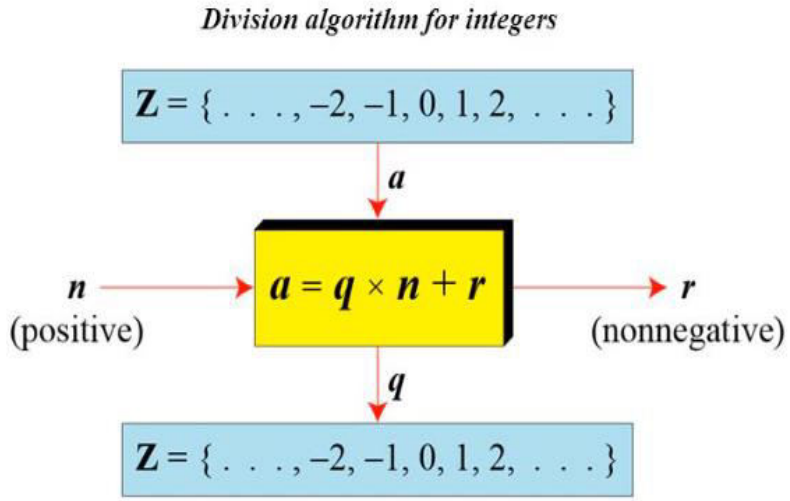
RAMAIAH Institute of Technology

Integer Arithmetic

Integer Division

To perform division in cryptography, we impose 2 restrictions

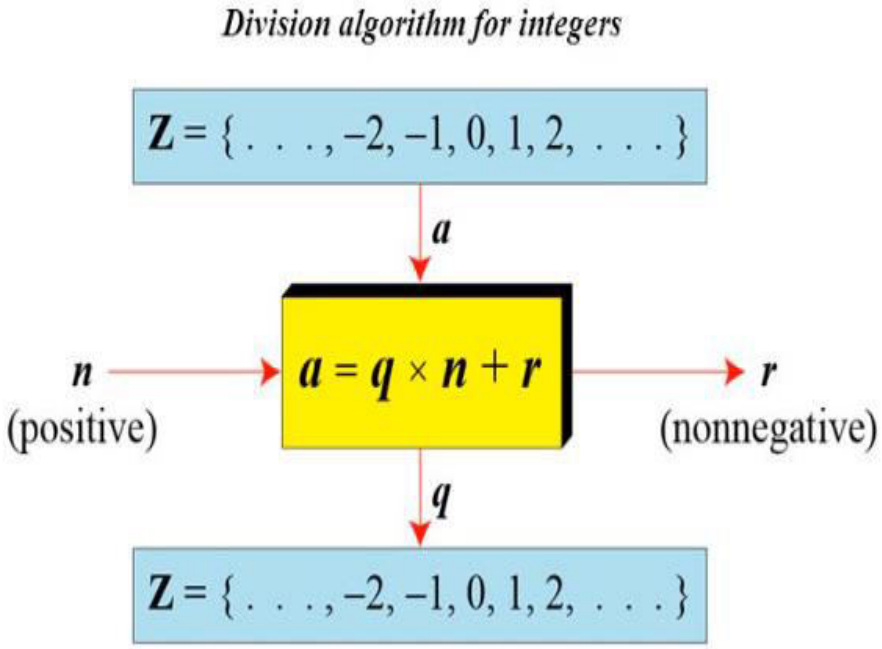
1. Require n should be a positive integer (n>0)
2. Require r remainder should be a nonnegative integer(r≥ 0)



Integer Arithmetic

Integer Division

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.



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

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

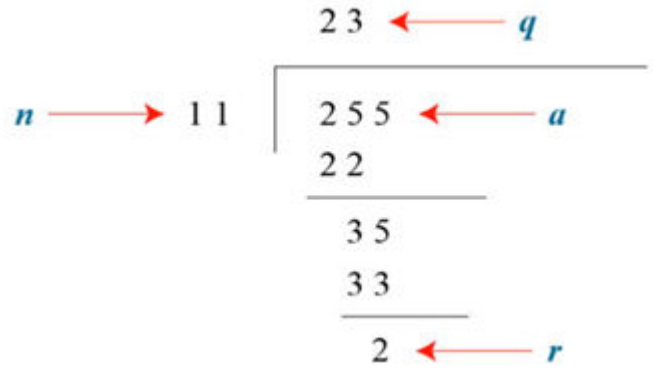
Divisbility

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

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

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

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



Property 1: if $a|1$, then $a = \pm 1$.

Property 2: if $a|b$ and $b|a$, then $a = \pm b$.

Property 3: if $a|b$ and $b|c$, then $a|c$.

Property 4: if $a|b$ and $a|c$, then
$a|(m \times b + n \times c)$,
where m and n are arbitrary integers

Note

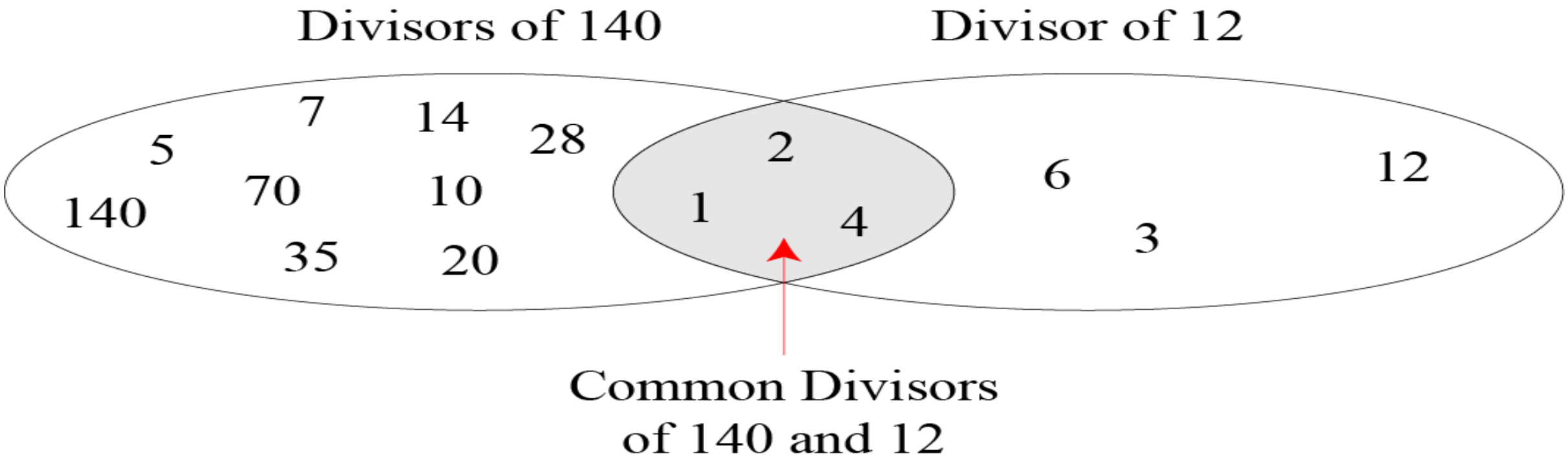
Fact 1: The integer 1 has only one divisor, itself.

Fact 2: Any positive integer has at least two divisors, 1 and itself (but it can have more).

Greatest Common Divisor

The greatest common divisor of two positive integers is the largest integer that can divide both integers.

Common divisors of two integers



Euclidean Algorithm

- Finding GCD of two positive integer by listing all common divisor is not easy when two integer are large.
- **Mathematician Euclid** developed algorithm to find gcd of 2 positive integer
- It is based on two facts

Fact 1: gcd (a, 0) = a
Fact 2: gcd (a, b) = gcd (b, r)
where r is the remainder of dividing a by b

GCD(36,10)

GCD(10,6)

GCD(6,4)

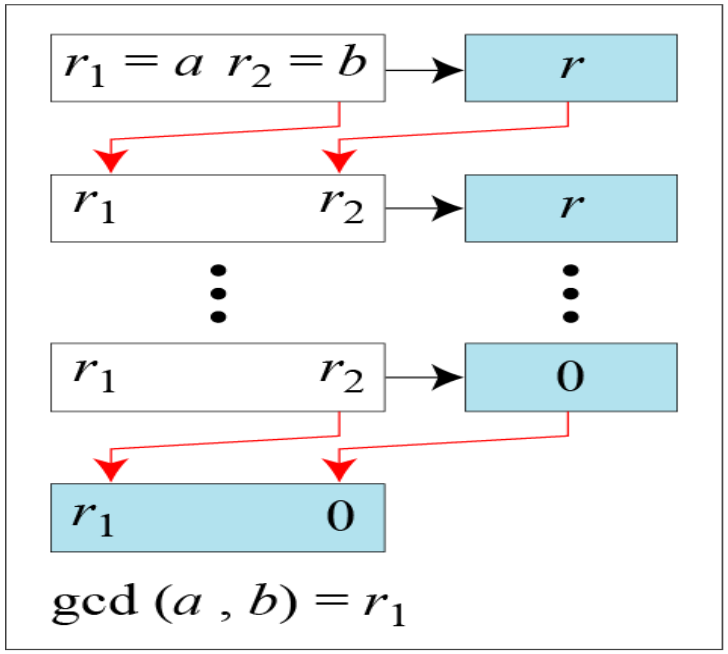
GCD(4,2)

GCD(2,0) = 2

```
10)36(3
   30
 ---------
   6 ) 10 (1
       6
   --------
     4) 6 ( 1
        4
     --------
       2 ) 4 (2
           4
       -------
           0
```

The second fact allow to change value of a and b , until b becomes 0, GCD(36,10) = 2

Euclidean Algorithm



a. Process

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$

}

gcd $(a, b) \leftarrow r_1$

b. Algorithm

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

Note

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

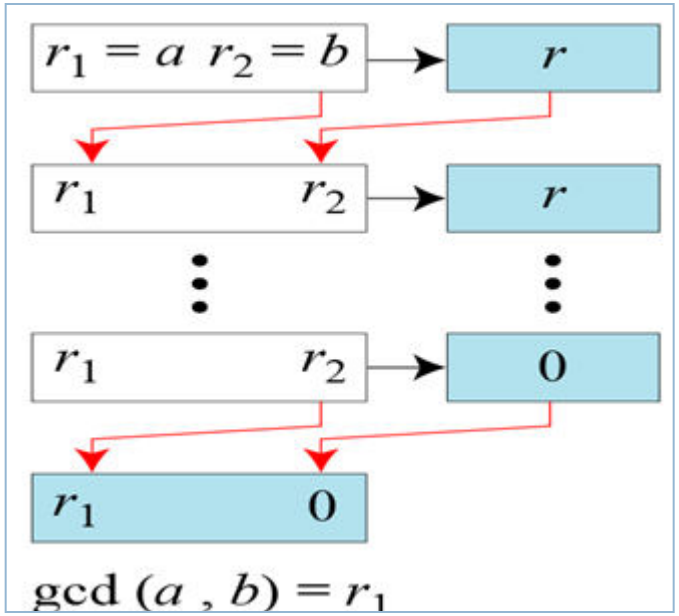
Find the greatest common divisor of 2740 and 1760.

Solution

We have gcd (2740, 1760) = 20.

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

$r_1 \leftarrow a; \quad r_2 \leftarrow b;$
while $(r_2 > 0)$
{
$q \leftarrow r_1 / r_2;$
$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$
}
gcd $(a, b) \leftarrow r_1$



q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

```
1760)2740( 1
      1760
      ---------
       980 ) 1760 (1
              980
              --------
               780) 980 ( 1
                     780
                     --------
                      200 ) 780 (3
                             600
                             -------
                              180 )200 (1
                                    180
                                    ----------
                                     20)180(9
                                          180
                                          -----
                                            0
```

```
r1 ← a;      r2 ← b;
while (r2 > 0)
  {
   q ← r1 / r2;
   r  ← r1 – q × r2;
   r1 ← r2 ;  r2 ← r ;
  }
gcd (a, b) ← r1
```

Find the greatest common divisor of 25 and 60.

$r_1 \leftarrow a; \quad r_2 \leftarrow b;$

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

}

gcd $(a, b) \leftarrow r_1$

Find the greatest common divisor of 25 and 60.

Solution

We have 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	

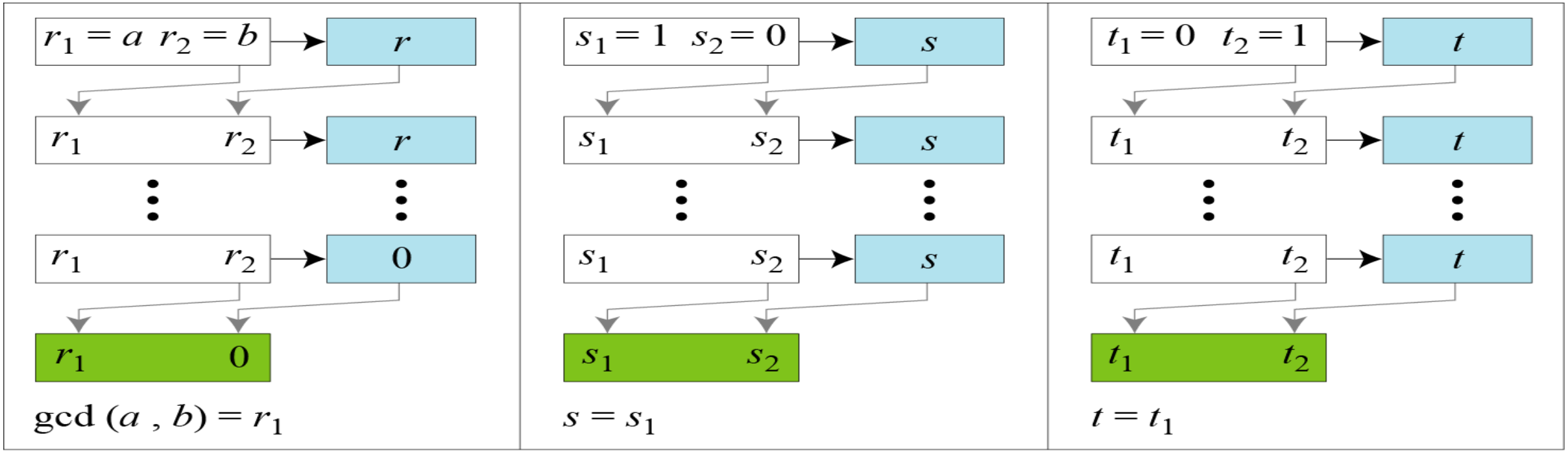
Extended Euclidean Algorithm

Given two integers a and b, we often need to find other two integers, s and t, such that

$$s \times a + t \times b = \gcd(a, b)$$

The extended Euclidean algorithm can calculate the gcd (a, b) and at the same time calculate the value of s and t.

Extended Euclidean algorithm, part a



a. Process

Extended Euclidean algorithm

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

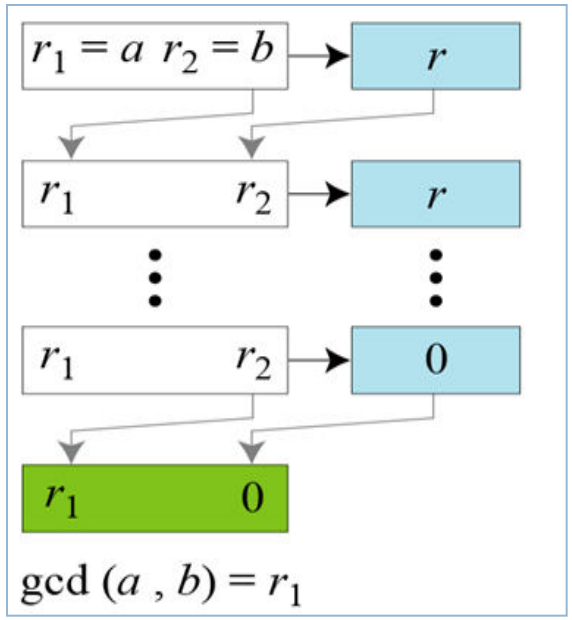
$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

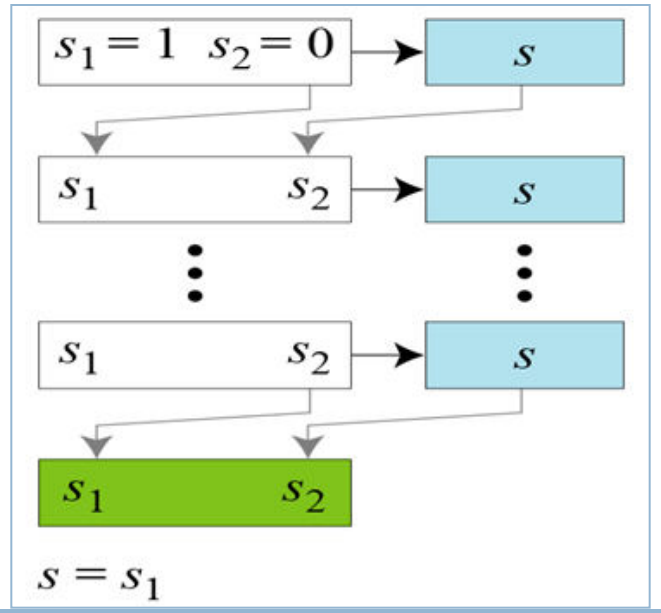
$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

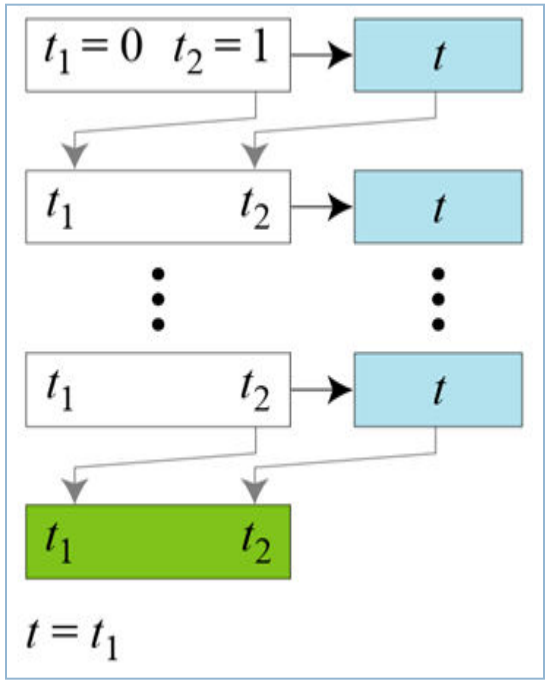
$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}

gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$







RAMAIAH
Institute of Technology

Given a = 161 and b = 28, find gcd (a, b) and the values of s and t.

Solution

We get gcd (161, 28) = 7, s = −1 and t = 6.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}

gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

$$s \times a + t \times b = \gcd(a, b)$$

-1 X 161 + 6 X 28 = 7

Given a = 17 and b = 0, find gcd (a, b) and the values of s and t.

Solution

We get gcd (17, 0) = 17, s = 1, and t = 0.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
	17	0		**1**	**0**		**0**	**1**	

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}

gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

Given a = 0 and b = 45, find gcd (a, b) and the values of s and t.

Solution

We get gcd (0, 45) = 45, s = 0, and t = 1.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
0	0	45	0	1	0	1	0	1	0
	45	0		0	1		**1**	0	

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$ (Initialization)

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}

gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

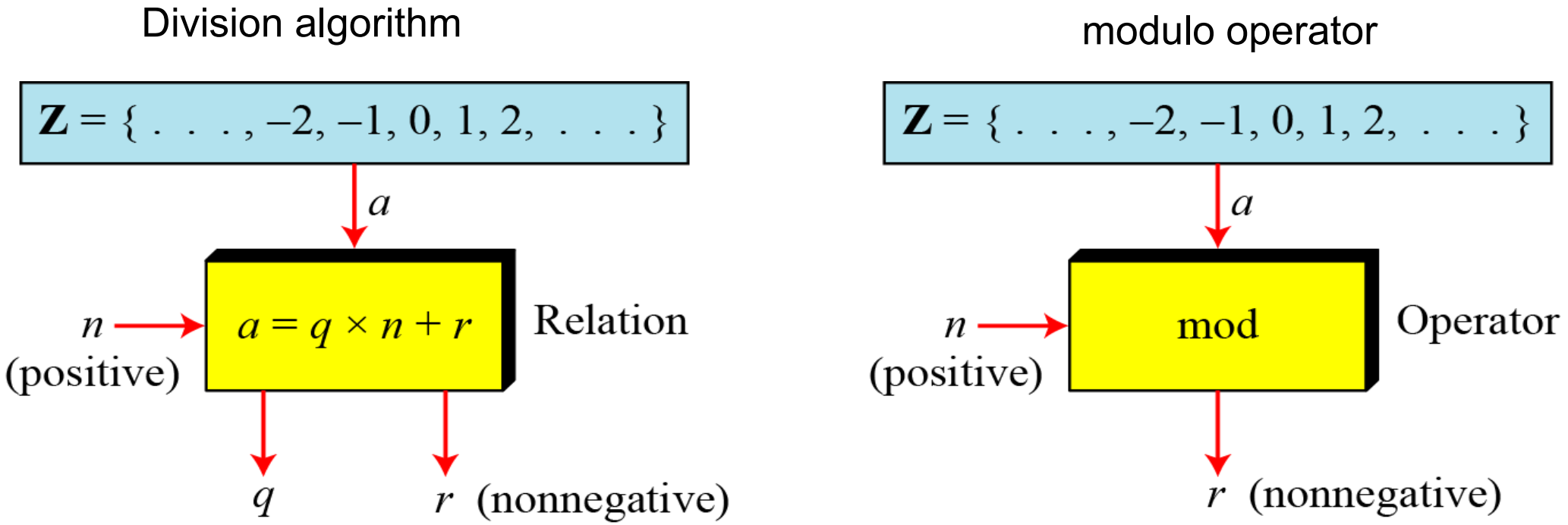
MODULAR ARITHMETIC

The division relationship ($a = q \times n + r$) discussed in the previous section has two inputs (a and n) and two outputs (q and r).

In modular arithmetic, we are interested in only one of the outputs, the remainder r.

Modulo Operator

The modulo operator is shown as mod. The second input (n) is called the modulus. The output r is called the residue.



Congruence

- In cryptography, we often use the concept of congruence instead of equality.
- To show that two integers are congruent, we use the congruence operator (≡).
- We add the phrase (mod n) to the right side of the congruence to define the value of modulus that makes the relationship valid.

For example

$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

Set of Residues

The result of the modulo operation with modulus n is always an integer between 0 and n-1.

The modulo operation creates a set, which in modular arithmetic is referred to as **the set of least residues modulo n, or Z_n.**

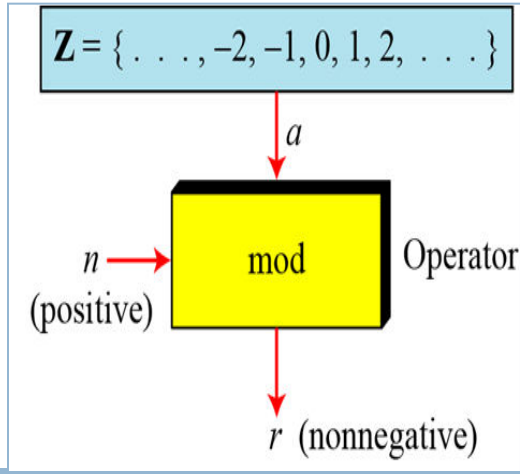
Some Z_n sets

$$\mathbf{Z}_n = \{ 0, 1, 2, 3, \ldots, (n-1) \}$$

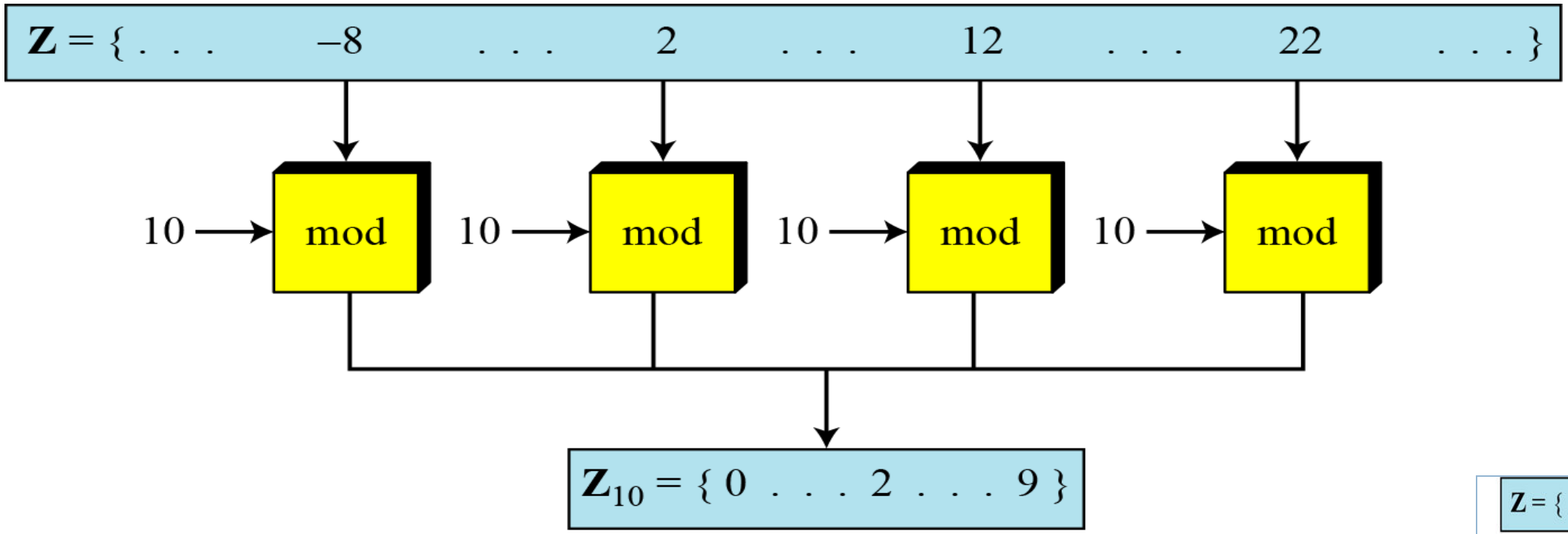
$$\mathbf{Z}_2 = \{ 0, 1 \}$$

$$\mathbf{Z}_6 = \{ 0, 1, 2, 3, 4, 5 \}$$

$$\mathbf{Z}_{11} = \{ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \}$$

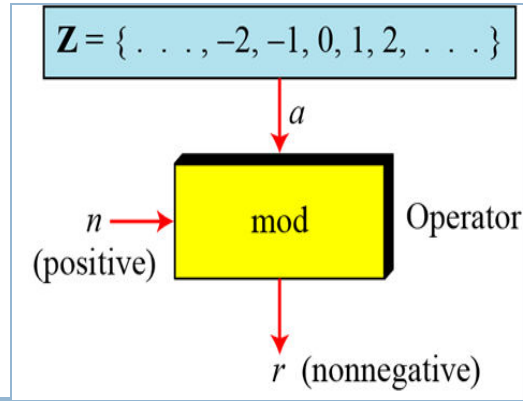


Concept of congruence



$$-8 \equiv 2 \equiv 12 \equiv 22 \pmod{10}$$

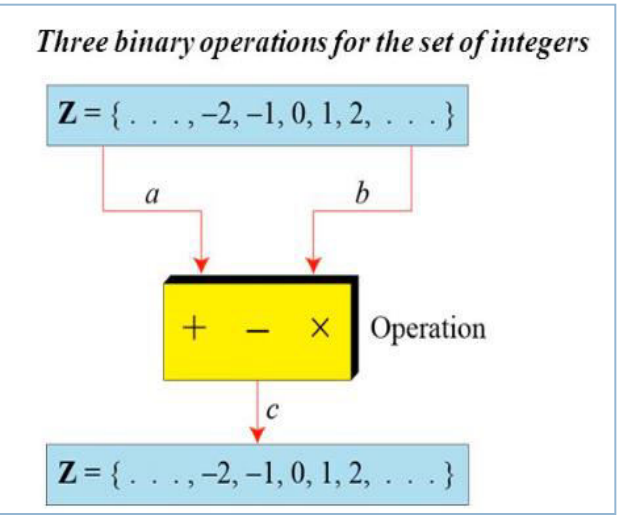
Congruence Relationship



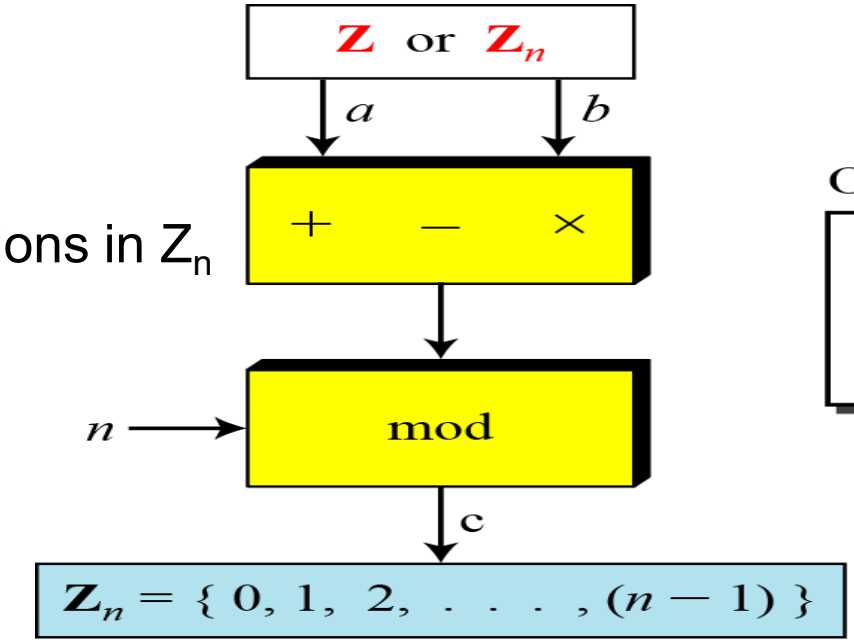
Operation in Z_n

The three binary operations that we discussed for the set Z can also be defined for the set Zn.

The result may need to be mapped to Zn using the mod operator.



Binary operations in Z_n



Operations

$(a + b) \bmod n = c$

$(a - b) \bmod n = c$

$(a \times b) \bmod n = c$

Perform the following operations (the inputs come from Z_n):

a. Add 7 to 14 in Z_{15}.
b. Subtract 11 from 7 in Z_{13}.
c. Multiply 11 by 7 in Z_{20}.

Solution

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

Perform the following operations (the inputs come from either Z or Z_n):

a. Add 17 to 27 in Z_{14}.
b. Subtract 43 from 12 in Z_{13}.
c. Multiply 123 by −10 in Z_{19}.

Solution

$$(17 + 27) \bmod 14 \rightarrow (44) \bmod 14 = 2$$
$$(12 - 43) \bmod 13 \rightarrow (-31) \bmod 13 = 8$$
$$(123 \times (-10)) \bmod 19 \rightarrow (-1230) \bmod 19 = 5$$

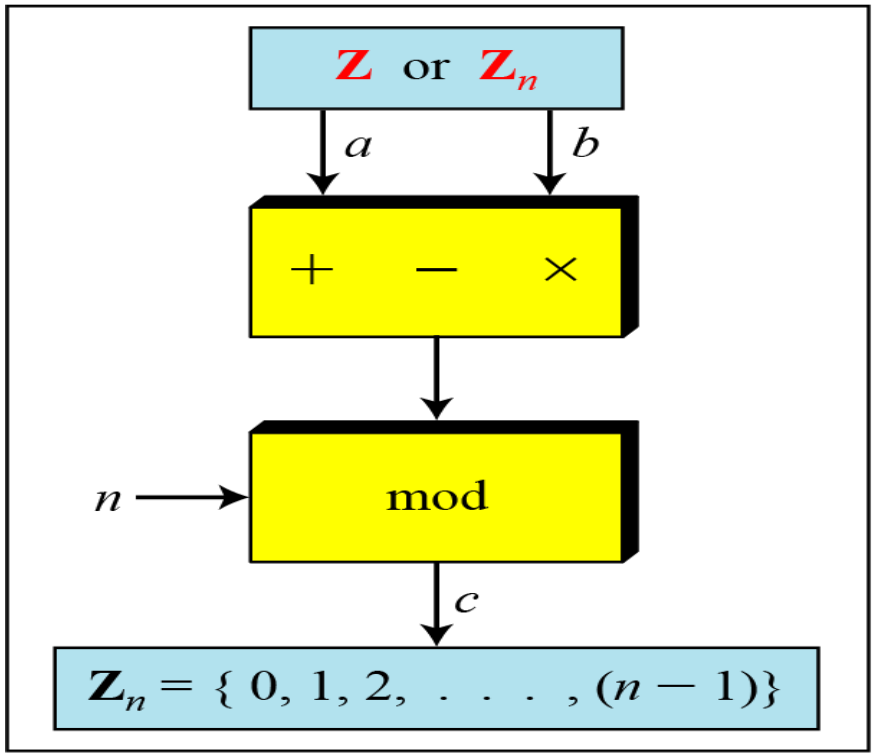
First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Properties of mode operator

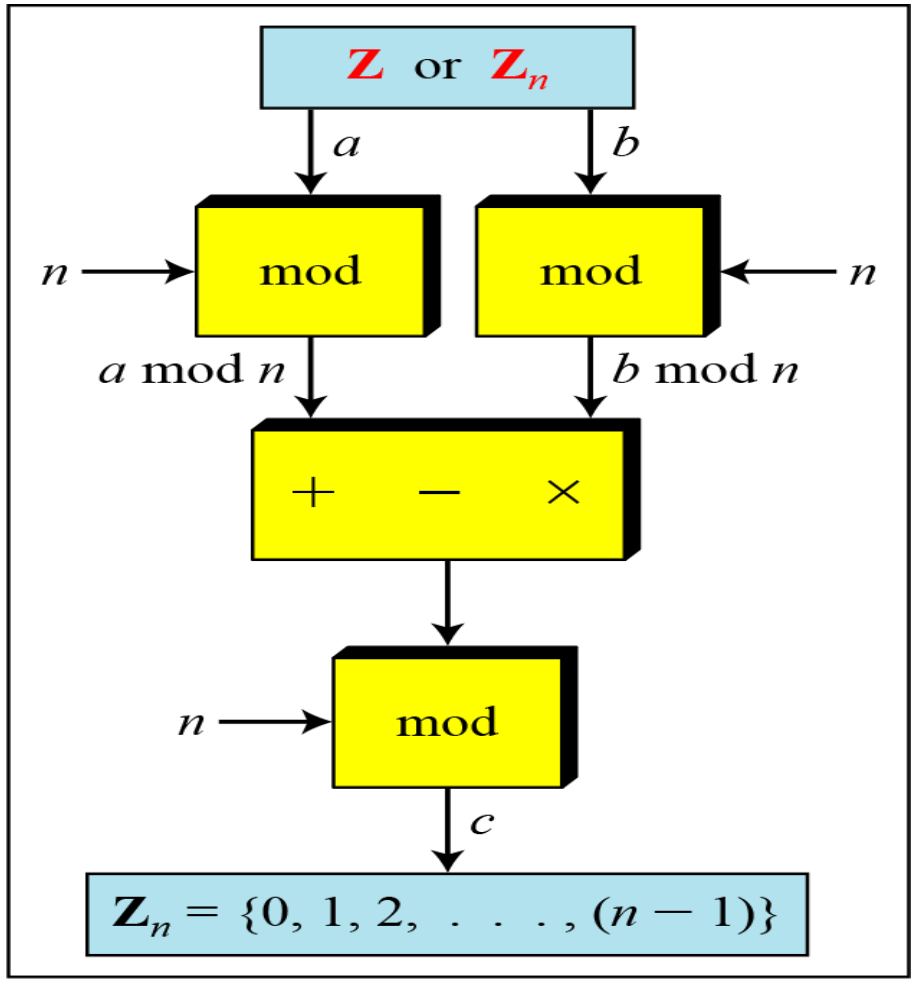
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$



a. Original process



b. Applying properties

Inverses

When we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation.

We are normally looking for an
•additive inverse (relative to an addition operation) or
•multiplicative inverse (relative to a multiplication operation).

Additive Inverse

In Z_n, two numbers a and b are additive inverses of each other if

$$a + b \equiv 0 \pmod{n}$$

Note

In Z_n , additive inverse a can be calculated as b=n-a

Find the additive inverse of 4 in Z_{10}.

Solution

The additive inverse of 4 in Z_{10} is 10 - 4 = 6

$$a + b \equiv 0 \pmod{n}$$

In Z_n , additive inverse a can be calculated as b= n - a

Multiplicative Inverse

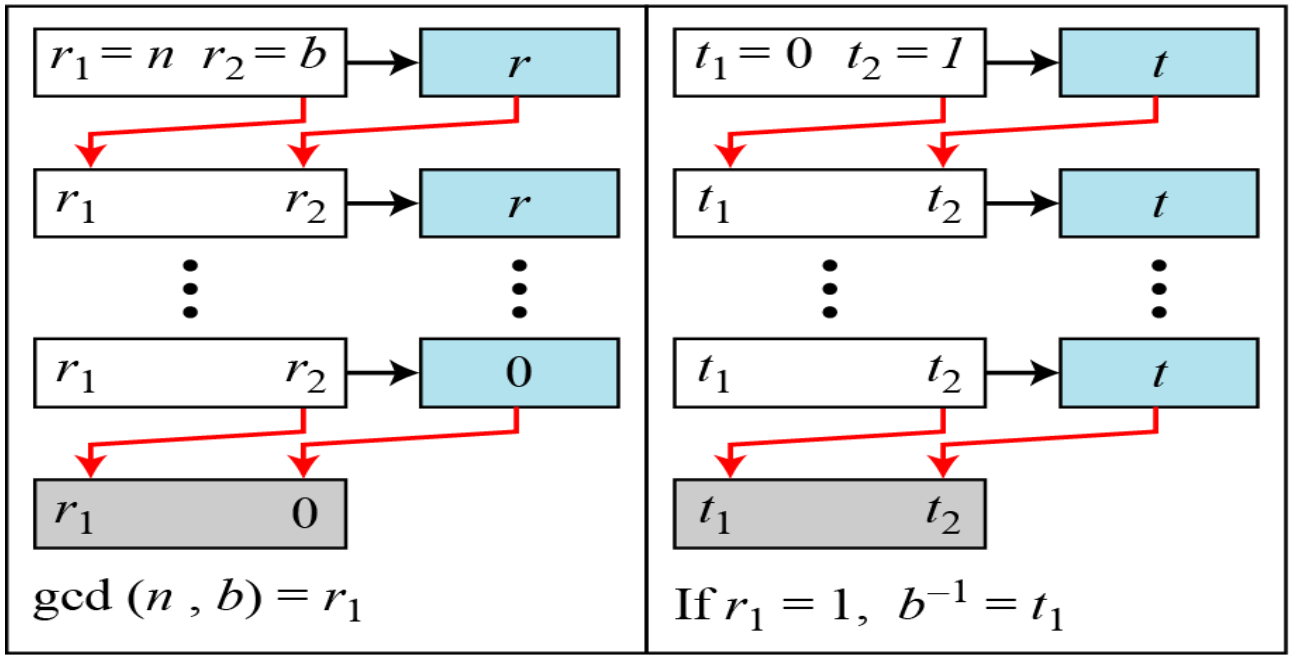
In Z_n, two numbers a and b are the multiplicative inverse of each other if

$$a \times b \equiv 1 \pmod{n}$$

Note

The integer a in Z_n has a multiplicative inverse if and only if **gcd(a , b) ≡ 1 (mod n)**

Using extended Euclidean algorithm to find multiplicative inverse of b in Z_n



a. Process

$r_1 \leftarrow n; \qquad r_2 \leftarrow b;$
$t_1 \leftarrow 0; \qquad t_2 \leftarrow 1;$

while $(r_2 > 0)$
{
$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2; \qquad r_2 \leftarrow r;$

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2; \qquad t_2 \leftarrow t;$

}
if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

b. Algorithm

Find the multiplicative inverse of 11 in Z_{26}.

Solution

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	–2
2	11	4	3	1	–2	5
1	4	3	1	–2	5	–7
3	3	1	0	5	–7	26
	1	0		–7	26	

$r_1 \leftarrow n; \quad r_2 \leftarrow b;$

$t_1 \leftarrow 0; \quad t_2 \leftarrow 1;$

while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2; \quad r_2 \leftarrow r;$

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2; \quad t_2 \leftarrow t;$

}

if $(r_1 = 1)$ then $b^{-1} \leftarrow t_1$

The gcd (26, 11) is 1; the inverse of 11 is –7 or -7mod 26 =19.

Find the multiplicative inverse of 23 in Z_{100}.

Solution

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	−4
2	23	8	7	1	−4	19
1	8	7	1	−4	9	−13
7	7	1	0	9	−13	100
	1	0		−13	100	

The gcd (100, 23) is 1; the inverse of 23 is −13 or 87.

Find the inverse of 12 in Z_{26}.

Solution

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	−2
6	12	2	0	1	−2	13
	2	0		−2	13	

The gcd (26, 12) is 2; the inverse does not exist.

THANK YOU