SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF COMPUTING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNIT-1 NETWORK SECURITY –SCS1316

I Network Security and Number Theory Basics

1.Introduction:

With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident. This is especially the case for a shared system, and the need is even more acute for systems that can be accessed over the Internet. The generic name for the collection of tools designed to protect data and to thwart hackers is **computer security**.

Network security: Introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer. Network security measures are needed to protect data during their transmission. The term network security in general refers to internet security.

1.1 EXAMPLES OF SECURITY VIOLATIONS

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

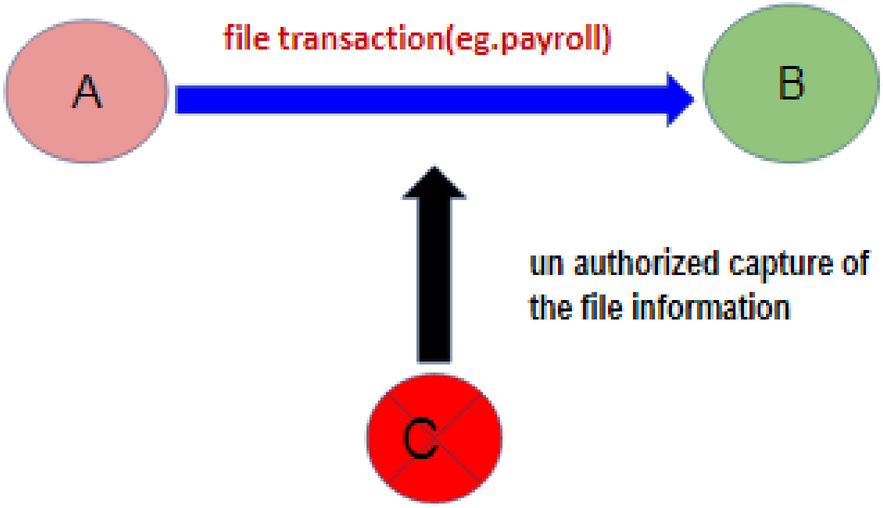


Fig 1.1 Example 1

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

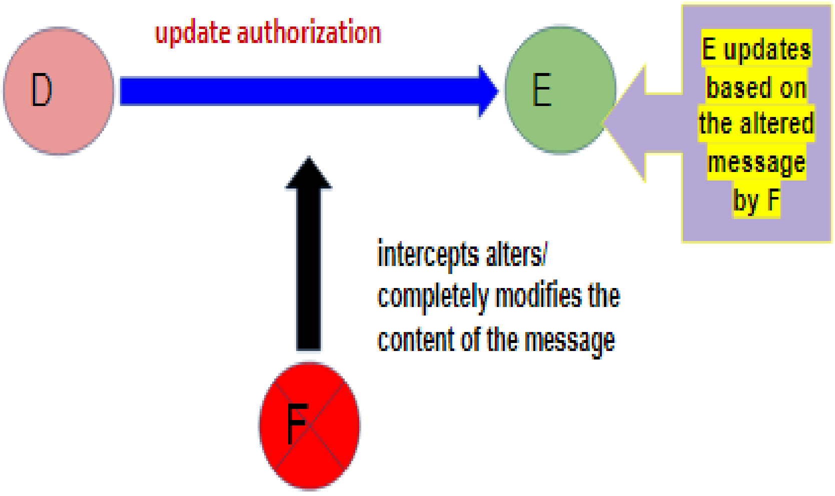

update authorization
D
E
E updates based on the altered message by F
intercepts alters/ completely modifies the content of the message
F

Fig 1.2 Example 2

3. Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

4. A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

Although this list by no means exhausts the possible types of security violations, it illustrates the range of concerns of network security.

1.2 COMPUTER SECURITY CONCEPTS

A Definition of Computer Security

The NIST *Computer Security Handbook* [NIST95] defines the term *computer security* as follows

1.2.1 COMPUTER SECURITY

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).

This definition introduces three key objectives that are at the heart of computer security.

1) **Confidentiality:** This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

2) **Integrity:** This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

3)Availability: Assures that systems work promptly and service is not denied to authorized users.

These three concepts form what is often referred to as the CIA triad (Figure 1.1). The three concepts embody the fundamental security objectives for both data and for information and computing services.

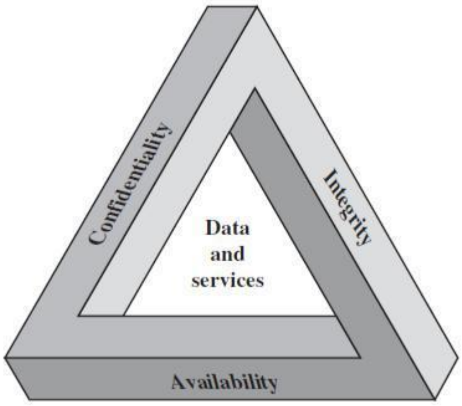


Figure 1.1 The Security Requirements Triad

• **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

• **Integrity:** Guarding against improper information modification or destruction,including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

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

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture. Two of the most commonly mentioned are,

• **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

• **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis

to trace security breaches or to aid in transaction disputes.

1.3 THE CHALLENGES OF COMPUTER SECURITY

Computer and network security is both fascinating and complex. Some of the reasons include:

1. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, non-repudiation, integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

3. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].

4. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information.

5. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

6. Security requires regular, even constant, monitoring, and this is difficult in today‟s short-term, overloaded environment.

7. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

8. Many users (and even security administrators) view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

1.4 VULNERABILITY AND HACKING

Vulnerability

In computer security, a vulnerability is a weakness which can be exploited by a threat actor, such as an attacker, to cross privilege boundaries (i.e. perform unauthorized actions) within a computer system. To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerabilities are also known as the attack surface.

Hacking

Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorised access to or control over computer network security systems for some illicit purpose. One can easily assume them to be intelligent and highly skilled in computers.

1.5 SECURITY ATTACKS

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.

Attack

An assault on system security that derives from an intelligent threat.That is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Security attack: Any action that compromises the security of information owned by an organization.

A useful means of classifying security attacks is in terms of passive attacks and active attacks.A passive attack attempts to learn or make use of information from the system but does not affect system resources.An active attack attempts to alter system resources or affect their operation.

Passive Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions as shown in Fig 1.4. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

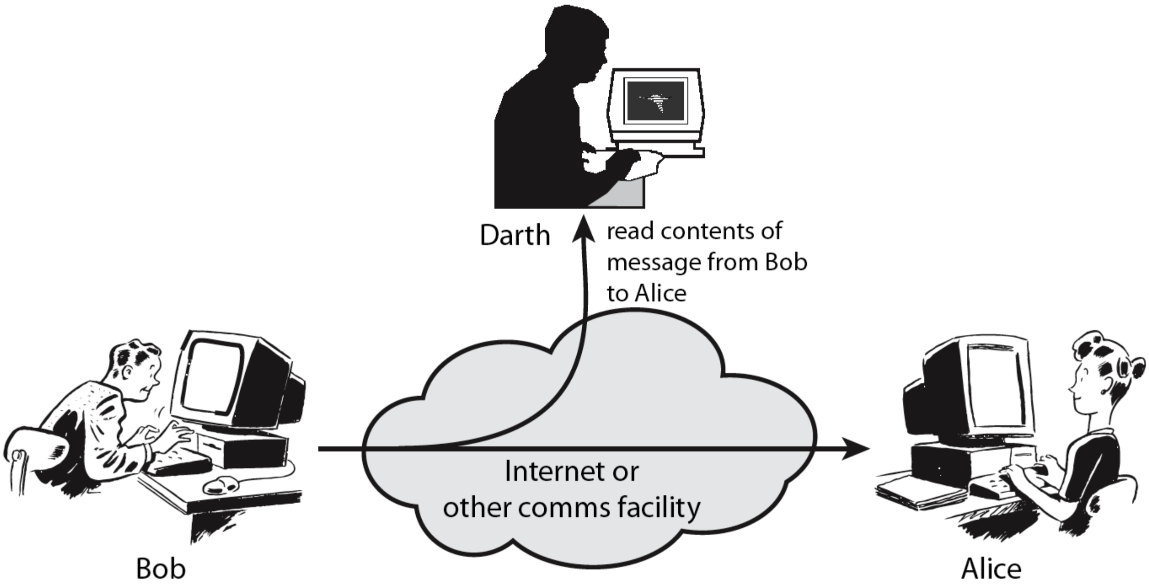

Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Fig 1.4 Passive Attacks

The release of message contents is easily understood (Figure 1.5). A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

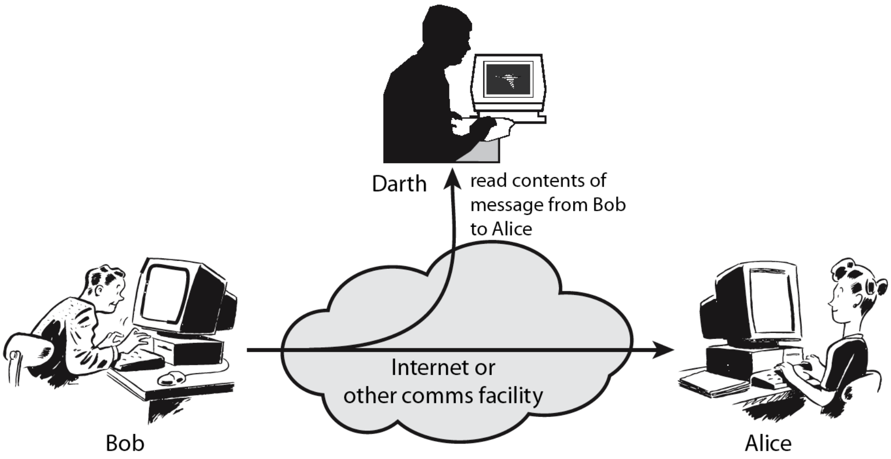
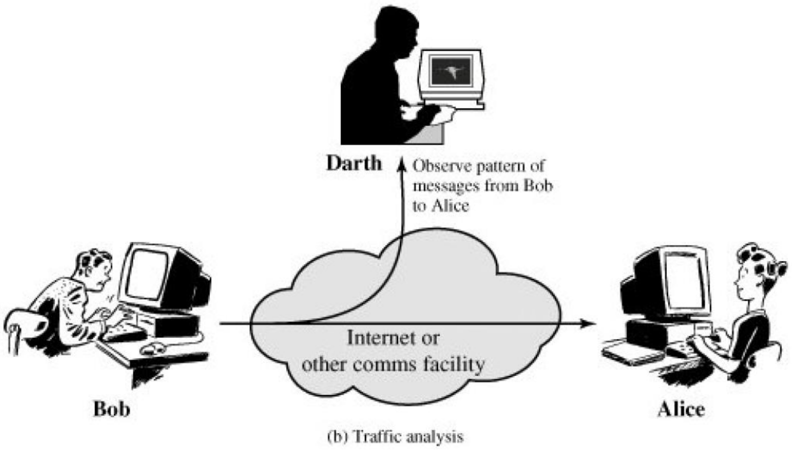


Fig 1.5 Release of Message

A second type of passive attack, traffic analysis, is subtler (Figure 1.6). Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption.



(b) Traffic analysis

Fig 1.6 Traffic analysis

Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor the receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A masquerade takes place when one entity pretends to be a different entity (Figure 1.7). A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 1.8).

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 (Figure 1.9). For example, a message meaning “Allow John

Smith to read confidential file accounts" is modified to mean "Allow Fred Brown to read confidential file accounts."

The denial of service prevents or inhibits the normal use or management of communications facilities (Figure 1.10). This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network—either by disabling the network or by overloading it with messages so as to degrade performance.

Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.All of the techniques for providing security have two components:

A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

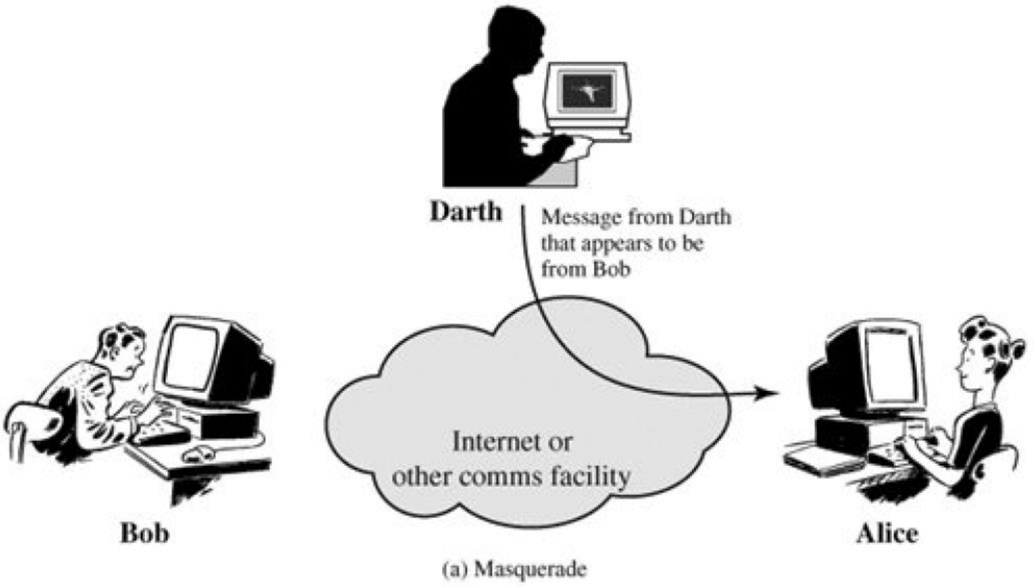

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice
(a) Masquerade

Fig 1.7 Masquerade

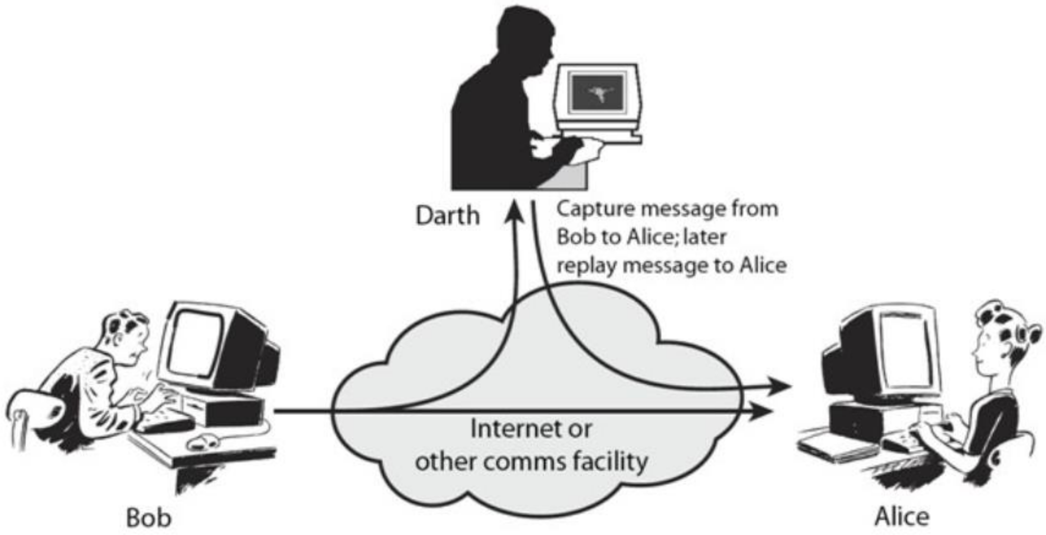

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Fig 1.8 Replay

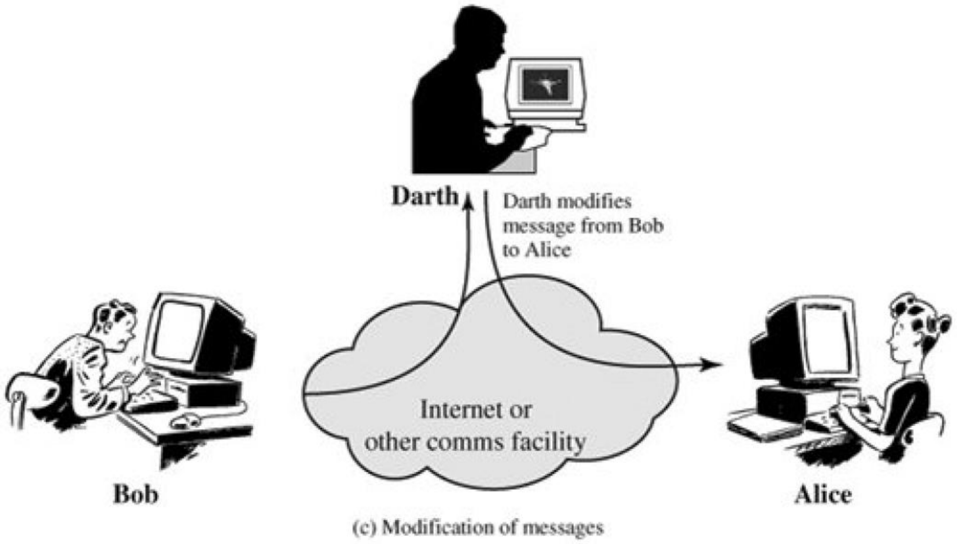

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice
(c) Modification of messages

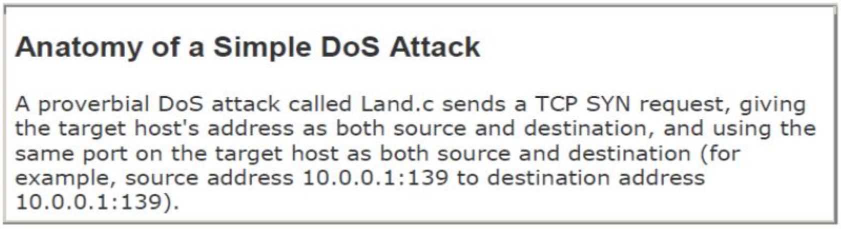
Fig 1.8 **Modification of messages**

Denial of Service Attacks

With a DoS attack, a hacker attempts to render a network or an Internet resource, such as a web server, worthless to users. A DoS attack typically achieves its goal by sending large amounts of repeated requests that paralyze the network or a server.

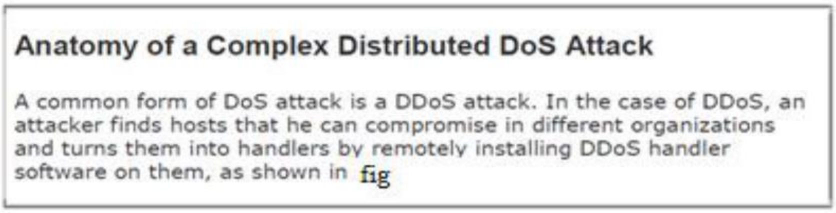
A common form of a DoS attack is a SYN flood, where the server is overwhelmed by embryonic connections. A hacker sends to a server countless Transmission Control Protocol (TCP) synchronization attempts known as SYN requests. The server answers each of those requests with a SYN ACK reply and allocates some of its computing resources to servicing this connection when it becomes a "full connection." Connections are said to be embryonic or half-opened until the originator completes the three-way handshake with an ACK for each request originated. A server that is inundated with half-opened connections soon runs out of resources to allocate to upcoming connection requests, thus the expression "denial of service attack."

The following sidebars provide the anatomy of DoS attacks and distributed DoS (DDoS) attacks.



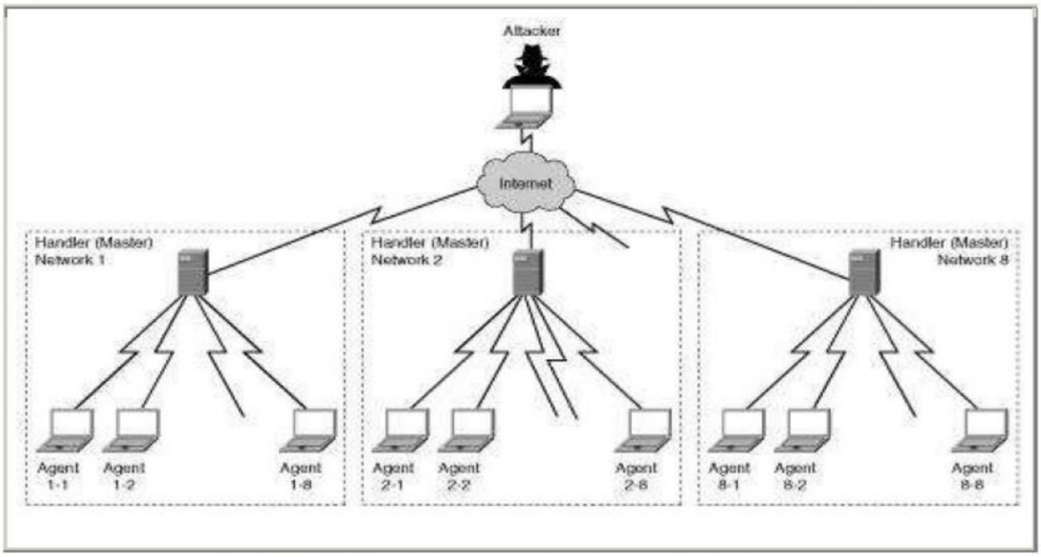
Anatomy of a Simple DoS Attack

A proverbial DoS attack called Land.c sends a TCP SYN request, giving the target host's address as both source and destination, and using the same port on the target host as both source and destination (for example, source address 10.0.0.1:139 to destination address 10.0.0.1:139).



Anatomy of a Complex Distributed DoS Attack

A common form of DoS attack is a DDoS attack. In the case of DDoS, an attacker finds hosts that he can compromise in different organizations and turns them into handlers by remotely installing DDoS handler software on them, as shown in fig



DDoSCreating an Army of Agents

Fig 1.9 DOS

Those handlers in turn scan their own corporate network, hunting for workstations to compromise and turn into DDoS agents. Those agents are also referred to as bots, thus the expression of botnets.

When his army of agents is strategically in place, the hacker launches the attack. He transmits his orders for the mission to the handlers and agents; these orders usually cause each of these hosts to send large quantities of packets to the same specific destination, at a precise time, thus overwhelming the victim and the path to it. It also creates significant congestion on corporate networks that are infected with handlers and agents when they all simultaneously launch their attack on the ultimate victim.

1.6 A MODEL FOR NETWORK SECURITY:

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

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

A logical route is defined through the network (Internet), from sender to the receiver and using the communication protocols both the sender and the receiver established communication.

Any security service would have the three components discussed below:

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the encryption of the message.

It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the secret information between sender and receiver of which the opponent must not any clue. Yes, we are talking of the encryption key which is used during the encryption of the message at the sender’s end and also during the decryption of message at receiver’s end.

3. There must be a trusted third party which should take the responsibility of distributing the secret information (key) to both the communicating parties and also prevent it from any opponent.

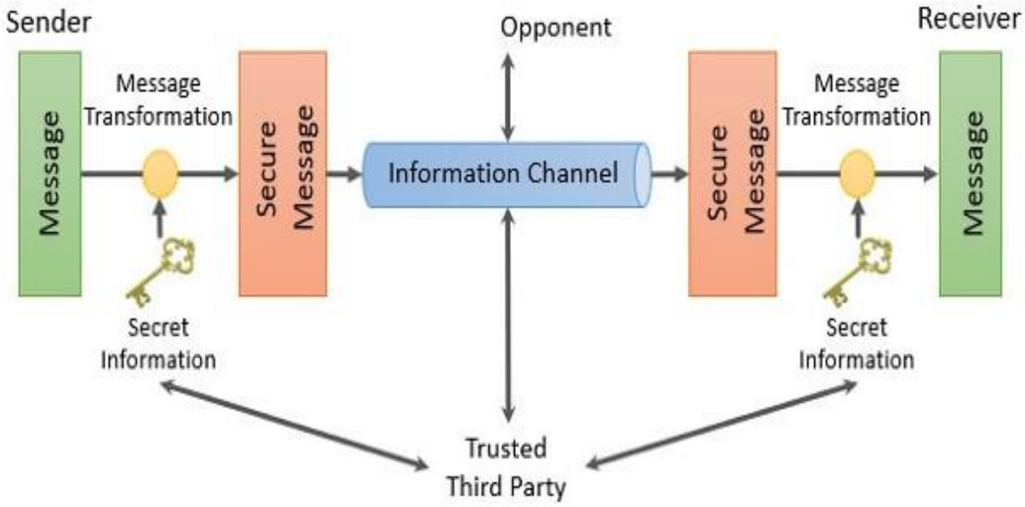


Fig 1.11 A Model For Network Security

The network security model presents the two communicating parties sender and receiver who mutually agrees to exchange the information. The sender has information to share with the receiver.

But sender cannot send the message on the information cannel in the readable form as it will have a threat of being attacked by the opponent. So, before sending the message through the information channel, it should be transformed into an unreadable format.

Secret information is used while transforming the message which will also be required when the message will be retransformed at the recipient side. That’s why a trusted third party is required which would take the responsibility of distributing this secret information to both the parties involved in communication.

So, considering this general model of network security, one must consider the following four tasks while designing the security model.

1. To transform a readable message at the sender side into an unreadable format, an appropriate algorithm should be designed such that it should be difficult for an opponent to crack that security algorithm.

2. Next, the network security model designer is concerned about the generation of the secret information which is known as a key. This secret information is used in conjunction with the security algorithm in order to transform the message.

3. Now, the secret information is required at both the ends, sender's end and receiver's end. At sender's end, it is used to encrypt or transform the message into unreadable form and at the receiver's end, it is used to decrypt or retransform the message into readable form. So, there must be a trusted third party who will distribute the secret information to both sender and receiver. While designing the network security model designer must also concentrate on developing the methods to distribute the key to the sender and receiver. An appropriate methodology must be used to deliver the secret information to the communicating parties without the interference of the opponent.

It is also taken care that the communication protocols that are used by the communicating parties should be supporting the security algorithm and the secret key in order to achieve the security service.

1.7 NETWORK ACCESS SECURITY MODEL

Network access security model which is designed to secure the information system which can be accessed by the attacker through the network.

Attackers who attack your system that is accessible through the internet. These attackers fall into two categories:

1. Hacker: The one who is only interested in penetrating into your system. They do not cause any harm to your system they only get satisfied by getting access to your system.

2. Intruders: These attackers intend to do damage to your system or try to obtain the information from the system which can be used to attain financial gain.

The attacker can place a logical program on your system through the network which can affect the software on your system. This leads to two kinds of risks:

a. Information threat: This kind of threats modifies data on the user's behalf to which actually user should not access. Like enabling some crucial permission in the system.

b. Service threat: This kind of threat disables the user from accessing data on the system.

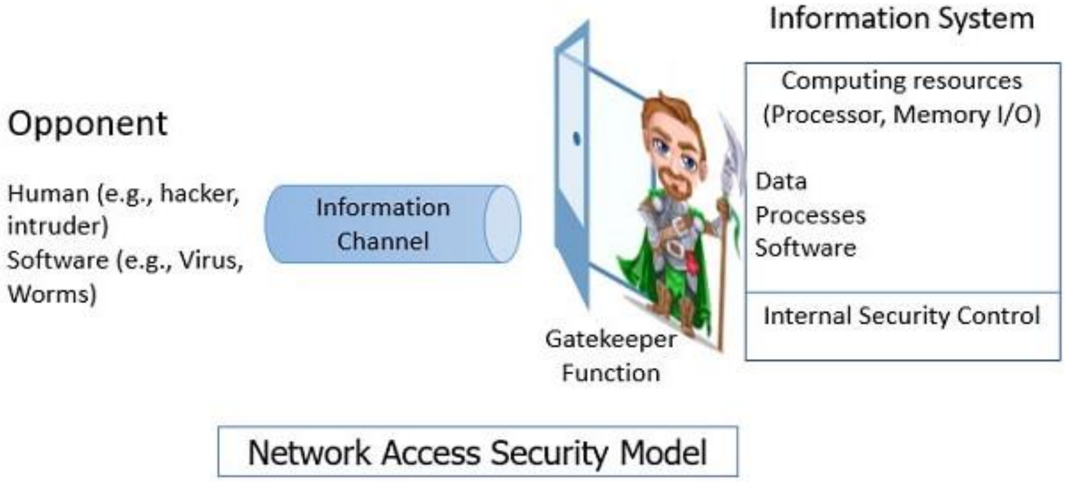


Fig 1.12 Network access security model

There are two ways to secure your system from attacker of which the first is to introduce the gatekeeper function. Introducing gatekeeper function means introducing login-id and passwords which would keep away the unwanted access.

In case the unwanted user gets access to the system the second way to secure your system is introducing internal control which would detect the unwanted user trying to access the system by analyzing system activities. This second method we call as antivirus which we install on our system to prevent the unwanted user from accessing your computer system through the internet.

1.8 MODULAR ARITHMETIC

Modulo, means remainder. Modulo arithmetic is the arithmetic of remainders.

If any integer a can be expressed as a = b+kn then in modulo arithmetic it can be stated as a mod n = b. F or example a=33 and n=5 then 33 mod 5= 3. (should be read as 3 mod 5)

This can be obtained by successive subtraction of n from a. In the above example the successive subtraction is as shown below.

1.8.1 The quotient remainder theorem

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

The quotient remainder theorem says:

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

$$\mathbf{A = B * Q + R \qquad where\ 0 \leq R < B}$$

When we divide A by B in long division, Q is the quotient and R is the remainder.

i.e A -DIVIDEND

B-DIVISOR /MODULUS

Q-QUOTIENT

R-REMINDER/ RESIDUE

If we can write a number in this form then A mod B = R

Examples

A = 7, B = 2

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

A = 8, **B = 4**

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

A = 13, **B = 5**

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

A = -16, **B = 26**

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

1.8.2 Modular addition and subtraction

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

Example:

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

Let's verify: **(A + B) mod C = (A mod C + B mod C) mod C**
LHS = Left Hand Side of the Equation
RHS = Right Hand Side of the Equation

LHS = (A + B) mod C
LHS = (**14 + 17**) mod 5
LHS = **31** mod 5
LHS = 1

RHS = (A mod C + B mod C) mod C
RHS = (**14 mod 5 + 17 mod 5**) mod 5
RHS = (**4 + 2**) mod 5
RHS = 1

LHS = RHS = 1

1.8.3 Multiplication

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

Example for Multiplication:

Let **A=4, B=7, C=6**

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

LHS= Left Hand Side of the Equation

RHS= Right Hand Side of the Equation

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

LHS = **(4 * 7)** mod 6

LHS = **28** mod 6

LHS = **4**

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

RHS = (**4 mod 6** * **7 mod 6**) mod 6

RHS = (**4 * 1**) mod 6

RHS = **4 mod 6**

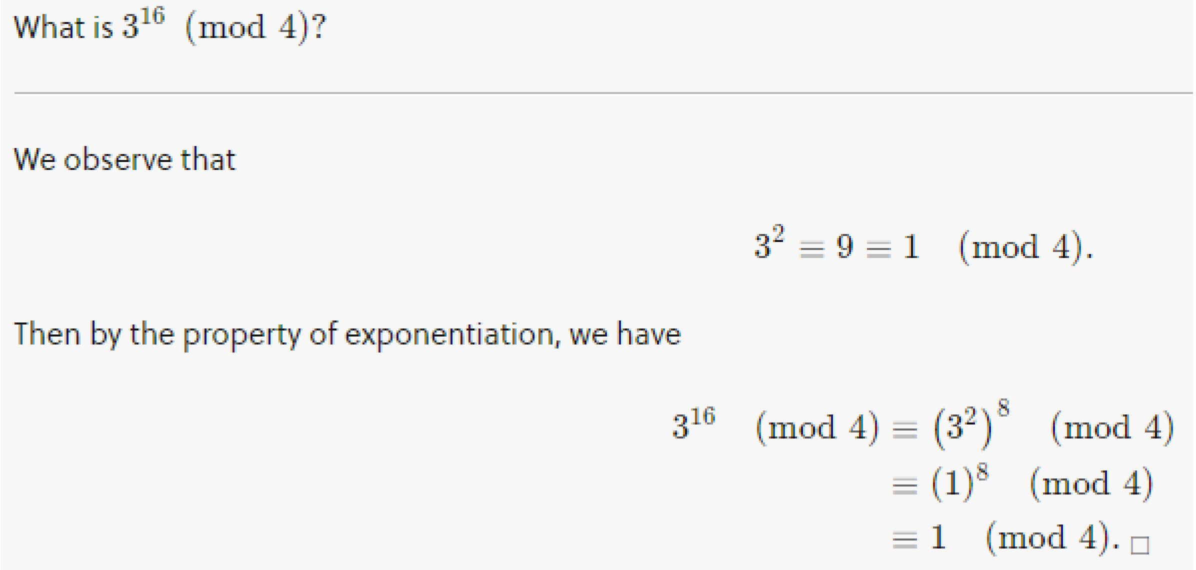
RHS = **4**

LHS = RHS = 4

1.8.4 Exponentiation

A^B mod C = ((A mod C)^B) mod C

Example



What is $3^{16} \pmod 4$?

We observe that

$$3^2 \equiv 9 \equiv 1 \pmod 4.$$

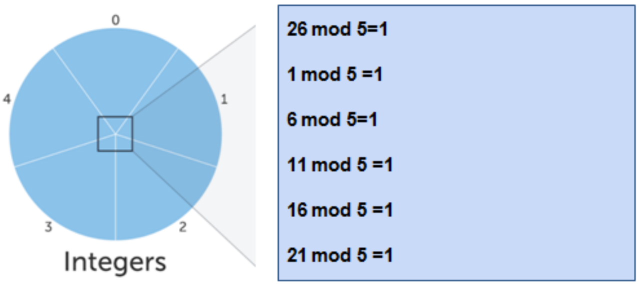
Then by the property of exponentiation, we have

$$\begin{aligned} 3^{16} \pmod 4 &\equiv \left(3^2\right)^8 \pmod 4 \\ &\equiv (1)^8 \pmod 4 \\ &\equiv 1 \pmod 4. \ \square \end{aligned}$$

1.9 CONGRUENCE MODULO

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

This says that A is congruent to B modulo C



26 mod 5=1

1 mod 5 =1

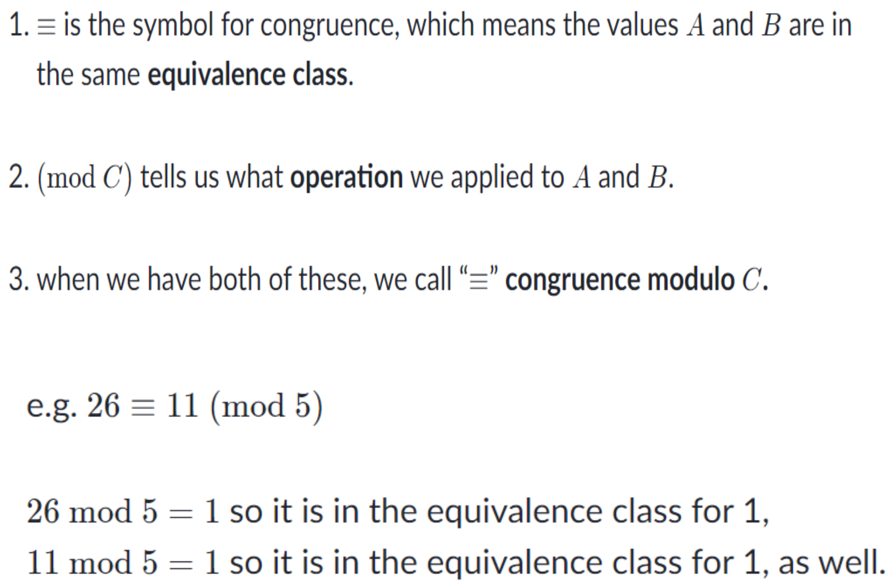
6 mod 5=1

11 mod 5 =1

16 mod 5 =1

21 mod 5 =1

Same Equivalence class



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

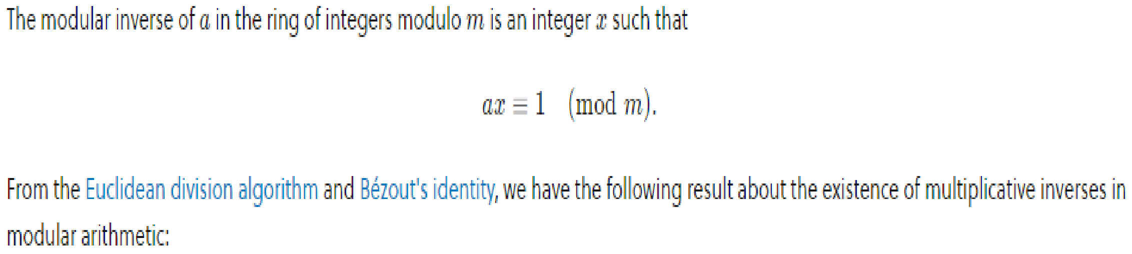
2. $(\text{mod } C)$ tells us what **operation** we applied to A and B.

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

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.

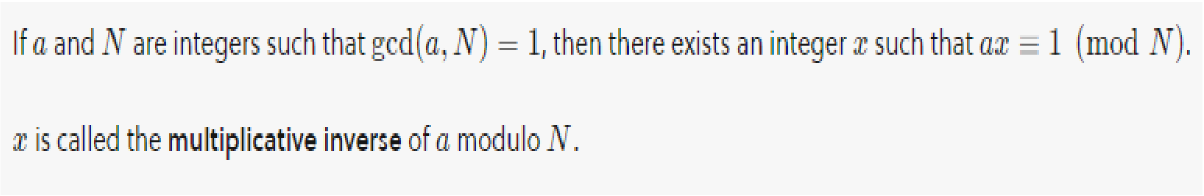
1.10 MULTIPLICATIVE INVERSES



The modular inverse of a in the ring of integers modulo m is an integer x such that

$$ax \equiv 1 \pmod{m}.$$

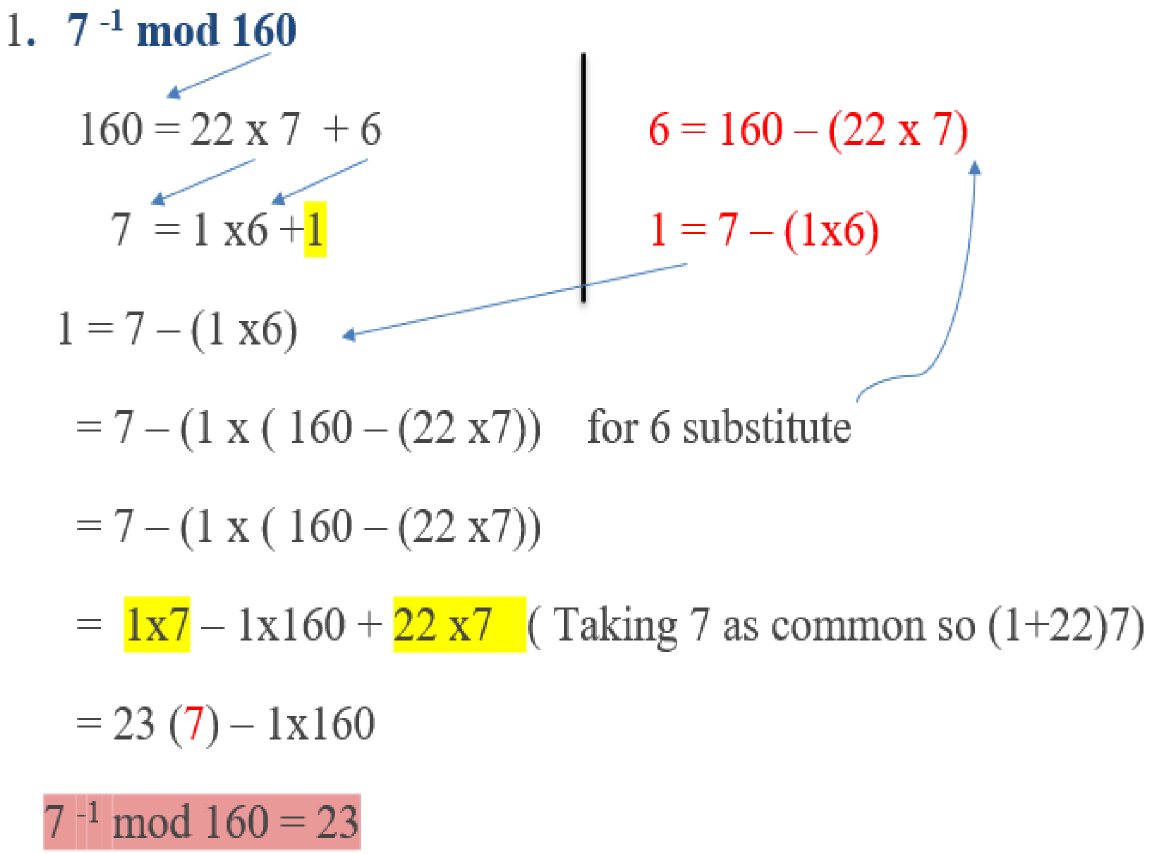
From the Euclidean division algorithm and Bézout's identity, we have the following result about the existence of multiplicative inverses in modular arithmetic:



If a and N are integers such that $\gcd(a, N) = 1$, then there exists an integer x such that $ax \equiv 1 \pmod{N}$.

x is called the **multiplicative inverse** of a modulo N.

SOLVED EXAMPLES



1. **7^{-1} mod 160**

160 = 22 x 7 + 6

7 = 1 x6 +1

6 = 160 – (22 x 7)

1 = 7 – (1x6)

1 = 7 – (1 x6)

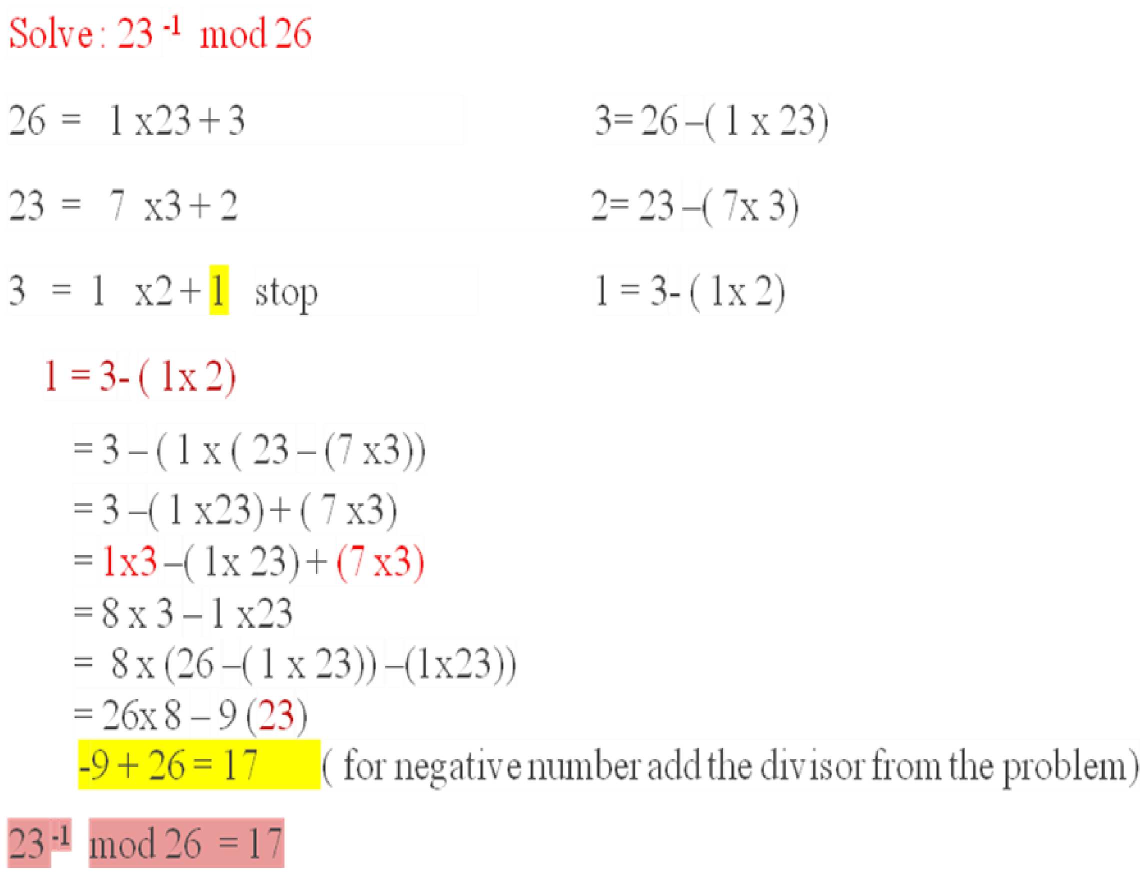
= 7 – (1 x (160 – (22 x7)) for 6 substitute

= 7 – (1 x (160 – (22 x7))

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

= 23 (7) – 1x160

7^{-1} mod 160 = 23



Solve: 23^{-1} mod 26

26 = 1 x23 + 3 3= 26 –(1 x 23)

23 = 7 x3 + 2 2= 23 –(7x 3)

3 = 1 x2 + 1 stop 1 = 3- (1x 2)

1 = 3- (1x 2)

= 3 – (1 x (23 – (7 x3))

= 3 –(1 x23) + (7 x3)

= 1x3 –(1x 23) + (7 x3)

= 8 x 3 – 1 x23

= 8 x (26 –(1 x 23)) –(1x23))

= 26x 8 – 9 (23)

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

23^{-1} mod 26 = 17

1.11 PRIME NUMBERS

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

For example,

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

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

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

****Always remember that 1 is neither prime nor composite**

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

1.11.1 Relative Prime Numbers

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

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

GCD – Greatest Common Divisor

For example,

Assume a=15 & b = 28

Factors of 15 are 1,3,5

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

GCD is the largest number that divides both of them.

In this case 1 is the common divisor

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

Practice Problem: Find GCD of 36 and 60

1.12 EULERS AND FERMATS THEOREM

1.12.1 Euler’s Totient Function

Euler’s Totient function is also known as PHI function ($\varphi(n)$) or $\phi(n)$

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

Example 1:

Assume ‘n’ = 10

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

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

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

Example 2:

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

Example 3: n=13. Find φ(13).

φ(13) = ?

Example 4: n= 11. Find φ(11).

Example 5: (non prime number)

n = 14. Find φ(14) = ?

Hint: Count of Relative Prime numbers for 14.

Example 6:

Determine φ(37) and φ(35).

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37.

Thus **φ(37) = 36.**

To determine φ(35), we list all of the positive integers less than 35 that are relatively prime to it:

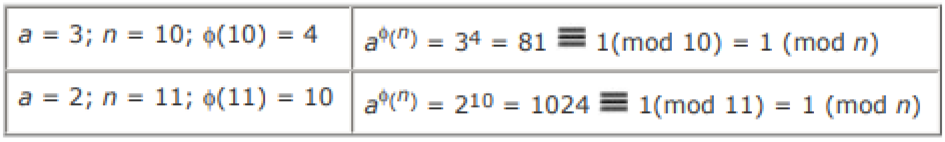
1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

There are 24 numbers on the list, so **φ(35) = 24.**

1.12.2 Euler’s Theorem

Euler's theorem states that for every a and n that are relatively prime:

$$a^{\phi(n)} \equiv 1(\text{mod } n)$$



$a = 3; n = 10; \phi(10) = 4$	$a^{\phi(n)} = 3^4 = 81 \equiv 1(\text{mod } 10) = 1 \ (\text{mod } n)$
$a = 2; n = 11; \phi(11) = 10$	$a^{\phi(n)} = 2^{10} = 1024 \equiv 1(\text{mod } 11) = 1 \ (\text{mod } n)$

aφ(n) ≡ 1 mod n

φ(n) is the totient function is defined as the number of positive integers less than n that are co prime to n. (n>=1)

φ(5) ={ 1 2 3 4}

Proof:

aφ(n) ≡ 1 mod n is true if n is prime, because in that case φ(n) = (n 1) and Fermat's theorem holds. However, it also holds for any integer n. Recall that φ(n) is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labeled as follows:

$$R \ \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with

gcd(x_i , n) = 1. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \text{ mod } n), (ax_2 \text{ mod } n), \ldots, (ax_{\phi(n)} \text{ mod } n)\}$$

The set S is a permutation of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n. 2. There are no duplicates in S.

. If ax_i mod n = ax_j mod n then $x_i = x_j$

Alternative form

Euler’s Theorem states that , If ‘p’ & ‘q’ are two prime numbers such that $p \neq q$ & $n = pq$,Then $\phi(n) \equiv (p-1)*(q-1)$.

Example 1:

Assume ‘p’ = 2 & ‘q’ = 5

$$\begin{aligned} n &= pq \\ &= 2*5 \\ &= 10 \\ \text{So } \phi(10) &\equiv (2-1)*(5-1) \\ &= 4 \end{aligned}$$

Example 2:

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

$$\varphi(77) \equiv (7-1)*(11-1) =6*10 =60$$

1.12.3 Fermat’s Theorem

Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

Proof:

Proof: Consider the set of positive integers less than p:{1,2,..., p 1} and multiply each element by a, modulo p, to get the set X = {a mod p, 2a mod p, . . . (p 1)a mod p}.

None of the elements of X is equal to zero because p does not divide a. Furthermore no two of the integers in X are equal. To see this, assume that

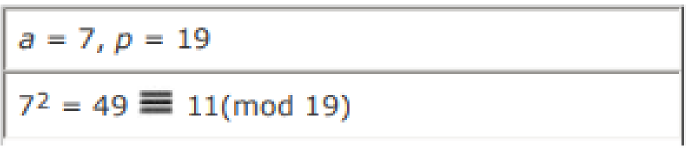
ja ≡ka(mod p) where 1 j < k p 1. Because a is relatively prime[5] to p, we can eliminate a from both sides of the equation ,resulting in:

j≡ k(mode p). This last equality is impossible because j and k are both positive integers less than p. Therefore, we know that the (p 1) elements of X are all positive integers, with no two elements equal. We can conclude the X consists of the set of integers {1,2,..., p 1} in some order. Multiplying the numbers in both sets and taking the result mod p yields

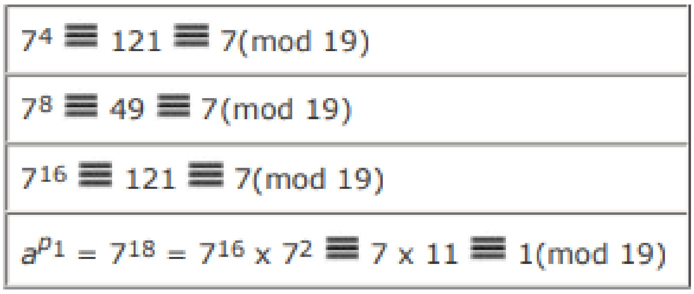
a x 2a x ... x (p 1) ≡ [(1 x 2 x ... x (p 1)](mode p)

ap1(p 1)! ≡ (p 1)!(mod p)

We can cancel the (p 1)! term because it is relatively prime to p



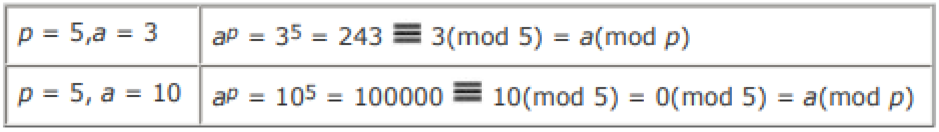
$a = 7, p = 19$
$7^2 = 49 \equiv 11(\text{mod } 19)$



$7^4 \equiv 121 \equiv 7(\text{mod } 19)$
$7^8 \equiv 49 \equiv 7(\text{mod } 19)$
$7^{16} \equiv 121 \equiv 7(\text{mod } 19)$
$a^{p1} = 7^{18} = 7^{16} \text{ x } 7^2 \equiv 7 \text{ x } 11 \equiv 1(\text{mod } 19)$

An alternative form of Fermat's theorem is also useful: If p is prime and a is a positive integer, then

$$a^p \equiv a(\text{mod } p)$$



$p = 5, a = 3$	$a^p = 3^5 = 243 \equiv 3(\text{mod } 5) = a(\text{mod } p)$
$p = 5, a = 10$	$a^p = 10^5 = 100000 \equiv 10(\text{mod } 5) = 0(\text{mod } 5) = a(\text{mod } p)$

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

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

Example: Let a = 3 and P = 7

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

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

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

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

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

Hence proved.

Key Points

● A prime number is an integer that can only be divided without remainder by positive and negative values of itself and 1. Prime numbers play a critical role both in number theory and in cryptography.

● Two theorems that play important roles in public-key cryptography are Fermat's theorem and Euler's theorem.

● An important requirement in a number of cryptographic algorithms is the ability to choose a large prime number. An area of ongoing research is the development of efficient algorithms for determining if a randomly chosen large integer is a prime number.

Solved Examples

Solve using Fermats Theorem

If n is prime and x is a positive integer not divisible by n then
$x^{n-1} \equiv 1 \mod n$

n- prime no.
x- is not divisible by n

x and n ---- coprime

Example 1:

x= 3 n=5

$3^{5-1} \equiv 3^{4} = 81$

$81 = 1 \mod 5$

Another form of fermats

$x^{n} \equiv x \mod n$

Example 2:

x= 3 n=5

$x^{n} = 3^{5} = 243$

$243 \equiv 3 \mod 5$

Example 3:

$2^{16} \mod 17$

By fermats

$x^{n-1} = 1 \mod n$

$2^{17-1} = 1 \bmod 17$

$2^{16} \bmod 17 = 1$

Example 4:

$7^{61} \bmod 31$

$x=7 \quad n=31$

$x^{n-1} = \bmod n$

$7^{31-1} = 1 \bmod 31$

$7^{30} \bmod 31 = 1$

Now,

$7^{61} = 7^{(30x2)\ +1}$

$\quad = (7^{30})^2 . 7^1$

$7^{61} \bmod 31 = (7^{30})^2 . 7^1 \bmod 31$

$[(7^{30})^2 \bmod 31 \ x \ 7^1 \bmod 31] \bmod 31$

$[1 x \ 7^1 \bmod 31] \bmod 31$

7

QUESTIONS

1. Prove Fermat’s Theorem .Consider a=2, P= 5
   i. $a^{P-1} = 1$ mod P
2. Prove Fermat’s Theorem Using a=3, P= 7
3. Solve 31^{-1}mod 37
4. Solve 5^{-1}mod 96
5. Solve 16^{-1} mod 23
6. Infer Eulers totient function
7. Compare passive and active attack
8. Interpret availability and authenticity
9. Distinguish threat and attacks.
10. Interpret Confidentiality and Integrity
11. Prove congruence modulo using an example.
12. Mention the types of active attacks.
13. State non repudiation.
14. Determine φ(37) and φ(35).
15. Explain computer security challenges.
16. Elaborate about security attacks with neat diagrams
17. Discuss the Key security concepts with the TRIAD diagram
18. State and prove the Eulers and Fermats theorem using examples.
19. With a neat sketch explain network security model.