UNIT-11 Computer Security

- Computer Security,
- Firewall,
- Cryptography
- Cyber Law, Digital
- Signature,
- Certificate Authority
- Security Awareness, Security Policy

Computer Security

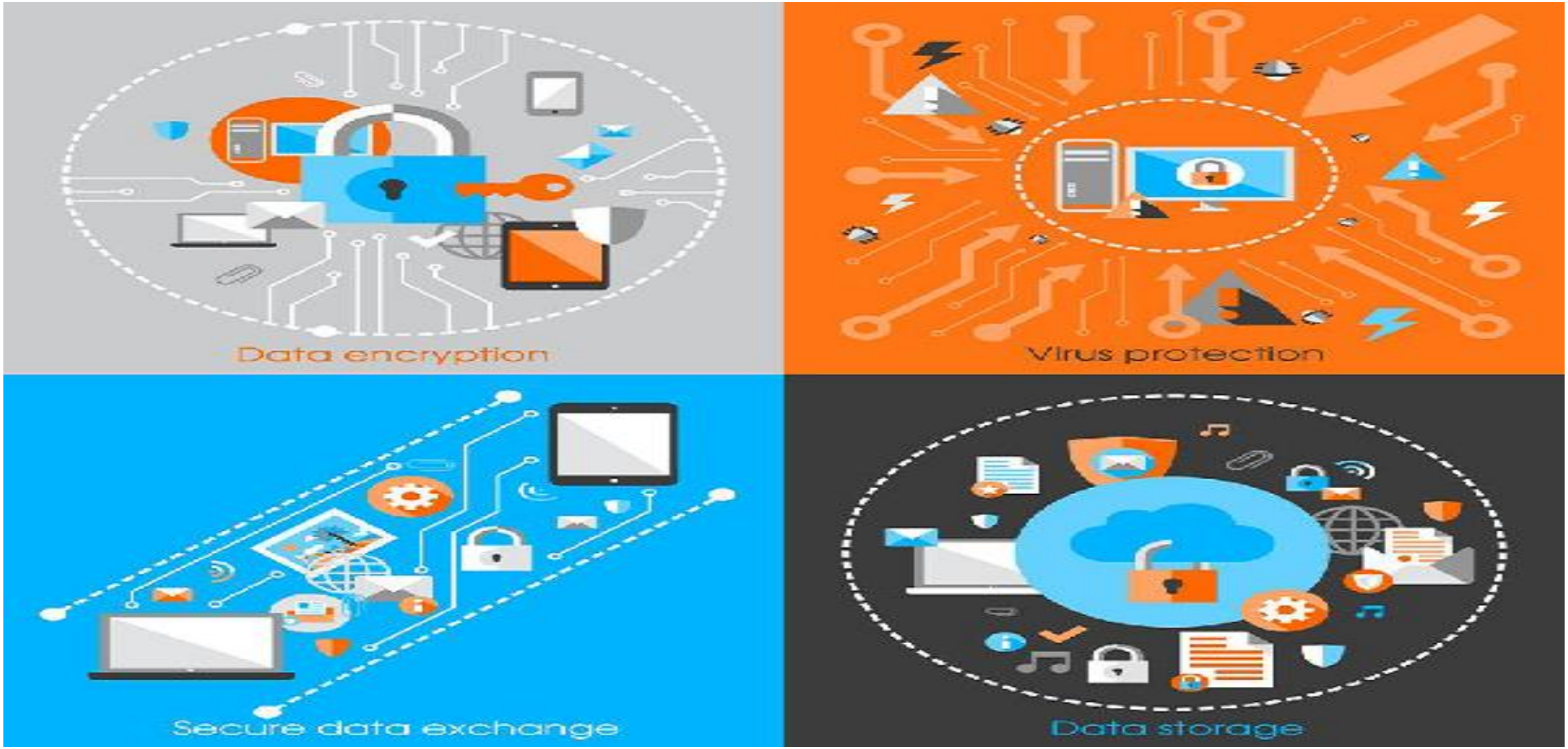
What is computer security?

- Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use.
- It is the process of preventing and detecting unauthorized use of your computer system.

What is Computer Security and its types?

- One way to ascertain the similarities and differences among Computer Security is by asking what is being secured. For example,
- *Information security* is securing information from unauthorized access, modification & deletion
- *Application Security* is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.
- *Computer Security* means securing a standalone machine by keeping it updated and patched
- *Network Security* is by securing both the software and hardware technologies
- *Cyber security* is defined as protecting computer systems, which communicate over the computer networks

What to Secure?



Potential Losses due to Security Attacks

Losing you data

- If your computer has been hacked or infected, there is a big chance that all your stored data might be taken by the attacker.

Bad usage of your computer resources –

- This means that your network or computer can go in overload so you cannot access your genuine services or in a worst case scenario, it can be used by the hacker to attack another machine or network.

Reputation loss –

- Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to your friends, business partners. You will need time to gain back your reputation.

Identity theft –

- This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.

Different Elements in Computer Security

- **Confidentiality, Integrity**, and **Availability** and the recently added **Authenticity and Utility**.

Different Elements in Computer Security cont..

- **Integrity**
  Integrity is the trustworthiness of data in the systems or resources by the point of view of preventing unauthorized and improper changes.
- Generally, Integrity is composed of two sub-elements – data-integrity, which it has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct.
- **Availability**
- Availability refers to the ability to access data of a resource when it is needed, as such the information has value only if the authorized people can access at right time.
- Denying access to data nowadays has become a common attack. Imagine a downtime of a live server how costly it can be.

Different terminology used in Computer Security

- **Unauthorized access** – An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.
- **Hacker** – Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.
- **Threat** – Is an action or event that might compromise the security.
- **Vulnerability** – It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.
- **Attack** – Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.
- **Antivirus or Antimalware** – Is a software that operates on different OS which is used to prevent from malicious software.
- **Social Engineering** – Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.
- **Virus** – It is a malicious software that installs on your computer without your consent for a bad purpose.
- **Firewall** – It is a software or hardware which is used to filter network traffic based on rules.

Hacking

- Hacking is **an attempt to exploit a computer system or a private network inside a computer**
- Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.
- Hacking is **the process of gaining unauthorized access into a computer system**, or group of computer systems.
- This is done through cracking of passwords and codes which gives access to the systems. ...
- The access to a password is obtained by the hacker through password cracking algorithms programs

Basic Security Concepts

- **Threats**
  - Anything that can harm a computer
  - Vulnerabilities are weaknesses in security
  - Security attempts to neutralize threats

Basic Security Concepts Cont..

- **Degrees of harm**
  - Level of potential damage
  - Include all parts of system
    - Potential data loss
    - Loss of privacy
    - Inability to use hardware
    - Inability to use software

Basic Security Concepts Cont..

- **Countermeasures**
  - Steps taken to block a threat
  - Protect the data from theft
  - Protect the system from theft

Computer Crime

- If computer of computer networks are used as a tool or a target or a place of criminal activity then it is known as computer crime.
- Unauthorized access to computer systems, data destruction, data alteration and theft of intellectual property is regarded as computer crime
- Also known as cyber crime. First recorded cyber crime took place in France.

Software Piracy

- Breaking security method of software
- Cracking programs
- Creating unauthorized copy or selling of software
- Renting a original software
- Reselling a original software is also a software piracy

Threats To Users

- Identity Theft
  - Impersonation by private information
    - Thief can 'become' the victim
  - Reported incidents rising
  - Methods of stealing information
    - Shoulder surfing
    - Snagging
    - Dumpster diving
    - Social engineering
    - High-tech methods

Threats To Users Cont..

- **Loss of privacy**
  - Personal information is stored electronically
  - Purchases are stored in a database
    - Data is sold to other companies
  - Public records on the Internet
  - Internet use is monitored and logged
  - None of these techniques are illegal

Threats to Users Cont..

- **Cookies**
  - Files delivered from a web site
  - Originally improved a site's function
  - Cookies now track history and passwords
  - Browsers include cookie blocking tools

Threats to Users Cont..

- **Spyware**
  - Software downloaded to a computer
  - Designed to record personal information
  - Typically undesired software
  - Hides from users
  - Several programs exist to eliminate

Threats to Users Cont..

- **Web bugs**
  - Small programs embedded in gif images
  - Gets around cookie blocking tools
  - Companies use to track usage
  - Blocked with spyware killers

Threats to Users Cont..

- **Spam**
  - Unsolicited commercial email
  - Networks and PCs need a spam blocker
    - Stop spam before reaching the inbox
  - Spammers acquire addresses using many methods
  - CAN-SPAM Act passed in 2003

Threats to Hardware

- **Affect the operation or reliability**
- Power-related threats
  - Power fluctuations
    - Power spikes or browns out
  - Power loss
  - Countermeasures
    - Surge suppressors
    - Line conditioners
    - Uninterruptible power supplies
    - Generators

Threats to Hardware Cont..

- **Theft and vandalism**
  - Thieves steal the entire computer
  - Accidental or intentional damage
  - Countermeasures
    - Keep the PC in a secure area
    - Lock the computer to a desk
    - Do not eat near the computer
    - Watch equipment
    - Chase away loiterers
    - Handle equipment with care

Threats to Hardware Cont..

- **Natural disasters**
  - Disasters differ by location
  - Typically result in total loss
  - Disaster planning
    - Plan for recovery
    - List potential disasters
    - Plan for all eventualities
    - Practice all plans

Threats to Data Cont..

- **The most serious threat**
  - Data is the reason for computers
  - Data is very difficult to replace
  - Protection is difficult
    - Data is intangible

Threats to Data Cont..

- **Viruses**
  - Software that distributes and installs itself
  - Ranges from annoying to catastrophic
  - Countermeasures
    - Anti-virus software
    - Popup blockers
    - Do not open unknown email

Threats to Data Cont..

- **Trojan horses**
  - Program that poses as beneficial software
  - User willingly installs the software
  - Countermeasures
    - Anti-virus software
    - Spyware blocker

Threats to Data Cont..

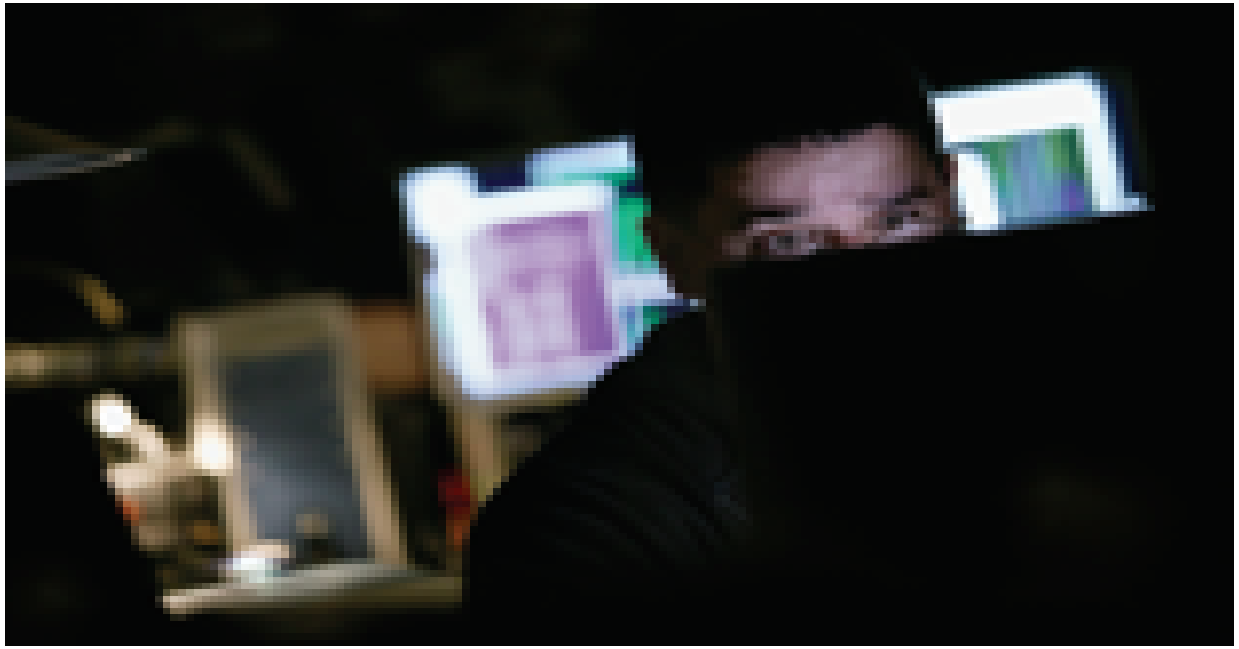
- **Cybercrime**
  - Using a computer in an illegal act
  - Fraud and theft are common acts

Threats to Data Cont..

- **Internet fraud**
  - Most common cybercrime
  - Fraudulent website
  - Have names similar to legitimate sites

Threats to Data Cont..

- **Hacking**
  - Using a computer to enter another network
  - Cost users $1.3 trillion in 2003
  - Hackers motivation
    - Recreational hacking
    - Financial hackers
    - Grudge hacking
  - Hacking methods
    - Sniffing
    - Social engineering
    - Spoofing



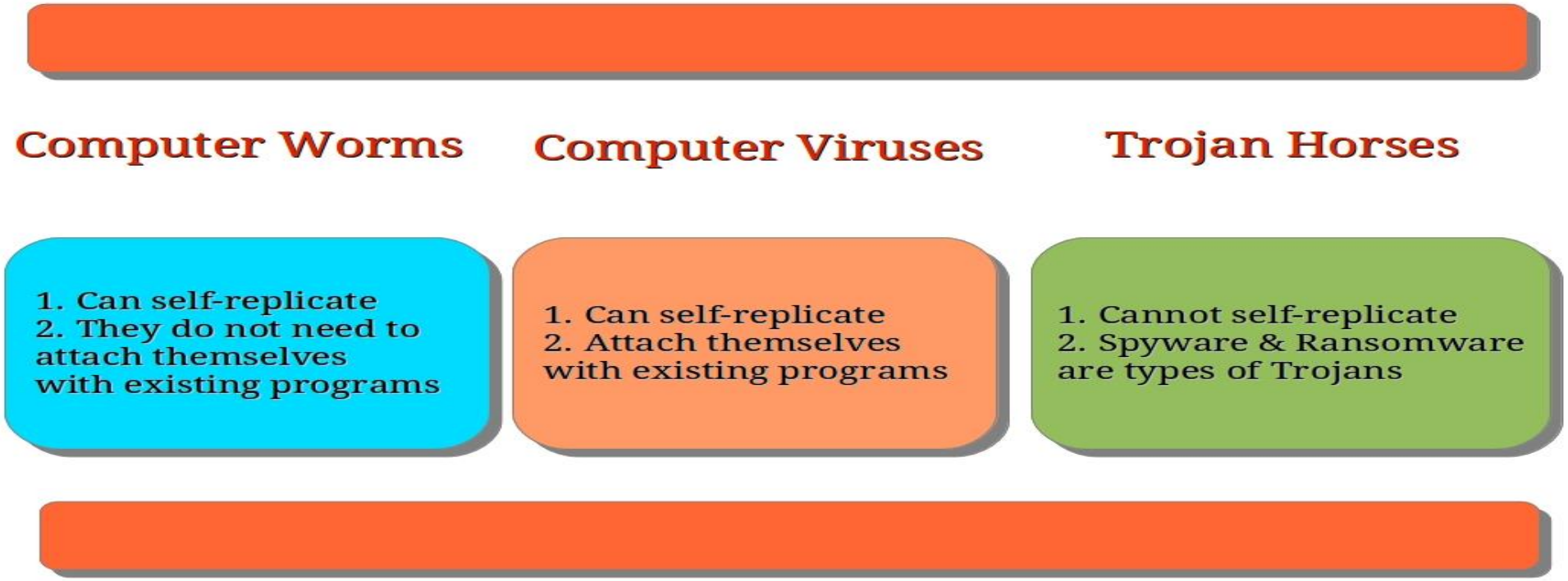
Threats to Data Cont..

- **Distributed denial of service attack**
  - Attempt to stop a public server
  - Hackers plant the code on computers
  - Code is simultaneously launched
  - Too many requests stops the server

Threats to Data Cont..

- **Cyber terrorism**
  - Attacks made at a nations information
  - Targets include power plants
  - Threat first realized in 1996
  - Organizations combat cyber terrorism
    - Computer Emergency Response Team (CERT)
    - Department of Homeland Security

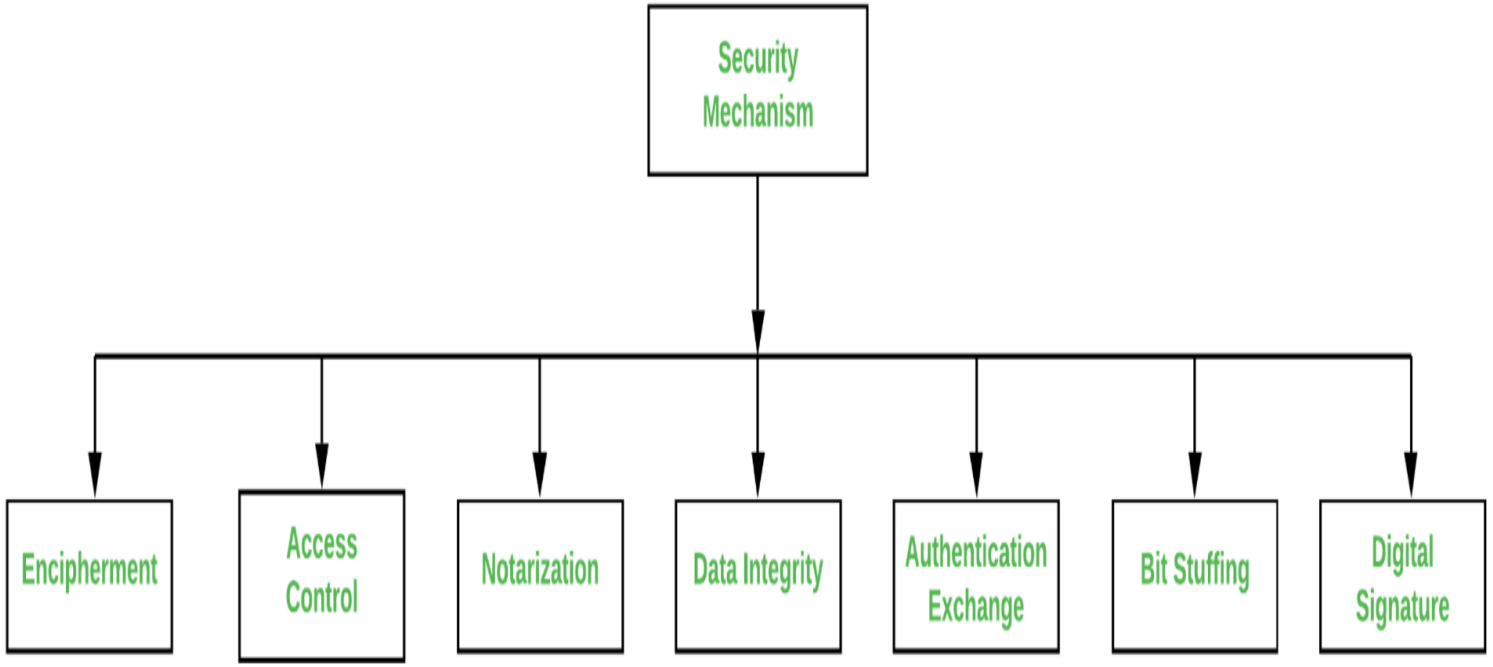
Virus, Worms & Spyware



Security Mechanism

Types of Security Mechanism

- Encipherment : This security mechanism deals with hiding and covering of data which helps data to become confidential
- Access Control
- Notarization
- Data Integrity
- Authentication exchange
- Bit stuffing
- Digital Signature



Types of Security Mechanism

- **Encipherment :**
  This security mechanism deals with hiding and covering of data which helps data to become confidential.
- It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form.
- **Access Control :**
  This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.
- **Notarization :**
  This security mechanism involves use of trusted third party in communication.
- It acts as mediator between sender and receiver so that if any chance of conflict is reduced.
- This mediator keeps record of requests made by sender to receiver for later denied.

Security Mechanism Cont..

- **Data Integrity :**
  This security mechanism is used by appending value to data to which is created by data itself.
- When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained.
- **Authentication exchange :**
  This security mechanism deals with identity to be known in communication.
- This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not
- **Bit stuffing :**
  This security mechanism is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving end and is achieved by Even parity or Odd Parity.
- **Digital Signature :**
  This security mechanism is achieved by adding digital data that is not visible to eyes.
- It is form of electronic signature which is added by sender which is checked by receiver electronically.
- This mechanism is used to preserve data which is not more confidential but sender's identity is to be notified.

Cyber Law

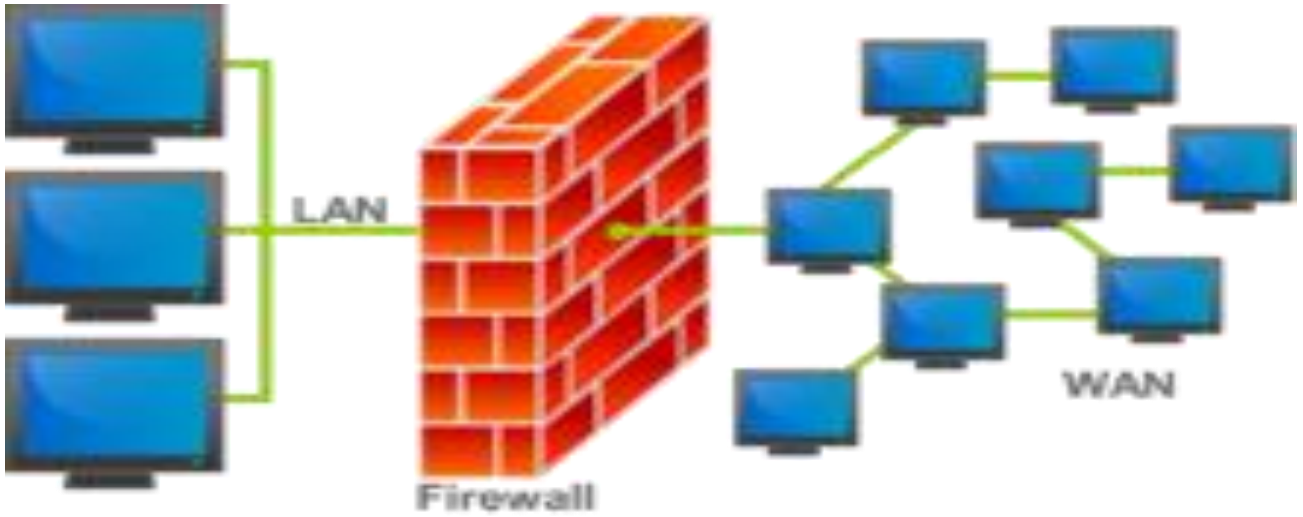
- **Cyber law** is the part of the overall legal system that deals with the Internet, cyberspace, and their respective legal issues.
- Cyber law covers a fairly broad area, encompassing several subtopics including freedom of expression, access to and usage of the Internet, and online privacy.
- Generically, cyber law is referred to as the Law of the Internet.
- It refers to all legal and regulatory aspects of internet and computers
- Primary purpose is to provide legal recognition of computer system and electronic act of a user
- In general, It is a law that bounds all the cyber crime.

Network Security

- Network security is a broad term that covers a multitude of technologies, devices and processes.
- In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks and data using both software and hardware technologies.
- Network security involves the authorization of access to data in a network.
- Network security covers a variety of computer networks, both public and private that are used in transaction of data.
- Network security helps to minimize cyber crime and data breaches

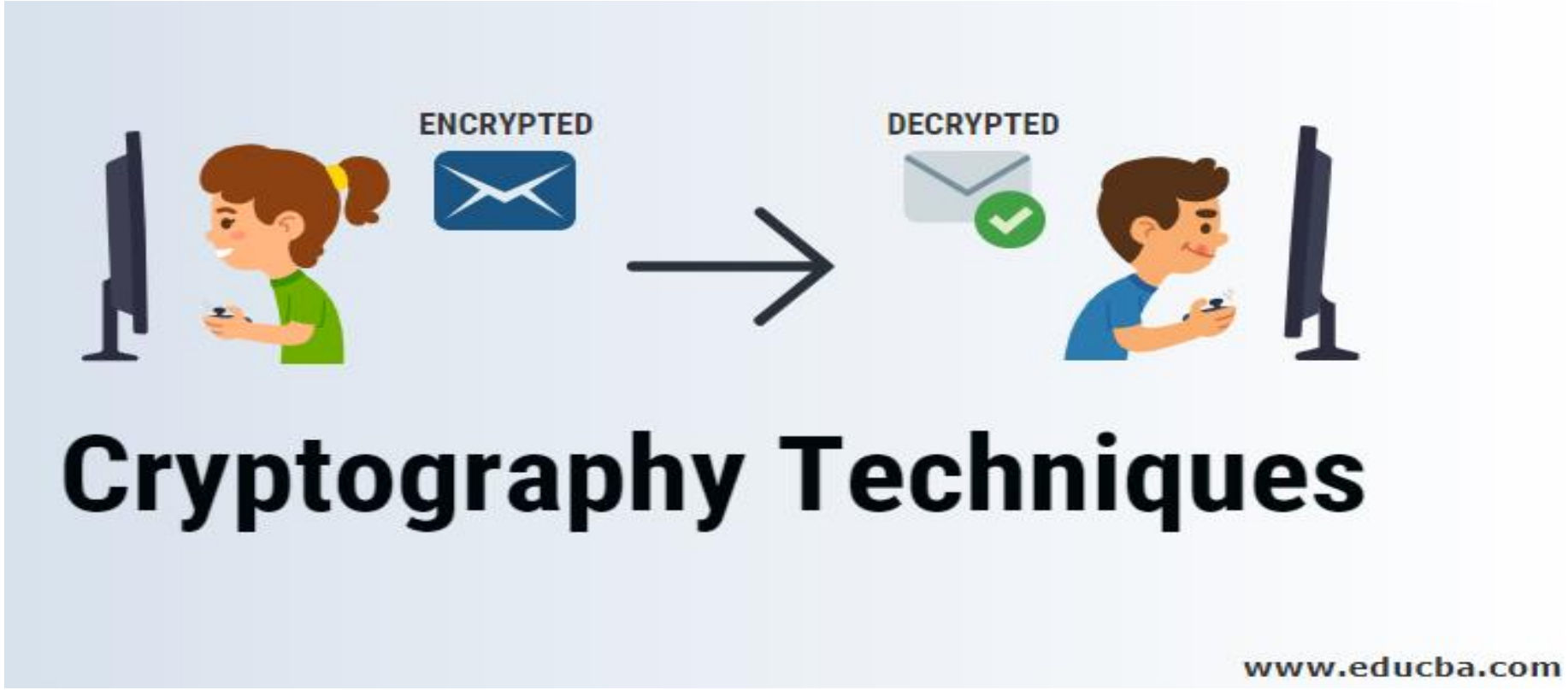
Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules
- Fire wall can be a device or a computer program. It provides secure connectivity between networks
- Fire wall helps to block the unauthorized access and spams in a network.It helps to enhance the network security



Cryptography

- Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents



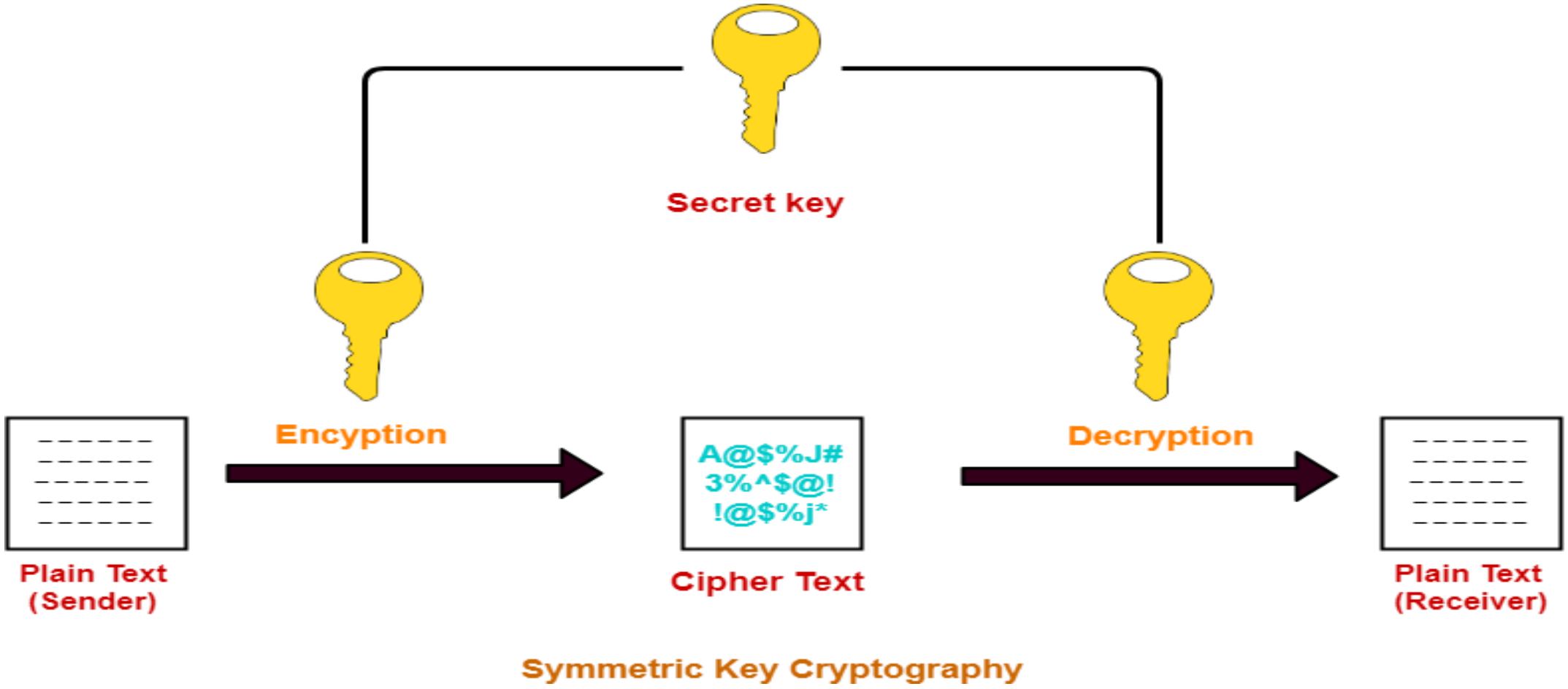
Cryptography Cont..

- Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it
- Cryptography is the study of securing communications from outside observers.
- Encryption algorithms take the original message, or plaintext, and converts it into ciphertext, which is not understandable.
- The key allows the user to decrypt the message, thus ensuring on they can read the message

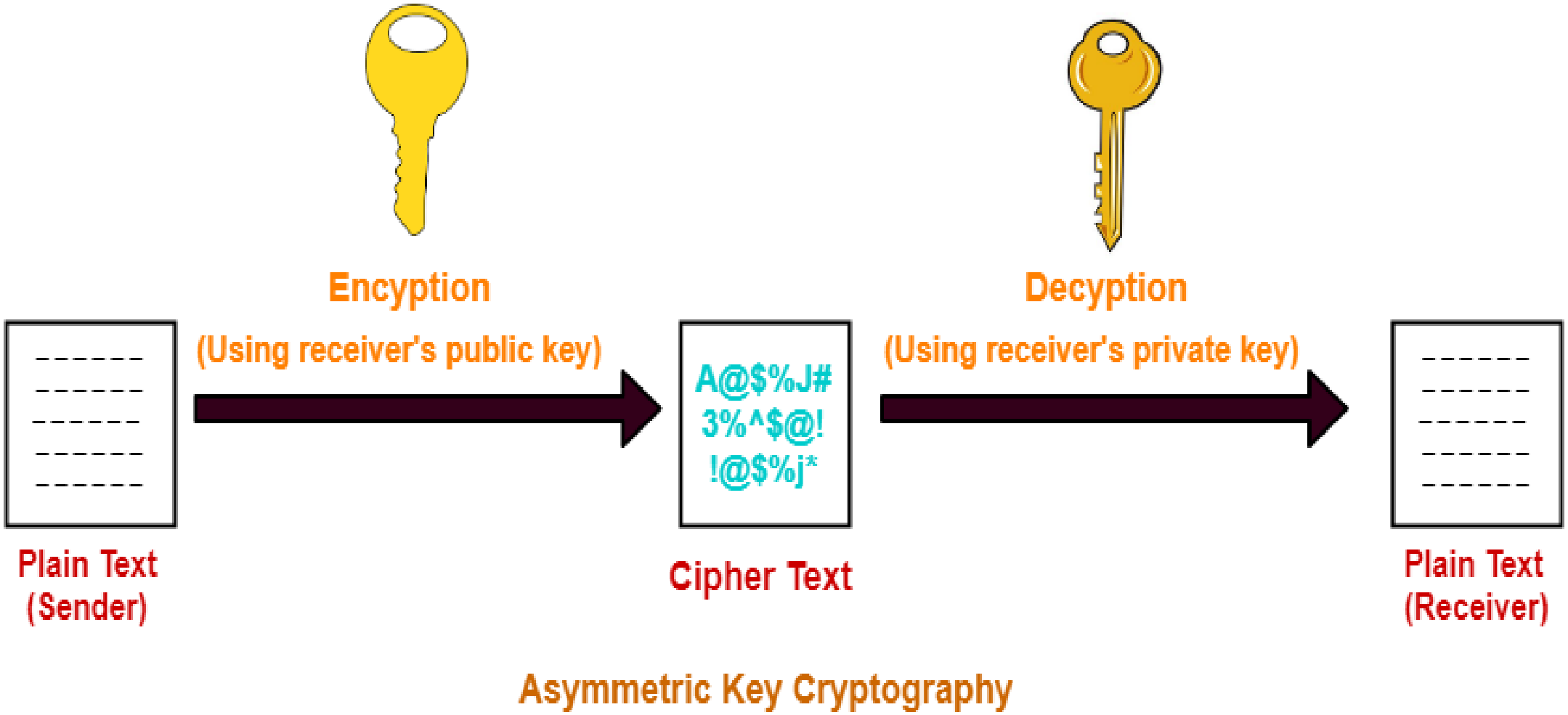
Cryptography Cont..

- The techniques that cryptographers utilize can ensure the confidential transfer of private data.
- Techniques relating to digital signatures can prevent imposters from intercepting corporate data, while companies can use hash function techniques to maintain the integrity of data.

Cryptography Cont..



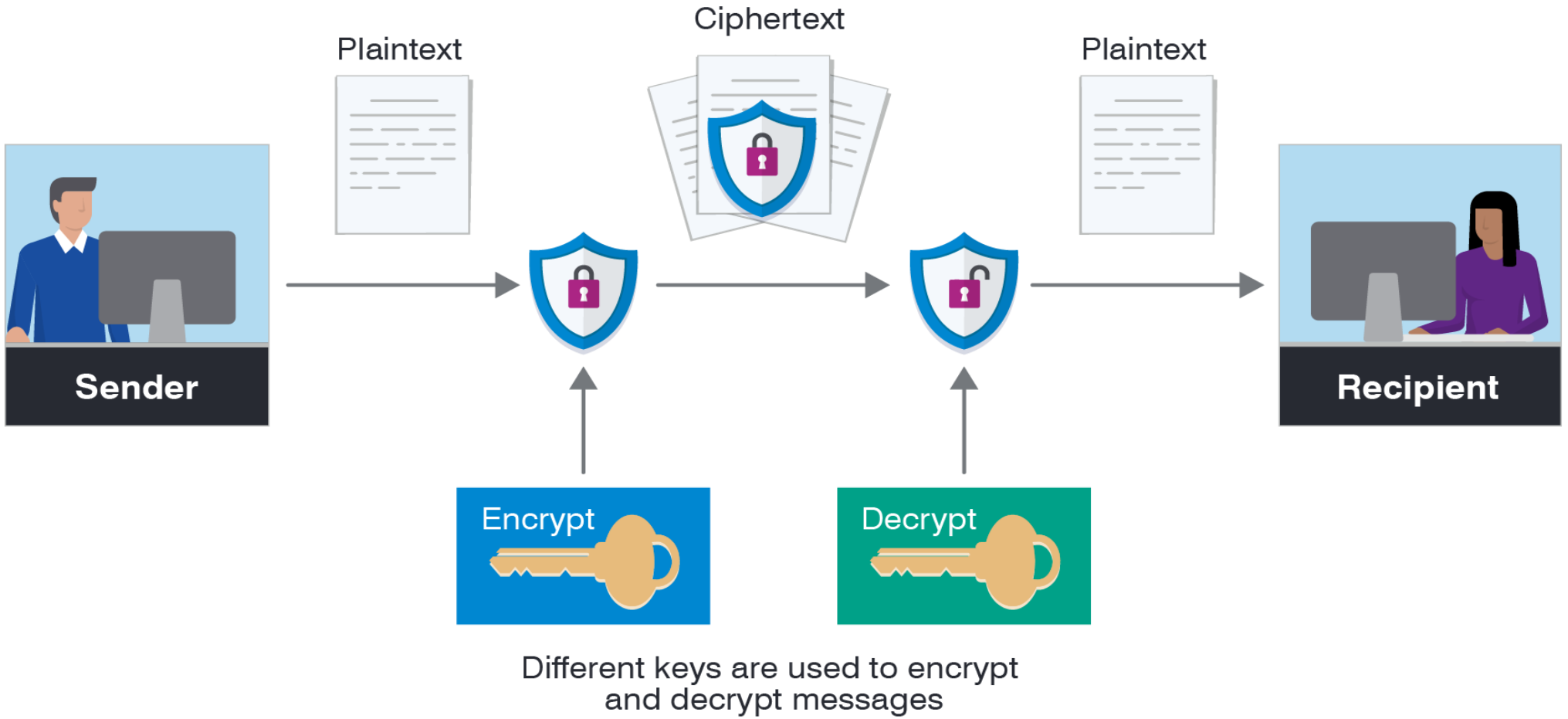
Cryptography Cont..



Data and Message security Cont..

- Data and message security means to provide a secure label to a data and information
- Data security can be maintained by using encryption method
- Encryption is the process of coding text so that unauthorized person cannot access.
- Decryption is the process of decoding to view the original data

Sample Encryption and Decryption Operation



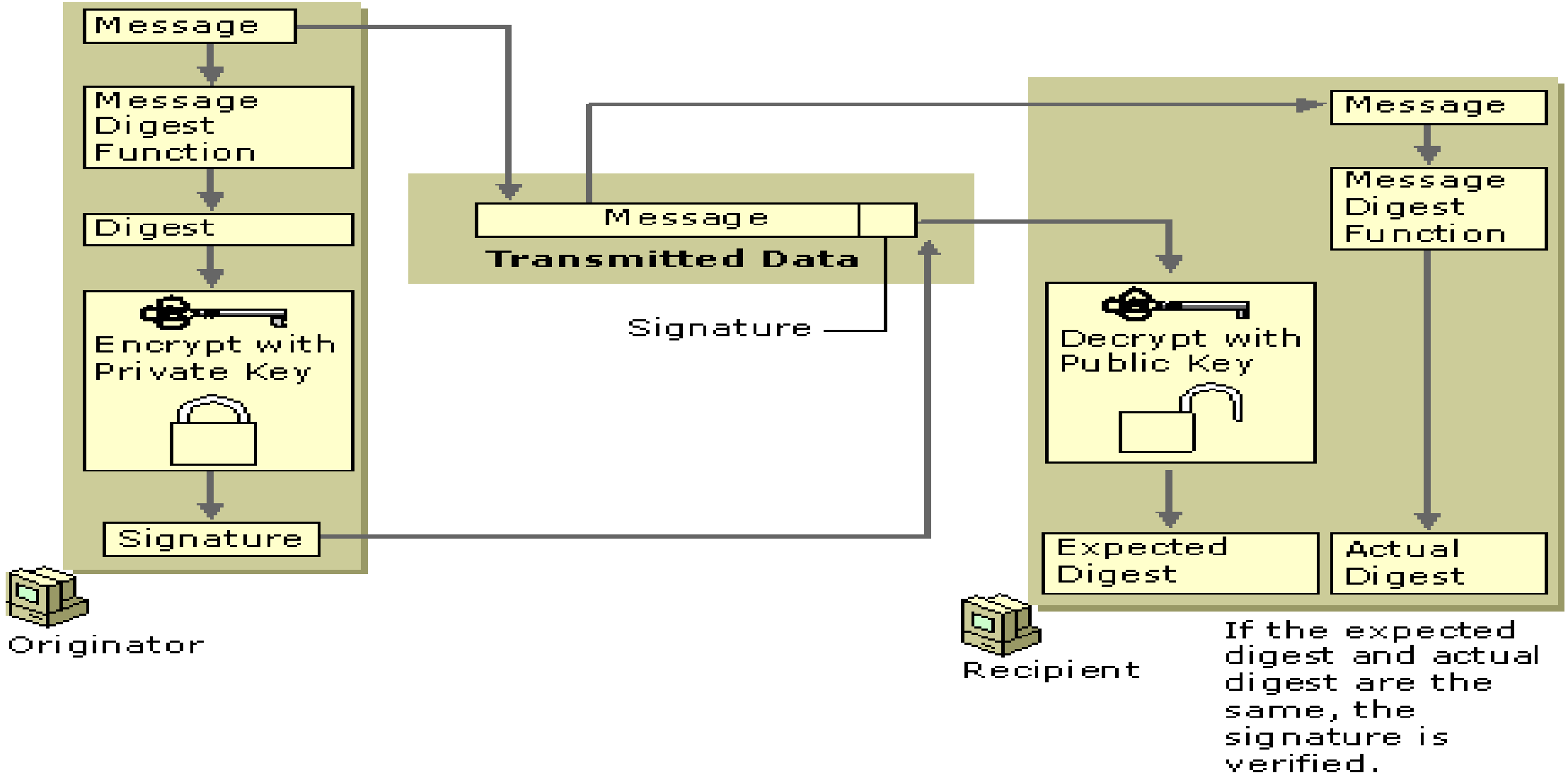
Digital Signature

- A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.
- One possible method for creating a digital signature is for the originator of data to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data.
- **However, encrypting all data to provide a digital signature is impractical for following two reasons:**
- *The cipher text signature is the same size as the corresponding plaintext, so message sizes are doubled, consuming large amounts of bandwidth and storage space.*
- *Public key encryption is slow and places heavy computational loads on computer processors*

Digital Signature Cont..

- Digital signature algorithms use more efficient methods to create digital signatures.
- The most common types of digital signatures today are created by signing **message digests** with the originator's private key to create a digital thumbprint of the data.
- Two of the most widely used digital signature algorithms today are the **RSA digital signature** process and the **Digital Signature Algorithm (DSA).**
- **RSA Data Security Digital Signature Process:** In the RSA digital signature process, the private key is used to encrypt only the message digest.
- The encrypted message digest becomes the digital signature and is attached to the original data.

Basic RSA Data Security Digital Signature Process



Advantages of Digital Signature

- Higher security
- Legal compliance and wide acceptance
- Time savings
- Workflow automation
- Cost savings
- Happier end-users
- Better company image and CSR

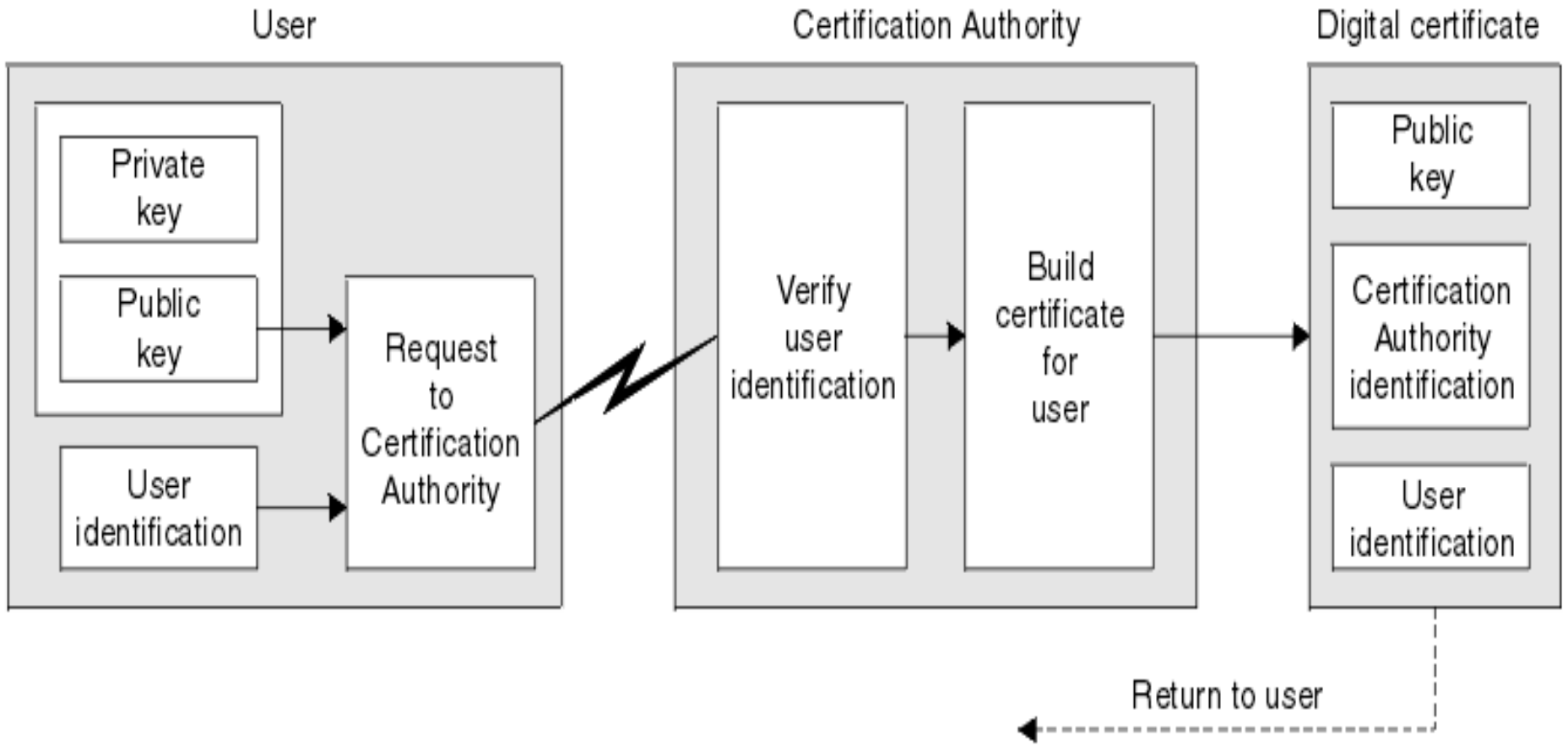
Digital Certificate and Certification Authority

- Digital certificates are electronic credentials that are used to assert the online identities of individuals, computers, and other entities on a network.
- **Digital certificates** function similarly to identification cards such as passports and drivers licenses.
- **Typically, certificates contain the following information:**
- The subject's public key value
- The subject's identifier information, such as the name and email address
- The validity period (the length of time that the certificate is considered valid)
- Issuer identifier information
- The digital signature of the issuer, which attests to the validity of the binding between the subject's public key and the subject's identifier information

Digital Certificate and Certification Authority Cont..

- **Process to obtain a Certificate From CA:**
- User can generate a Key pair of its own and generate a Certificate Signing Request (CSR) and then send the CSR to Issuing CA for a certificate.
- CSR contains the public key of the user and user identity information in a format that issuing CAs would normally expect as shown in figure below.

Digital Certificate and Certification Authority Cont..



Digital Certificate and Certification Authority

- A **Certificate Authority (CA)** issues digital certificates that contain a public key and the identity of the owner.
- The matching private key is not made available publicly, but kept secret by the end user who generated the key pair.
- The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate.
- In essence, the Certificate Authority is responsible for saying "yes, this person is who they say they are, and we, the CA, verify that".

Digital Certificate and Certification Authority Cont..

- **Third Party Authentication**
- In third-party authentication systems, the password or encryption key itself never travels over the network.
- Rather, an "authentication server" maintains a file of obscure facts about each registered user.
- There are many variations on this theme.
- **Kerberos:** Kerberos is a popular third-party authentication protocol.
- Kerberos is an encryption-based system that uses secret key encryption designed to authenticate users and network connections

The authentication process

- Client A sends a request to the Kerberos authentication server (KAS) requesting "credentials" for a given server, B.
- **The KAS responds with the following information, which is encrypted in A's key:**
- A "ticket" for the server. This ticket contains B's key.
- A temporary encryption key (often called a "session key").
- A then transmits—the client's identity and a copy of the session key, both encrypted in B's key—to B.
- The session key (now shared 'by the client and server) is used to authenticate the client and used to authenticate the server in future transaction.
- The session key is then used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

Security Awareness

- Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization
- Security awareness training is a strategy used **by IT and security professionals to prevent and mitigate user risk**.
- A security awareness program is **a formal program with the goal of training users of the potential threats to an organization's information and how to avoid situations** that might put the organization's data at risk.

The key elements of a security awareness program

- Research.
- Development.
- Implementation.
- Monitoring and Review.

Security Policy

- Security policy is a definition of what it means to be secure for a system, organization or other entity.
- For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and wall
- A security policy is of no use to an organization or the individuals within an organization if they cannot implement the guidelines or regulations within the policy.
- It should be **concise, clearly written and as detailed as possible** in order to provide the information necessary to implement the regulation
- There are 2 types of security policies:
- **technical security and administrative security policies**.
- Technical security policies describe the configuration of the technology for convenient use; body security policies address however all persons should behave. All workers should conform to and sign each the policies.

Security Policy Cont..

- An IT Security Policy **identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources**.
- Effective IT Security Policy is a model of the organization's culture, in which rules and procedures are driven from its employees' approach to their information and work.

Five Components of Security Policy:

- It relies on five major elements: **confidentiality, integrity, availability, authenticity, and non-repudiation**.


Thank you!