Introduction to Cryptography and Network Security

The term is derived from the Greek word *kryptos*, which means hidden.
Cryptography is the *study of secure communications techniques* that allow only the sender and intended recipient of a message to view its contents.

- **Cryptography is the science of writing in secret code so that no other person except the intended recipient could read**

NETWORK SECURITY

Network Security consists of the *provisions and policies* adapted by network Administrator to *prevent and monitor* unauthorized access, misuse, modification, or denial of a computer network and network-accessible-resources

Cryptography is the practice and study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of attackers or outside people and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Applications of cryptography include ATM cards, computer passwords.

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols that prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security. Secure Communication refers to the scenario where the message or data shared between two parties can't be accessed by an adversary. In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security. PAIN principles are Privacy, Integrity, Authentication and Non-repudiation are core principles of modern-day cryptography.

Privacy refers to certain rules and guidelines usually executed under confidentiality agreements which ensure that the information is restricted to certain people or places.

Integrity refers to maintaining and making sure that the data stays accurate and consistent over its entire life cycle.

Authentication is the process of making sure that the piece of data being claimed by the user belongs to it.

Non-repudiation refers to the ability to make sure that a person or a party associated with a contract

or a communication cannot deny the authenticity of their signature over their document or the sending of a message.

Encryption and Decryption:

Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel. So, what happens is as follows. The sender's message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of received, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

For example:

Plaintext : hellongitkmec
Ciphertext : ifmmpohjulnfd

Types of Cryptography:

There are several types of cryptography, each with its own unique features and applications. Some of the most common types of cryptography include:

1. Symmetric-key cryptography: This type of cryptography involves the use of a single key to encrypt and decrypt data. Both the sender and receiver use the same key, which must be kept secret to maintain the security of the communication.

2. Asymmetric-key cryptography: Asymmetric-key cryptography, also known as public-key cryptography, uses a pair of keys – a public key and a private key – to encrypt and decrypt data. The public key is available to anyone, while the private key is kept secret by the owner.

Hash functions: A hash function is a mathematical algorithm that converts data of any size into a fixed-size output. Hash functions are often used to verify the integrity of data and ensure that it has not been tampered with.

Applications of Cryptography:

Cryptography has a wide range of applications in modern-day communication, including:

Secure online transactions: Cryptography is used to secure online transactions, such as online banking and e-commerce, by encrypting sensitive data and protecting it from unauthorized access.
Digital signatures: Digital signatures are used to verify the authenticity and integrity of digital documents and ensure that they have not been tampered with.
Password protection: Passwords are often encrypted using cryptographic algorithms to protect them from being stolen or intercepted.
Military and intelligence applications: Cryptography is widely used in military and intelligence applications to protect classified information and communications.

Challenges of Cryptography:
While cryptography is a powerful tool for securing information, it also presents several challenges, including:

Key management: Cryptography relies on the use of keys, which must be managed carefully to maintain the security of the communication.

Along with these there are many challenges as listed below:

Not simple – easy to get it wrong
must consider potential attacks
procedures used counter-intuitive
involve algorithms and secret information
must decide where to deploy mechanisms
battle of wits between attacker / admin
not perceived to be of benefit until it fails
requires regular monitoring : a process, not an event

Security Principles are P A I N

1. **Privacy/Confidentiality:**

   The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.

   For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. **Authentication / Availability**

   The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

   Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

3. **Integrity:**

   Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

- **System Integrity:** System Integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- **Data Integrity:** Data Integrity assures that information (both stored and in transmitted packets) and programs are changed only in a specified and authorized manner.

4. **Non-Repudiation:**

Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

The following categories are used to categorize ethical dilemmas in the security system.

Individuals' right to access personal information is referred to as privacy.

Property: It is concerned with the information's owner.

Accessibility is concerned with an organization's right to collect information.

Accuracy: It is concerned with the obligation of information authenticity, fidelity, and accuracy.

Security Goals

The security goals in cryptography and network security revolve around preserving data's confidentiality, integrity, and availability. These goals are achieved through encryption, access control, and IP security architecture in cryptography and network security to ensure data safety while it is in motion and stored.

The Main Goals of cryptography

- Data Confidentiality
- Data Integrity
- Data Availability

Confidentiality

- Confidentiality is most commonly addressed goal
- The meaning of a message is concealed by encoding it
- The sender encrypts the message using a cryptographic key
- The recipient decrypts the message using a cryptographic key that may or may not be the same as the one used by the sender

Data Integrity

- Integrity Ensures that the message received is the same as the message that was sent
- Uses hashing to create a unique message digest from the message that is sent along with the message
- Recipient uses the same technique to create a second digest from the message to compare to the original one
- This technique only protects against unintentional alteration of the message
- A variation is used to create digital signatures to protect against malicious alteration

Data Availabilty

Availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

What are Security Attacks?

A vulnerable application could subject people and systems to several kinds of harm. An attack occurs when a malevolent actor takes advantage of security flaws or vulnerabilities to harm others. In this article, we'll examine various attack methods, so that you'll know what to watch out for when safeguarding your application.

Accessing of data by unauthorized entity is called as attack
Passive Attacks
ActiveAttacks

PassiveAttacks:
Inapassiveattack,theattacker'sgoalisjusttoobtaininformation.Thismeansthattheattackdoesnot modify data or harm the system. Active Attacks:
Anactiveattackmaychangethedataorharmthesystem.Attacksthatthreatentheintegrityandavailability are active attacks.

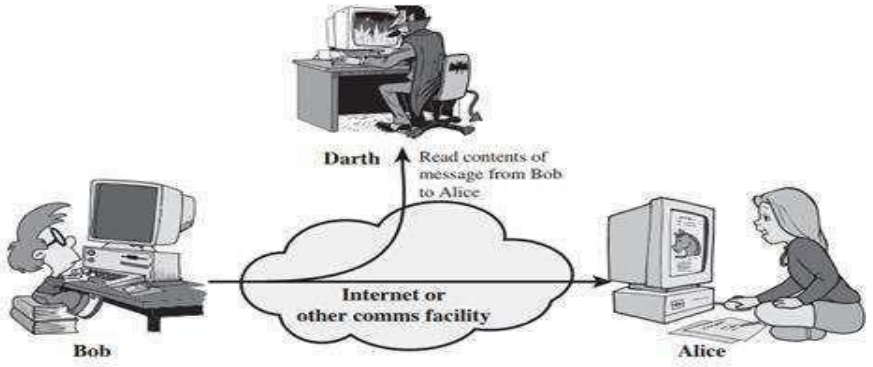
- Passive attacks
  - Interception
    - Release of message contents
    - Traffic analysis
- Active attacks
  - Interruption, modification, fabrication
    - Masquerade
    - Replay
    - Modification
    - Denial of service

PassiveAttacks

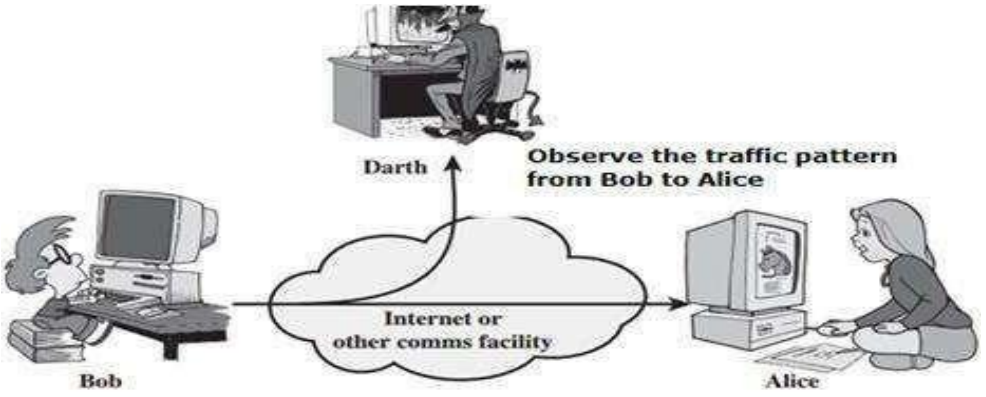
(a) Releaseofmessagecontent–
Captureandreadthecontenttransmissions.

(b) TrafficAnalysis–

- can'treadtheinformation,butobservethepattern
- determinethelocationandidentityofcommunicatingparties
- observefrequencyandlengthofcommunication



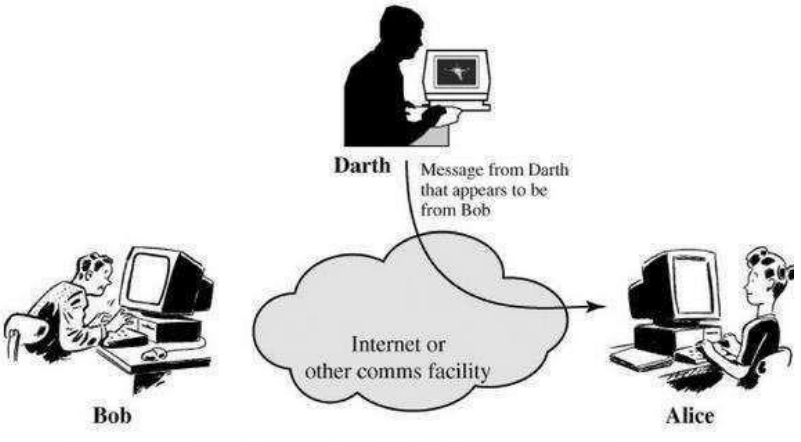
(a) Release of Message content



(b) Traffic Analysis

ActiveAttacks

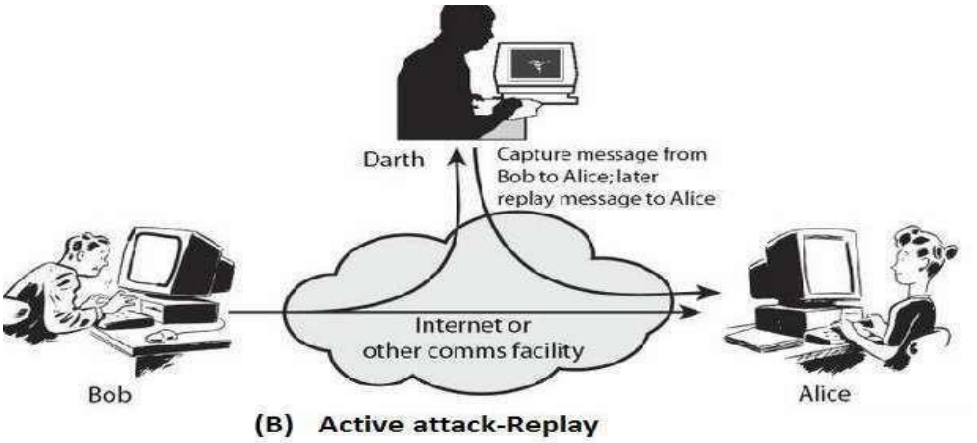
(a) Masquerading:Masqueradingorsnoopinghappenswhentheattackerimpersonatessomebodyelse.



Active Attack – Masquerade

(b) Replay–

Theattackerobtainsacopyofamessagesentbyauserandlatertriestoreplayit.

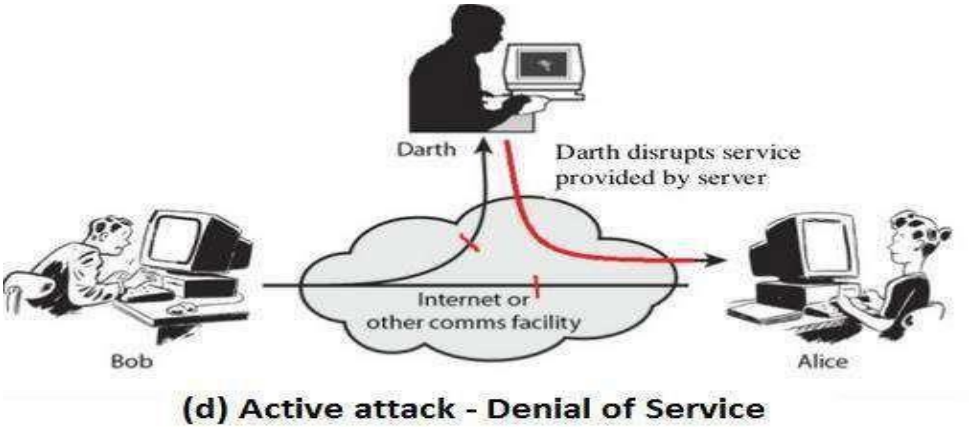


(B) Active attack-Replay

(c) Modification:Afterinterceptingor accessing information, the attackermodifies the informationthen send to receiver.

Active Attack – Modification of messages

(d) Denialof service: Denialofservice (Dos)is averycommonattack.itmayslowdownortotally interrupt the service of a system.



(d) Active attack - Denial of Service

Cryptographic Attacks Categories

Cryptographicattackscanbebroadlycategorizedintotwodistincttypes:

- Cryptanalytic
- Non-Cryptanalytic Cryptanalytic Attacks:
- These attacks arecombinationsofstatistical and algebraic techniquesaimedat discover thesecret key of a cipher.

- The attacker thus guesses the key and looksforthedistinguishingproperty.if the property is detected,theguessiscorrectotherwisethenextguessistried.

Non-CryptanalyticAttacks:

- The other types of attacks arenon-cryptanalytic attacks,whichdonotexplain themathematical weakness of the cryptographic algorithm.

Summary:

Types of Security Attacks

Cyber security attacks can be of the following two types:

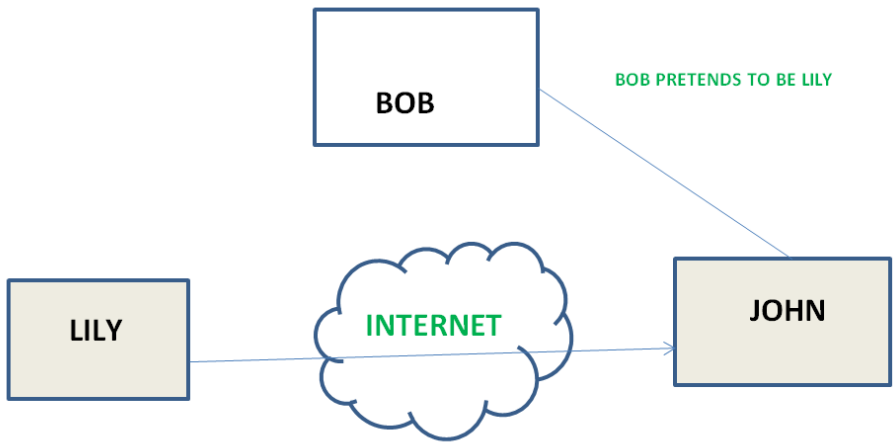
- Active attacks
- Passive attacks

1. Active Attacks

An active assault tries to change system resources or interfere with their functionality. Active attacks entail some form of data stream manipulation or false statement generation. Active attacks can take the following forms:

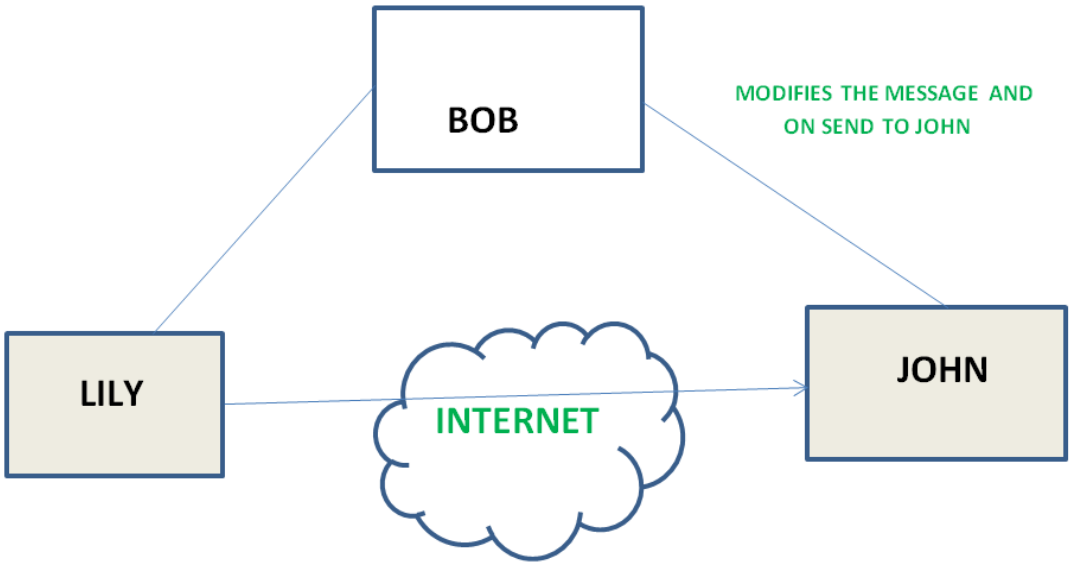
1.1. Masquerade

When one entity impersonates another, it commits a masquerade attack. One of the other active attack types is included in a masquerade attack. An authorisation process can become extremely vulnerable to a disguised attack if it isn't always completely safeguarded. Masquerade attacks can be carried out via stolen logins and passwords, by spotting holes in programmes, or by figuring out a way to get around the authentication procedure.



1.2. Modification of Messages

Modification denotes that a communication has been delayed, reordered, or had a piece of it changed to achieve an unlawful effect. Modification compromises the accuracy of the source data. In essence, it indicates that unauthorised individuals not only access data but also spoof it by initiating denial-of-service attacks, such as modifying sent data packets or flooding the network with false data. An assault on authentication is manufacturing. A notification that originally said, “Allow JOHN to view confidential file X,” for instance, is changed to say, “Allow Smith to read confidential file X.”

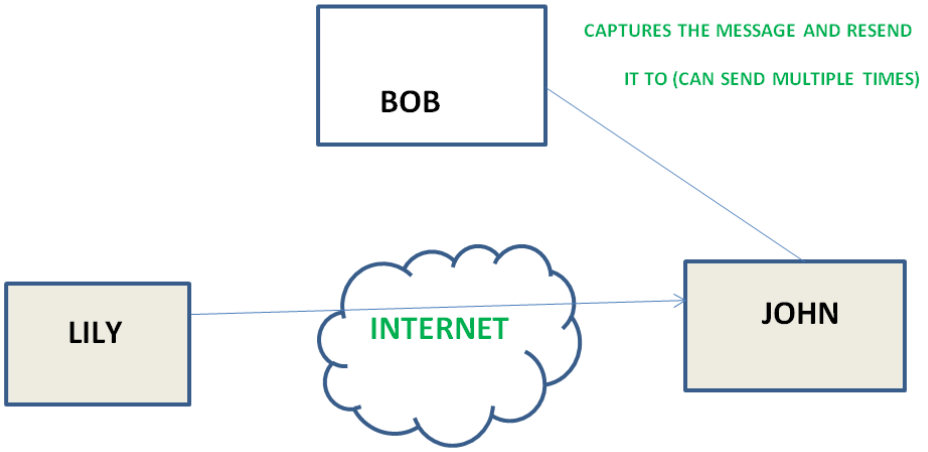


1.3. Repudiation

This attack happens when the login control gets tampered with or the network is not totally secure. With this attack, the author’s information can be altered by malicious user actions in order to save fake data in log files, up to the broad alteration of data on behalf of others, comparable to the spoofing of email messages.

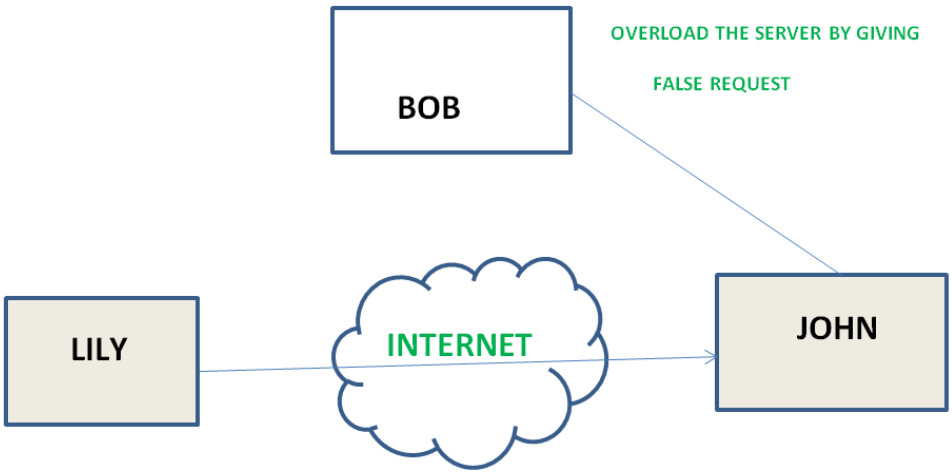
1.4. Replay

When the network is not completely secure or the login control is tampered with, an attack occurs. With this attack, the information of the author can be changed by malicious user actions to save suspicious data in log files, up to the widespread alteration of data on behalf of others, similar to the spoofing of email messages.



1.5. Denial of Service

Denial of service hinders the regular use of communication infrastructure. There may be a specified target for this attack. An entity might, for instance, suppress all messages sent to a specific location. Another example of service denial is when an entire network is disrupted, either by network disablement or message overload that lowers performance.

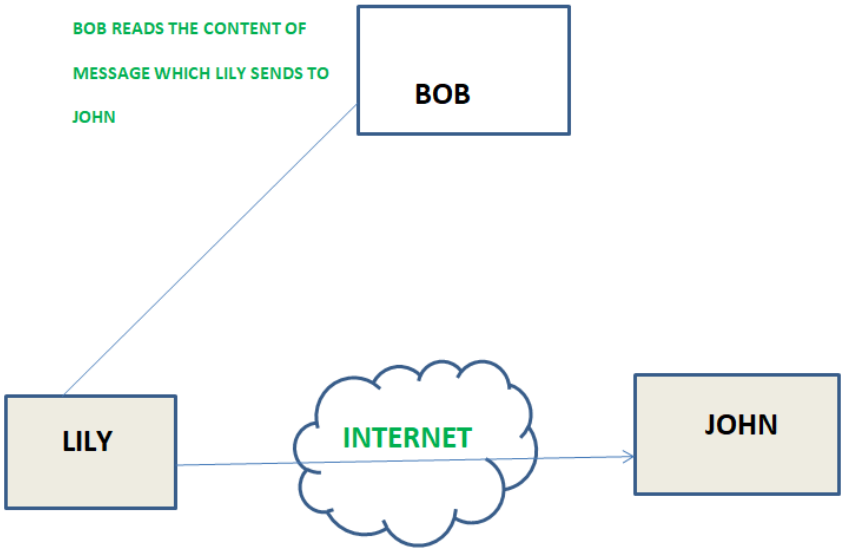


2. Passive Attacks

A passive attack does not eat up system resources and instead makes an effort to gather or use information from the system. Attacks that are passive in nature spy on or keep track of transmission. The adversary wants to intercept the transmission of information in order to collect it. The following are examples of passive attacks:

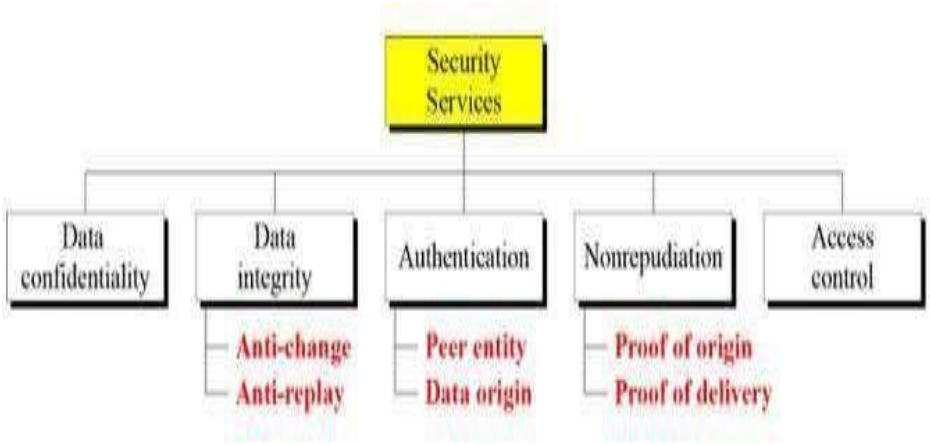
2.1. Releasing Message Content

Sensitive or confidential information may be present in a telephone conversation, an email, or a transmitted file. We want to keep an adversary from finding out what is being transmitted. In this type of passive attack, the information transmitted from one person to another gets into the hands of a third person/hacker. It jeopardises the confidentiality factor in a conversation.



SECURITY SERVICES

It is a processing or communication service that is provided by a system to give a specific kind of production to system resources. Security services implement security policies and are implemented by security mechanisms.



Confidentiality

Confidentiality is the protection of transmitted data from passive attacks. It is used to prevent the disclosure of information to unauthorized individuals or systems. It has been defined as "ensuring that information is accessible only to those authorized to have access".

The other aspect of confidentiality is the protection of traffic flow from analysis. **Ex:** A credit card number has to be secured during online transaction.

Authentication

This service assures that a communication is authentic. For a single message transmission, its function is to assure the recipient that the message is from intended source. For an ongoing interaction two aspects are involved. First, during connection initiation the service assures the authenticity of both parties. Second, the connection between the two hosts is not interfered allowing a third party to masquerade as one of the two parties. Two specific authentication services defines in X.800 are

Peer entity authentication: Verifies the identities of the peer entities involved in communication. Provides use at time of Mediaconnectionestblishment and during data transmission. Provides confidence against a masquera or replay attack

Data origin authentication: Assumes the authenticity of source of data unit, but does not provide protection against duplication or modification of data units. Supports applications like electronic mail, where no prior interactions take place between communicating entities.

Integrity

Integrity means that data cannot be modified without authorization. Like confidentiality, it can be applied to a stream of messages, a single message or selected fields within a message. Two t pes of integrity services are available. They are

Connection-Oriented Integrity Service: This service deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering or replays. Destruction of data is also covered here. Hence, it attends to both message stream modification and denial of service.

Connectionless-Oriented Integrity Service: It deals with individual messages regardless of larger context, providing protection against message modification only.

An integrity service can be applied with or without recovery. Because it is related to active attacks, major concern will be detection rather than prevention. If a violation is detected and the service reports it, either human intervention or automated recovery machines are required to recover.

Non-repudiation

Non-repudiation prevents either sender or receiver from denying a transmitted message. This capability is crucial to e-commerce. Without it an individual or entity can deny that he, she or it is responsible for a transaction, therefore not financially liable.

Access Control

This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. It is the ability to limit and control the access to host systems and applications via communication links. For this, each entity trying to gain access must first be identified or authenticated, so that access rights can be tailored to the individuals.

Availability

It is defined to be the property of a systemMediaorasystemresource being accessible and usable upon demand by an authorized system entity. The v ilability can significantly be affected by a variety of attacks, some amenable to automated counter measures i.e authentication and encryption and others need some sort of physical action to prevent or recover from loss of availability of elements of distributed system.

SECURITY MECHANISMS

According to X.800, the sec rity mechanisms are divided into those implemented in a specific protocol layer and those that are not specific to any particular protocol layer or security service. X.800 also differentiates reversible & irreversible encipherment mechanisms. A reversible encipherment mechanism is simply an encryption algorithm that allows data to be encrypted and subsequently decrypted, whereas irreversible encipherment include hash algorithms and message authentication codes used in digital signature and message authentication applications

Specific Security Mechanisms

Incorporated into the appropriate protocol layer in order to provide some of the OSI security services,

Encipherment: It refers to the process of applying mathematical algorithms for converting data into a form that is not intelligible. This depends on algorithm used and

encryption keys.

Digital Signature: The appended data or a cryptographic transformation applied to any data unit allowing to prove the source and integrity of the data unit and protect against forgery.

Access Control: A variety of techniques used for enforcing access permissions to the system resources.

Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

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

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

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

Notarization: The use of a trusted third party to assure cert in properties of a data exchange

Pervasive Security Mechanisms

These are not specific to any particular OSI security s rvice or protocol layer.

Trusted Functionality: That which is perceived to b correct with respect to some criteria

Security Level: The marking bound to a re ource (which may be a data unit) that names or designates the security attrib tes of that resource.

Event Detection: It is the process of detecting all the events related to network security.

Security Audit Trail: Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities. **Security Recovery:** It deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Relationship between Security services and mechanisms

Services	Mechanisms
Confidentiality	Encryption, routing control
Integrity	Digital Signature, Encryption
Authentication	Encryption, Digital Signature
Non-repudiation	Digital Signature, Notarization
Access Control	Interactive Proofs, access control mechanisms and policies.

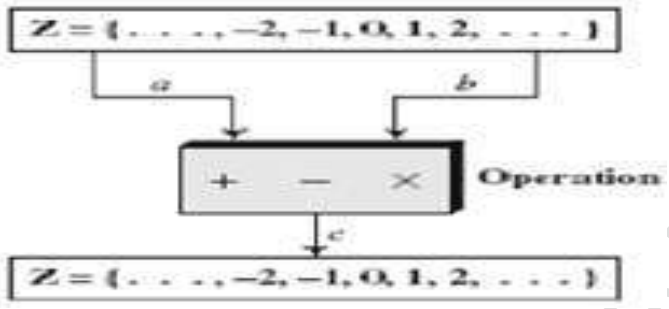
MATHEMATICSOFCRYPTOGRAPHY

Integer Arithmetic: In Integer arithmetic,we are use a set and a few operations.

➢ Set of Integers: The set of Integers, denoted by z, contains all integral numbers (with no fraction) from negative infinity to positive infinity.

Fig. 2.1 *The set of integers*

➢ Binary Operations: A Binary operation takes two inputs and creates one output. Three common binary operations defined for integers are addition, subtraction and multiplication.



➢ Examples:

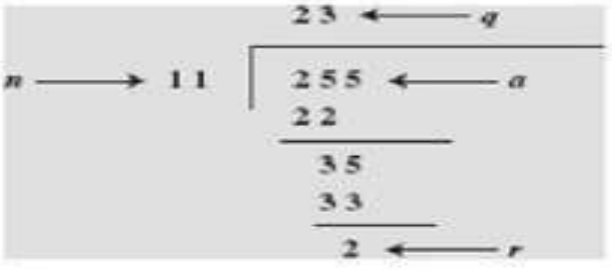
Add:	5+9=14	(-5)+9=4	5+(-9)=-4
Subtract:	5-9=-4	(-5)-9=14	5-(-9)=14
Multiply:	5x9=45	(-5)x9=-45	5x(-9)=45

Integer Division: if we divide a by n, we can get q and r. The relationship between these four integers can be shown as

a=q x n + r

a is dividend, n is the divisor, q is quotient, r is remainder

➢ Examples:Assume that a= 255 and n = 11.We can find q = 23 and r = 2 using the division algorithm. We have shown in following

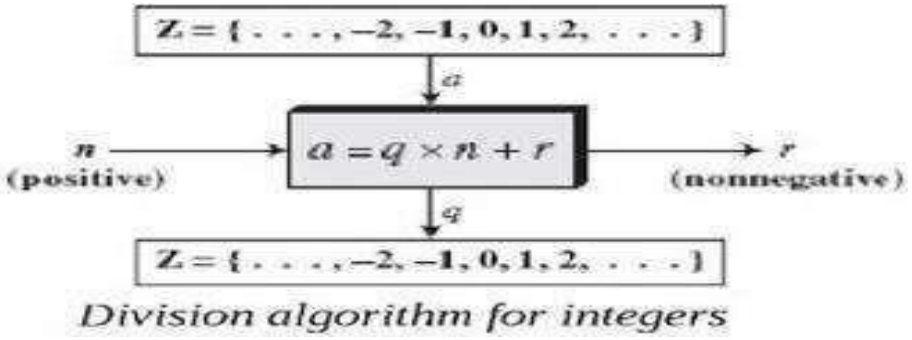


finding the quotient and the remainder

Two Restrictions:

- First, we require that the divisor be a positive integer(n>0).
- Second, we require that the remainder be a non-negative integer(r≥0).

Integer Division



Division algorithm for integers

Examples: Assume r and q are negative when 'a' is negative.

- To make r positive, decrement q by 1 and add value of n to r
- Consider -255=(-23x11)+(-2)↔-255=(-24x11)+9
- We have decremented -23 to -24 and added 11 to -2 to make 9. The relation is still valid

Divisibility:

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

We then say that n divides a (or n is a divisor of a). We can also say that a is divisible by n. The above is n | a .

If the remainder is not zero, then n does not divide a and we can write the relationship as a + n.

- Ex: The integer 4 divides the integer 32 because 32 = 8 x 4. We show this is as 4 |32
- The number 8 does not divide the number 42 because 42=5x8+2. There is a remainder, the number 2, in the equation. We show this as 8+42.

Examples:

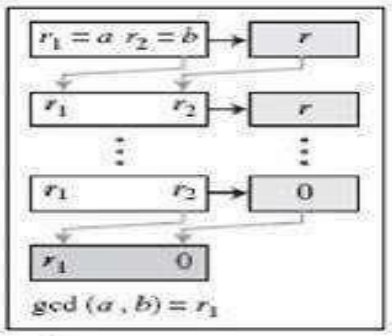
1) Since3|15and15|45,accordingtothirdproperty,3|45
2) Since3| 15and3| 9,accordingtothefourthproperty,3|(15x2+9x4),whichmeans3|66.

Greatest Common Divisor(GCD)

The greatest common divisoroftwopositiveintegersisthelargestintegerthatcandividebothintegerswe can write the relationship as a + n.

Examples: GCD of 15 and 20 is 2 because divisors of 15 are 3,5 and divisors of 20 are 2,4,5,10.The GCD is 5

- Euclidean algorithm is used to finding the greatest common divisor (gcd)of two positive integers. The Euclidean algorithm is based on the following two facts
  - Fact1:gcd(a,0)=a
  - Fact2:gcd(a,b)=gcd(b,r),where r is the remainder of dividing a by b
  - When gcd(a,b)=1,we say that a and b are relatively prime.



a. Process

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

b. Algorithm

-

Example:gcd(36,10)=?

```
gcd (36, 10) = gcd (10, 6) = gcd (6, 4) = gcd (4, 2) = gcd (2, 0) = 2
```

Example:gcd(2740,1760)=?

*Solution:*we initialize r_1 to 2740 and r_2 to1760 Answer:

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	

ModularArithmetic

The division relationship (a=qxn+r) has two inputs (a and n) and two outputs(q and r).

Modulo Operator:

- Modulo operator is shown as *mod*.

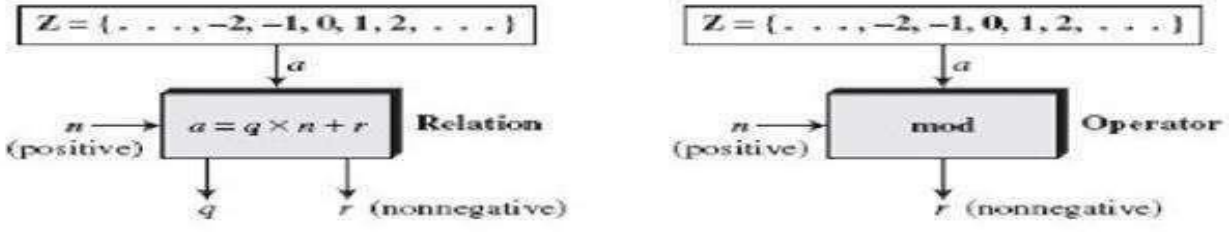


Fig. : *Division relation and modulo operator*

The modulo operator (mod) takes an integer (a) from these t Z and a positive modulus(n). The operator creates a non-negative residue (r).

A mod n=r

CONGRUENCE(≡)

If two numbers A and B have the property that their difference A-B is integrally divisible by a number-C

(i.e.,(A-B)/C is an integer), then A and B are said to be "congruent modulo C. "The number C is called the modulus, and the statement "A is congruent to B(moduloC)" is written mathematically as

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

This says that "A is congruent to B modulo C".

Examining the expression closer:

1. ≡ is the symbol for congruence, which means the values A and B are in the same **equivalence class**.
2. (mod C) tells us what **operation** we applied to A and B.
3. when we have both of these, we call "≡" **congruence modulo** C.

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

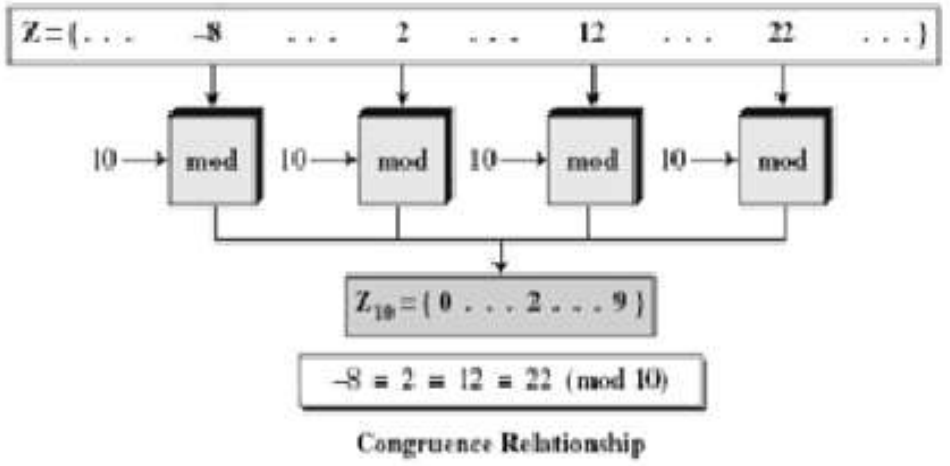
$26 \bmod 5 = 1$ so it is in the equivalence class for 1,

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

So, 26 is congruent to 11 modulo 5

Example2:

Assume,-8≡12(mod10) 2≡12(mod10) 12≡22(mod10) 22≡32(mod10)



Congruence Relationship

RESIDUE CLASSES

A residue class[a] is the set of integers congruent modulo n. In other words it is the set of all integers such that x=a(mod n).

For example, if n=5,we have five sets[0],[1],[2],[3],[4] as shown below

[0]= {....., -15 -10 ,-5,0, 5,10,15,...}
[1]= {....., -16 -11 ,-6,1, 6,11,16,...}
[2]= {....., -17 -12 ,-7,2, 7,12,17,...}
[3]= {....., -18 -13 ,-8,3, 8,13,18,...}
[4]= {....., -19 -14 ,-9,4, 9,14,19,...}

0 in [0], 1 in [1], 2 in [2], 3 in[3] and 4 in [4].. The set of these residues are shown as

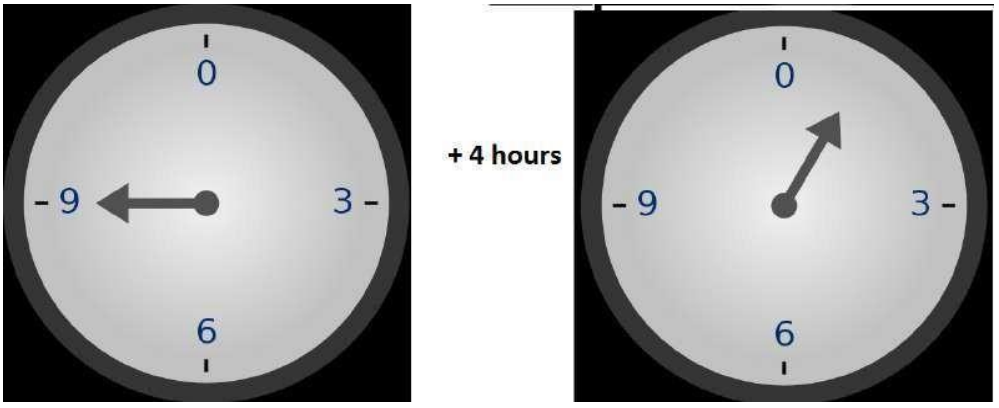
Z_5={0,1,2,3,4}

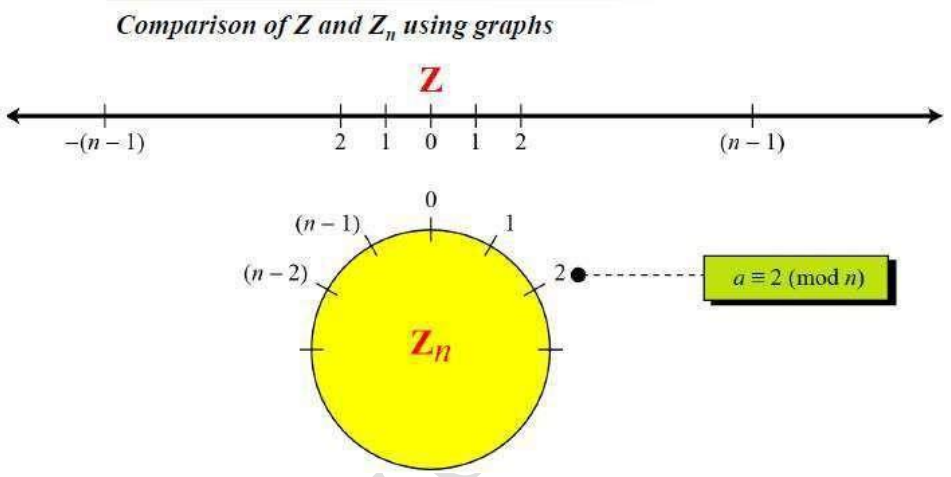
Applications:

We use a clock to measure time. Our clock system uses modulo 12 arithmetic. However instead of

a 0 we the 12

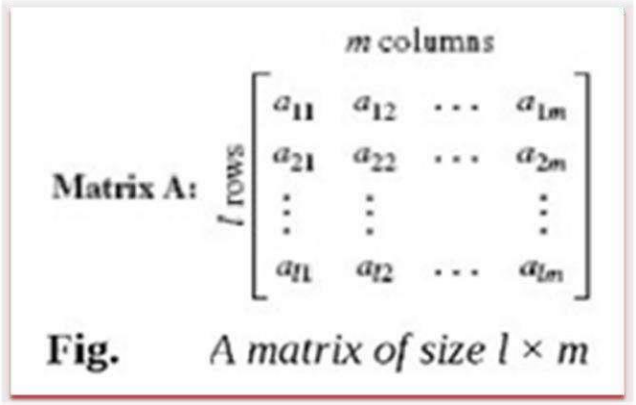
.





MATRICES

A matrix is a rectangular array of *lxm* elements; in which
L is the number of rows and
M is the number of columns.
A matrix is normally denoted with an Uppercase Letter such as A. The element a_{ij} is located in the ith row and jth column.



DIFFERENT TYPES OF MATRICES

$$\begin{bmatrix} 2 & 1 & 5 & 11 \end{bmatrix}$$
Row matrix

$$\begin{bmatrix} 2 \\ 4 \\ 12 \end{bmatrix}$$
Column matrix

$$\begin{bmatrix} 23 & 14 & 56 \\ 12 & 21 & 18 \\ 10 & 8 & 31 \end{bmatrix}$$
Square matrix

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$
0
Zero Matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
I
Identity Matrix

OPERATIONSANDRELATIONS

Relation operation: Equality:

If two matrices are equal sized and content is same then they have equality Four operations:

1. Addition
2. Subtraction
3. Multiplication
4. Scalar multiplication

Examples:

Addition:$C_{IJ}=A_{IJ}+B_{IJ}$

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

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

Subtraction::$C_{IJ}=A_{IJ}-B_{IJ}$

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

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

Multiplication

If each element of matrix **A** is called a_{ij}, each element of matrix **B** is called bj_k, then each element of matrix **C**, c_{ik}, can be calculated as

$$c_{ik} = \Sigma\, a_{ij} \times b_{jk} = a_{i1} \times b_{1j} + a_{i2} \times b_{2j} + \cdots + a_{im} \times b_{mj}$$

Examples:

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

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

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

❑ ***Scalar Multiplication*** We can also multiply a matrix by a number (called a **scalar**). If **A** is an $l \times m$ matrix and x is a scalar, $\mathbf{C} = x\mathbf{A}$ is a matrix of size $l \times m$, in which $c_{ij} = x \times a_{ij}$.

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

Multiplicationunitmatrixwithnormalmatrixgivesthesame matrix

AXI=IXA=A

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} x \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 1X2 + 0X3 & 1X4 + 0X1 \\ 0X2 + 1X3 & 0X4 + 1X1 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix}$$

DETERMINANT

IfAissquarematrixofmxmthendeterminantofAisdet(A)

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

Where$A_{ij}$is amatrix obtained fromAby deleting the ith rowand jth column. Determinant is obtainedfor onlysquarematrices

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

=5x4-2x3=14

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

Det(2x2) matrix

Example:det(3x3)matrix

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

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

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

$$+ (+1)\times 1\times (3)$$

$$= -25$$

MATRICES-Inverses

AdditiveInverse

Theadditive inverseof thematrixAisanothermatrixBsuch thatA+B=0. In other words $b_{ij}=-a_{ij}$
Generally additive inverse is of A=-A Multiplicative Inverse:
Themultiplicative Inverse of asquare matrix A is a B such thatAX B= I. NormallyMultiplicativeinverseofAisdefinedbyA^{-1}
Multiplicativeinverseisdefinedforonlysquarematrices

Linear Congruence

SinglevariableLinearEquations:
Equationsoftheformax≡b(modn)mighthavenosolutionoralimitednumberofsolutions
Assumethatthegcd(a,n)=d.
If d + b (d not divides b), there is no solution.If d | b (d divides b), there are d solutions.
Ifd|b,weusethefollowingstrategytofindthesolutions:

- Reducetheequationbydividingbothsidesoftheequation(includingthemodulus)byd.
- Multiplybothsides of the reducedequationbythemultiplicativeinverseof 'a' tofind theparticular solution x_0.
- The General solutions are $x = x_0 + k (n / d)$ for k = 0, 1, 2,, (d-1). Congruence-Example

Example1:Solvethe equation
10x=2(mod15).
Solution:-
Given Linear equation 10x≡ 2(mod15) In basic form ax ≡ b(mod n)
a=10;b=2;n=15
Now,findd=?
d=gcd(a,n)=gcd(10,15)
=gcd(15,10)=gcd(10,5)

=gcd(5,0)

=5

check if d+b (d not divides b), then no solution 5+2 means '5' not divides '2', so, The given equation has No solution.

Example2:Solvethe equation

14 x= 12 (mod 18) Solution :- Given Linear equation

14x ≡ 12(mod 18) In basic form ax ≡ b(mod n)

a=14;b=12;n=18

d=gcd(a,n)=gcd(14,18)=gcd(18,14)

= gcd (14,4) = gcd (4,2)=gcd(2,0)=2 check, d b or d+ b

d| b→ 2|12means"2divides12",sothegivenequationhave"2solutions".

Givenequation 14x12(mod18)

divides'd'onbothsidesofequation

7x6(mod9)

multiply7^{-1}onbothsidesofabovetogetparticularsolution'x_0'.

7^{-1}x 7*x_0≡6* 7^{-1} (mod9)

x_0≡6x7^{-1}(mod9) i.e7^{-1}mod9≡4

x_0≡6x4(mod9)

x_0≡ 24mod 9

x_0≡ 6

solutionsarex=x_0+k(n/d)wherek=0,1

(d=2)

if k = 0 x = x_0+ 0 (n/d) x = 6+ 0 (18/2) = 6

x=6

ifk=1 x=x_0+1((n/d)=6+1(18/2)

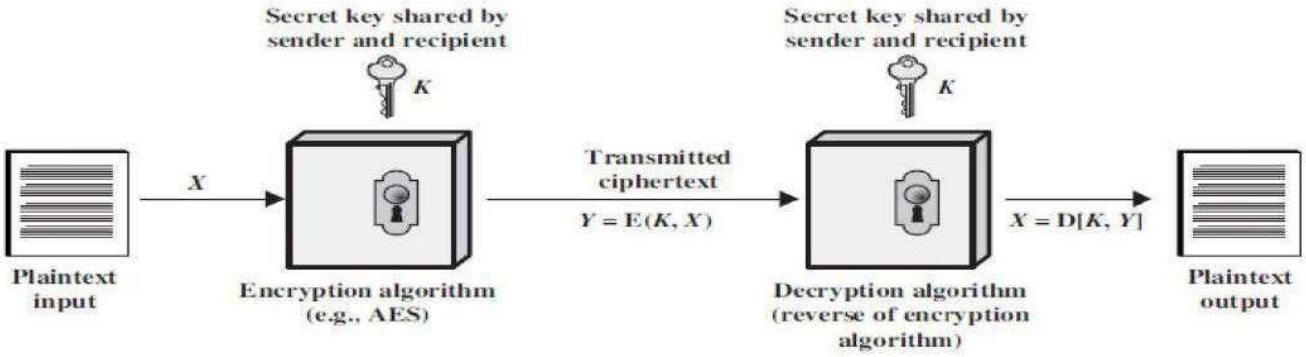
x=15

'6'and'15'aresolutionto14x12(mod18)

TERMINOLOGY

- Plain text-the original message
- Cipher text-the coded message
- Cipher-algorithm for transforming plaintext to cipher text
- Key-info used in cipher known only to sender/receiver
- Encipher(Encrypt)-converting plaintext to cipher text
- Decipher(Decrypt)-recovering plain text from cipher text
- Cryptography-study of encryption principles/methods
- Cryptanalysis(code breaking)-the study of principles/methods of deciphering cipher text w*ithout* knowing key
- Cryptology-the field of both cryptography and cryptanalysis

MODEL FOR NETWORK SECURITY



When we send our data from the source side to the destination side we have to use some transfer method like the internet or any other communication channel by which we are able to send our message. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. When the transfer of data happened from one source to another source some logical information channel is established between them by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. When we use the protocol for this logical information channel the main aspect of security has come. who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

1. A security-related transformation on the information to be sent.
2. Some secret information is shared by the two principals and, it is hoped, unknown to the opponent.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission. This model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of secret information.
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.