Network Security

Contents

- Introduction
- Security Services
- Message Confidentiality
- Cryptography
- Two fundamental Cryptographic Principles
- Communication Security: Firewalls
- Web Security
- Mobile Code Security
- Social Issues

As per SPPU Syllabus 2013 Pattern for T.Y.B.Sc. (Computer Sci.) Sem IV
Prepared by : Prof. Upendra D. Choudhari, Tuljaram Chaturchand College, Baramati

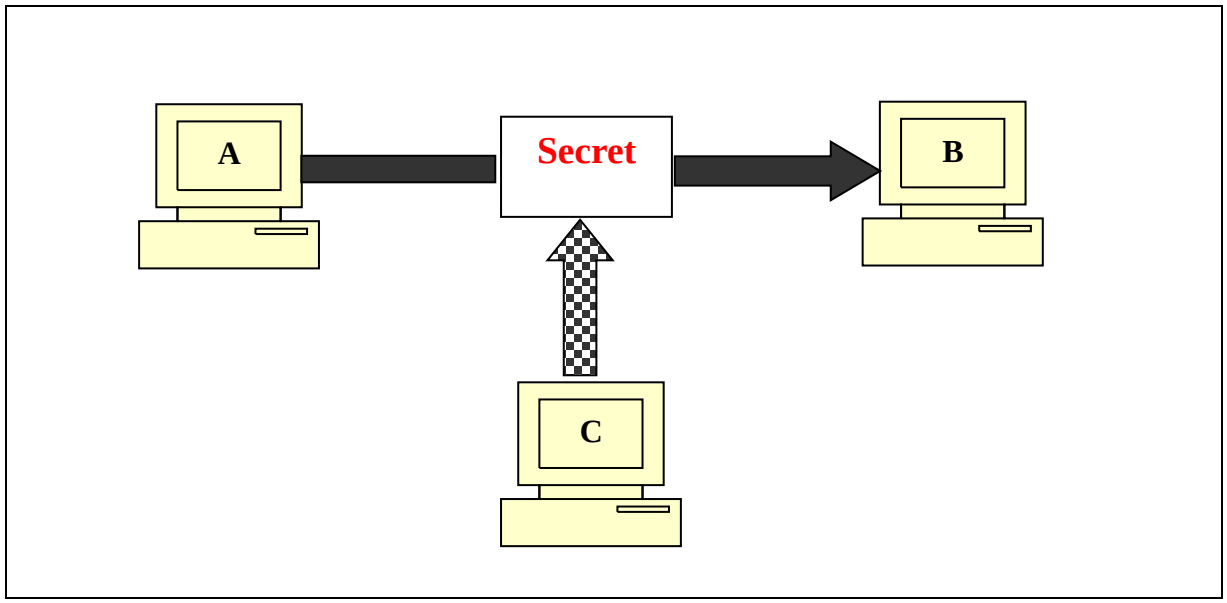
Introduction :

- ✓ Computer Security means to protect information. It deals with prevention and detection of unauthorized actions by users of a Computer.
- ✓ Network Security is a specialized field in computer networking that involves securing a computer network infrastructure.
- ✓ Network Security issues includes protecting data from unauthorized access, from damage and development, implementing policies, procedures for recovery and data losses.
- ✓ Security becomes an important issue, when data is transmitted between applications on a network, it can be read by unauthorized users i.e. intruder.
- ✓ Security in networking is based on cryptography. Cryptography is the science and art of achieving security by encoding messages to make them non readable.
- ✓ Cryptography can provide confidentiality, integrity, authentication and non-repudiation of messages.

Security Services :

✓ Network Security can provide one of the five services, first four related to message exchanged i.e. confidentiality, integrity, authentication and non-repudiation of messages and the fifth service provides entity authentication or identification. We briefly describe these services.

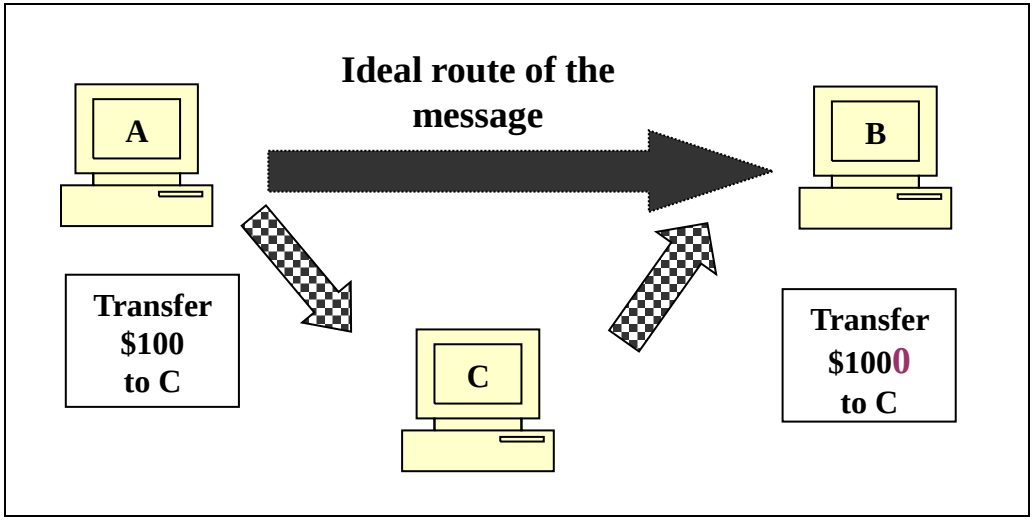
1. Confidentiality, also known as secrecy: Is the message seen by someone else? only an authorized recipient should be able to extract the contents of the message from its encrypted form. Otherwise, it should not be possible to obtain any significant information about the message contents.



Has someone seen it?

2. Integrity: The recipient should be able to determine if the message Has been altered during transmission.

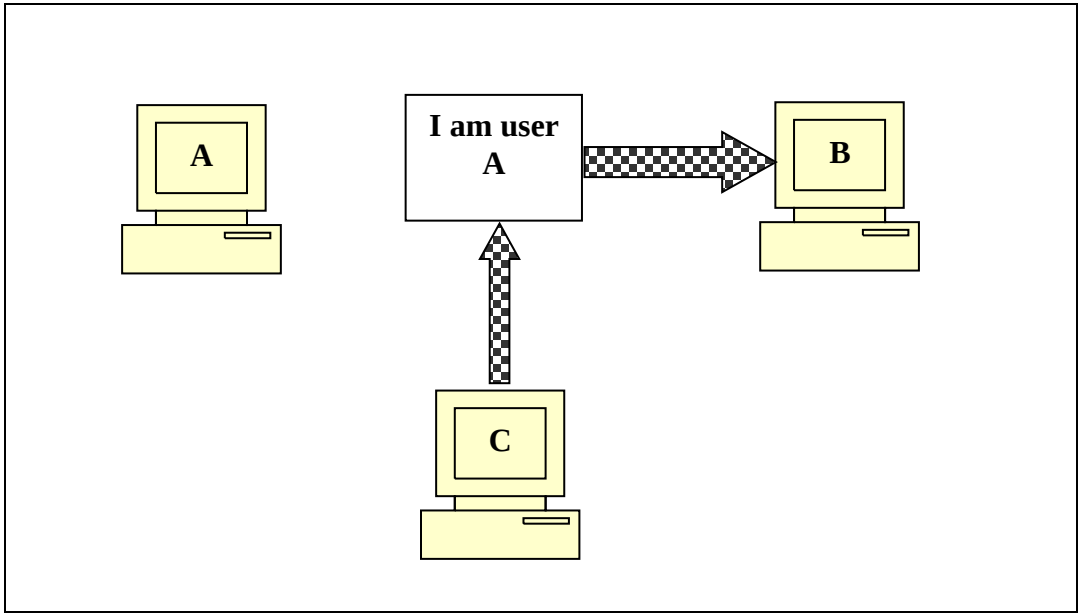
Has the Message Changed?



3. Authentication: Do you trust the sender of a message?

The recipient should be able to identify the sender, and verify that the purported sender actually did send the message.

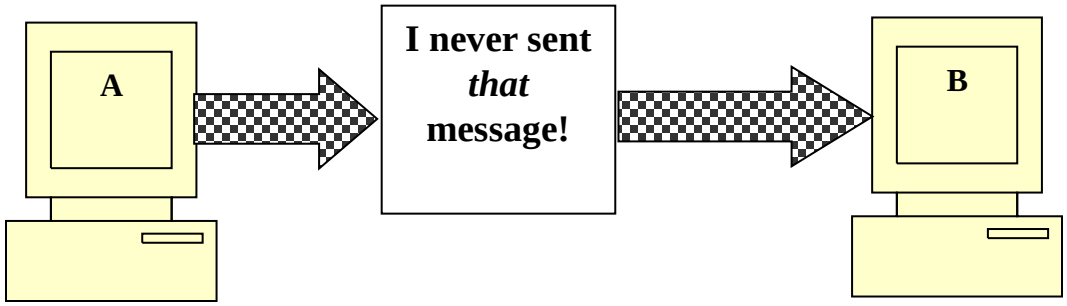
Who am I?



4. Non-repudiation:

The sender should not be able to deny sending the message.

A sends a message and refutes it later.



5. Entity (User) Authentication :

In entity authentication or user authentication the entity or user is verified prior to access the system resources. Consider user A want to access his bank account needs to be authenticated during the logging process.

Message Confidentiality :

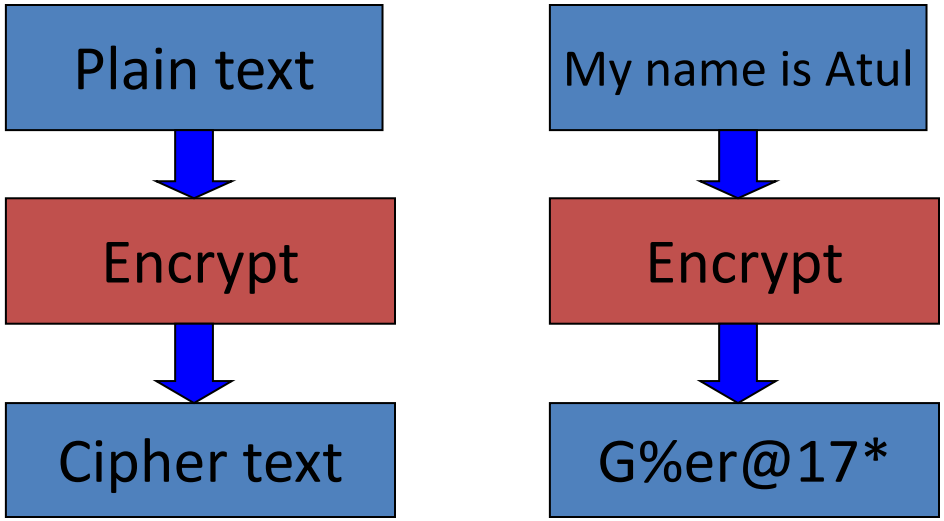
To achieve the message confidentiality or privacy one technique is used from thousands of Years i.e. encryption.

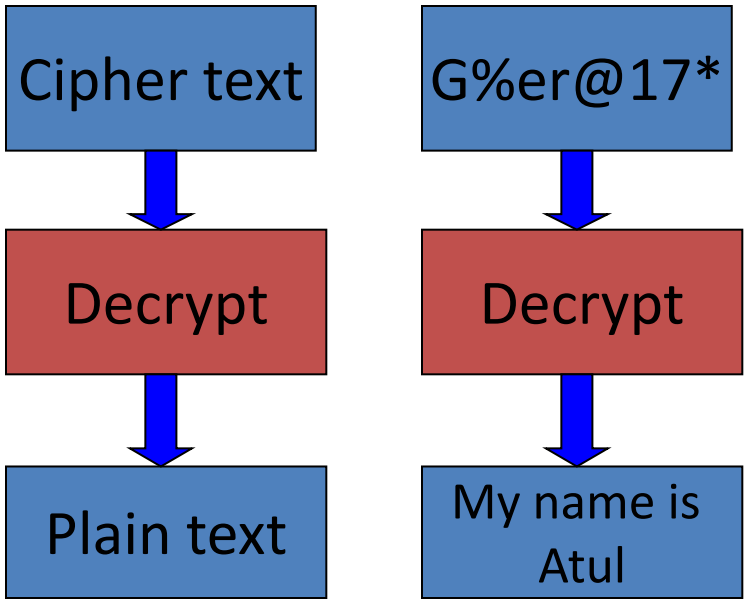
Encryption: Conversion of *plain text* into *cipher text.* In technical terms, the process of plain text message into cipher text message is called encryption.

Plain text:

All understandable messages ,

Example: “My name is Atul”





Decryption: Conversion of *cipher text* into *plain text,* the reverse process of transforming cipher text message back to plain text message is called decryption.

Cipher text:

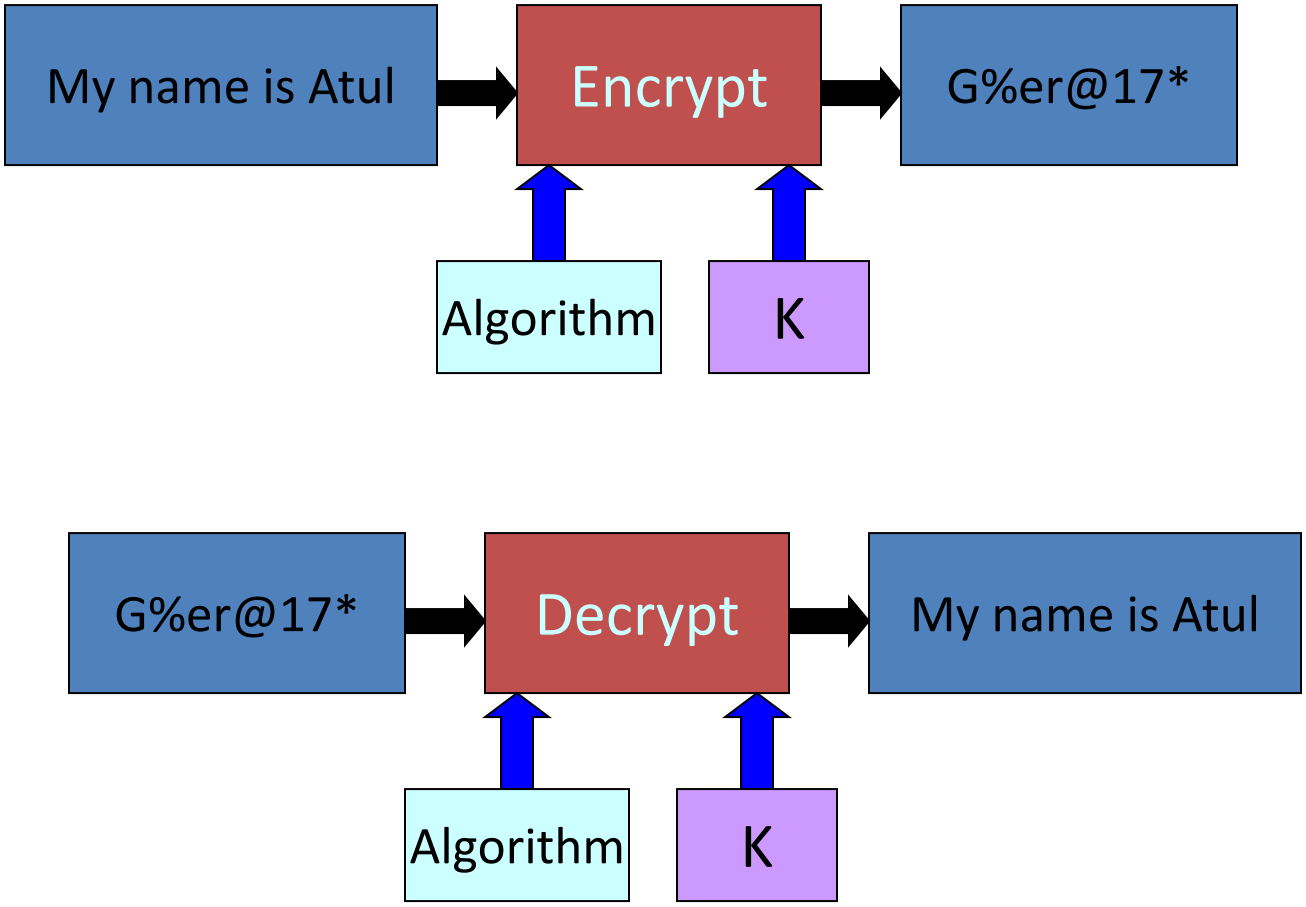
All non-understandable messages,

Example: “G%er@17*0-1>-”

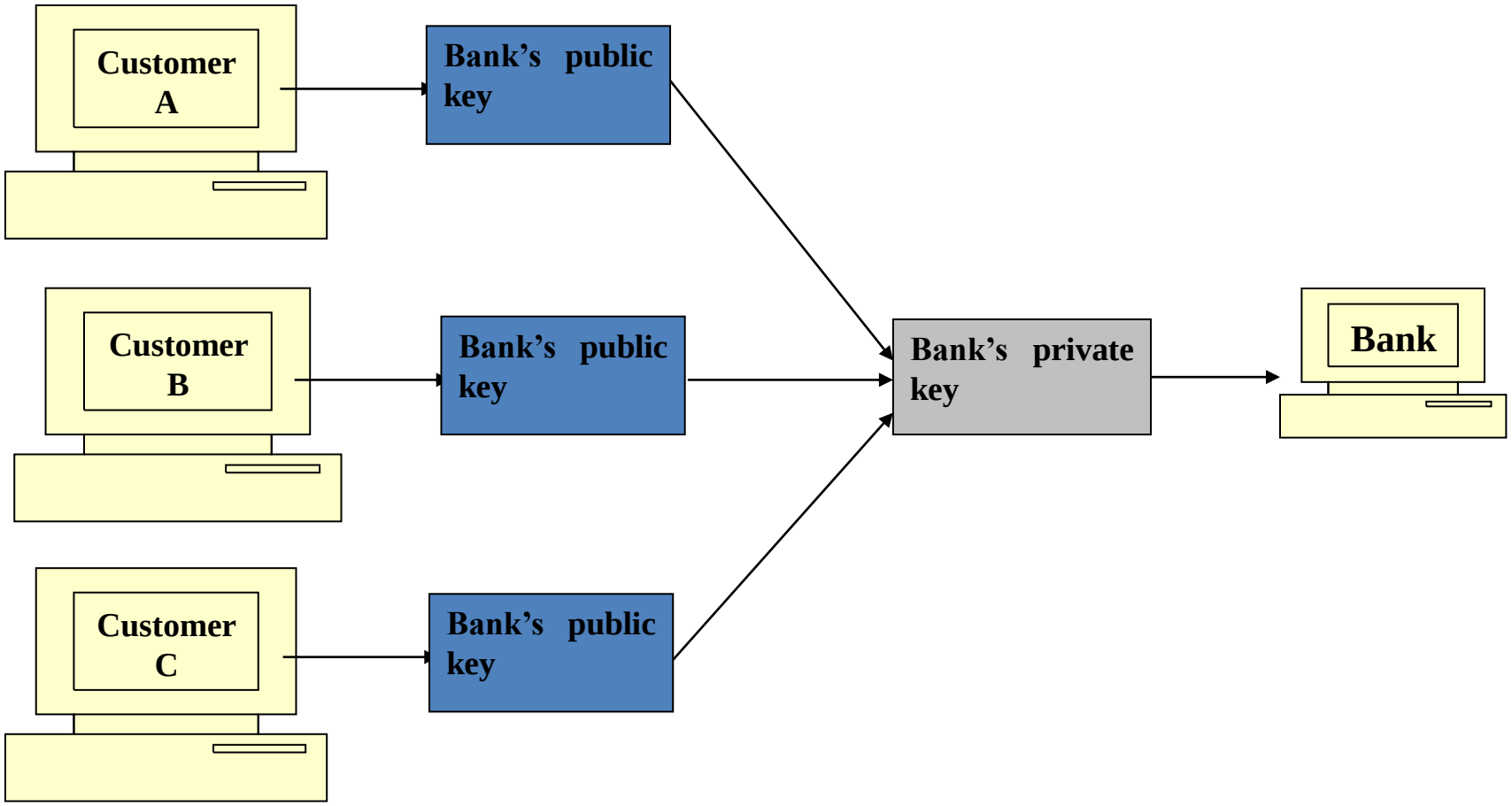
Confidentiality with Symmetric and Asymmetric key cryptography :

Symmetric Key Cryptography	Asymmetric Key Cryptography
The *same* key is used for encryption and decryption	One key used for encryption and another, *different* key used for decryption.
Also called as Private Key Encryption.	Also called as Public Key Encryption.
Each party has only one key	Each party has two keys : Public Key (say *K1*) and Private Key (say *K2*)
Key must be kept secret	Public Key is known to everybody. Private Key must be kept secret. Encrypt with *K1*, Decrypt with *K2*.
For long message, it is very fast and more efficient.	It is slower
Problem of Key Exchange	No Problem of Key Exchange
Every Pair Needs a Key	Only One Key-pair Per Party
Easier to implement	Practically more used
Examples: DES (Data Encryption Standard), AES (Advanced Encryption Standard), Blowfish	Examples: RSA (R.**R**ivest, A.**S**hamir, L.**A**dleman)

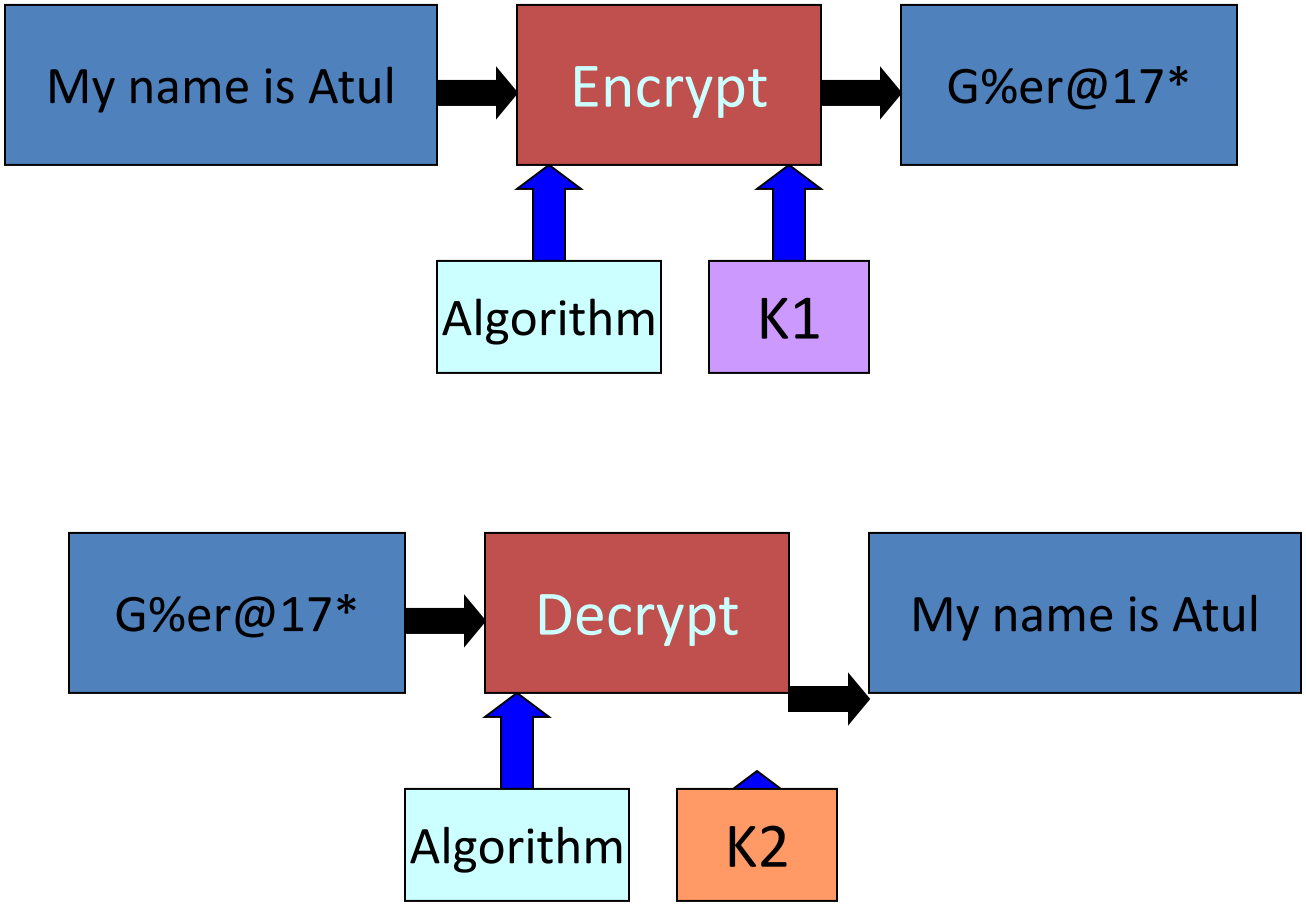
Symmetric Key Encryption: Example



Asymmetric Key Encryption: Concept



Asymmetric Key Encryption: Example



Cryptography:

Cryptography is the study of **Secret** (crypto-) **writing** (-graphy). It is a technique to provide message confidentiality. It is an art and science of transforming messages to make them secure and immune to attacks. Cryptography involves the process of encryption and decryption.

Encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

Basic Concepts :

Plaintext : The original intelligible message.

Cipher text: The transformed message.

Message: Is treated as a non-negative integer hereafter.

Cipher : An algorithm for transforming an intelligible message into unintelligible by transposition and/or substitution, or some other techniques

Keys : Some critical information used by the cipher, known only to the sender and/or receiver.

Encipher (encode): The process of converting plaintext to cipher text.

Decipher (decode): The process of converting cipher text back into plaintext.

There are two primary ways in which a plaintext message can be codified to obtain the corresponding cipher text:

1. Substitution cipher/Technique 2. Transposition cipher/Technique

Substitution Cipher/Techniques: Replace one or more characters with other characters. One of the oldest substitution cipher is Caesar Cipher.
Example: Replace each **a** with **d**, **b** with **e**, **c** with **f** and so on.
Another method is mono-alphabetic cipher. In this method, random substitution is used.

Example: By using Caesar cipher, transform the message "Happy birthday to you"

Solution: Plain text: "Happy birthday to you"

Key : character + 3

Caesar cipher : kdssb eluwkgdb wr brx

In substitution cipher other methods like **polygram substitution cipher, polyalphabetic substitution cipher, playfair cipher, hill cipher** etc. are also used.

Transposition Techniques: Rearrange the text. They performs some permutation over to the plaintext alphabet. Example: Replace 1st character with 4th, 2nd with 5th, etc.

Example: Plain Text: Consider a plain text " How are you when you arrived ?" by using a key NCBTZQARX, use transposition cipher on the plaintext.

Solution: steps:

1 Write the key and give numbers to the alphabets.

2 Write the plaintext horizontally, in rows, padded to fill the matrix if the need be.

3 Write the ciphertext by columns, starting with the column whose key letter is lowest.

N	C	B	T	Z	Q	A	R	X
4	3	2	7	9	5	1	6	8
H	o	w	a	r	e	y	o	u
w	h	e	n	y	o	u	a	r
r	i	v	e	d	a	b	c	d

Cipher text: **YUBWEVOHIHWREOAOACANEURDRYD**

Example: Plain Text: Please transfer one million dollar to my swiss bank account six two two. Key : MEGABUCK

Solution: Use transposition cipher on the plain text

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
P	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	t	o
m	y	s	w	i	s	s	b
a	n	k	a	c	c	o	u
n	t	s	i	x	t	w	o
t	w	o	a	b	c	d	e

Cipher text: AFLLWAIASELAICXBTOOTSOWDLNMOYNTWESILSKSORNNOBUOEPAEDMANT

Two fundamental Cryptographic Principles:

Two fundamental principles are underlying to all cryptographic system, they are Redundancy & Freshness.

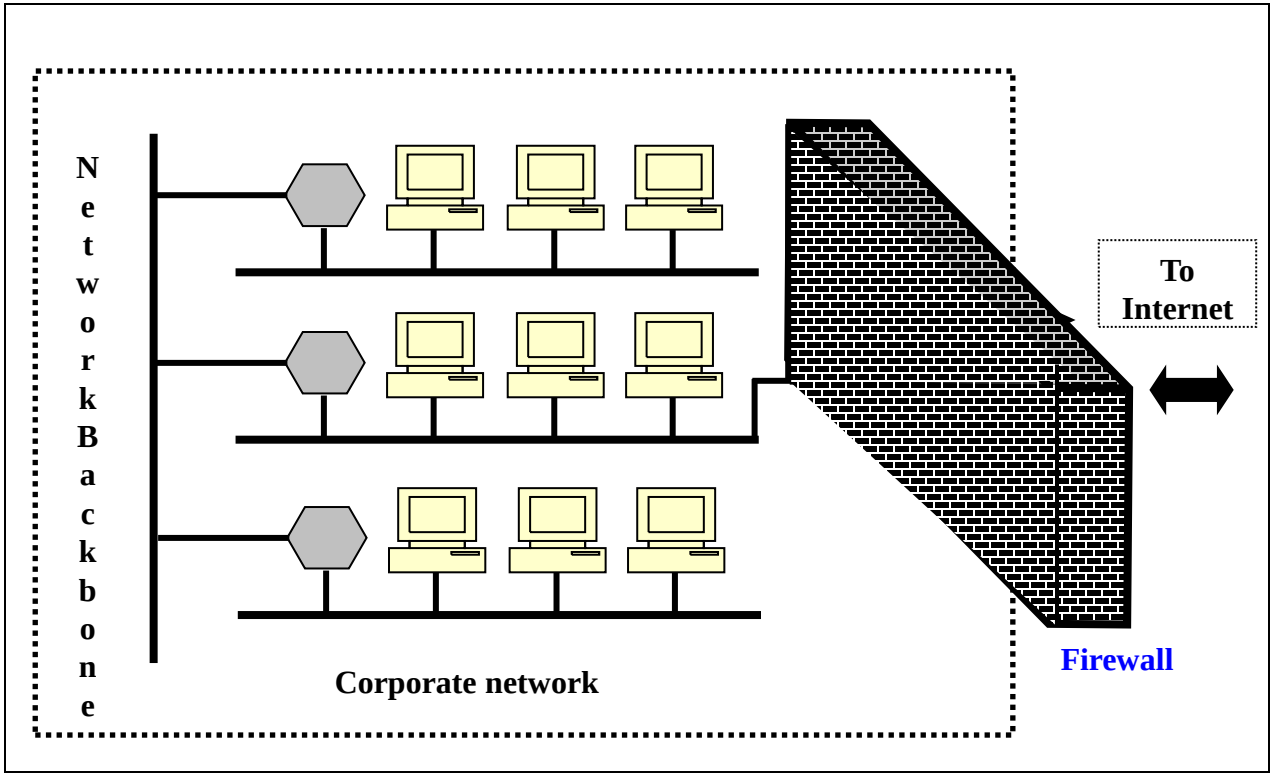
1. **Redundancy :** Every cryptographic system is all encrypted messages must contain Some redundancy. We know that passive intruders cannot decrypt the messages. But active intruder can cause a massive amount of trouble, even through intruder cannot understand the messages.

- Passive intruders cannot decrypt the message, since it is not knowing the key. However, passive intruders can make guesses about the text. Now consider a recently fixed employee who wants to take a revenge. He takes customers list and writes a program to generate fictitious order using real customer names. This ex-employee is not having the keys of customers so not able to encrypt it but can cause massive amount of trouble to the company. Company's server may not be able to find which records are valid and which are not.
- To prevent this, some additional information should be added to every record/every message. All messages must contain considerable redundancy so that active intruders cannot send random junk and have it be interpreted as a valid message.

2. **Freshness :** The second cryptographic principle is that some measures must be taken to ensure that each message received can be verified as being fresh, that is, sent very recently. This measure is needed to prevent active intruders from playing back old message.

- One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates.
- Message older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

Communication Security: Firewall :-



- **Similar to a Security Guard.**
- **Protects an organization's network.**
- **Stands between internet and Intranet.**
- **Network Layer Security.**

We must have mechanisms which can ensure that the inside information remain safe and also prevent the outside attackers from entering inside a corporate network. This Is where a firewall comes into picture.

One of the most basic and easily implemented methods of network security is the Firewall. The main purpose of a firewall is to separate a secure area from a less secure area and to control communications between the two.

Firewall also controlling inbound and outbound communications on anything From a single machine to an entire network.

A Firewalls can serve following functions:

1. Limit Internet access to e-mail only, so that no other types of information can pass between the internet and the intranet.
2. Control who can telnet into your intranet.
3. Limit what other kinds of traffic can pass between your intranet and internet.

Based on the criteria used for filtering traffic. Firewalls are generally classified into Two types : **1) Packet Filters 2) Application Gateways**

1) Packet Filters:

- Packet filters applies a set of rules to each packet and based on the outcome decides to either forward or discard the packet.
- It is also called as screening router or screening filter. Such a firewall implementation involves a router, which is configured to filter packets going in either direction.
- The filtering rules are based on a number of fields in the IP and TCP/UDP headers, such as source and destination IP addresses, IP Protocol field, TCP/UDP port numbers.

Advantages and disadvantages of packet filter:

Advantages:

The biggest advantage of packet filtering firewalls is cost and lower resource usage and best suited for smaller networks.

Disadvantages:

Packet filtering firewalls can work only on the network layer and these firewalls do not support complex rule based models and its also vulnerable to spoofing in some cases.

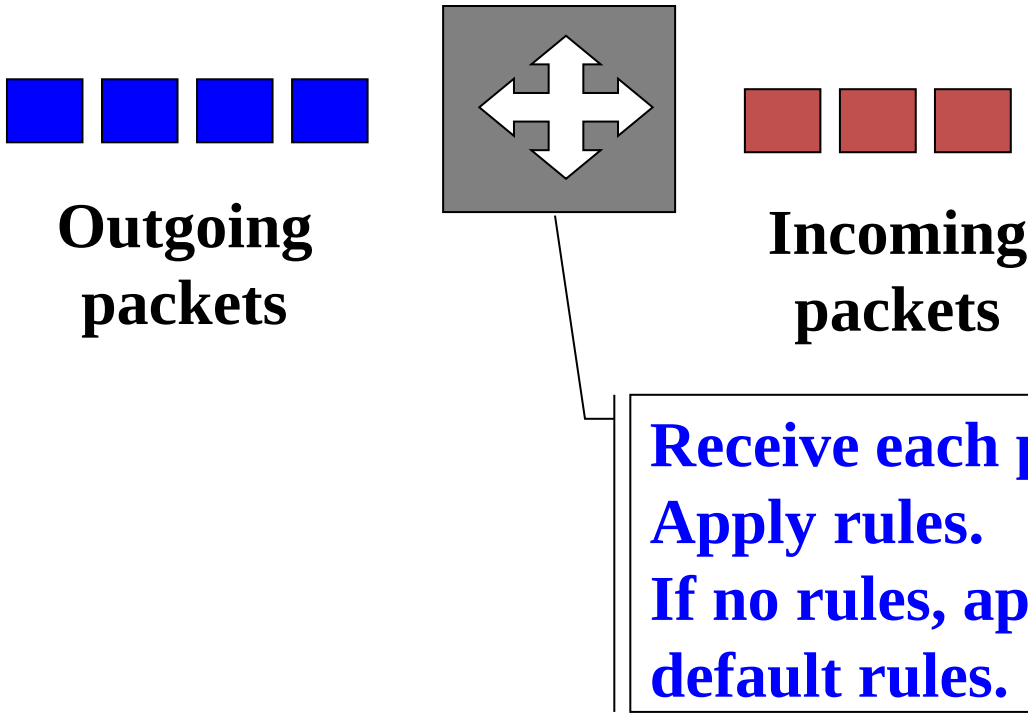


Fig: Packet Filter

2) Application Gateways :

- Application gateway is also called as a proxy server.
- Application gateway are generally more secure than packet filters.

Advantages and disadvantages of packet filter:

Advantages:

- Better logging handling of traffic , Highest level of security

Disadvantages:

- The overhead in terms of connections.
- Complex setup of application firewall needs more and detailed attentions to the applications that use the gateway.

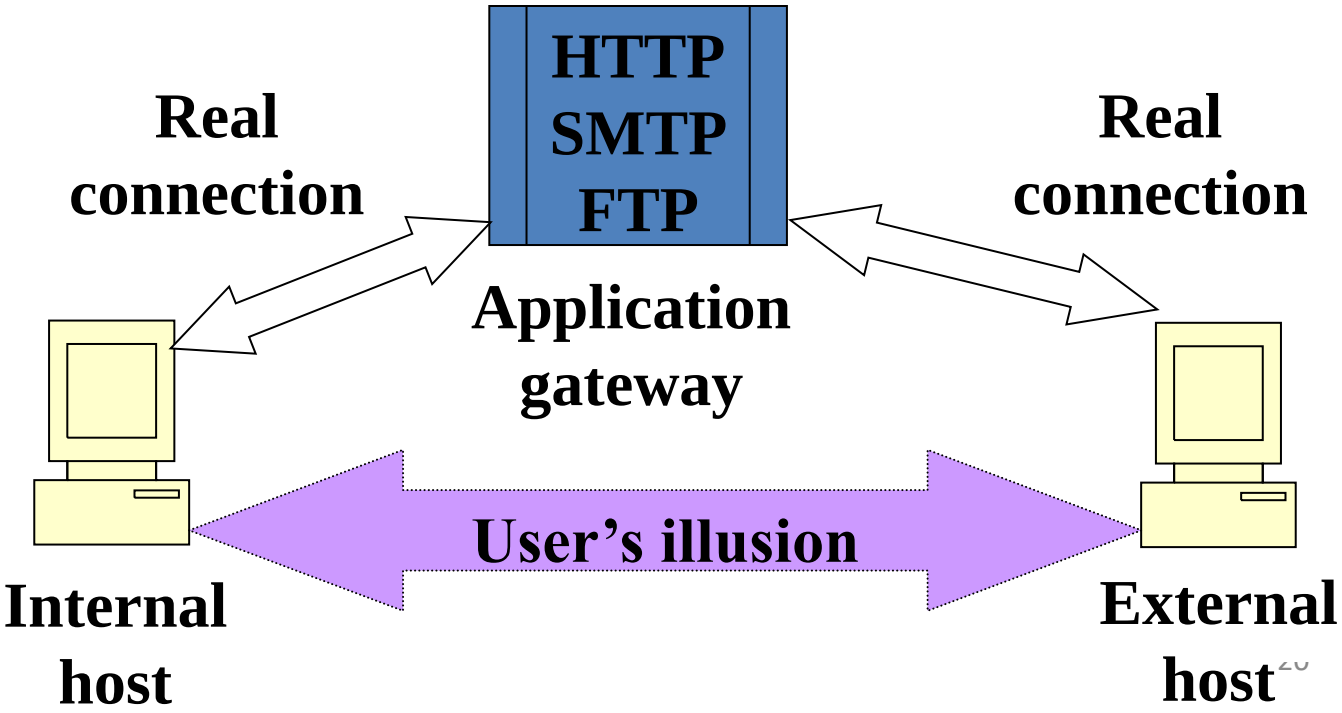


Fig: Application Gateway Concept

Web Security : Web security is very important issue, because of modern nature of attack. The Web is where most of the intruders resides.

Threats:

In the context of computer security, threats refers to anything that has the potential to cause serious harm to a computer system.

- It can be defined as "threats are anything i.e. object, substance, human etc that are capable of acting against an asset in a manner that can result in harm."
- There are several types of problems and threats related with web security. Some examples are:

A) Home page has been attacked and replaced by a new home page.

B) Sites have been brought down by denial of service attack. In which hacker flood the site and unable to respond to the queries.

C) A mirror image of website can also be created by a hacker.

D) Hack the E-commerce websites and know the details of credit cards.

E) Hackers done the fake announcement about share's prices, fake prizes etc.

- Threats are potentials for vulnerabilities to turn into attacks on computer systems, networks and more. So Vulnerabilities have to be fixed so that attackers cannot infiltrate the system and cause damage.

Network delivered threats are of two basic types:

Passive network threats: Activities such as wiretapping and idle scans that are designed to intercept traffic travelling through the network.

Active Network threats: Activities such as Denial of Service (DoS) attacks and SQL Injection attacks.

Some technical issues related to web security:

DNS Spoofing: Using the Domain Name System (DNS) people can identify web sites with human readable names and computers can continue to treat them as IP addresses. DNS server maintains the mapping between domain names and corresponding IP addresses. DNS server is usually located with the ISP. DNS Spoofing attacks are common and cause a lot of havoc. A protocol called secure DNS and self certifying names are used for such attack.

Secure DNS : IETF a working group was introduced to make DNS fundamentally secure. This project is known as DNSsec (DNS security). It is based on public key cryptography. Every DNS zone has a public/private key pair. All information sent by DNS server is encrypted with the senders private key, so the receiver can verify its authenticity.

Mobile Code Security : Mobile codes are small executable programs. In early days, web pages were static by using HTML only and not containing any executable code.

Now a days, web pages contain small programs including a java applets, ActiveX Control and Java Scripts. Downloading and executing such mobile code is security risk. Various methods have been devised to minimize it.

Java Applet Security: Java applets are small java programs compiled to a stack oriented machine language called Java Virtual Machine. They can be placed on a web page for downloading along with the page. After the page is loaded, the applets are inserted into a JVM interpreter inside the browser.

ActiveX Security: ActiveX controls are Pentium binary programs that can be embedded in web pages. Microsoft uses code signing method for decision. Every ActiveX control is a accompanied by a digital signature. The Microsoft system for verifying ActiveX control is called Authentic Code.

JavaScript Security : It does not have any formal security model. Every browser handles security in a different way. Example: Netscape navigator V4 uses code signing model.

Viruses: Viruses are another form of mobile code. The difference between a virus and ordinary mobile code is that viruses are written to reproduce themselves.

Viruses have become huge problem on the internet. Only user can install a good antivirus software.

==========

Social Issues: The internet and its security technology is an area where social Issues, public policy and technology meet. We examine three areas i.e. **privacy, freedom of speech** and **Copyright.**

Privacy: It is on the public agenda from the last 200 years. In the 18th Century, if the government Wanted/needed to check the documents of citizen, it had to do so by actually sending a Government official. Now today, telephone companies and ISP make everything easy.

Freedom of Speech: It is another social issue, which is opposite of censorship. Government wants to restrict what individuals can read and publish. But on website there are millions of pages which should be banned.

Eternity service has been proposed to counter censorship. Its goal is to make sure that the published information cannot be republished or rewritten. To use this service, the user specifies how long the material is to be preserved, pays a fee proportional to its duration and size and upload it. Thereafter, no one can remove or edit it, not even the uploaded.

Steganography : Steganography is a technique that facilities hiding of message that is to be kept secret inside other messages. It is the science of hiding information/messages. People hide secret messages within graphic images.

Copyright: Copyright is a form of intellectual property protection granted under particular country law to the creators of original works of ownership such as literary works including computer software, computer databases etc.

It is a legal right created by the law of a country that grants the creator of an original work exclusive rights for its use and distribution.

==========

Thank You