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 – CSE555

Credits - 3:0:0

UNIT -1

Term: Oct 2023 – Jan 2024

Prepared by: Dr. Sangeetha. V
Associate Professor

RAMAIAH Institute of Technology

Textbooks

1. **Behrouz A. Forouzan, DebdeepMukhopadhyay** - Cryptography and Network Security, Tata McGraw-Hill, 3rd Edition, 2015
2. **William Stallings** - Cryptography and Network Security, Pearson Education, 7th Edition, 2018

Reference Books:

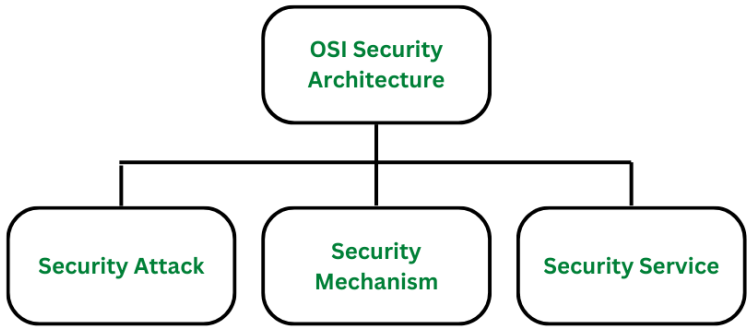
1. **Bernard Menezes**: Cryptography, Network Security and Cyber Laws , Cengage Learning, First edition, 2018.
2. **AtulKahate**: Cryptography and Network Security", 4th Edition, Tata McGraw Hill, 2019.
3. **William Stallings**: Network Security Essentials: Applications and Standards by, 6th edition, Pearson Education, 2018.

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:

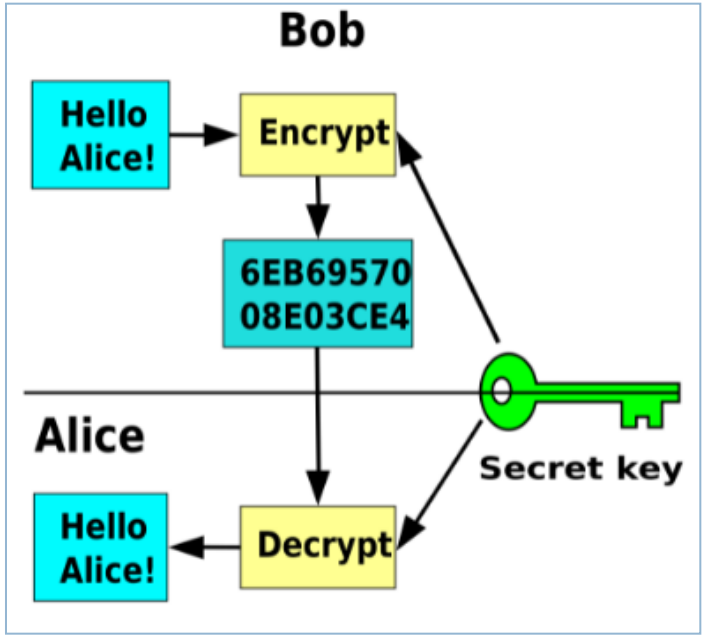
- Protect the Confidentiality of data
- Preserve the Integrity of data
- Promote the Availability of data for authorized use

Taxonomy of security goals

Security Goals

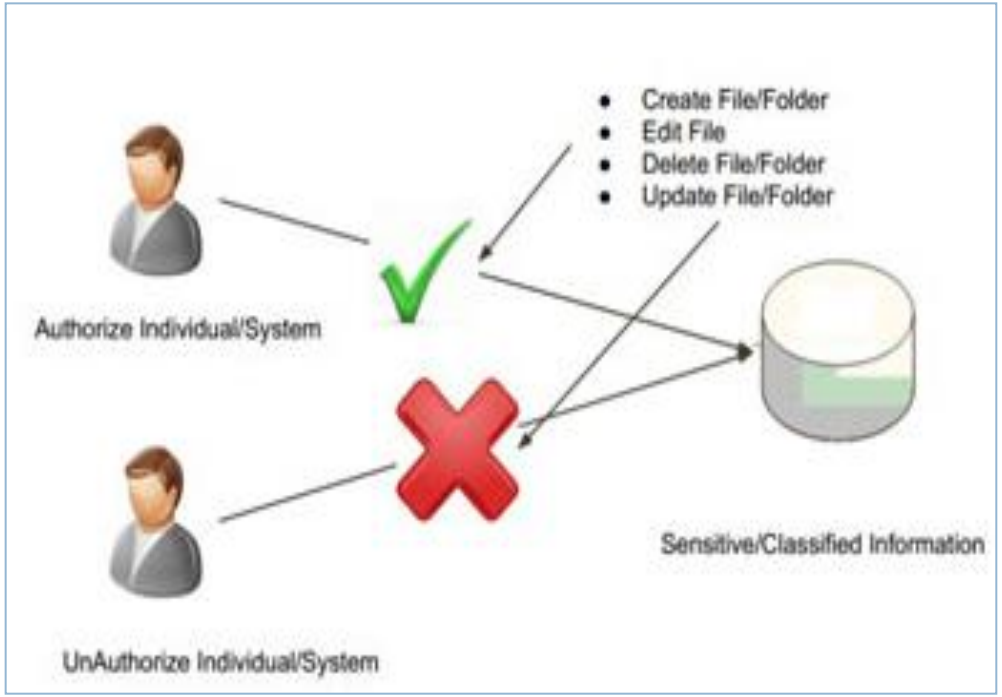
- **Confidentiality** is probably the most common aspect of information security. We need to protect confidential information.
- Confidentiality is the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.
- Confidentiality is concerned with preventing unauthorized access to sensitive information.
- Example : Banking, Military, Industry

Personal information of a person should be confidential



Security Goals

- Integrity means that data or information maintained in system is not modified or deleted by unauthorized parties.
- **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 by concerned staff only

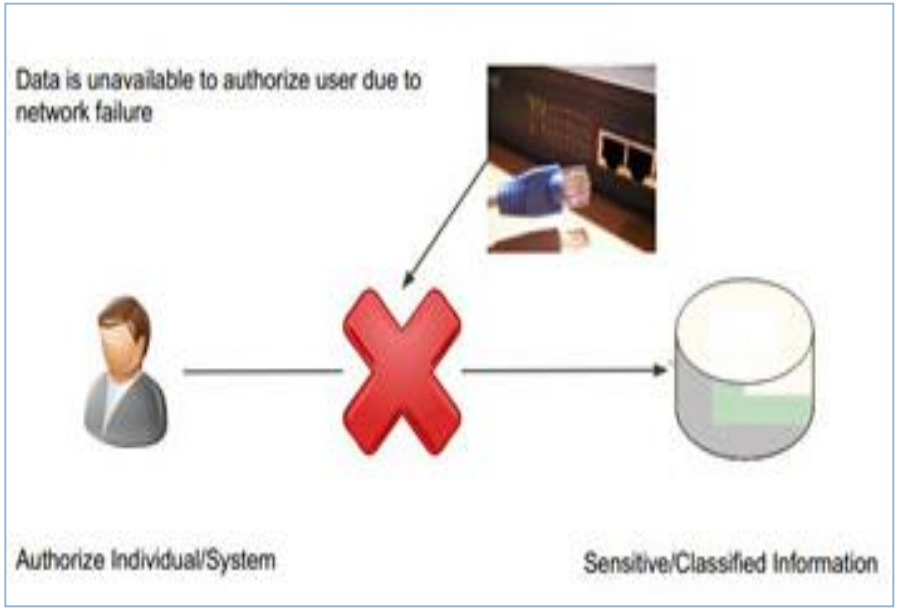


RAMAIAH
Institute of Technology

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.

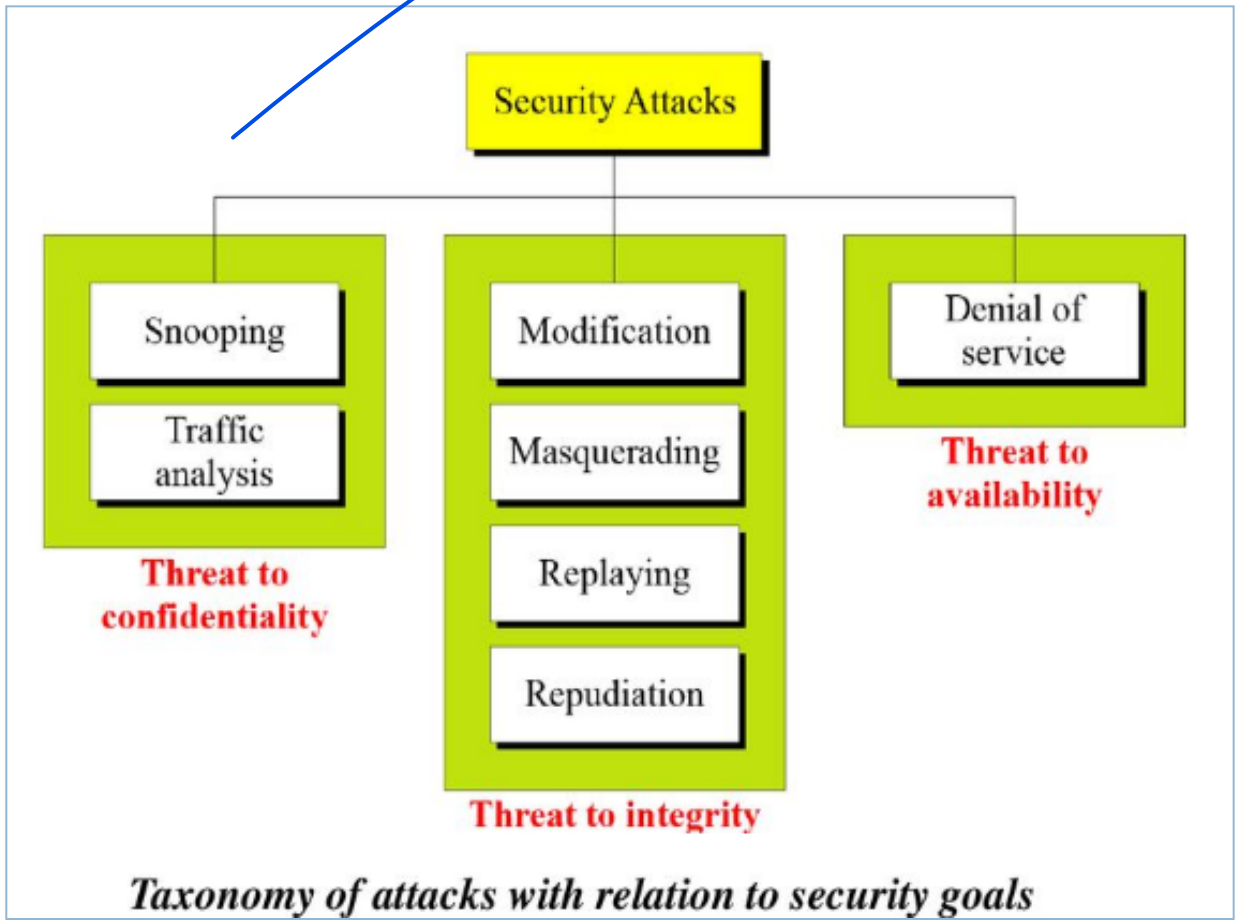
Example : Imagine what would happen to a bank if the customers could not access their accounts for transactions.



Attacks

- The three goals of security
  - Confidentiality
  - Integrity
  - 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

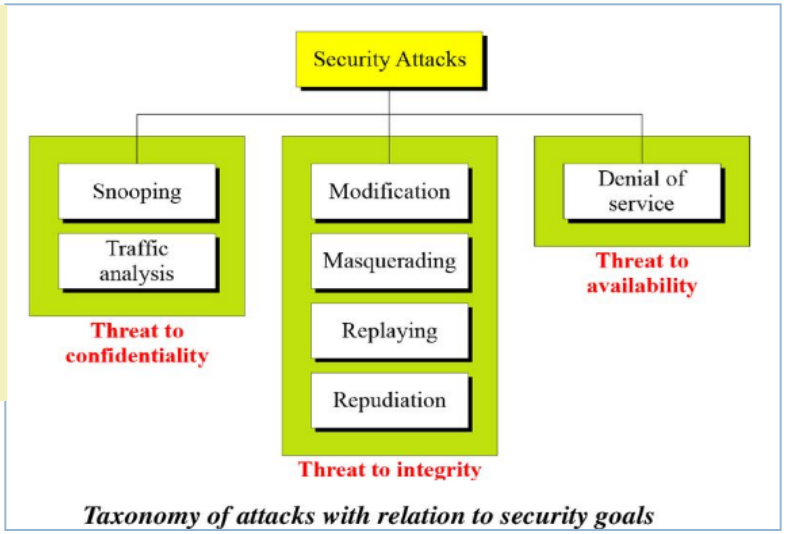
RAMAIAH Institute of Technology

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.

RAMAIAH
Institute of Technology

Attacks



Taxonomy of attacks with relation to security goals

Attacks Threatening Confidentiality

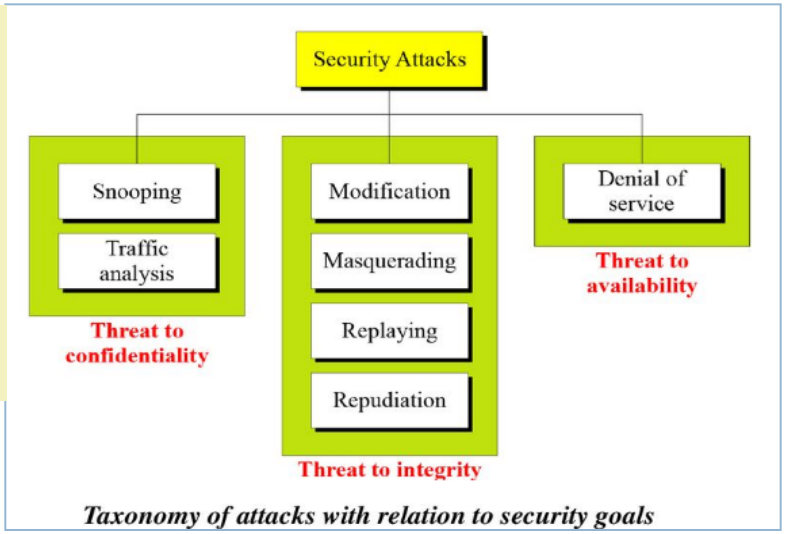
1. Snooping

Imagine a person standing by a window, secretly watching what others inside the house are doing without being noticed.

They gather information about the conversations and actions inside, without ever entering the house.

Snooping attack- the attacker monitors data traffic without directly interfering, gathering sensitive information, such as passwords, messages, or personal data.

Attacks



Taxonomy of attacks with relation to security goals

Attacks Threatening Confidentiality

1. **Snooping** is a technique in which attackers get unauthorized access to another person's data or company's data.

Snooping uses software programs to remotely monitor activity on a computer/network device.

Snooping leads to loss of privacy: password, financial data, private data

Example : Snoop server is used to capture network traffic for analysis, and the snooping protocol monitors information on a computer bus to ensure efficient processing.

Attacks

Attacks Threatening Confidentiality

2. Traffic analysis

Imagine you're outside an office building.

You can't hear the conversations inside, but by watching people enter and leave, noting the frequency of deliveries, and observing which departments are most active, you could deduce key events happening within the building, such as a major project or a meeting.

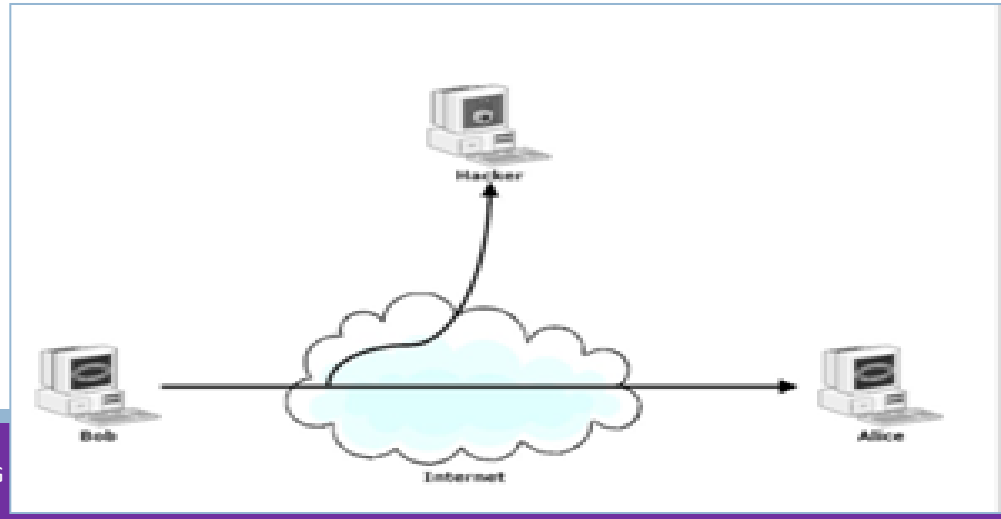
Attacks

Attacks Threatening Confidentiality

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

   Example : File transferred through internet

In this attack the eavesdropper analyzes the traffic, determine the location, identify communicating hosts, observes the frequency and length of message being exchanged. Using all these information they predict the nature of communication . All incoming and out going traffic of network is analyzed but not altered.



Attacks

Attacks Threatening Integrity

1. Modification

Imagine you write a letter and send it through the mail.

Along the way, someone intercepts the letter, changes some of the words or adds new information, then reseals the envelope and sends it on its way to the original recipient.

The person receiving the letter thinks it came directly from you, unaware that the message was altered.

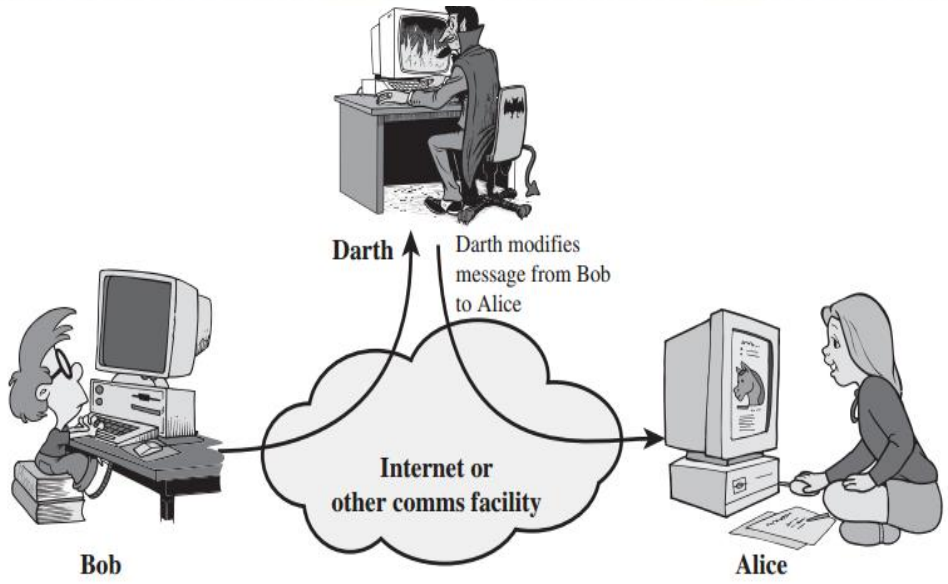
Attacks

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.

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.



Attacks

Attacks Threatening Integrity

2. Masquerading or spoofing

Imagine a person disguising themselves as a delivery driver wearing an official uniform.

They approach a house, claiming they are from a well-known delivery company, and the homeowner, believing them, opens the door and allows them in.

Once inside, the impersonator can steal valuables or gather information without the homeowner's knowledge that they were an imposter.

RAMAIAH Institute of Technology

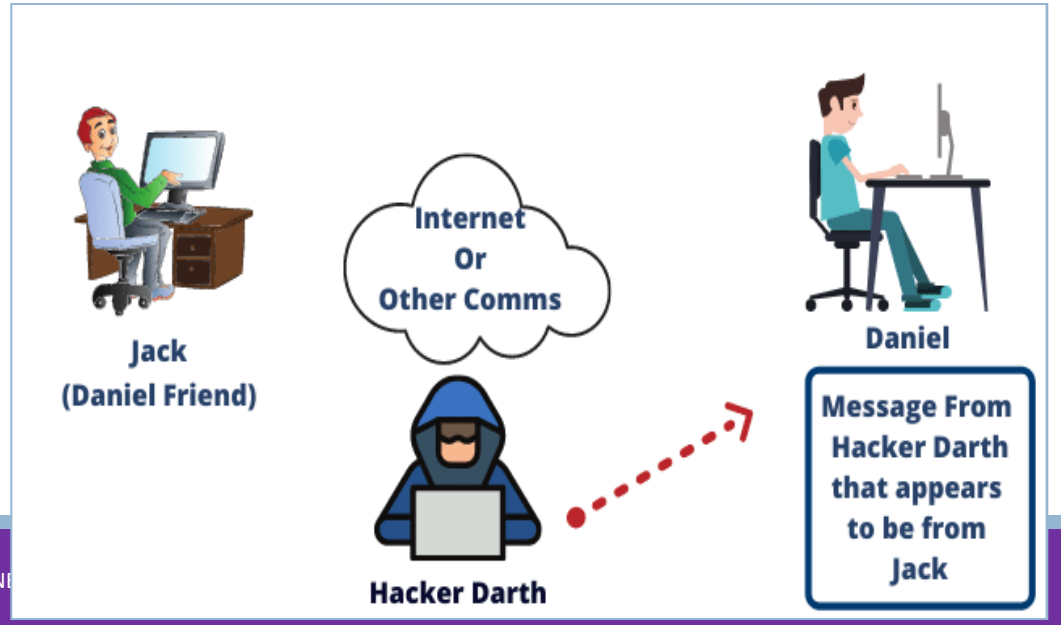
Attacks

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

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



Attacks

Attacks Threatening Integrity

3. Replaying

Imagine you receive a gift card and use it to buy something at a store.

After your purchase, someone finds the receipt you dropped, which includes the transaction information. They then return to the store, present the same transaction details, and claim another item as if they were the original customer who purchased it, tricking the store into thinking it's a valid purchase again.

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.

Replay involves the capture of a data unit and its subsequent retransmission to produce an unauthorized effect (replay previous messages)

Attacks

Attacks Threatening Integrity

4. Repudiation

Imagine you sign for a package delivery.

Later, when a dispute arises about whether you received the package, you claim you never signed for it, and there's no video recording or solid evidence proving that you did.

Without a reliable proof of the delivery, you can deny your involvement.

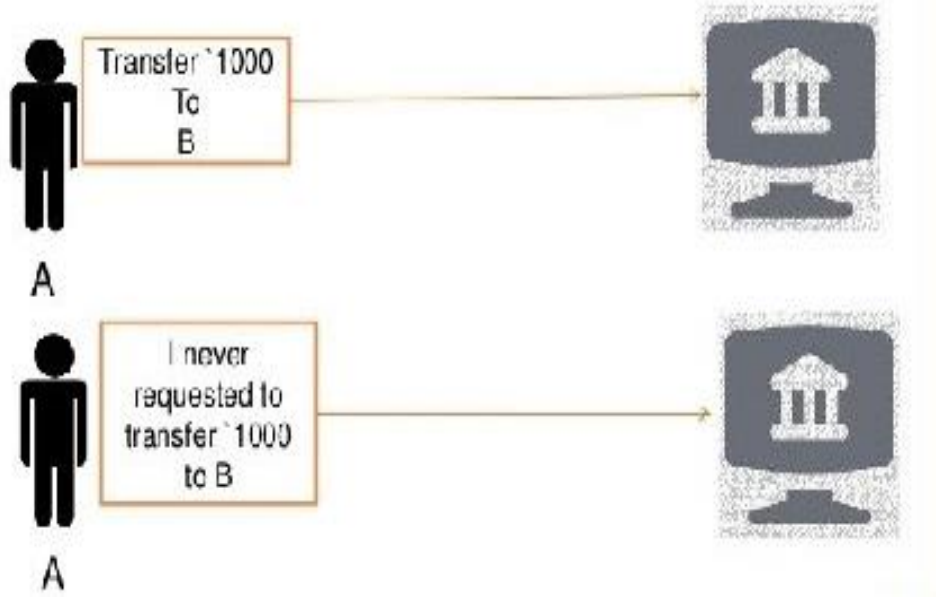
Attacks

Attacks Threatening Integrity

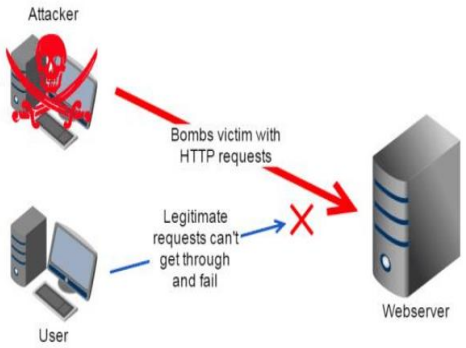
4. Repudiation

A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction.

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) -**a type of aimed at making a computer system, service, or network resource unavailable to its intended users by overwhelming it with a flood of illegitimate requests or data.

   Attack 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

RAMAIAH
Institute of Technology

Attacks

A telephonic conversation, an E-mail message or a transferred file may contain confidential data. A passive attack (Release of Message Content) may monitor the contents of these transmission

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

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

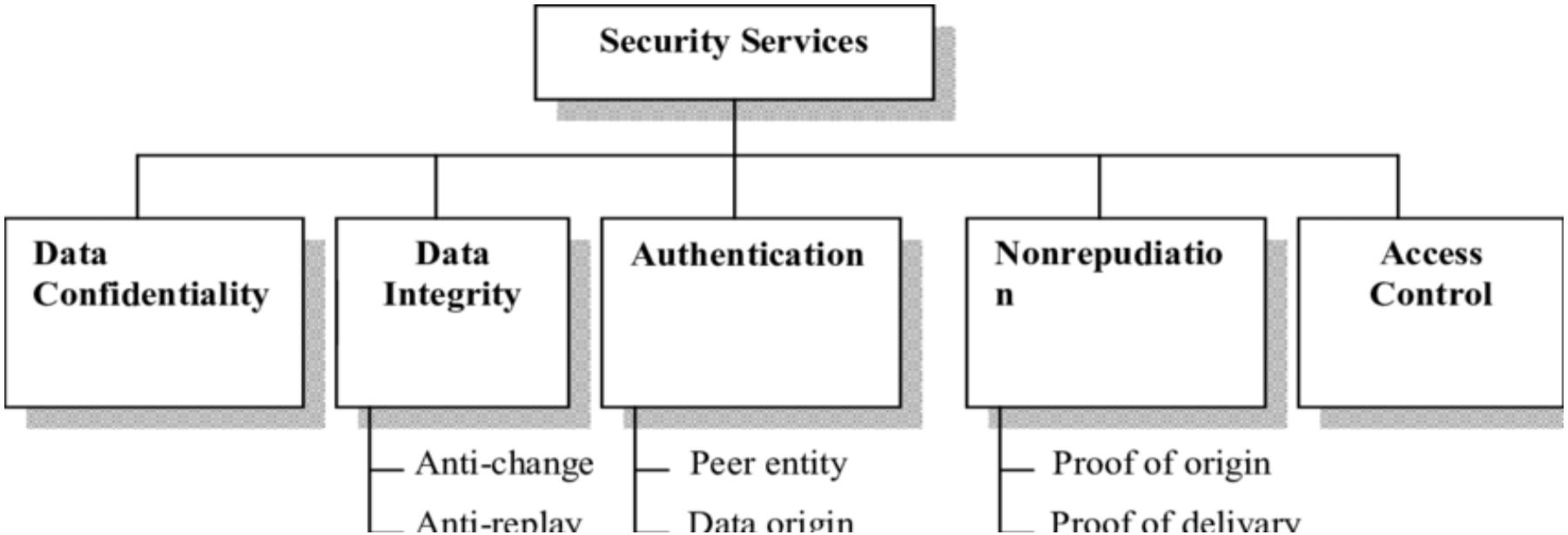
Services and Mechanisms

- 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

Example

In an online banking system, customers enter their login credentials (username and password) to access their accounts.

To maintain **data confidentiality**, the system encrypts these credentials as they are transmitted over the network.

Even if an attacker intercepts the data, they would not be able to read the encrypted login details. Additionally, once logged in, the user's personal information, bank balance, and transaction history are visible only to them and the authorized bank staff, not to unauthorized users.

Services and Mechanisms

Security Services

2.Data Integrity

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

RAMAIAH Institute of Technology

Services and Mechanisms

Example

Consider an online payment system where a customer is transferring $500 to another person.

To ensure **data integrity**, the system generates a cryptographic hash (a unique value based on the transaction details) when the transaction is initiated.

As the payment data (amount, recipient, etc.) is transmitted to the bank's server, the system checks that the hash of the received data matches the original hash.

Services and Mechanisms

Security Services

3.Authentication

Imagine you are attending a VIP event, and at the entrance, there is a security checkpoint where attendees must show their invitations and provide identification (like a driver's license).

The security team checks both to confirm that the person is who they claim to be and that they are on the guest list.

RAMAIAH Institute of Technology

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

4. Nonrepudiation

Imagine you send a formal letter to a business partner, and you use a registered mail service that requires a signature upon delivery.

When the letter is received, the recipient signs a receipt confirming that they received the letter.

This receipt serves as proof that the recipient cannot later deny having received your letter.

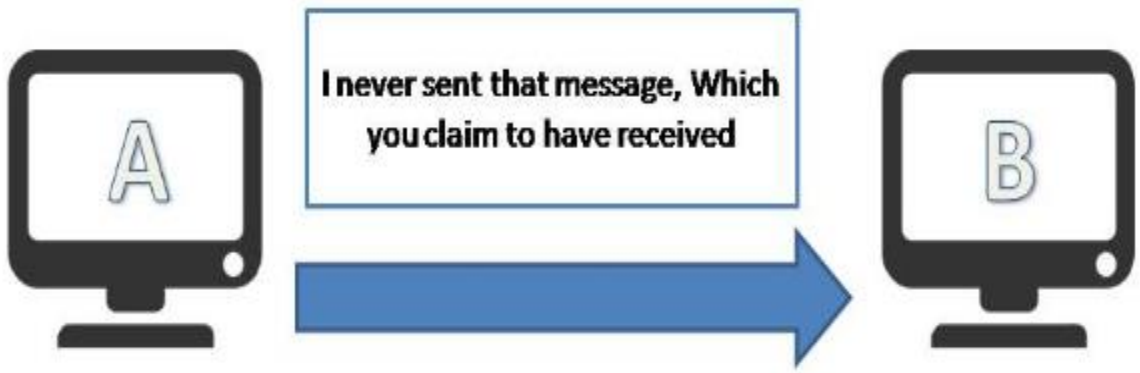
RAMAIAH Institute of Technology

Services and Mechanisms

4. Nonrepudiation

Nonrepudiation ensures that no party can deny that it sent or received a message via encryption and/or digital signatures or approved some information.

It also cannot deny the authenticity of its signature on a document.
Nonrepudiation is achieved through cryptography, like digital signatures



- Scenario 1:
  - Alice sends a stock buy request to Bob
  - Bob does not buy and claims that he never received the request
- Scenario 2:
  - Alice sends a stock buy request to Bob
  - Bob sends back an acknowledge message
  - Again, Bob does not buy and claims that he never received it
  - Alice presents the ack message as proof

Services and Mechanisms

Security Services

5. Access control

Imagine a library with different sections, such as a students area, a reference section, and a restricted archive of research books.

To ensure that only authorized individuals can enter specific areas, the library employs a system of access control.

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.

Prevent unauthorized access to resources

Example:

Bank 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**

Imagine you want to send a secret message to a friend.

Instead of writing it in plain language that anyone could read, you decide to use a special code known only to you and your friend.

For example, you might replace each letter with a different letter (A becomes D, B becomes E, etc.).

Services and Mechanisms

Security Mechanisms

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.
- Hiding or covering data can provide confidentiality.
- Two techniques are Cryptography and Steganography

Services and Mechanisms

Security Mechanisms

2. Data Integrity

A variety of mechanisms used to assure the integrity of a data unit or stream of data units

Data integrity mechanism appends to the data a short check value that has been created by a specific process from the data itself.

Services and Mechanisms

Security Mechanisms

3. 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).

Sender can electronically sign the data and the receiver can electronically verify the signature.

Services and Mechanisms

Security Mechanisms

4. Authentication exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

Services and Mechanisms

Security Mechanisms

5.Traffic Padding –

Imagine you're sending a small gift to a friend, but you want to keep it a secret.

Instead of just putting the small gift in a plain envelope, you fill the envelope with crumpled paper or extra items so it looks much bulkier.

When the envelope arrives, it appears large and full, making it hard for anyone looking at it to guess what the real gift is inside.

The extra padding disguises the size of the actual gift.

Services and Mechanisms

Security Mechanisms

5.Traffic Padding –

- The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- Traffic padding may be used to hide the traffic pattern, which means to insert dummy traffic into the network and present to the intruder a different traffic pattern.
- Traffic padding produces ciphertext output continuously, even in the absence of plaintext.

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.

Communicating systems on detection of persistent passive or active attacks, wish to instruct the network service provider to establish a connection via a different route.

Similarly, data carrying certain security labels may be forbidden by a security policy to pass through certain networks or links.

Services and Mechanisms

Security Mechanisms

7.Notarization

This security mechanism involves use of trusted third party in communication.

It acts as mediator between sender and receiver so that if any chance of conflict is reduced.

This mediator keeps record of requests made by sender to receiver for later denied.

Services and Mechanisms

Security Mechanisms

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

It can be achieved by various techniques such as

- applying passwords,
- using firewall,
- adding PIN to data.

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

	Steganography	Cryptography
Definition	Depend on hiding the message existence	Depend on hiding the message meaning
Purpose	Keep communication secure.	Provide protection for data
Visibility	Never	Always
Failure	When discover the presence of a hidden message	When able to decrypt and read the message
Concern	Embedding capacity and detectability of cover object	Robustness against deciphering.
Carrier	Any type of digital media	Depend on text as a carrier
Key	Optional, but provide more security	Necessary

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

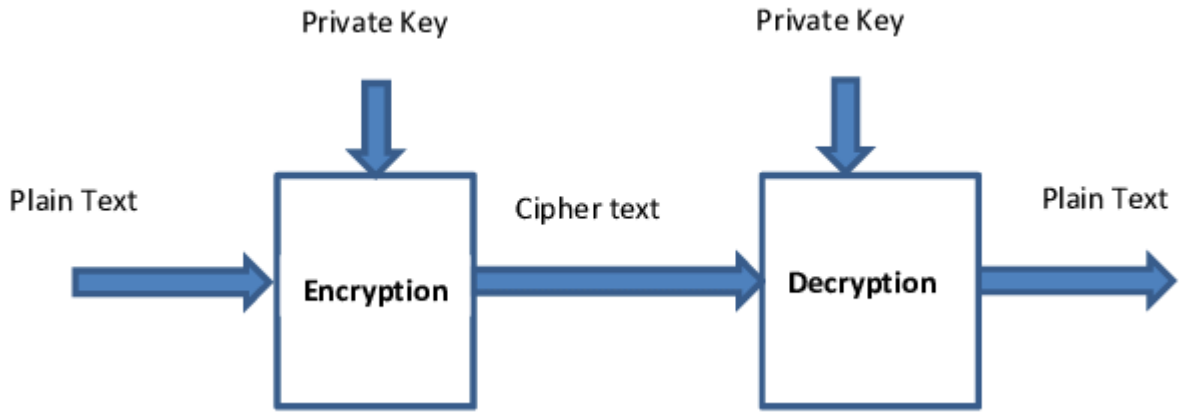
- Key - is a string of characters used within an encryption algorithm for altering data so that it appears random.
- The length of a key is normally expressed in bits.
- A longer key makes it more difficult to crack the encrypted data; however, a longer key results in longer time periods to perform encryption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

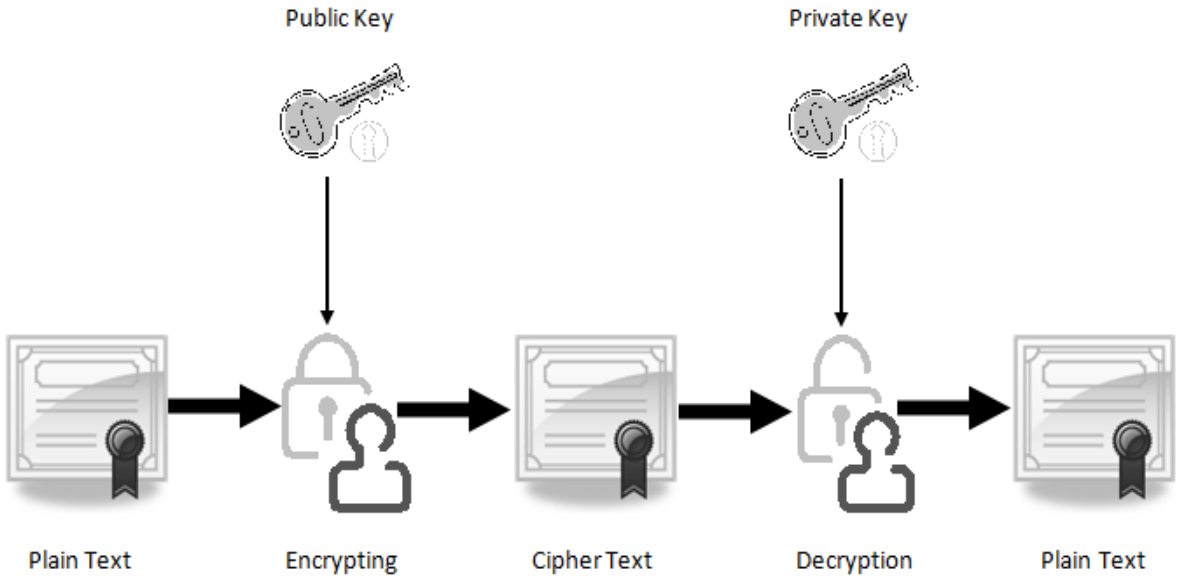


Techniques

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.

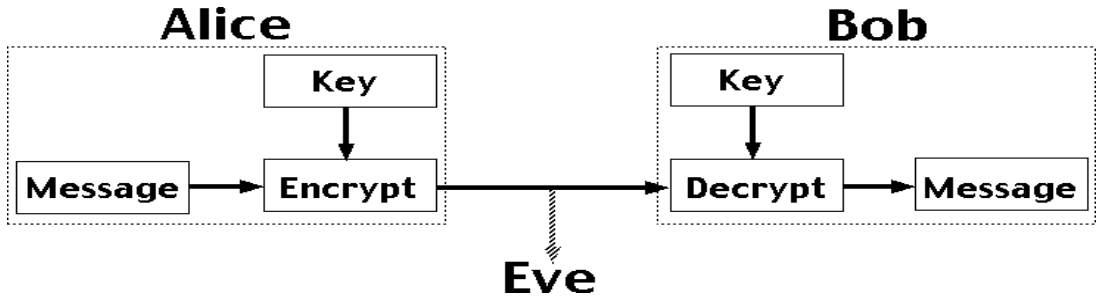
Techniques

- Symmetric key Encipherment

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

  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.

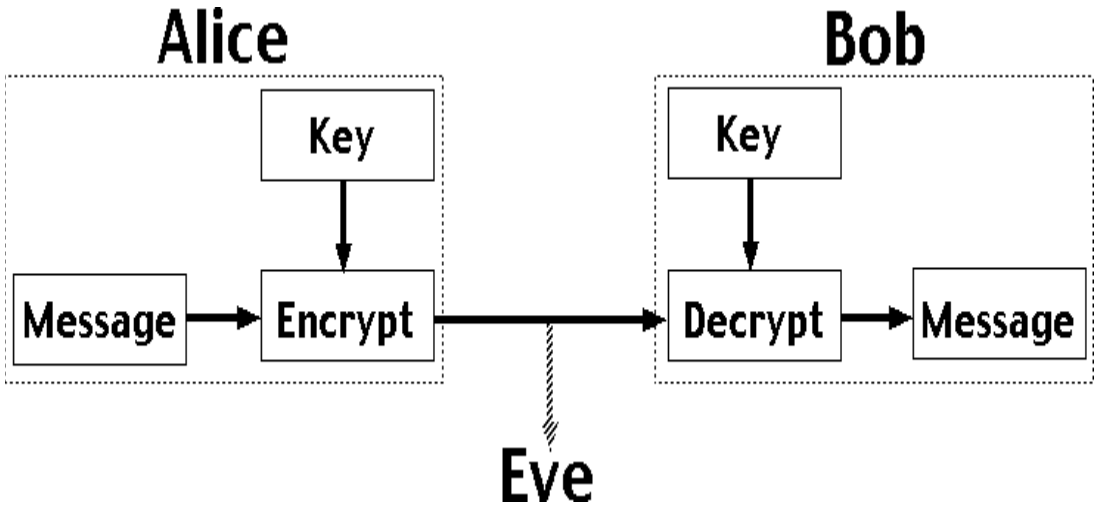


Techniques

- Symmetric key Encipherment

  Alice encrypts the message using an encryption algorithm.

  Bob decrypts the message using a decryption algorithm.



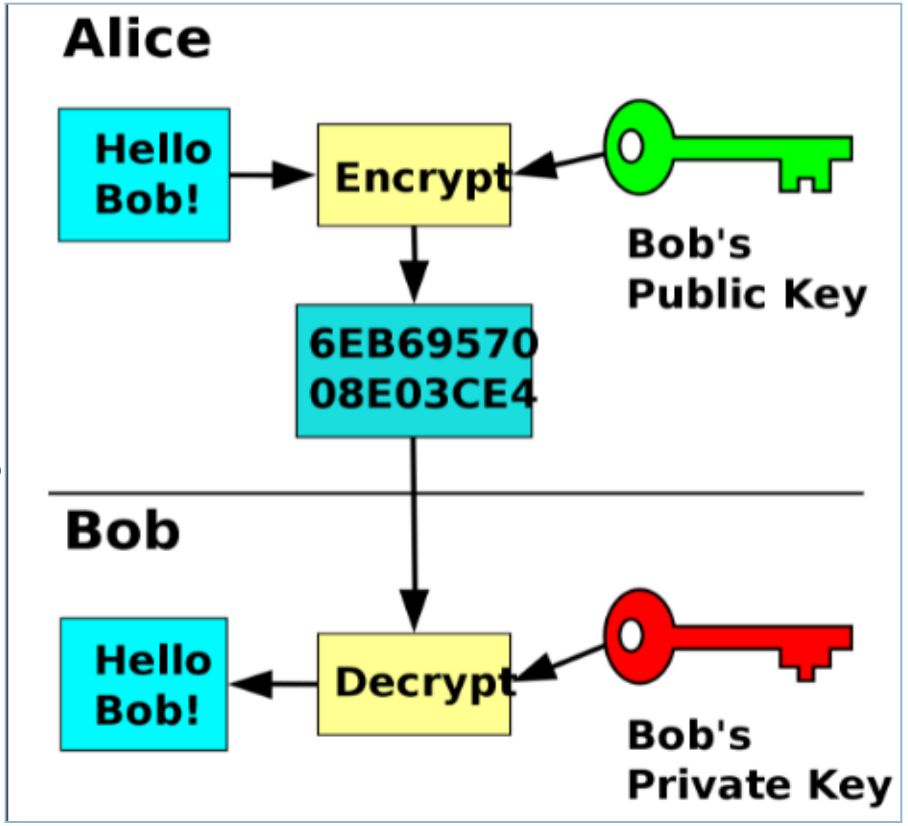
Techniques

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



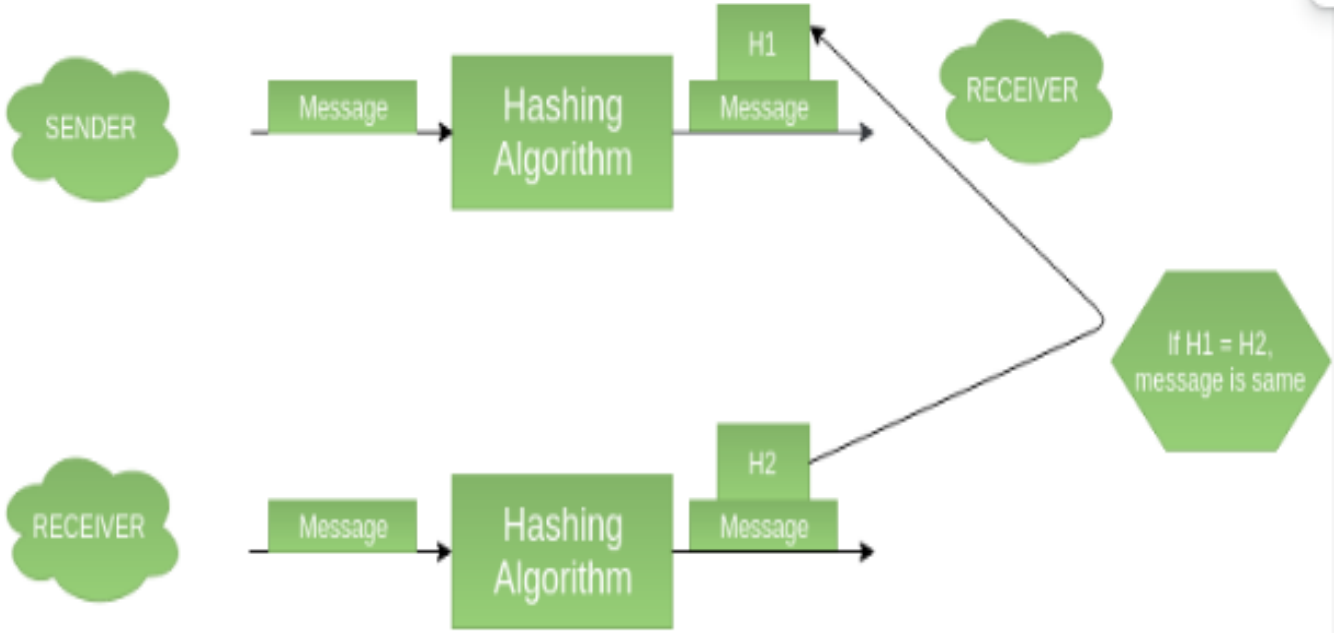
Techniques

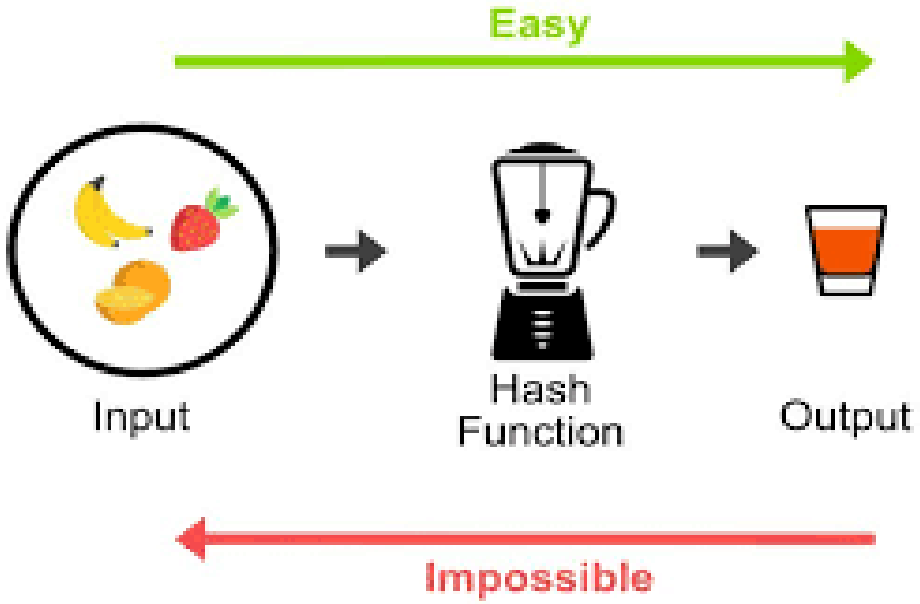
Hashing

- 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





RAMAIAH
Institute of Technology

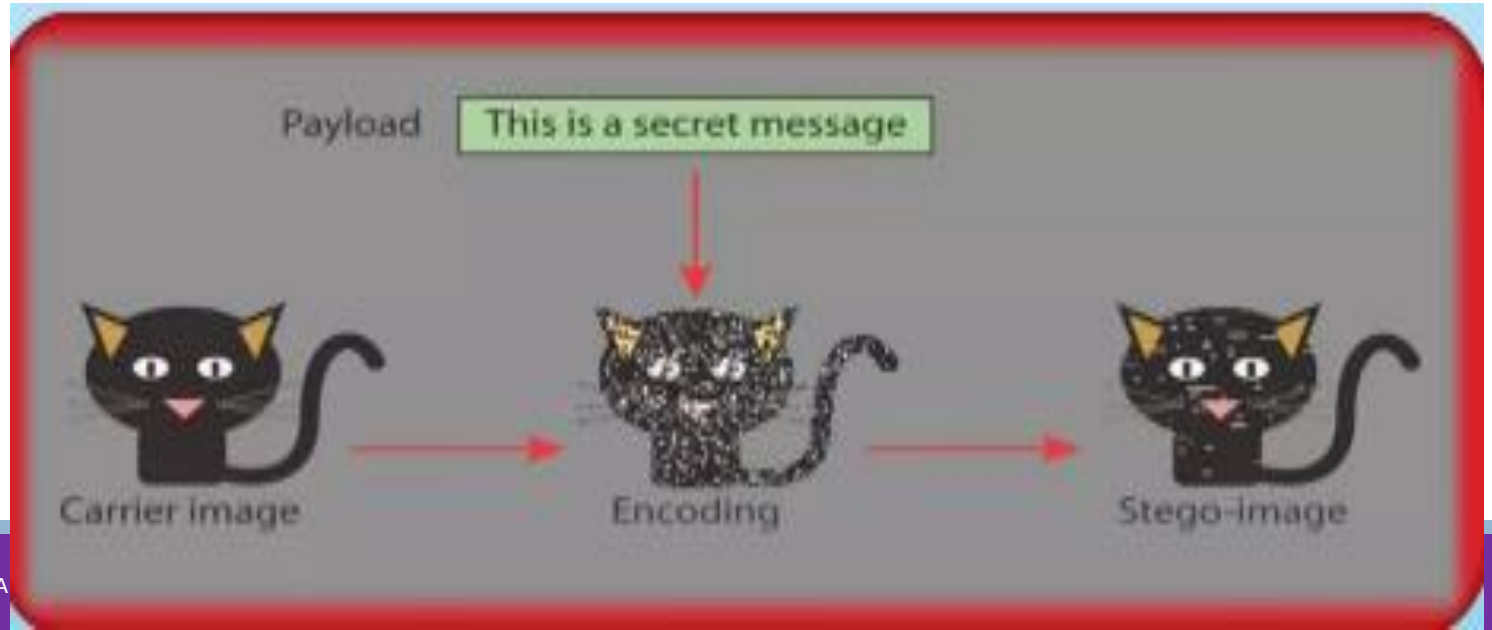
Techniques

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

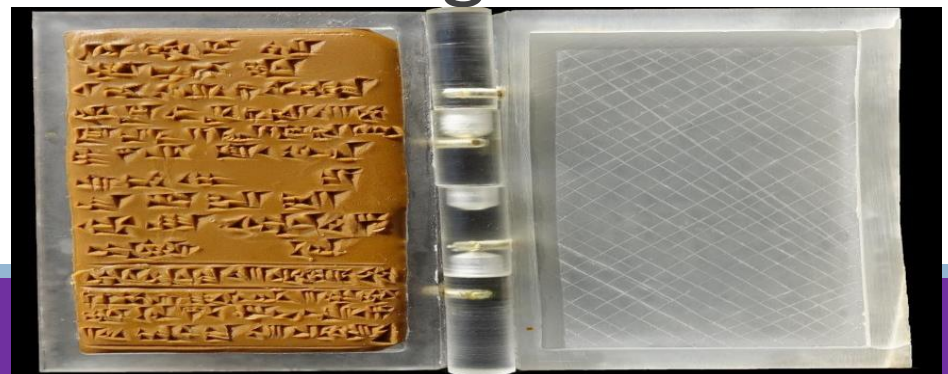


RAMAIAH Institute of Technology

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.



RAMAIAH
Institute of Technology

Techniques

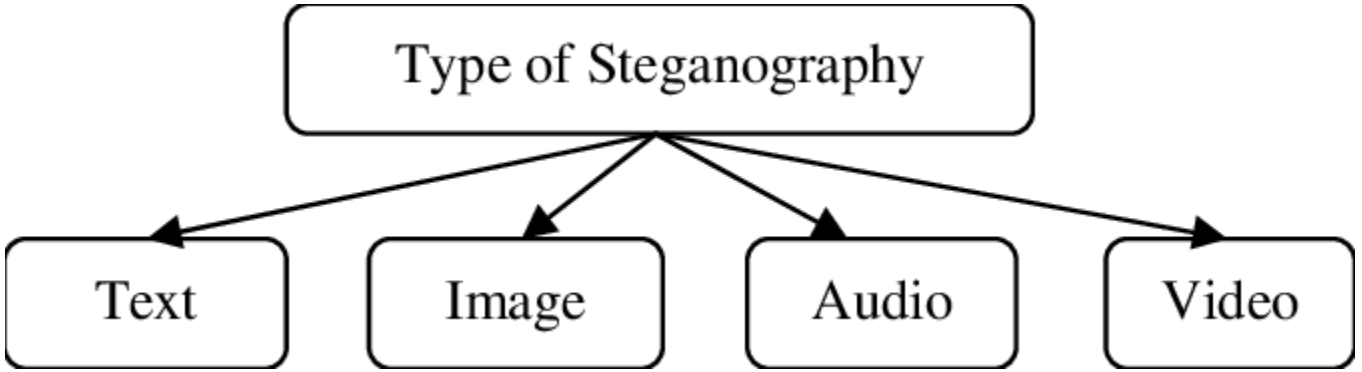
Steganography - Historical use

- 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 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

RAMAIAH Institute of Technology

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

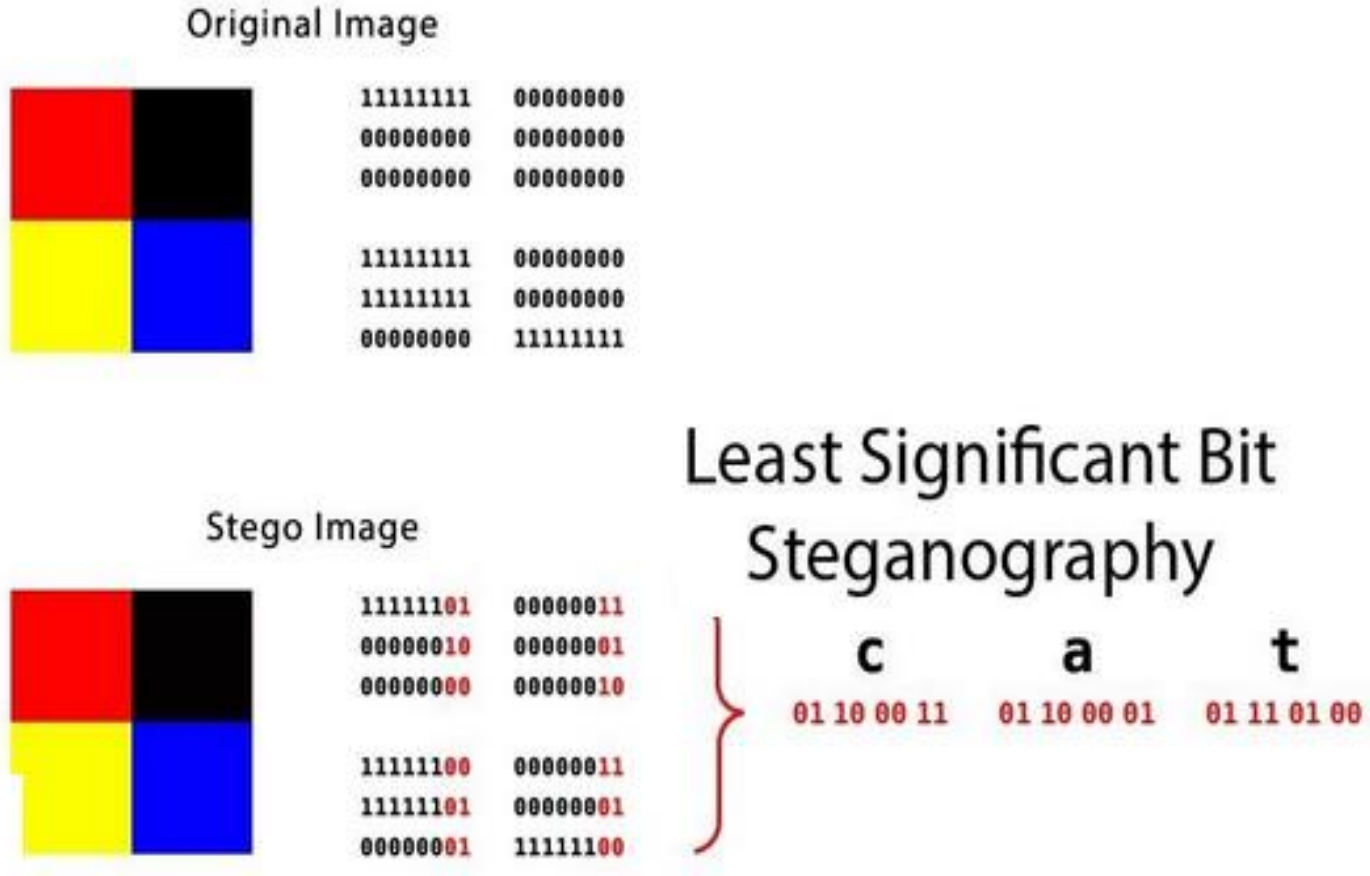
Techniques

Steganography –

Modern use – Image cover

- Secret data can also be covered under a color image.
- Digitized Image are made of pixels (24 bits – 3 bytes)

(red,green,blue)



Techniques

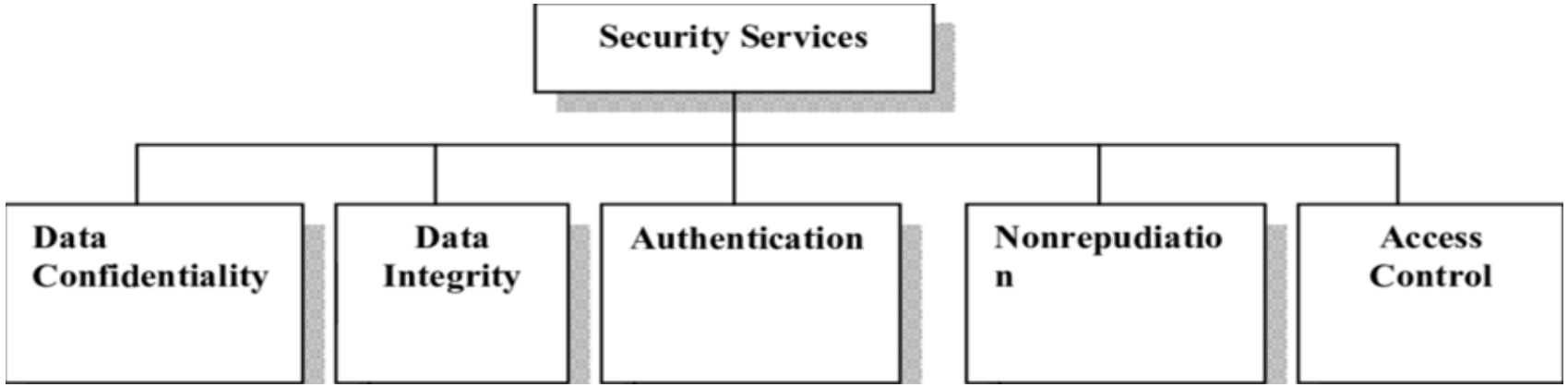
Steganography – Modern use – Other cover

- Secret data can also be covered using audio and video

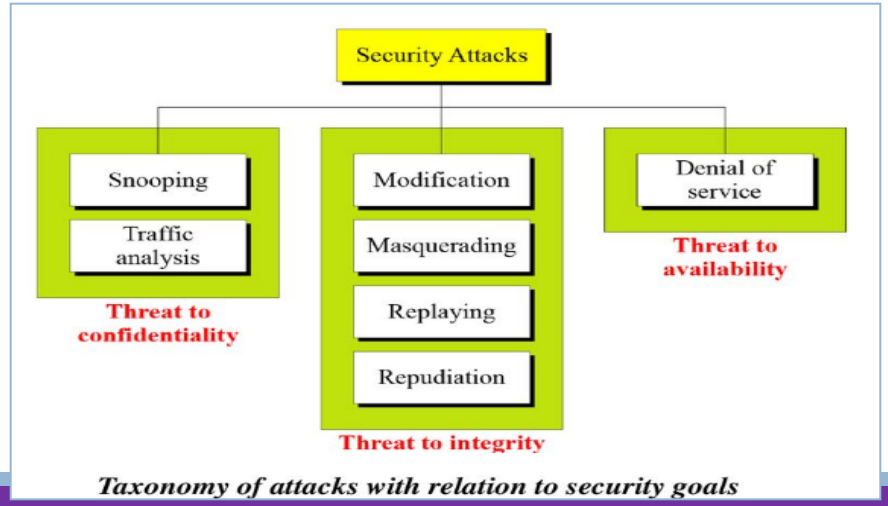
Review Questions

1. Define the three security goals.
2. Distinguish between passive and active security attacks. Name some passive attacks. Name some active attacks.
3. List and define five security services discussed in this chapter.
4. Define eight security mechanisms discussed in this chapter.
5. Distinguish between cryptography and steganography.

6. Which security service(s) are guaranteed when using each of the following methods to send mail at the post office?
   a. Regular mail
   b. Regular mail with delivery confirmation
   c. Regular mail with delivery and recipient signature
   d. Certified mail
   e. Insured mail
   f. Registered mail



7. Define the type of security attack in each of the following cases:
   a. A student breaks into a professor's office to obtain a copy of the next day's test.
   b. A student gives a check for $10 to buy a used book. Later she finds that the check was cashed for $100.
   c. A student sends hundreds of e-mails per day to another student using a phony return e-mail address.



Taxonomy of attacks with relation to security goals

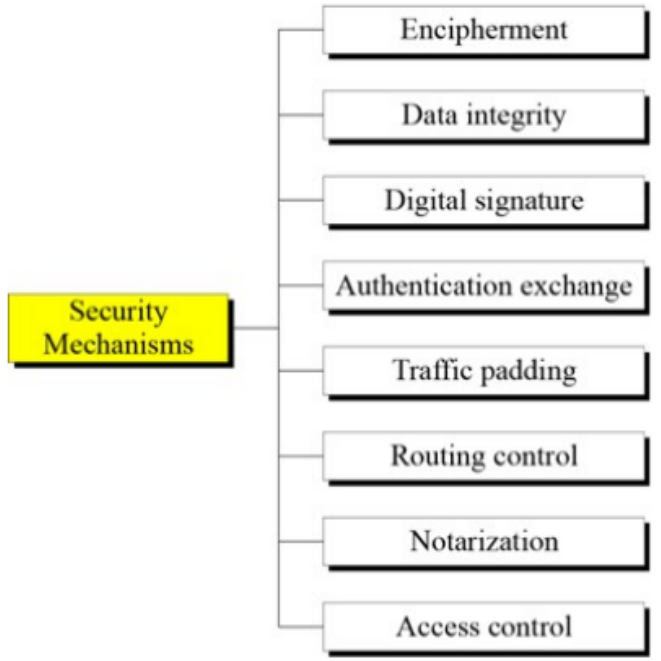
8. Which security mechanism(s) are provided in each of the following cases?

a. A school demands student identification and a password to let students log into the school server.

b. A school server disconnects a student if she is logged into the system for more than two hours.

c. A professor refuses to send students their grades by e-mail unless they provide student identification they were preassigned by the professor.

d. A bank requires the customer's signature for a withdrawal.



9. Which technique (cryptography or steganography) is used in each of the following cases for confidentiality?
   a. A student writes the answers to a test on a small piece of paper, rolls up the paper, and inserts it in a ball-point pen, and passes the pen to another student.
   b. To send a message, a spy replaces each character in the message with a symbol that was agreed upon in advance as the character's replacement.
   c. A company uses special ink on its checks to prevent forgeries.
   d. A graduate student uses watermarks to protect her thesis, which is posted on her website.
10. What type of security mechanism(s) are provided when a person signs a form he has filled out to apply for a credit card?

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

Integer Arithmetic

- In integer arithmetic, use
  - a set
  - a few operations.
- Integer arithmetic are used 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

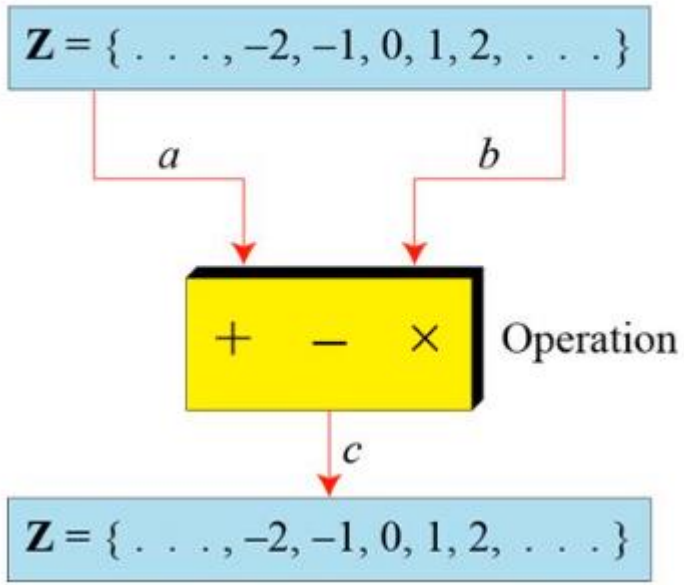
Binary Operations

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



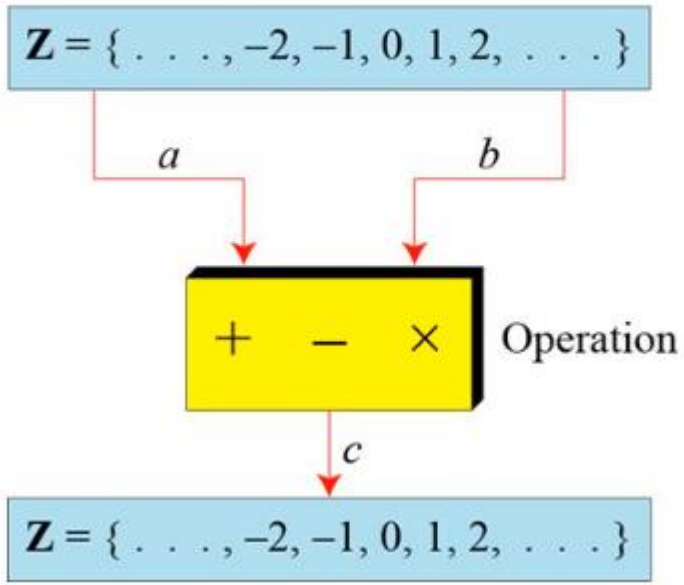
Integer Arithmetic

Binary Operations

Figure shows three binary operations for the set of integers

- addition
- subtraction
- multiplication

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:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

RAMAIAH Institute of Technology

Integer Arithmetic

Integer Division

In integer arithmetic, if we divide a by n, we can get q and r . We call it **Division relation**

The relationship between these four integers can be shown

a is dividend

q is quotient

n is divisor

r is remainder

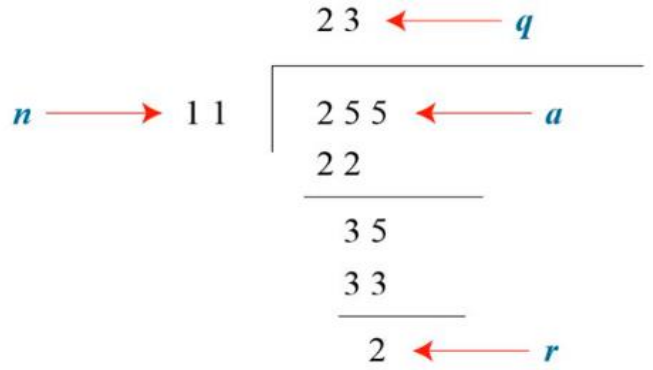
$$a = q \times n + r$$

Operator / for quotient

% 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.

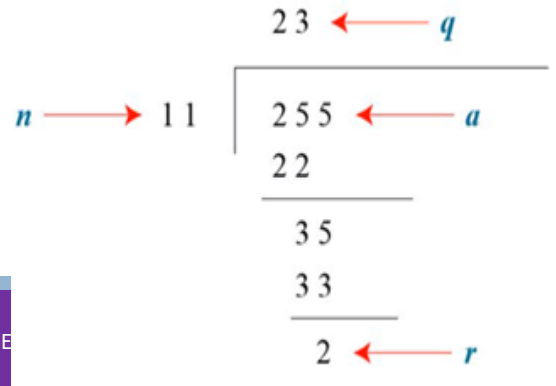


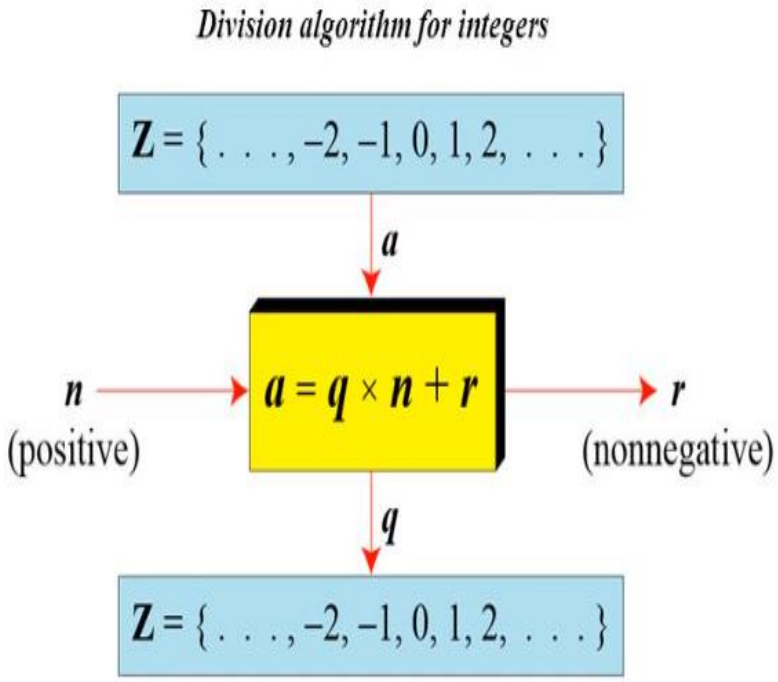
Integer Arithmetic

Integer Division

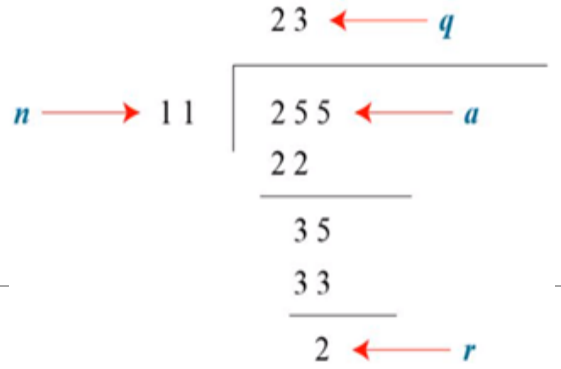
When we use division relationship in cryptography, we impose 2 restrictions

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



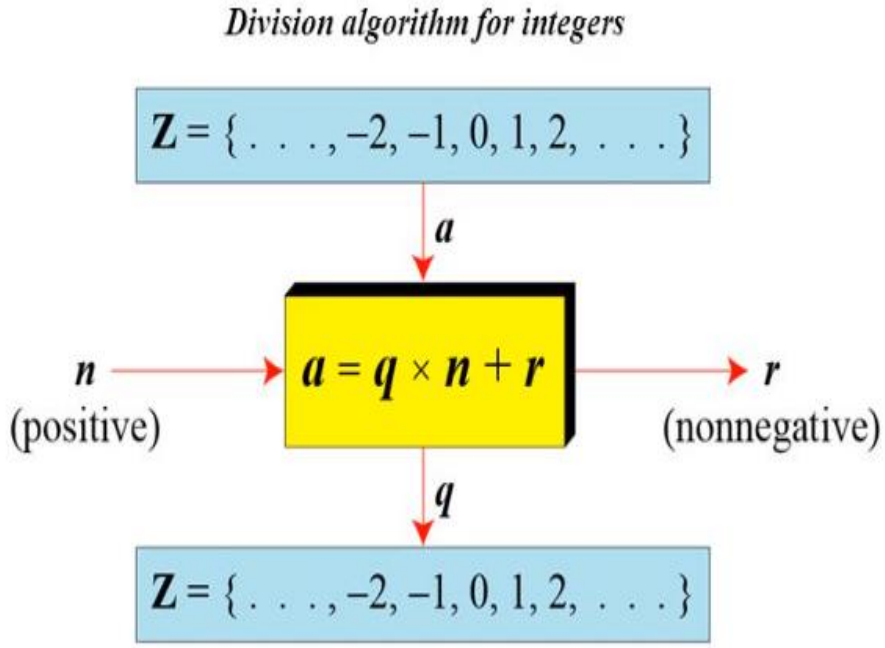


Integer Arithmetic



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.



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

$a = q \times n + r$

Divisbility

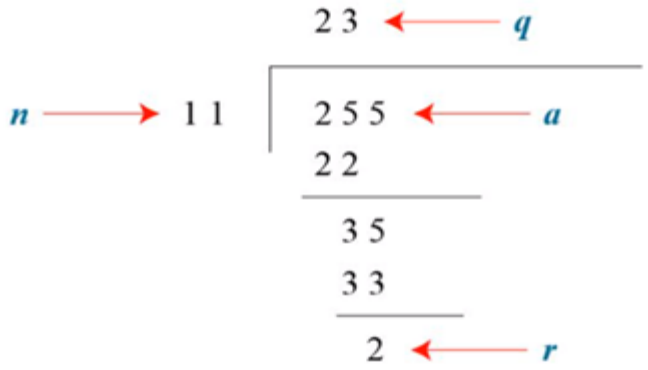
Divisibility we encounter in cryptography.
If a is not zero and we let r = 0 in the division relation, we get

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

When not interest with the value of q , we can write the above relation as

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

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



Divisibility - Properties

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

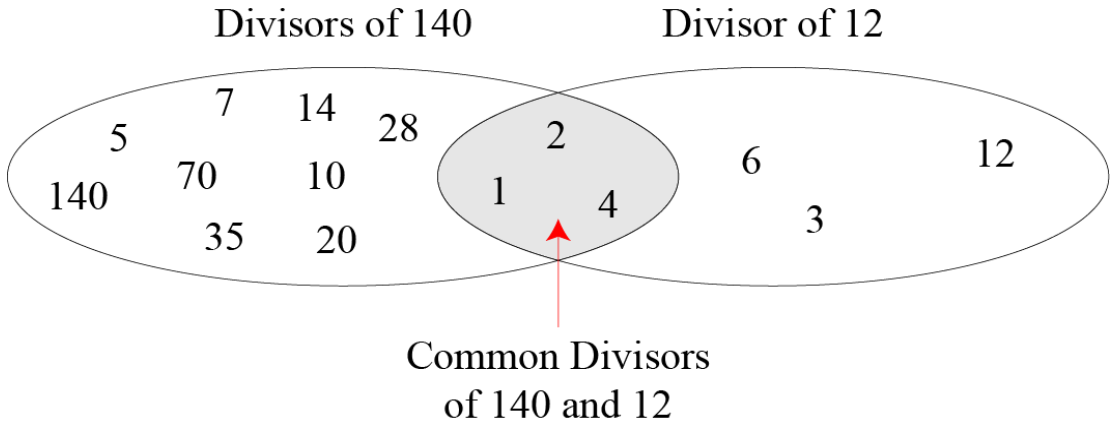
Fact 1: The integer 1 has only one divisor, itself.

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

Greatest Common Divisor

One Integer needed in Cryptography is the greatest common divisor of two positive integer

GCD=4



The greatest common divisor of two positive integers is the largest integer that can divide both 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 an 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(a,b)

GCD(36,10) 36 = 10*3 + 6

GCD(10,6) 10 = 6*1 + 4

GCD(6,4) 6 = 4*1 + 2

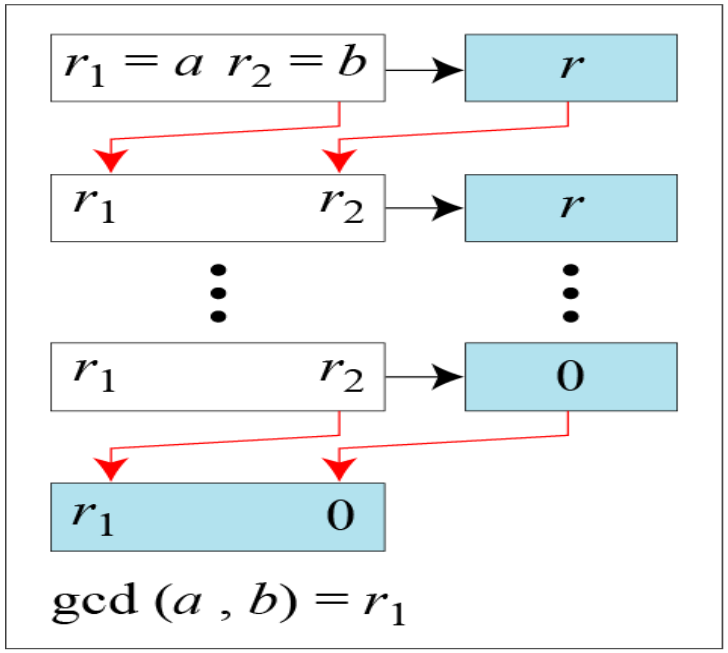
GCD(4,2) 4 = 2*2 + 0

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.

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
```

c) Using Euclidean Algorithm, determine the GCD for the following pair of integers
1760 and 2740

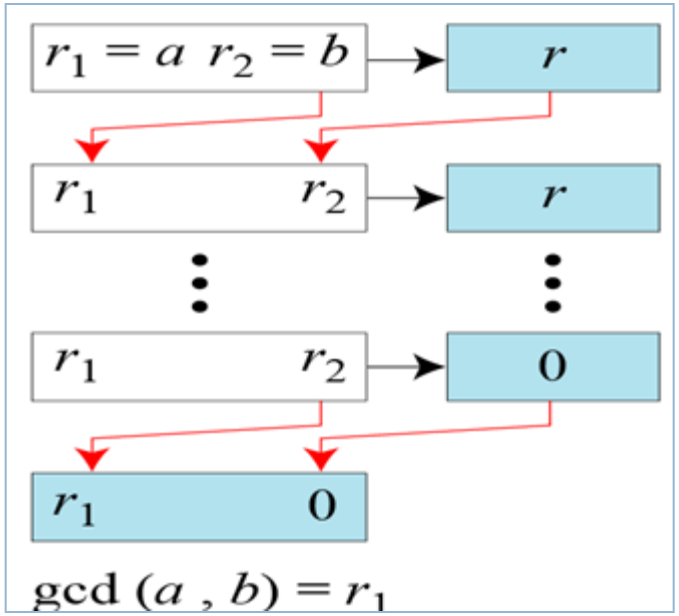
Find the greatest common divisor of 2740 and 1760.

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 $(a, b) \leftarrow r_1$



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	

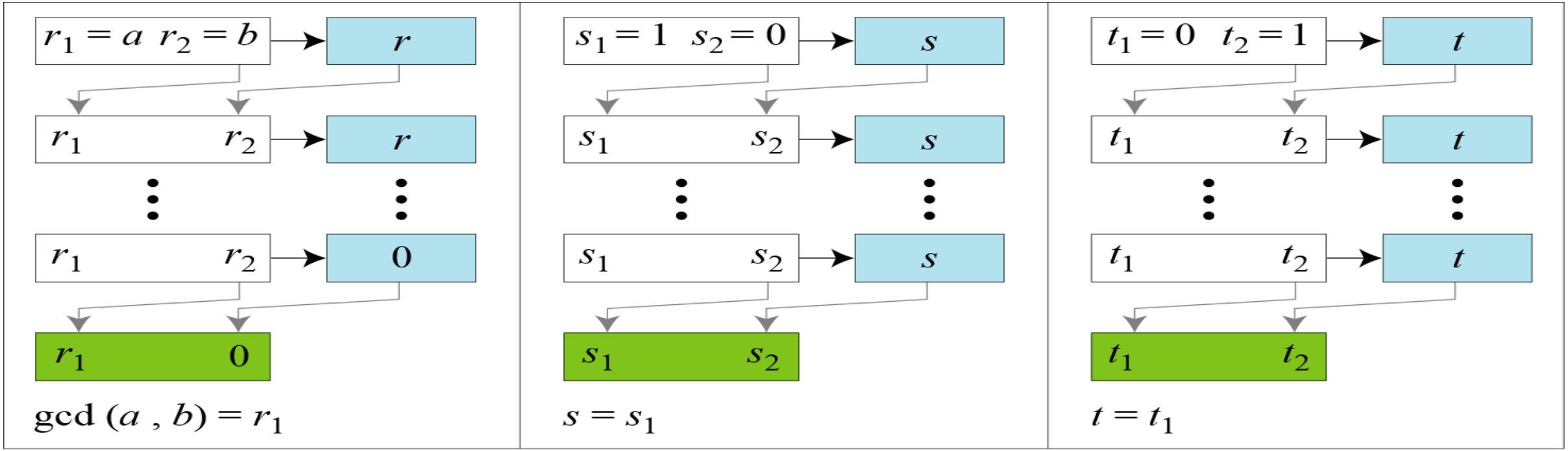
Extended Euclidean Algorithm

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 $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2;$

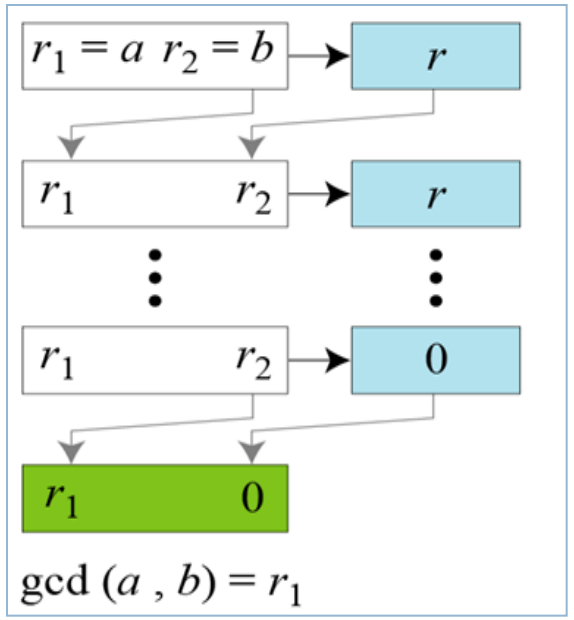
$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

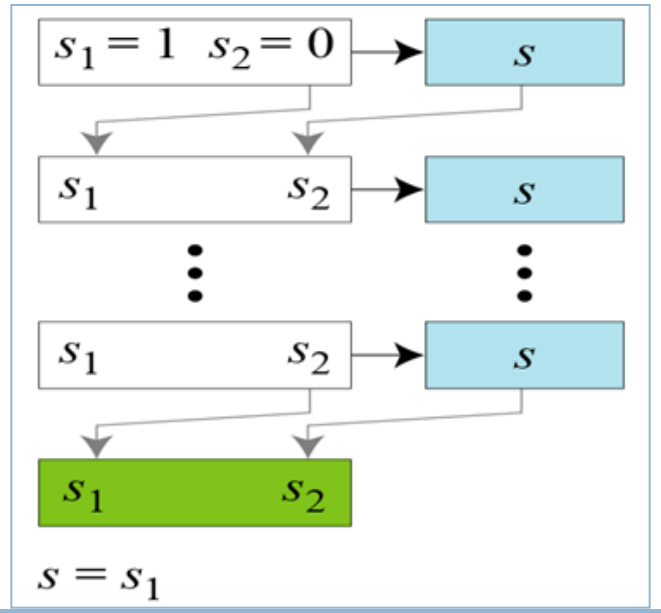
$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

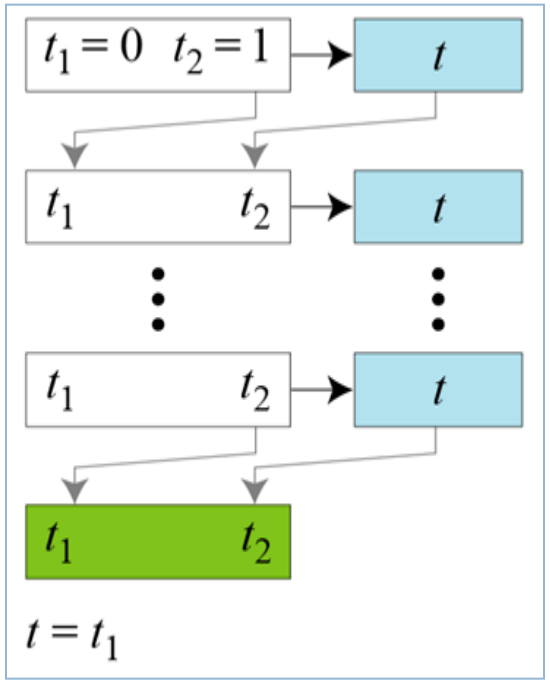
$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}

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.

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$
(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 = 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 $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

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

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

16. Using the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t.
    a. 4 and 7
    b. 291 and 42
    c. 84 and 320
    d. 400 and 60

Linear Diophantine Equation

- Application of Extended Euclidean Algorithm is to find the solutions to the Linear Diophantine Equation of two variables, an equation of type **ax+by =c**
- We need to find the integer value of x and y that satisfy the equation
- This type of equation has either no solution or an infinite number of solutions

Particular solution:
$x_0 = (c/d)s$ and $y_0 = (c/d)t$

General solutions:
$x = x_0 + k\,(b/d)$ and $y = y_0 - k(a/d)$
where k is an integer

Linear Diophantine Equation

Find the particular and general solution to the equation 21x + 14y =35

Solution

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$
General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$

Particular solution:
$x_0 = (c/d)s$ and $y_0 = (c/d)t$

General solutions:
$x = x_0 + k\,(b/d)$ and $y = y_0 - k(a/d)$
where k is an integer

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

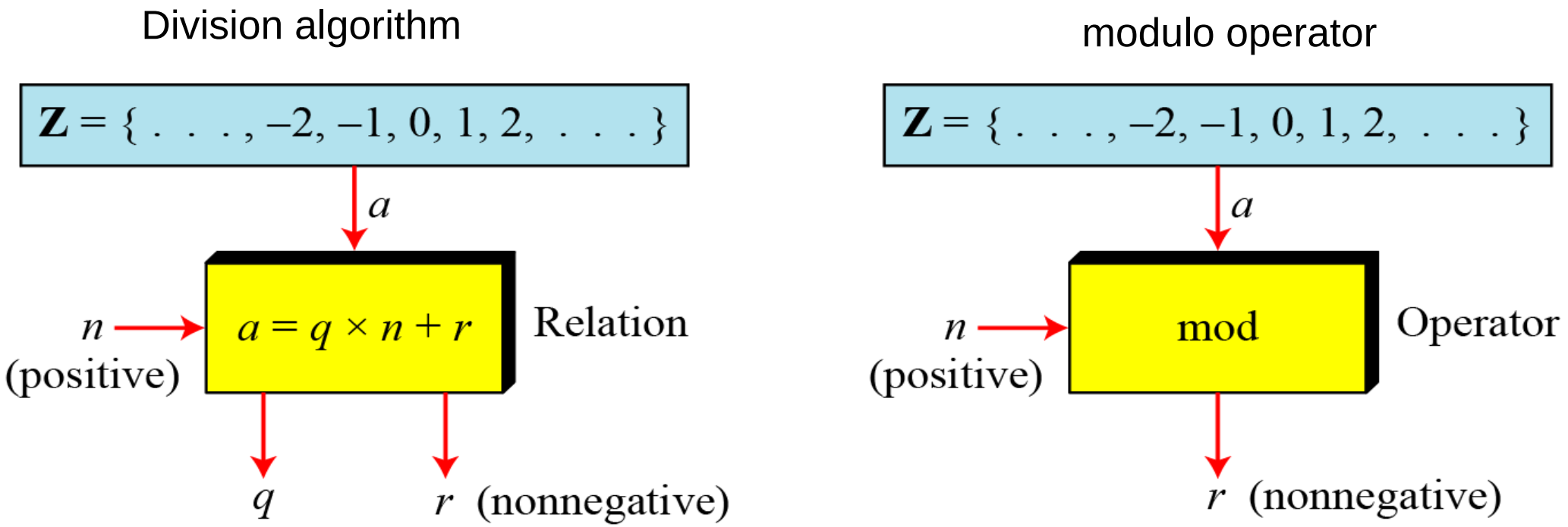
MODULAR ARITHMETIC

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.



$a \bmod n = r$

Find the result of the following operations:

a. 27 mod 5
b. 36 mod 12
c. −18 mod 14
d. −7 mod 10

We are looking for the residue r.
We can divide the a by n and find q and r.
We can then disregard q and keep r.

Dividing 27 by 5 results in r = 2. This means that 27 mod 5 = 2.

Dividing 36 by 12 results in r = 0. This means that 36 mod 12 = 0.

Dividing −18 by 14 results in r = −4.
However, we need to add the modulus (14) to make it nonnegative. We have r = −4 + 14 = 10.
This means that −18 mod 14 = 10.

Dividing −7 by 10 results in r = −7. After adding the modulus to −7, we have r = 3.
This means that −7 mod 10 = 3.

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.**

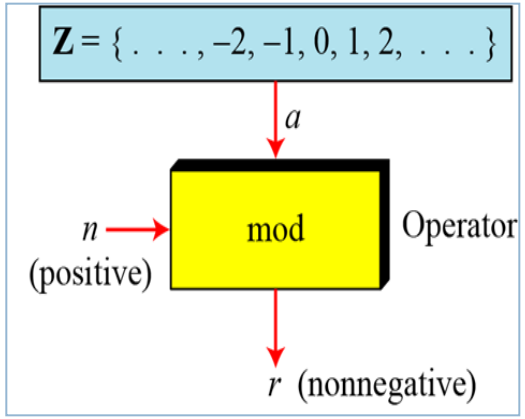
Some Z_n sets

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

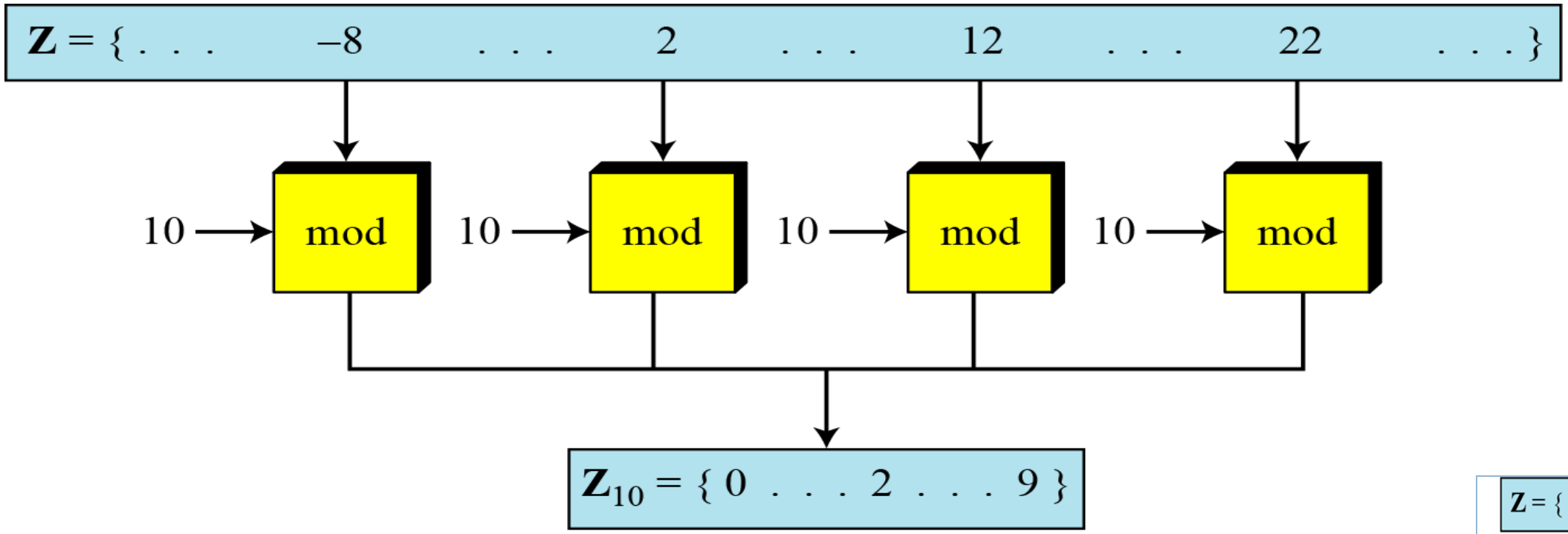
$$\mathbf{Z}_2 = \{ 0, 1 \}$$

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

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

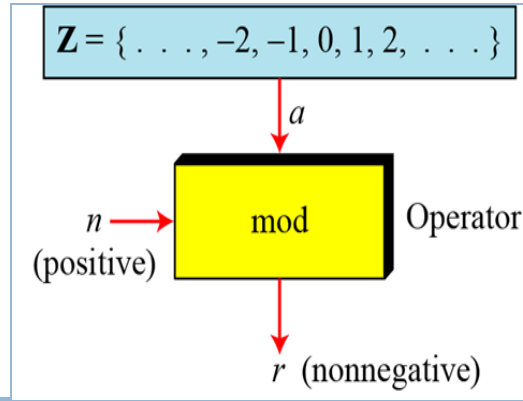


Concept of congruence



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

Congruence Relationship



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.

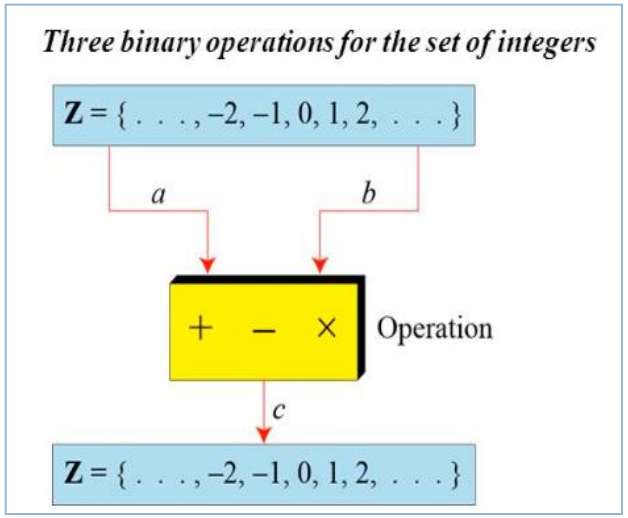
For example

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

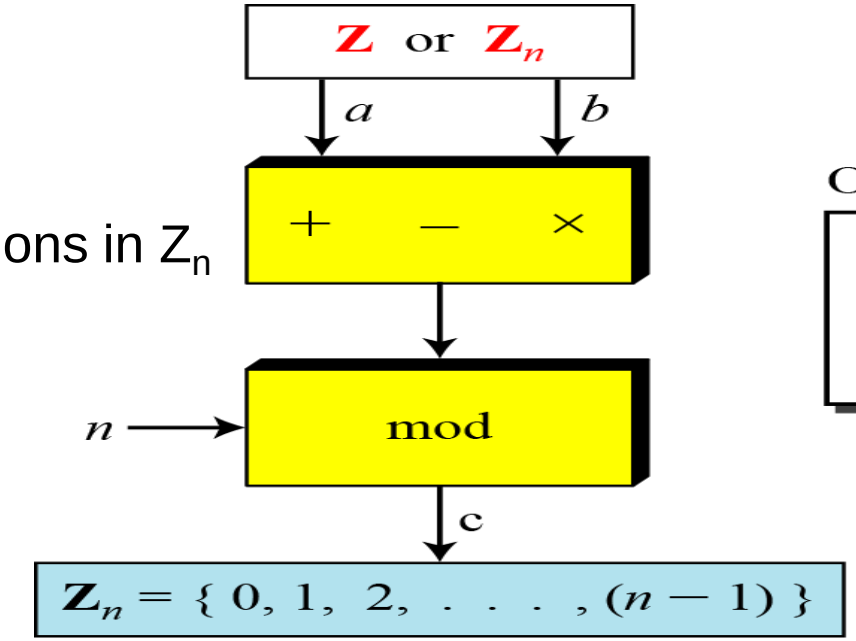
Operation in Z_n

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

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

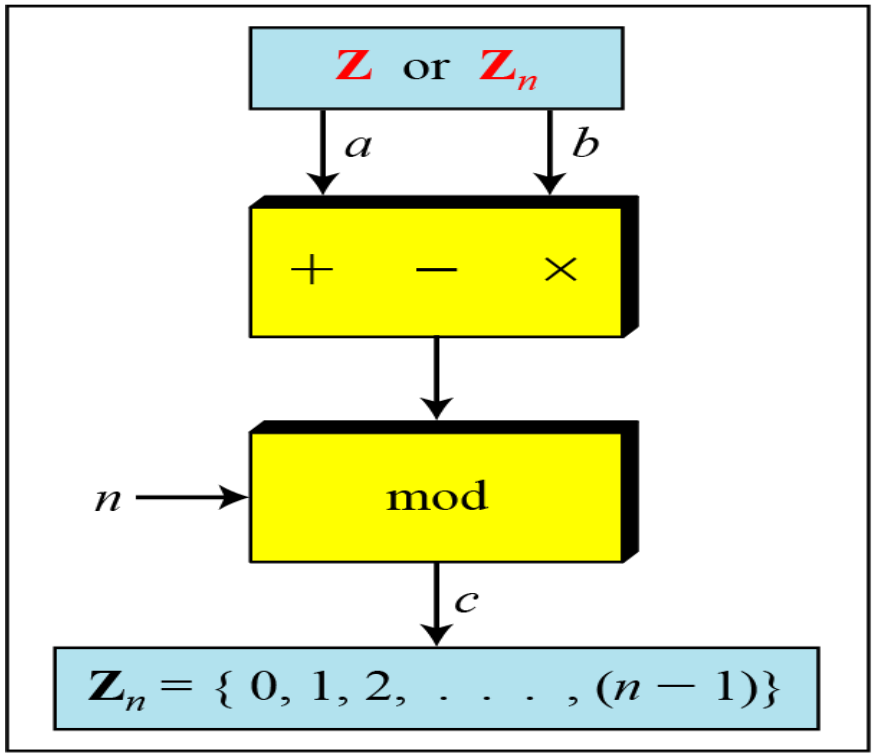
First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Properties of mode operator

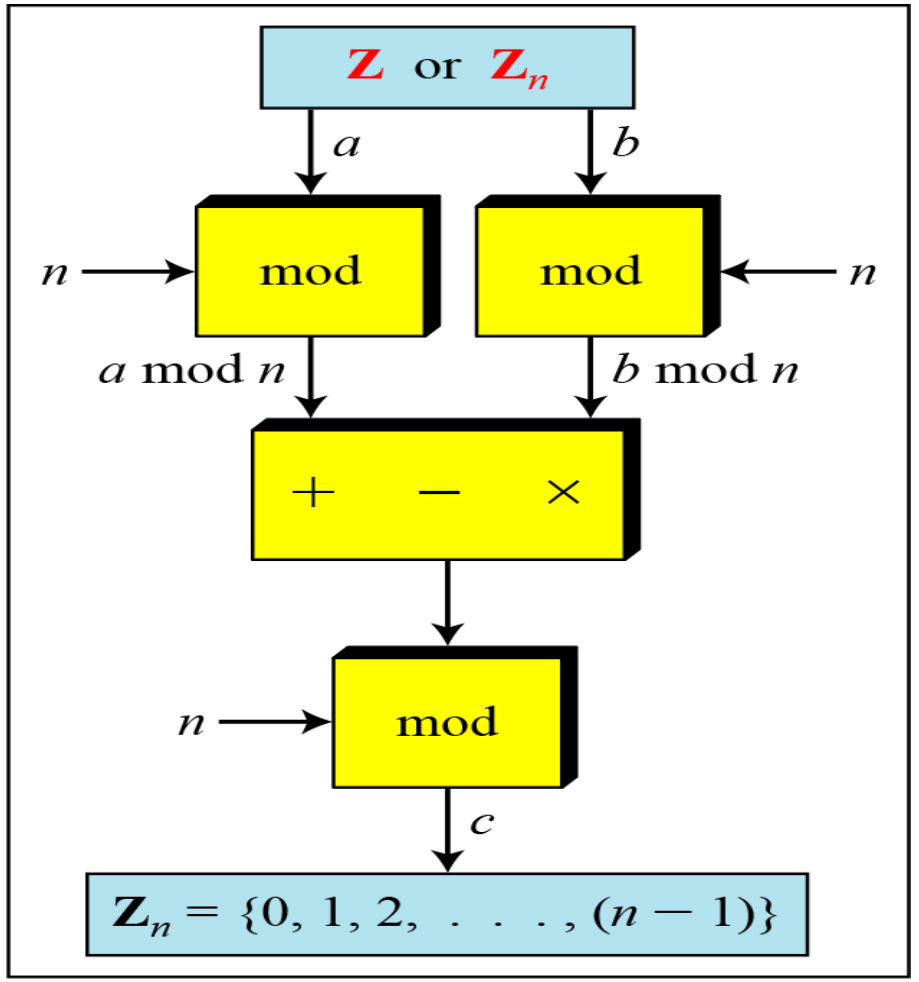
First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

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

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

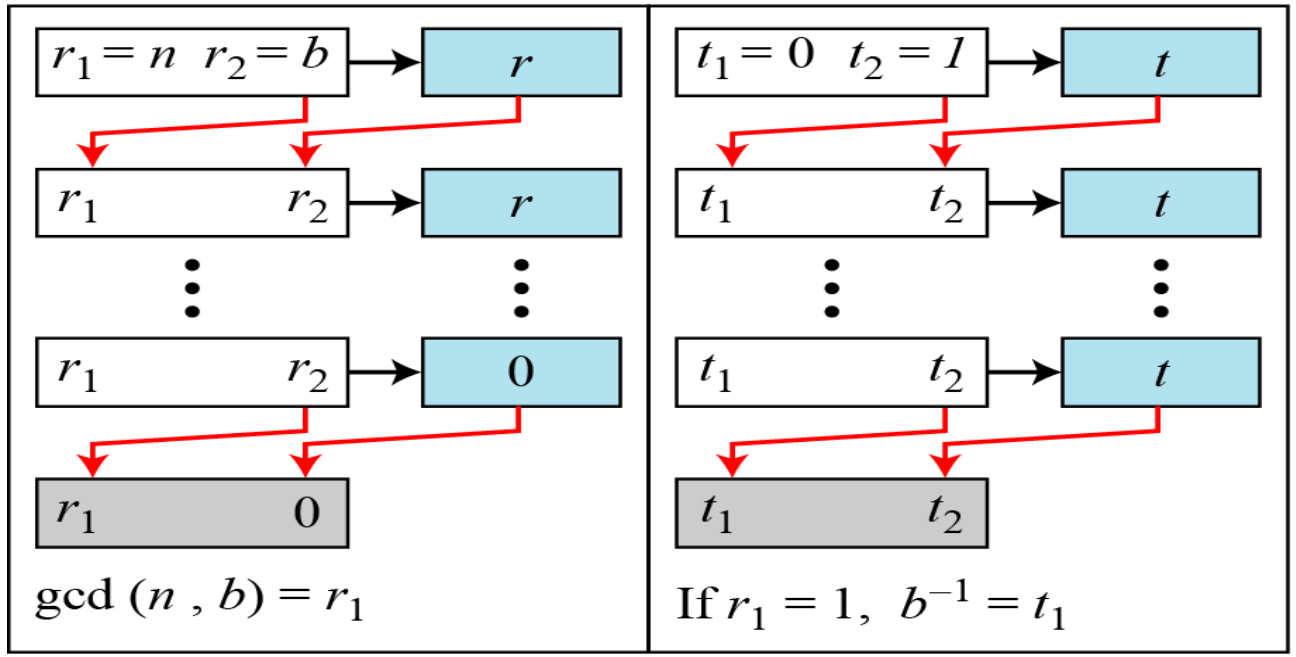
Note

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

We can say that the algorithm can find s and t such s × n + b × t = gcd (n, b).
However, if the multiplicative inverse of b exists, gcd (n, b) must be 1.

So the relationship is $(s \times n) + (b \times t) = 1$

Using extended Euclidean algorithm to find multiplicative inverse of b in Z_n when n and b are given and the inverse exists.



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

Using extended Euclidean algorithm to find multiplicative inverse of b in Z_n when n and b are given and the inverse exists.

The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and gcd $(n, b) = 1$.

The multiplicative inverse of b is the value of t after being mapped to Z_n.

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	

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

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

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

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

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

INVERSE EXISTS IF GCD IS 1

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

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

Solution

a) Calculate the multiplicative inverse using extended Euclidean for 23 in Z_{100} ? CO1 (10)

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

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.

32. Find the multiplicative inverse of each of the following integers in $\mathbf{Z}_{180}$ using the extended Euclidean algorithm.
    a. 38
    b. 7
    c. 132
    d. 24

Matrix

In cryptography we need to handle matrices. Although this topic belongs to a special branch of algebra called linear algebra, the following brief review of matrices is necessary preparation for the study of cryptography.

Definitions
Operations and Relations
Determinants
Residue Matrices

Matrix

example of addition and subtraction.

$$\begin{bmatrix} 12 & 4 & 4 \\ 11 & 12 & 30 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} + \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

$$\mathbf{C = A + B}$$

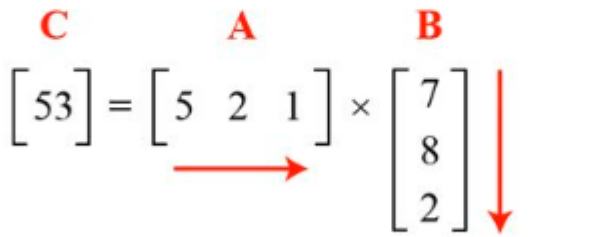
$$\begin{bmatrix} -2 & 0 & -2 \\ -5 & -8 & 10 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} - \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

$$\mathbf{D = A - B}$$

Matrix

shows the product of a row matrix (1 × 3) by a column matrix (3 × 1). The result is a matrix of size 1 × 1.

Multiplication of a row matrix by a column matrix



In which: $53 = 5 \times 7 + 2 \times 8 + 1 \times 2$

Matrix

shows the product of a row matrix (1 × 3) by a column matrix (3 × 1). The result is a matrix of size 1 × 1.

Multiplication of a row matrix by a column matrix

$$\underset{C}{\begin{bmatrix}53\end{bmatrix}} = \underset{A}{\begin{bmatrix}5 & 2 & 1\end{bmatrix}} \times \underset{B}{\begin{bmatrix}7\\8\\2\end{bmatrix}}$$

In which: $53 = 5 \times 7 + 2 \times 8 + 1 \times 2$

Matrix

shows the product of a 2 × 3 matrix by a 3 × 4 matrix. The result is a 2 × 4 matrix.

Multiplication of a 2 × 3 matrix by a 3 × 4 matrix

$$\underset{C}{\begin{bmatrix} 52 & 18 & 14 & 9 \\ 41 & 21 & 22 & 7 \end{bmatrix}} = \underset{A}{\begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix}} \times \underset{B}{\begin{bmatrix} 7 & 3 & 2 & 1 \\ 8 & 0 & 0 & 2 \\ 1 & 3 & 4 & 0 \end{bmatrix}}$$

2 × 4 2 × 3 3 × 4

Matrix

shows an example of scalar multiplication.

Scalar multiplication

$$\mathbf{B} \qquad\qquad\qquad\qquad \mathbf{A}$$

$$\begin{bmatrix} 15 & 6 & 3 \\ 9 & 6 & 12 \end{bmatrix} = 3 \times \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 4 \end{bmatrix}$$

Determinant

The determinant of a square matrix A of size m × m denoted as det (A) is a scalar calculated recursively as shown below:

1. If $m = 1$, $\det(\mathbf{A}) = a_{11}$
2. If $m > 1$, $\det(\mathbf{A}) = \sum_{\cdot} (-1)^{i+j} \times a_{ij} \times \det(\mathbf{A}_{ij})$

Where $\mathbf{A}_{ij}$ is a matrix obtained from $\mathbf{A}$ by deleting the ith row and jth column.

Determinant

shows how we can calculate the determinant of a 2 × 2 matrix based on the determinant of a 1 × 1 matrix.

Calculating the determinant of a 2 × 2 matrix

$$\det\begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix}$$

Determinant

shows how we can calculate the determinant of a 2 × 2 matrix based on the determinant of a 1 × 1 matrix.

Figure 2.24 *Calculating the determinant of a 2 × 2 matrix*

$$\det\begin{bmatrix} 5 & 2 \\ 3 & 4 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det[\,4\,] + (-1)^{1+2} \times 2 \times \det[\,3\,] \longrightarrow 5 \times 4 - 2 \times 3 = 14$$

or

$$\det\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

$$\begin{bmatrix} 1 & -2 & 3 \\ 2 & 0 & 3 \\ 1 & 5 & 4 \end{bmatrix} = \begin{bmatrix} \boxed{1} & -2 & 3 \\ 2 & \lceil 0 & 3 \rceil \\ 1 & \lfloor 5 & 4 \rfloor \end{bmatrix} - \begin{bmatrix} 1 & \boxed{-2} & 3 \\ \lceil 2 & 0 & 3 \rceil \\ \lfloor 1 & 5 & 4 \rfloor \end{bmatrix} + \begin{bmatrix} 1 & -2 & \boxed{3} \\ \lceil 2 & 0 \rceil & 3 \\ \lfloor 1 & 5 \rfloor & 4 \end{bmatrix}$$

$$= \boxed{1} \times \begin{vmatrix} 0 & 3 \\ 5 & 4 \end{vmatrix} - \boxed{-2} \times \begin{vmatrix} 2 & 3 \\ 1 & 4 \end{vmatrix} + \boxed{3} \times \begin{vmatrix} 2 & 0 \\ 1 & 5 \end{vmatrix}$$

$$= 1 \times (0 - 15) + 2 \times (8 - 3) + 3 \times (10 - 0)$$

$$= 1(-15) + 2(5) + 3(10)$$

$$= -15 + 10 + 30$$

$$= 25$$

Calculate the determinant of a 3*3 Matrix

$$\begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix}$$

Determinant

shows the calculation of the determinant of a 3 × 3 matrix.

Calculating the determinant of a 3 × 3 matrix

$$\det\begin{bmatrix} 5 & 2 & 1 \\ 3 & 0 & -4 \\ 2 & 1 & 6 \end{bmatrix} = (-1)^{1+1} \times 5 \times \det\begin{bmatrix} 0 & -4 \\ 1 & 6 \end{bmatrix} + (-1)^{1+2} \times 2 \times \det\begin{bmatrix} 3 & -4 \\ 2 & 6 \end{bmatrix} + (-1)^{1+3} \times 1 \times \det\begin{bmatrix} 3 & 0 \\ 2 & 1 \end{bmatrix}$$

$$= (+1) \times 5 \times (+4) \quad + \quad (-1) \times 2 \times (24) \quad + \quad (+1) \times 1 \times (3) = -25$$

Linear Congruence

- Cryptography often involves solving an equation or a set of equations of one or more variables with coefficient in Zn.
- This section shows how to solve equations when the power of each variable is 1 (linear equation).

- Single-Variable Linear Equations
- Set of Linear Equations

Single-Variable Linear Equations

Equations of the form $ax \equiv b \pmod{n}$ might have no solution or a limited number of solutions.

Assume that the gcd $(a, n) = d$.

If $d \nmid b$, there is no solution.

If $d \mid b$, there are d solutions.

Single-Variable Linear Equations

If $d|b$, there are d solutions.

Strategies to Find the solution

1. Reduce the equation by dividing both sides of the equation(including modulus) by d
2. Multiply both sides of the reduced equation by the multiplicative inverse of a to find the particular solution x_0.
3. The general solutions are $x = x_0 + k(n \mid d)$ for k =0,1,.....(d – 1)

Single-Variable Linear Equations

Example 1

$10x \equiv 2 \pmod{15}$ → $ax \equiv b \pmod{n}$

a=10 ,b=2 ,n=15

gcd(a,n) = gcd(10,15) = 5 , so d=5

Check for b/d → 2/5 = Since 5 does not divide 2, solution does not exist

Single-Variable Linear Equations

Example 2

14 x ≡ 12 (mod 18) a x ≡ b (mod n)

a=14 ,b=12 ,n=18

Solution

$14x \equiv 12 \pmod{18} \rightarrow \quad 7x \equiv 6 \pmod{9} \quad \rightarrow \quad x \equiv 6\,(7^{-1}) \pmod{9}$

$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$

$x_1 = x_0 + 1 \times (18/2) = 15$

Step1:gcd(a,n) = gcd(14,18) = 2 , so d=2

Step2: Check for b/d → 12/2 = 6, solution does exist

Step3: Find d mod n → 2 mod 18 = 2, so two solution exist(i.e two values of x exist)

Single-Variable Linear Equations

Step4: Divide both sides by d, d=2

$$\frac{14}{2}x \equiv \frac{12}{2} \pmod{\frac{18}{2}}$$

→ $7x \equiv 6 \bmod 9$

Single-Variable Linear Equations

Step5: Multiply both the side by multiplicative inverse of a, a=7

$7x \equiv 6 \bmod 9$

$7 * 7^{-1}\ x \equiv 6 * 7^{-1} \bmod 9$

$x \equiv 6 * 7^{-1} \bmod 9$

$x \equiv 6 * 7^{-1} \bmod 9$

$x = 6 * 4 \bmod 9$

$x = 24 \bmod 9$

$x_0 = 6$

$7 (?) \bmod 9 = 1$
$7 (1) \bmod 9 = 7 \bmod 9 \neq 1$
$7 (2) \bmod 9 = 14 \bmod 9 \neq 1$
$7 (3) \bmod 9 = 21 \bmod 9 \neq 1$
$7 (4) \bmod 9 = 28 \bmod 9 = 1$
$7^{-1} = 4$

Single-Variable Linear Equations

Step6: Now to find the second value of x

$x_k = x_0 + k (n / d)$

$x_1 = 6 + 1 (18 / 2)$

$= 6 + 1 (9)$

$x_1 = 15$

7 (?) mod 9 = 1
7 (1) mod 9 = 7 mod 9 ≠1
7 (2) mod 9 = 14 mod 9 ≠1
7 (3) mod 9 = 21 mod 9 ≠1
7 (4) mod 9 = 28 mod 9 = 1
7^{-1} = 4

RAMAIAH Institute of Technology

Single-Variable Line

Solution

First we change the equation to the form $ax \equiv b \pmod{n}$. We add −4 (the additive inverse of 4) to both sides, which give $3x \equiv 2 \pmod{13}$. Because gcd (3, 13) = 1, the equation has only one solution, which is $x_0 = (2 \times 3^{-1}) \bmod 13 = 18 \bmod 13 = 5$. We can see that the answer satisfies the original equation: $3 \times 5 + 4 \equiv 6 \pmod{13}$.

Example 3

3 x + 4 ≡ 6 (mod 13) convert to a x ≡ b (mod n)

Add -4 to both sides, so 3x +4 -4 ≡ 6 -4 (mod 13) → 3x ≡ 2 mod 13

a=3 ,b=2 ,n=13

Step1:gcd(a,n) = gcd(3,13) = 1 , so d=1

Step2: Check for b/d → 2/1 = 1, solution does exist

Step3: Find d mod n → 1 mod 13 =1, so one solution exist(i.e one values of x exist)

Single-Variable Linear Equations

Step4: Divide both sides by d, d=1

$$\underset{1}{3x} \equiv \underset{1}{2} \pmod{\underset{1}{13}}$$

→ $3x \equiv 2 \bmod 13$

Single-Variable Linear Equations

Step5: Multiply both the side by multiplicative inverse of a, a=3

$3x \equiv 2 \bmod 13$

$3 * 3^{-1}\ x \equiv 2 * 3^{-1} \bmod 13$

$x \equiv 2 * 3^{-1} \bmod 13$

$x \equiv 2 * (9) \bmod 13$

$x = 18 \bmod 13$

$x_0 = 5$

$3 (?) \bmod 13 = 1$
$3 (1) \bmod 13 = 6 \bmod 13 \neq 1$
$3 (2) \bmod 13 = 9 \bmod 13 \neq 1$
$3 (3) \bmod 13 = 12 \bmod 13 \neq 1$
$3 (4) \bmod 13 = 15 \bmod 13 \neq 1$
.
.
.
.
$3 (9) \bmod 13 = 27 \bmod 13 = 1$

$3^{-1} = 9$

Single-Variable Linear Equations

Solve the linear equation:

i. $3x + 5 = 4 (\text{mod } 5)$

ii. $9x + 4 = 12 (\text{mod } 7)$

Set of Linear Equations

We can also have set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible.

We make three matrices

1. Square matrix is made from the coefficients of variables
2. Column matrix is made from the variables
3. Column matrix made from the values at the RHS of the congruence operator

RAMAIAH
Institute of Technology

Set of Linear Equations

We can interpret the set of equations as matrix multiplication.

If both sides of congruence are multiplied by the multiplicative inverse of the first matrix , the result is variable matrix at the right hand side, which means the problem can be solved by a matrix multiplication as shown in figure.

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &\equiv b_1 \\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &\equiv b_2 \\
\vdots \quad\quad \vdots \quad\quad\quad\quad \vdots \quad\quad &\vdots \\
a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n &\equiv b_n
\end{aligned}
$$

a. Equations

$$
\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}
\equiv
\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

b. Interpretation

$$
\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}
\equiv
\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}^{-1}
\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}
$$

c. Solution

Use extended Euclidean algorithm to find GCD of a= 290, b= 75.

Using Euclidean Algorithm, Solve for GCD of the following pair of integers 1760 and 2740.

How is GCD calculated with Euclid's algorithm? Calculate the GCD of (270, 192).

Find particular and general solution for the following linear equation

$9x+4 \equiv 12 \pmod 7$

$25x+10y=15.$

$4x+6 \equiv 4 \pmod 6$

$3x + 5 = 4 \pmod 5$

$9x + 4 = 12 \pmod 7$

THANK YOU