❖ What Is E-Commerce?

- Electronic commerce or ecommerce is a term for any type of business, or commercial transaction that involves the transfer of information across the Internet.

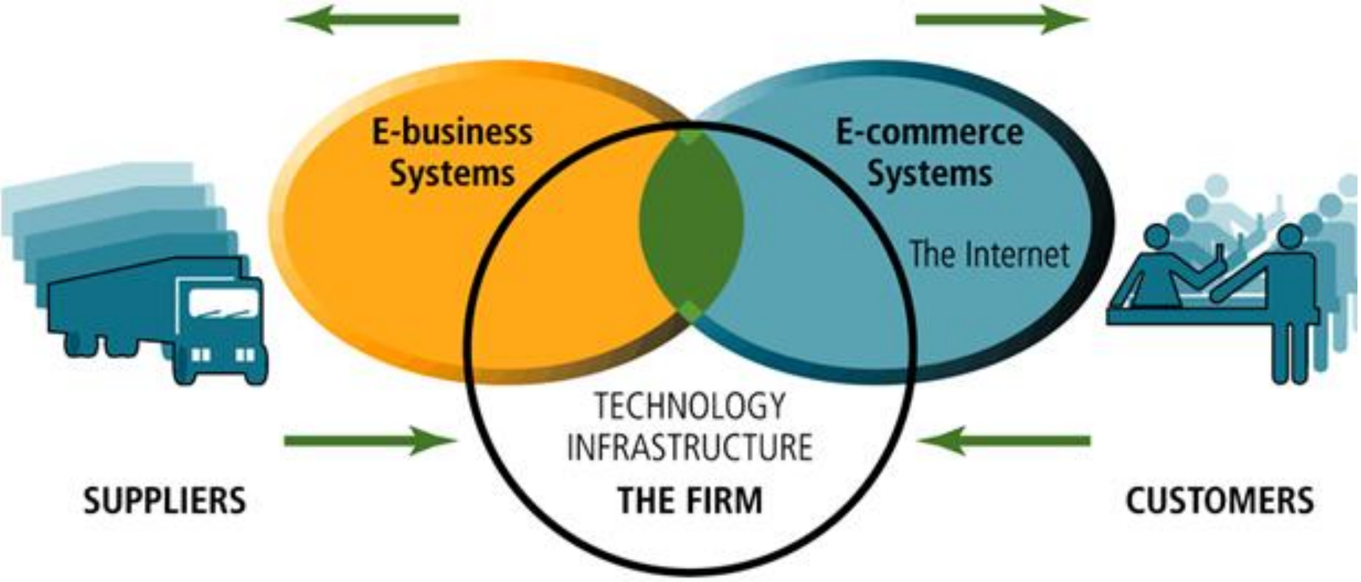
- E-commerce is the use of the internet and the web to transact business. More formally, digitally enabled commercial transactions between and among organizations and individuals.

- There are two types of transactions occurs in E-Commerce
  1. **Digitally enabled transactions** include all transactions mediated by digital technology. This means transactions that occur over the Internet and the Web.
  2. **Commercial transactions** involve the exchange of value (e.g., money) across organizational or individual boundaries in return for products and services.

❖ Difference between E-Commerce and E-Business

E-Commerce	**E-Business**
When a **commercial transaction takes** place over electronic network, then it is termed as e-commerce.	When **electronic medium is used** in all the day-to-day activities, then it may be termed as e-business.
E-Commerce covers outward facing processes that touch customer, suppliers and external partners.	E-Business covers internal processes such as production, inventory management, product management, risk management etc.
E-Commerce usually requires just a use of website.	E-Business involves use of CRM's, ERP's that connect different processes
It is more appropriate in B2C context	It is used in context of B2B transactions
E-Commerce involves mandatory use of internet	E-Business can involves use of internet, internet or extranet
Example:Buying pendrive from	Example: using of inerrnet for

Amazon.com is considered as e-Commerce	maintaining business processes like online customer support, supply chain management etc.



❖ <u>**Eight Unique Features of E-Commerce Technology**</u>

1) Ubiquity

- Internet/Web technology is available everywhere: at work, at home, and elsewhere via mobile devices, anytime.

- It liberates the market from being restricted to a physical space and makes it possible to shop from your desktop, at home, at work, or even from your car, using mobile commerce. The result is called a **marketspace**—a marketplace extended beyond traditional boundaries and removed from a temporal and geographic location

2) Global Reach

- The technology reaches across cultural and across national boundaries, around the Earth.

- E-commerce technology permits commercial transactions to cross cultural and national boundaries far more conveniently and cost-effectively than is true in traditional commerce. As a result, the potential market size for e-commerce merchants is roughly equal to the size of the world's online population (over 1.2 billion in 2007, and growing rapidly)

3) Universal Standards

- The technical standards for conducting e-commerce are universal standards—they are shared by all nations around the world.

- The universal technical standards of the Internet and e-commerce greatly lower market entry costs—the cost merchants must pay just to bring their goods to market. At the same time, for consumers, universal standards reduce search costs—the effort required to find suitable products.

4) Richness

- E-commerce technologies have changed the traditional trade-off between richness and reach. The Internet and Web can deliver, to an audience of millions, "rich" marketing messages with text, video, and audio, in a way not possible with traditional commerce technologies such as radio, television, or magazines.

- The internet has potential for more information richness because it is interactive and can adjust the message to individual users.

5) Interactivity

- The technology works through interaction with the user.

- Interactivity allows an online merchant to engage a consumer in ways similar to a face-to-face experience, but on a much more massive, global scale.

6) Information Density

- The Internet and the Web vastly increase information density—the total amount and quality of information available to all market participants, consumers, and merchants.

- E-commerce technologies reduce information collection, storage, processing, and communication costs. At the same time, these technologies increase greatly the currency, accuracy, and timeliness of information.

7) Personalization/Customization

- E-commerce technologies permit **personalization**: merchants can target their marketing messages to specific individuals by adjusting the message to a person's name, interests, and past purchases. The technology also permits **customization**—changing the delivered product or service based on a user's preferences or prior behavior.

8) Social Technology: User Content Generation and Social Networking

- The Internet and e-commerce technologies have evolved to be much more social by allowing users to create and share content in the form of text, videos, music, or photos with a worldwide community

❖ Introduction to Web 2.0

- Web 2.0. The term means such internet applications which allow sharing and collaboration opportunities to people and help them to express themselves online.

- The Internet and the Web have evolved to the point where users can now create, edit, and distribute content to millions of others; share with one another their preferences, bookmarks, and online personas; participate in virtual lives; and build online communities. This "new" Web is called by many "Web 2.0,"

- **Web 2.0 is:**
  1. Dynamic
  2. Interactive
  3. Participatory
  4. Freedom of information

- **Examples**

- Wikipedia is one of the oldest and best-known wiki-based sites.

- Social networking: The practice of expanding the number of one's business and/or social contacts by making connections through individuals. Social networking sites include Facebook, Twitter, LinkedIn and Google+.

- User-generated content (UGC): Writing, images, audio and video content among other possibilities -- made freely available online by the individuals who create it.

- Photobucket zooms from 4 million to 50 million users and 3 billion consumer generated photos to become the most popular Web photo posting site, offering users an easy way to post and send photos and video, and provides a convenient link to YouTube, MySpace, and blog pages

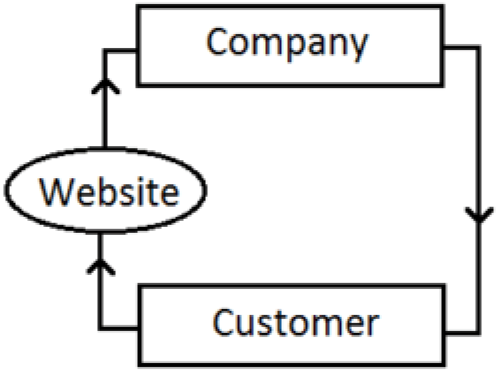
- YouTube, owned by Google after a $1.65 billion purchase, grows to the largest online consumer-generated video posting site and still searches for a profitable business model.

❖ <u>Types of E-commerce</u>

➢ There are a variety of different types of e-commerce and many different ways to characterize these types.

1) B2C—Business-to-Consumer
2) B2B—Business-to-Business
3) C2C—Consumer-to-Consumer
4) P2P—Peer-to-Peer
5) M-commerce—Mobile commerce

1) B2C—Business-to-Consumer

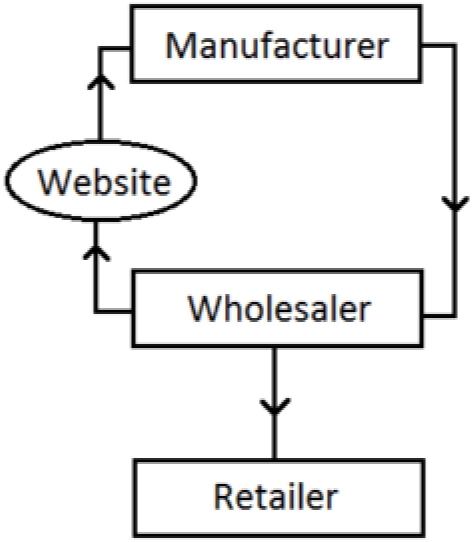


➢ The most commonly discussed type of e-commerce is Business-to-Consumer (B2C) e-commerce, in which online businesses attempt to reach individual consumers.

➢ In this model, the company sells their products, goods or services directly to the consumer online. Here the customer can view products on the website that they want to buy and can order it. After receiving the order details, the company will process the order and then send the products directly to the customer.

- For example, Amazon, Flipkart etc are this type of e-commerce business model which we are using in our daily life. We can view products on the websites like Amazon, Flipkart and can order it. After receiving the order, the selling company of the products processes it and sends it to us. Here a business company is selling their products to the customer with the help of an e-commerce website.

2) B2B—Business-to-Business



- Business-to-Business (B2B) e-commerce, in which businesses focus on selling to other businesses, is the largest form of e-commerce, The ultimate size of B2B e-commerce could be huge.

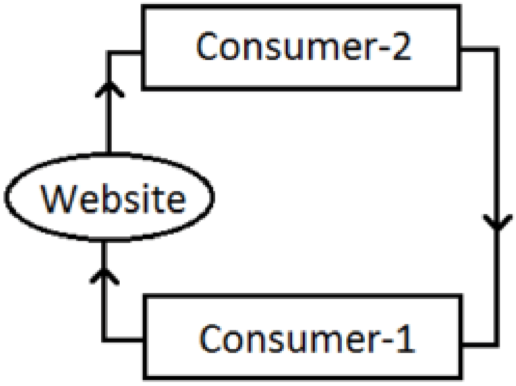
- B2B e-commerce can be simply defined as the commerce between companies. **In** Business-to-Business type of electronic commerce system, companies do business with each other. For say, a manufacturer selling a product to a wholesaler, a wholesaler selling a product to the retailer. Here manufacturer, wholesaler and retailer all are doing their separate businesses.

- Above diagram illustrates the B2B model. There are 3 businesses- wholesaler, manufacturer and the retailer. Here manufacturer has a website using which wholesalers can purchase products from the manufacturer. When a wholesaler places an order on the website, the information regarding the order will be received by the manufacturer through the website. Then after processing the order, the manufacturer will send the product to the wholesaler. After receiving the products wholesaler can sell it to the retailers. This type of business is called B2B model.

- There are two primary business models used within the B2B arena: **Net marketplaces**, which include e-distributors, e-procurement companies, exchanges and industry consortia, and **private industrial networks**, which include single firm networks and industry-wide networks.

3) C2C—Consumer-to-Consumer

- Here a consumer sells products, goods or services to other consumers using the internet or the web technologies. The C2C business model helps us to sell our assets or properties like a car, house, bike, electronics etc via online to other consumers. OLX, Quickr etc are this type of business model.



- Here, if consumer-1 wants to sell a product then he/she can publish the details of the product on the website like OLX or Quickr. The consumer-2 can view the details of the product on that website that consumer-1 wants to sell. If consumer-2 is willing to buy the product that consumer-1 is selling, then the buyer can directly contact the seller and the product will be sold. Here products are selling directly from a consumer to another consumer via the website.

4) P2P—Peer-to-Peer

- A peer-to-peer (P2P) service is a decentralized platform whereby two individuals interact directly with each other, without intermediation by a third-party. Instead, the buyer and the seller transact directly with each other via the P2P service.

- Use of peer-to-peer technology, which enables Internet users to share files and computer resources directly without having to go through a central Web server, in e-commerce.

- Peer-to-peer services bring together individuals, as opposed to bringing together businesses (B2B) or a consumer to a business. Some popular examples of P2P services are:

    - Open-source Software – anybody can view and/or modify code for the software
    - BitTorrent – a popular anonymous file-sharing platform where uploaders and downloaders meet to swap media and software files.
    - Air BnB – allows property owners to lease all or part of their property to short-term renters.
    - Uber – a platform for car owners to offer livery service to people seeking a taxi ride

- eBay – a marketplace for private sellers of goods to find interested buyers.

5) M-commerce—Mobile commerce

- Mobile commerce, or m-commerce, refers to the use of wireless digital devices to enable transactions on the Web. M-commerce involves the use of wireless networks to connect cell phones, handheld devices and personal computers to the Web.
- These wireless devices interact with computer networks that have the ability to conduct online merchandise purchases. Any type of cash exchange is referred to as an e-commerce transaction. Mobile e-commerce is just one of the many subsets of electronic commerce.

❖ The Internet: Technology Background

- **Internet:** interconnected networks of thousands of networks and millions of computers: links businesses, educational institutions, government agencies and individuals. The Internet provides around 400 million people around the world (and over 170 million people in the United States) with services such as e-mail, newsgroups, shopping, research, instant messaging, music, videos, and news

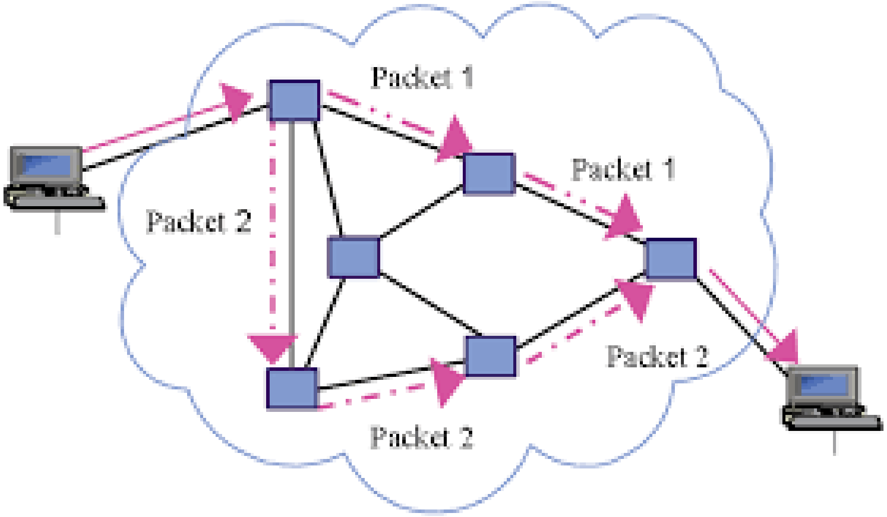
- **The World Wide Web:** The World Wide Web, or Web for short, is one of the Internet's most popular services, providing access to over one billion Web pages, which are documents created in a programming language called HTML and which can contain text, graphics, audio, video, and other objects, as well as "hyperlinks" that permit a user to jump easily from one page to another.

❖ <u>The Internet: Key Technology Concepts</u>

- Behind this formal definition are three extremely important concepts that are the basis for understanding the Internet: packet switching, the TCP/IP communications protocol, and client/server computing.

1) Packet Switching

- Packet switching is a method of slicing digital messages into parcels called "packets," sending the packets along different communication paths as they become available, and then reassembling the packets once they arrive at their destination. Each packet is then transmitted individually and can even follow different routes to its destination



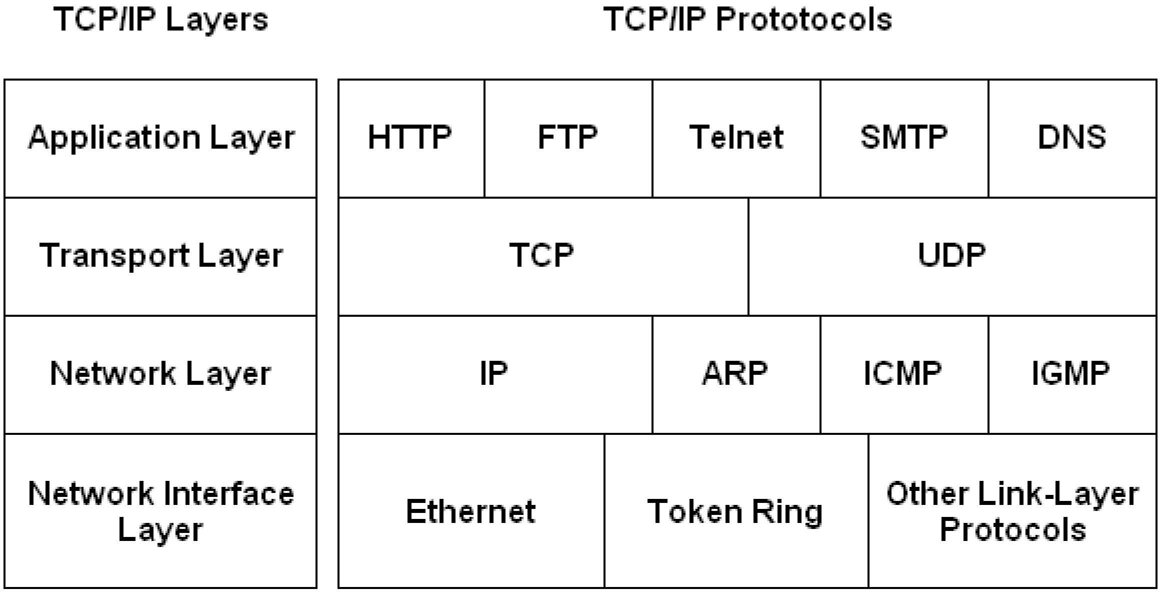
- Messages are first broken down into packets. Appended to each packet are digital codes that indicate a source address (the origination point) and a destination address, as well as sequencing information and error control information for the packet. Rather than being sent directly to the destination address, in a packet network, the packets travel from computer to computer until they reach their destination. These computers are called routers.

2) TCP/IP

- TCP refers to the Transmission Control Protocol (TCP). IP refers to the Internet Protocol (IP). A protocol is a set of rules for formatting, ordering, compressing, and error-checking messages. It may also specify the speed of transmission and means by which devices on the network will indicate they have stopped sending and/or receiving messages.

- TCP establishes the connections among sending and receiving Web computers, handles the assembly of packets at the point of transmission, and their reassembly at the receiving end.

- TCP/IP is divided into four separate layers, with each layer handling a different aspect of the communication problem



TCP/IP Layers	TCP/IP Prototocols				
Application Layer	HTTP	FTP	Telnet	SMTP	DNS
Transport Layer	TCP			UDP	
Network Layer	IP		ARP	ICMP	IGMP
Network Interface Layer	Ethernet		Token Ring	Other Link-Layer Protocols	

- **The Network Interface Layer** is responsible for placing packets on and receiving them from the network medium, which could be a Local Area Network (Ethernet) or Token Ring Network, or other network technology.

- **The Internet Layer** is responsible for addressing, packaging, and routing messages on the Internet.

- **The Transport Layer** is responsible for providing communication with the application by acknowledging and sequencing the packets to and from the application.

- **The Application Layer** provides a wide variety of applications with the ability to access the services of the lower layers. Some of the best known applications are HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP)

3) IP Addresses

- IP provides the Internet's addressing scheme. Every computer connected to the Internet must be assigned an address—otherwise it cannot send or receive TCP packets.

- An IP is a 32-bit number comprised of a host number and a network prefix, both of which are used to uniquely identify each node within a network.

- The format of an IP address is a 32-bit numeric address written as four numbers separated by periods and **each part is known as octet**. Each number can be zero to 255.

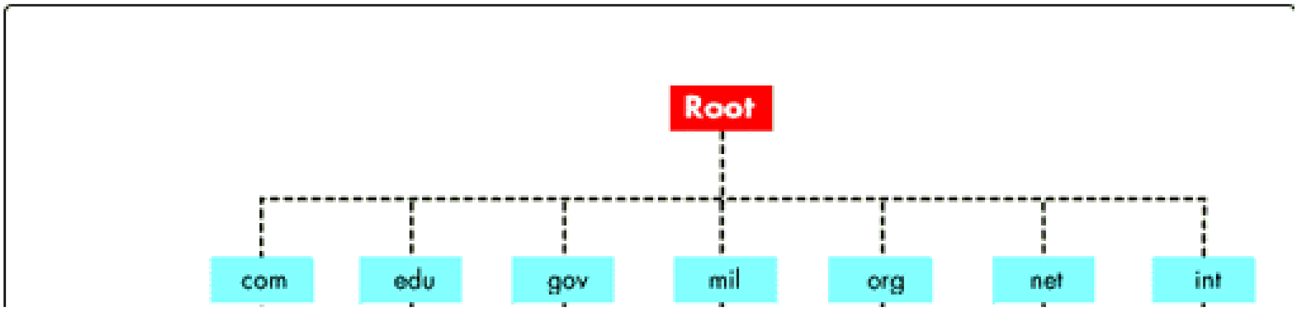
- The current version of IP is called Version 4, or IPv4. Because many large corporate and government domains have been given millions of IP addresses a new version of the IP protocol, called IPv6 is being adopted. This scheme contains 128-bit addresses

4) Domain Names and URLs

- Most people cannot remember 32-bit numbers. IP addresses can be represented by a natural language convention called domain names.

- The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses

- **Uniform resource locators (URLs)**, which are the addresses used by Web browsers to identify the location of content on the Web, also use domain names as part of the URL. A typical URL contains the protocol to be used when accessing the address, followed by its location.



- how TCP/IP and packet switching work together to send data over the Internet.

How TCP/IP Works

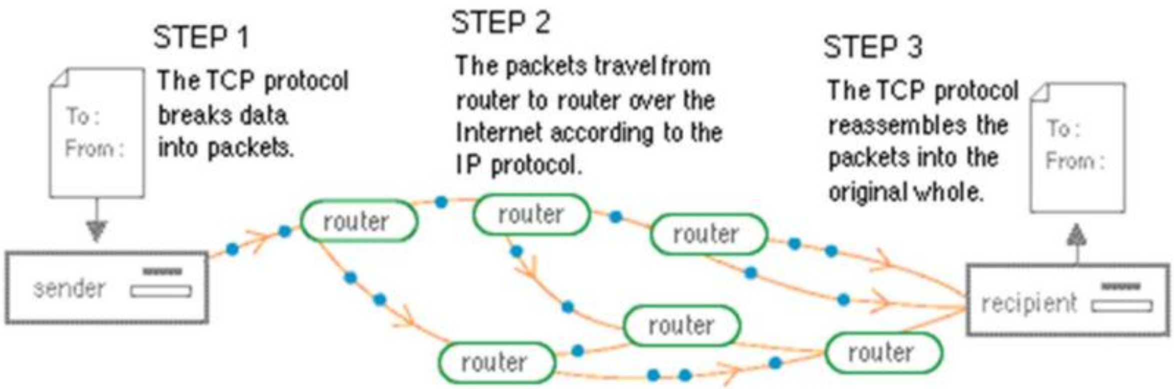
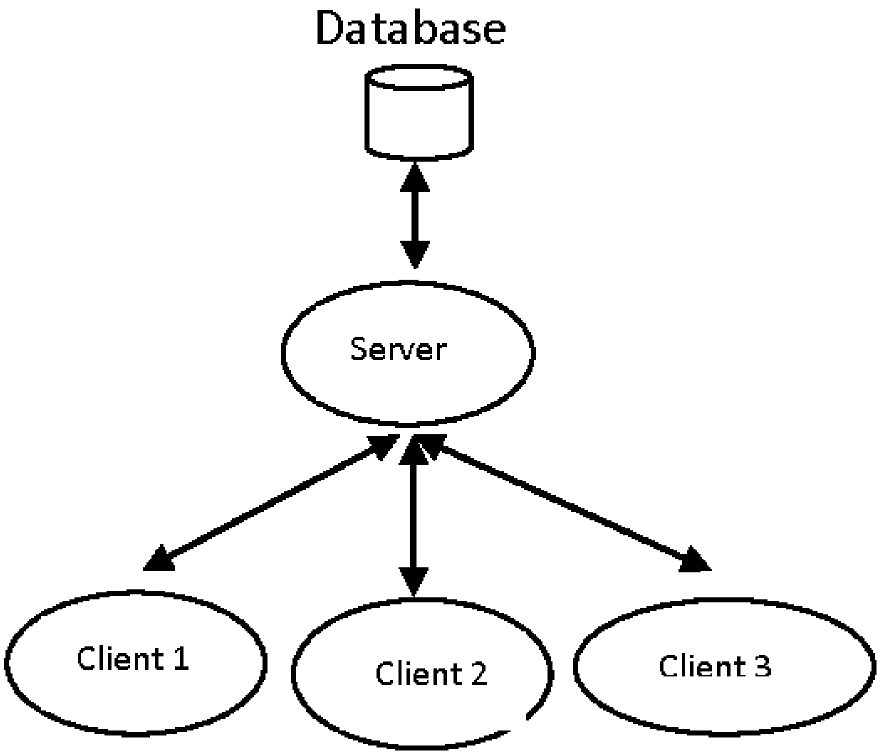

STEP 1
The TCP protocol breaks data into packets.
To:
From:
sender
STEP 2
The packets travel from router to router over the Internet according to the IP protocol.
router
router
router
router
router
router
STEP 3
The TCP protocol reassembles the packets into the original whole.
To:
From:
recipient

Figure 2. How data travels over the Net.

5) Client/Server Computing

- is a model of computing in which very powerful personal computers called clients are connected together in a network together with one or more server computers.

- Servers are networked computers dedicated to common functions that the client machines on the network need, such as storing files, software applications, utility programs such as Web connections, and printers.



❖ <u>Other Internet Protocols and Utility Programs</u>

1) HTTP:

- Hypertext Documents. HTTP (short for HyperText Transfer Protocol) is the Internet protocol used for transferring Web pages.

- The HTTP protocol runs in the Application Layer of the TCP/IP model .An HTTP session begins when a client’s browser requests a Web page from a remote Internet server. When the server responds by sending the page requested, the HTTP session for that object ends.

2) SMTP, POP, and IMAP:

- **Sending E-mail**. E-mail is one of the oldest, most important,and frequently used Internet services. STMP (Simple Mail Transfer Protocol) is the Internet protocol used to send mail to a server.

- **POP (Post Office Protocol)** is used by the client to retrieve mail from an Internet server

- **IMAP (Internet Message Access Protocol)** is a more current e-mail protocol supported by many servers and all browsers. IMAP allows users to search, organize, and filter their mail prior to downloading it from the server.

3) FTP:

- Transferring Files. FTP (File Transfer Protocol) is one of the original Internet services. It is a part of the TCP/IP protocol and permits users to transfer files from the server to their client machine, and vice versa. The files can be documents, programs, or large database files. FTP is the fastest and most convenient way to transfer files larger than 1 megabyte, which many mail servers will not accept.

4) SSL:

- Security. SSL (Secure Sockets Layer) is a protocol that operates between the Transport and Application Layers of TCP/IP and secures communications between the client and the server. SSL helps secure e-commerce communications and payments through a variety of techniques such as message encryption and digital signatures.

5) Telnet:

- Running Remote. Telnet is a terminal emulation program that runs in TCP/IP. You can run Telnet from your client machine. When you do so, your client emulates a mainframe computer terminal .

- Telnet was the first “remote work” program that permitted users to work on a computer from a remote location.

6) Finger:

- Finding People. You can find out who is logged onto a remote network by using Telnet to connect to a server, and then typing “finger” at the prompt.

- Finger is a utility program supported by UNIX computers. When supported by remote computers, finger can you tell you who is logged in, how long they have been attached,and their user name.

7) Ping:

- Testing the Address. You can “ping” a host computer to check the connection between your client and the server. The ping (Packet InterNet Groper) program will also tell you the time it takes for the server to respond, giving you some idea about the speed of the server and the Internet at that moment.

- You can run ping from the DOS prompt on a personal computer with a Windows operating system by typing: Ping <domain name>.

8) Tracert:

- Checking Routes. Tracert is one of a several route-tracing utilities that allow you to follow the path of a message you send from your client to a remote computer on the Internet.

❖ Intranets And Extranets

Intranet

- An intranet is a TCP/IP network located within a single organization for purposes of communications and information processing.

- An intranet is a private network that allows employees and staff in an enterprise to securely share knowledge and information easily within the company or organization. Information, tools, directories, and services available on a company’s intranet are typically unavailable to the general public.

- The prefix "intra" implies that an intranet is designed for internal communications only. Intranets are usually restricted to specific local area networks (LANs) or wide area networks (WANs).

Extranet

- Extranets are formed when firms permit outsiders to access their internal TCP/IP networks.

- An extranet is a private network that leverages internet technology and public telecommunication system to share part of a business's information or operations over a secure system with suppliers, vendors, partners, customers, or other businesses. An extranet is often considered part of a company's intranet that is extended to authorized users outside of the organization.

❖ Security Threats in the E-commerce Environment

- Three key points of Weakness
  1. Client
  2. Server
  3. Communications pipeline

- Following are most common and damaging forms of security threats to e-commerce consumers and site operators.

1. Malicious code

- Malicious code (sometimes referred to as “ malware”) includes a variety of threats such as viruses, worms, Trojan horses.

Virus

- A virus is a small program designed to infect your computer and cause errors, computer crashes, and even destroy your computer hardware.

- Unlike spyware, a virus can grow and replicate itself and spread to other files. Most computer viruses deliver a “payload.”

- The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive destroying files, reformatting the computer’s hard drive, or causing programs to run improperly.

- Computer viruses fall into several major categories as follows.

1) **Macro viruses**

- are application specific, meaning that the virus affects only the application for which it was written, such as Microsoft Word, Excel, PDF, or PowerPoint.

- When user open infected document, the virus copies itself/replicate to the templates in the application, so that when new documents are created, they are infected with the macro virus as well.

- Macro virus can easily be spread when sent in an e – mail attachment or by flash drive from one computer to another along with infected documents (word, excel, PDF etc).

2) **File - Infecting viruses**

- usually infect executable files, such as *.com, *exe, *dll files. These type of viruses may activate every time, when the infected file is executed by copying themselves into other executable files.File – infecting viruses are also easily spread through e – mails and any file transfer system.

3) **Script viruses**

- These are written in script programming languages such as VBScript (visual Basic Script) and JavaScript. The viruses are activated simply by double – clicking an infected *.vbs or *.js file.

Trojan Horses

- The Trojan horse is not itself a virus because it does not replicate, but is often a way for viruses or other malicious code such as bots or rootkits.

- RootKit: a program whose aim is to subvert (weaken) control of the computer's operating system)

Bots:

- It is a type of malicious code that can be covertly installed on a computer when attached to the internet. Once installed, the bot responds to external commands sent by the attacker and your computer becomes a "zombie," and is able to be controlled by an external third party (who programmed it).

- Botnet: collection of captured bot computers used for malicious actvities such as participating in a DDoS attacks.

Worms

- Worms that is designed to spread from computer to computer.Worm is more dangers than a virus , reason is simple Viruses infect a single computer, and may destroy but produce very little crash but a worm that can propagate from one computer to another, perhaps to millions.

- A worm does not necessarily need to be activated by a user or program in order for it to replicate itself. For example, the Slammer worm, which targeted a known vulnerability in Microsoft’s SQL Server database software, infected more than 90% of vulnerable computers worldwide within 10 minutes of its release on the Internet.

2. Unwanted programs

- Applications that install themselves on a computer, typically without the user’s informed consent. Such Spyware, Adware Browser parasites.

- Such programs are found on social networking and user generated content sites.

Spywares

- a user’s keystrokes, copies of e – mail and instant messages, and even take screenshots (and thereby capture passwords or other confidential data)

- A common spyware type is a keylogger which records keystrokes typed on your keyboard. This is how people lose their bank account or personal details. Any information collected by spyware is usually with the intent to sell.

Adwares

- Adware is exactly as the name suggests, software with advertising. Adware is software that displays advertisements on your computer.

- Adwares is typically used to call for pop – up ads to display when the user visits certain sites. Adware can be downloaded and sometimes included in free programs.some pop-up windows will have a button that says "Close Window."

- The close button is actually an install button. When the user clicks the close button, more adware is installed on his computer.The most common changes that adware makes on a computer are to the Internet browser. It can change the homepage and add a toolbar to the browser.If you get attacked by pop-up ads when you're not even connected to the Internet, you may have adware on your computer.

- Adware may be contain spyware that can track your online activities, collect your web surfing habits, addresses, and purchase preferences. It can also gather information about the hardware and software installed on your home computer and sends that information to marketers.

- Example: Alexa Toolbar, Zingo search , purityScan are examples of adware programs that open the webpages or display pop – up ads of partner sites when certain keywords are used in Internet searches.Windows Live messenger and Yahoo messenger contain adware.

Browser Parasites

- A browser parasite is a program that can monitor and change the settings of a user's browser, for instance, changing the browser home page, or sending information about the sites visited to a remote computer.

- Browser Parasites often a component of adware.For example, websearch toolbar is adware component that modifies IE default home page and search settings.

3. Phishing and identity theft

- Phishing is any deceptive, online attempt by a third party to obtain confidential information for financial gain. Phishing attacks do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so – called " social engineering" techniques.

- Examples:1. The most popular e – mail scam letter.2. You receive a contain message you won a lottery but first deposit some amount in the following account a/c.

4. Hacking and cyber vandalism

- Hacking: A hacker is an individual who intends to gain unauthorized access to a computer system.Cracker: Within the hacking community, a term typically used to denote a hacker with criminal intent.

- The terms hacker and cracker tends to be used interchangeably.Hackers and crackers gain unauthorized access by finding weaknesses in the security procedures of web sites and computer systems.

- Cybervandalism: Intentionally disrupting , defacing , or even destroying the site is called Cybervandalism.

- Groups of hackers called tiger teams are sometimes used by corporate security departments to test their own security measures.By hiring hackers to break into the system from outside, they company, can identify weaknesses in the computer system’s.

➢ **Types of hackers:**

1. **White Hats:** “good” hackers who help organizations locate and fix security flaws.Whites hats do their work under contract, with agreement from clients that they will no be prosecuted for their efforts to break in.

2. **Black Hats:** Hackers who act with the intention of causing harm.They break into web sites and reveal the confidential information they find. They believe strongly that information should be free and they share it with others.

3. **Grey Hats:** hackers who believe they are pursuing some greater good by breaking in and revealing systems flaws.Grey hats discover weaknesses in a system’s security, and then publish the weakness without disrupting the site or attempting to profit from their finds.

5. Credit card fraud/theft

➢ Credit card fraud is when someone uses your credit card or credit account to make a purchase you didn't authorize. This activity can happen in different ways:

- If you lose your credit card or have it stolen, it can be used to make purchases or other transactions, either in person or online.

- Fraudsters can also steal your credit card account number, PIN and security code to make unauthorized transactions, without needing your physical credit card. (Unlawful transactions like these are known as card-not-present fraud.)

6. Spoofing (Pharming) & spam (junk) web sites

- Misrepresenting self by using fake address and redirecting a Web link to a new, fake Web site is called Spoofing.Spoofing a website is also called Pharming.

- How it work:Links that are designed to lead to one site users to to a totally unrelated site.Spoofing threatens the integrity, confidentiality, Authenticity and privacy of a site.For example, if hackers redirect customers to a fake web site that looks almost exactly like the true site, they can then collect and process orders, credit card info, usernames/passwords, effectively stealing business from the true sites.

- **Spam Web sites**: typically appear on search results, and do not involve .Spam web sites that promise to offer some product or service, but in fact are a collection of advertisements for other sites, some of which contain malicious code.

7. Sniffing

- Sniffing is a program/software that monitors information traveling over a network.Sniffers enable hackers to steal proprietary information from anywhere on a network, including e – mail messages, company files and confidential reports.The threat of sniffing is that confidential or personal information will be made public.

- **E – mail wiretaps** are a variation on the sniffing threat. An email wiretap is hidden code in an e- mail message that allows someone to monitor all succeeding messages forwarded with the original message. E –mail wiretaps can be installed on servers and client computers.

- A more practical location for this attack is near the shopper's computer or the server. Wireless hubs make attacks on the shopper's computer network the better choice because most wireless hubs are shipped with security features disabled. This allows an attacker to easily scan unencrypted traffic from the user's computer.

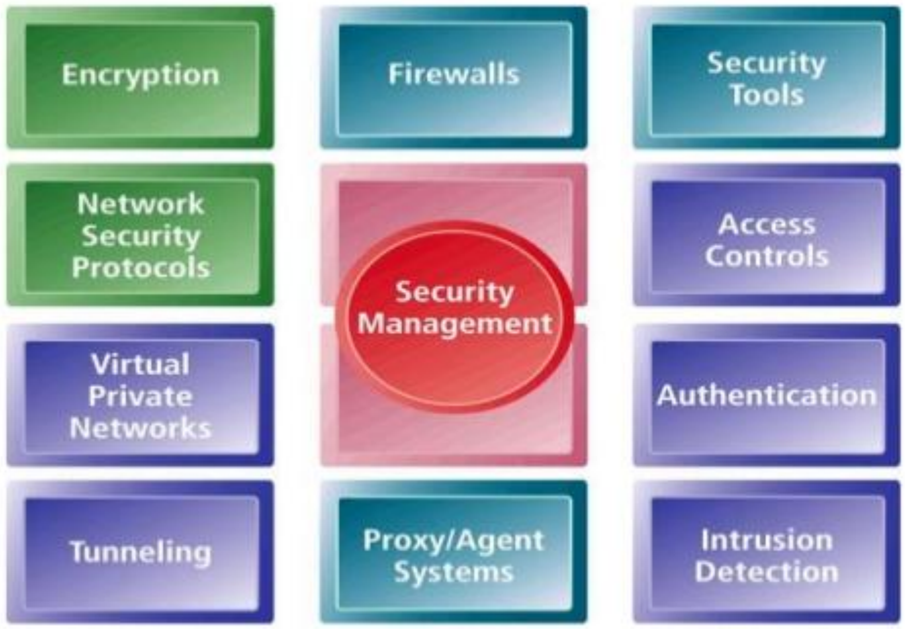
8. **Insider Attacks**

- Single largest financial threat we tend to think of security threats to a business as originating outside the organization. In fact, the largest financial threats to business institutions come not from robberies but from by insiders.

- Bank employees steal far more money than bank robbers. The same is true for e – commerce sites. Some of the largest disruptions to service, destruction to service, destruction to sites, and diversion of customer credit data and personal information have come from insiders once trusted employees.

❖ Technology Solutions

Following diagram shows major tools available to achieve site security.



- **Protecting internet communications**

- A number of tools available to protect the security of internet communications, the most basic of which is message encryption.

Encryption:

- Process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver.

- Purpose: Secure stored information and information transmission.

- Provides:

  Message integrity

  Authentication

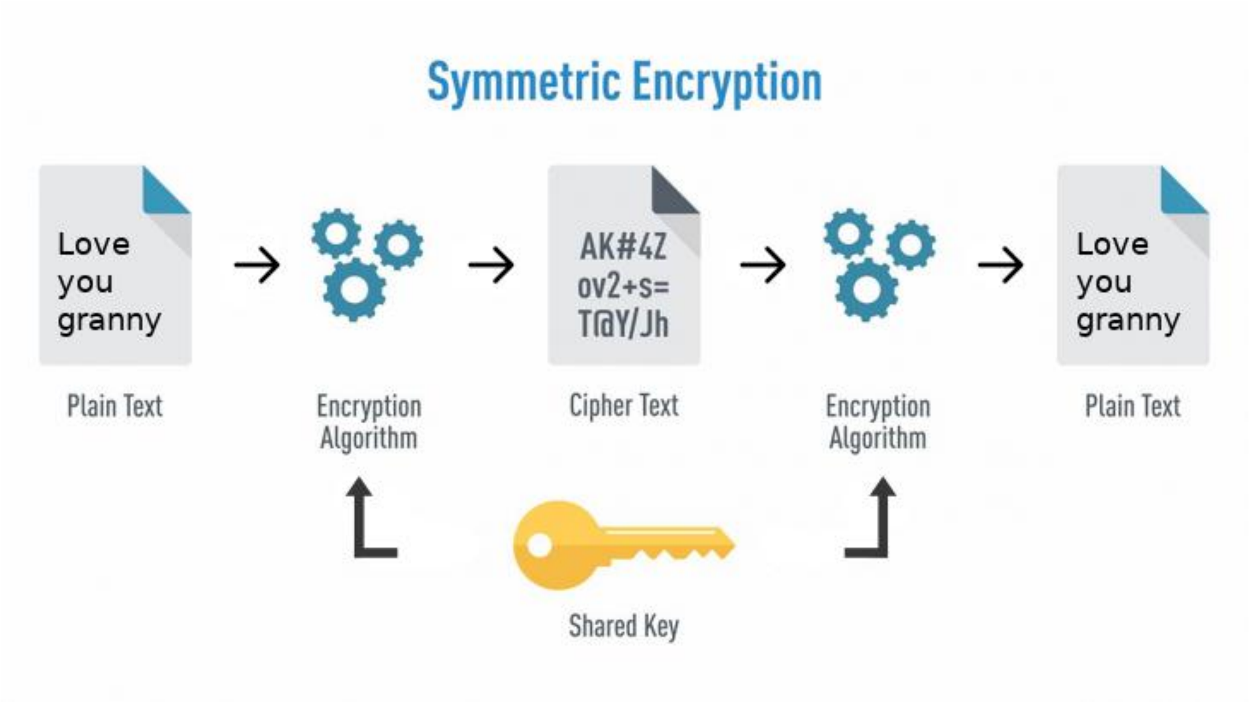
  Confidentiality

1. Symmetric Key Encryption

- Also known as secret key encryption.

- In **symmetric encryption**, you use the same key for both **encryption** and **decryption** of your data or message. i.e. Both the sender and receiver use the same digital key to encrypt and decrypt message.

- Modern encryption system are digital. The cipher or keys used to transform plain text into cipher text are digital strings.



- It requires a different set of keys for each transaction.

- Modern digital encryption systems use keys with 56, 128, 256 or 512 binary digits.

- Data Encryption Standard (DES) was developed by national security agency (NSA) and IBM in 1950.The DES uses a 56-bit key. To cop up with faster computers, it has been improved by Triple DES, which applies the DES algorithm three times with different keys.

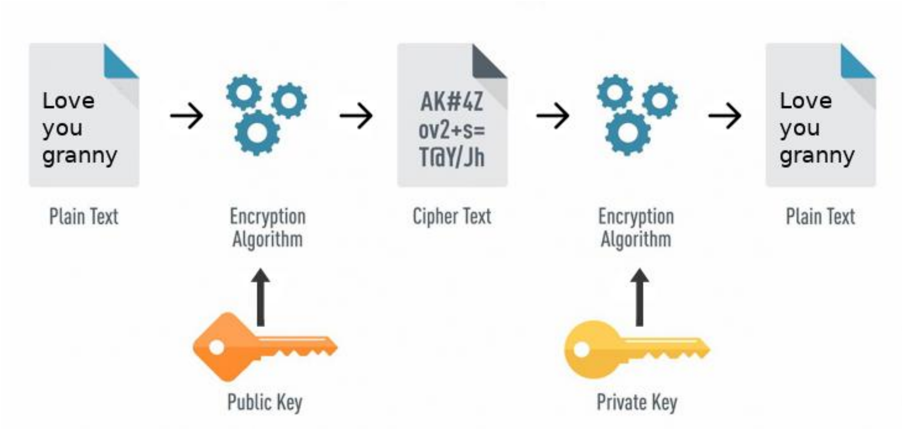
- DES has since been replaced by the **Advanced Encryption Standard (AES),** which uses 128-, 192- or 256-bit keys. Most people believe that AES will be a sufficient encryption standard for a long time coming

2. Public Key Encryption

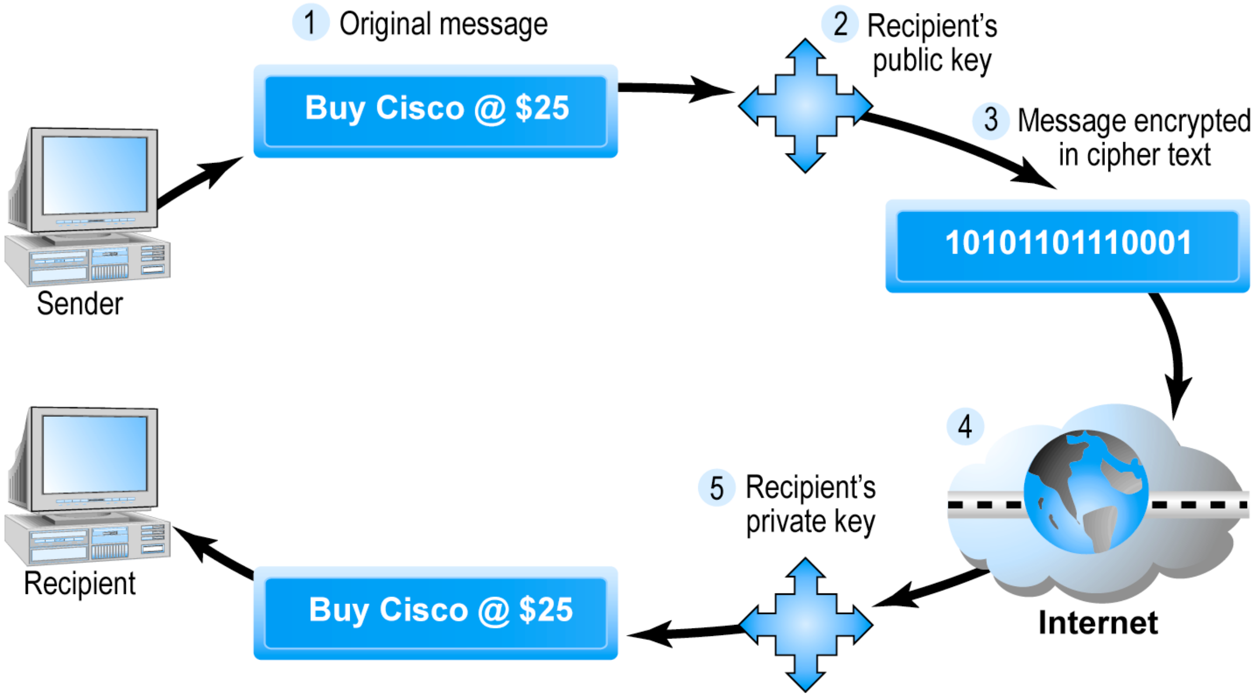
- Solves symmetric key encryption problem of having to exchange secret key.

- It uses not one key but a pair of keys: a **private** (kept secret by owner) one and a **public**(widely disseminated) one.Both keys used to encrypt and decrypt message

- Once key used to encrypt message, same key cannot be used to decrypt message



- For example, sender uses recipient's public key to encrypt message recipient uses his/her private key to decrypt it



Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other to decrypt.
The size of ciphertext is the same or smaller than the original plaintext.	The size of ciphertext is the same or larger than the original plaintext.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data needs to be transferred.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher

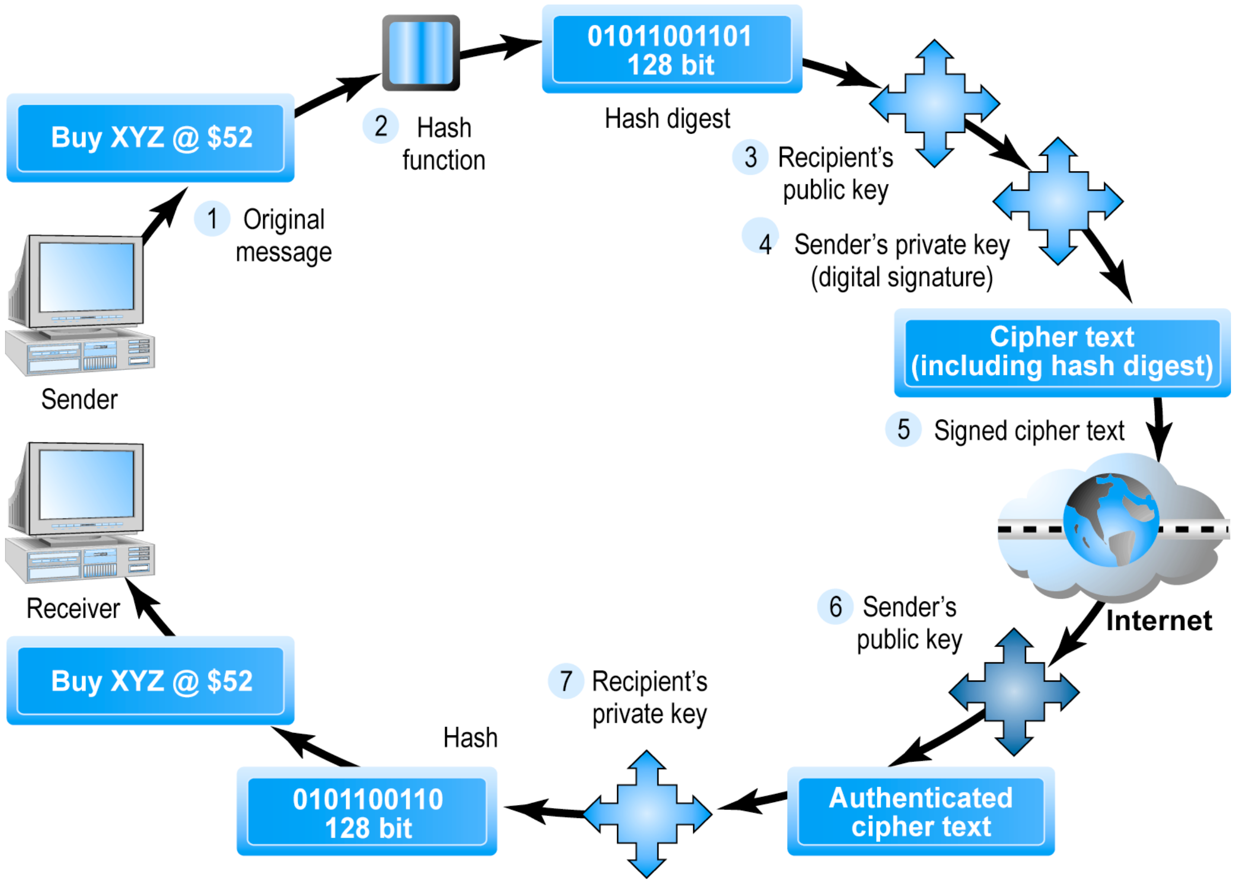
In symmetric key encryption, resource utilization is low compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is lower as only one key is used for both encryption and decryption purposes.	Security is higher as two keys are used, one for encryption and the other for decryption.

3. Public Key Encryption using Digital Signatures and Hash Digests

- To check confidentiality of a message a hash function is used to create a digest of a message. **A hash function** is an algorithm that produces a fixed-length number call hash or message digest.

- One more step is required to ensure authenticity of a message , the sender encrypts the entire block of cipher text one or more time using sender’s private key produces **digital signature.**

- When used to sign a hased document, the digital signature is also unique to the document, and changes for every document.



- The receiver of this signed cipher text first uses the sender's public key to authenticate the message.once authenticated, the receiver uses his or her private key to obtain hash result and original message.

- As a final step the receiver applies the same function to the original text and compares the result with the result sent by sender.

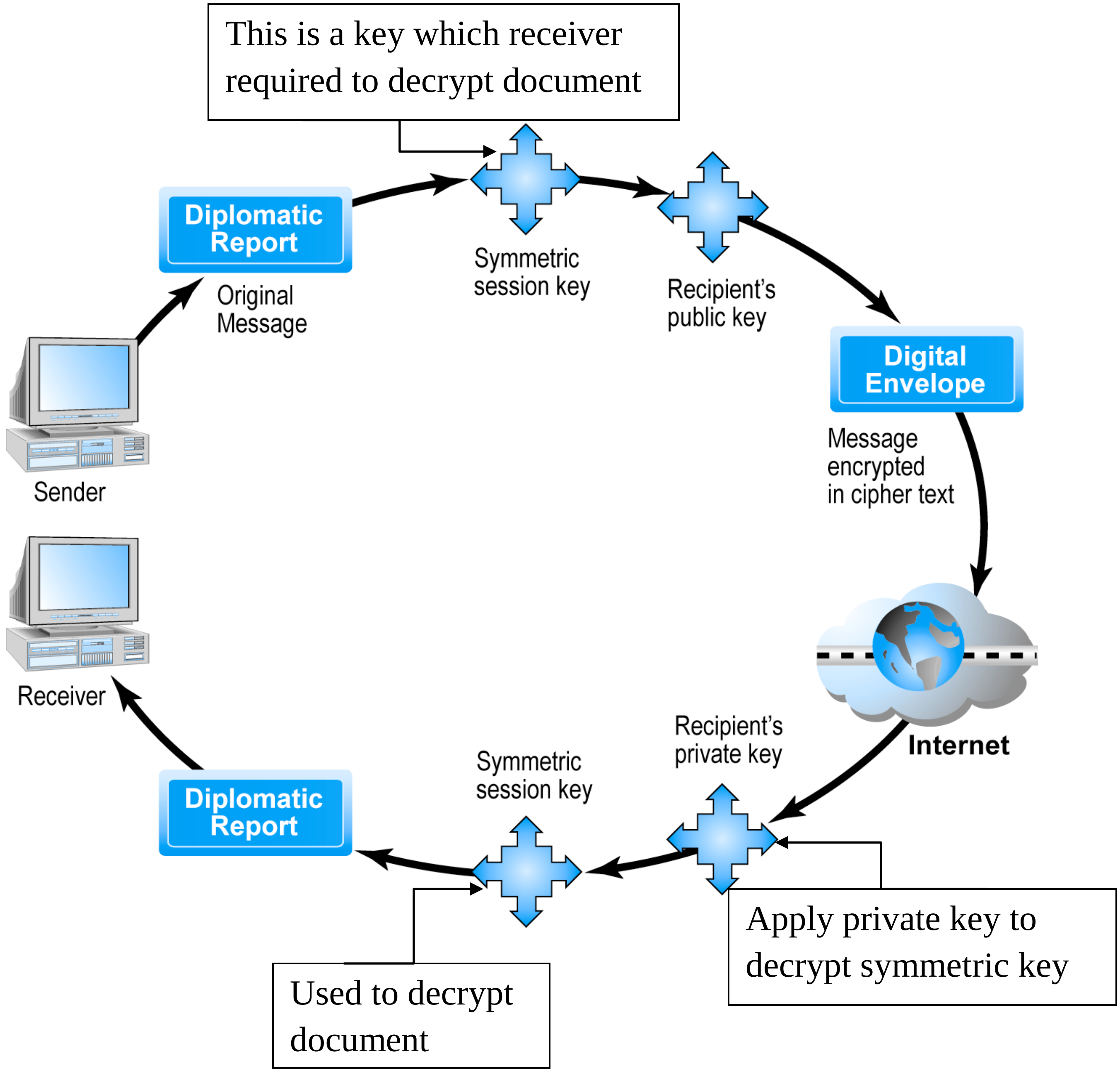
4. Digital Envelopes

- A type of security that uses two layers of encryption to protect a message. Secret (symmetric) key and public key encryption.

- First, the message itself is encoded using symmetric encryption, and then the key to decode the message is encrypted using public-key encryption.

- This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption.

- Following diagram shows how it works.



This is a key which receiver required to decrypt document

Apply private key to decrypt symmetric key

Used to decrypt document

5. Digital Certificates and Public Key Infrastructure (PKI)

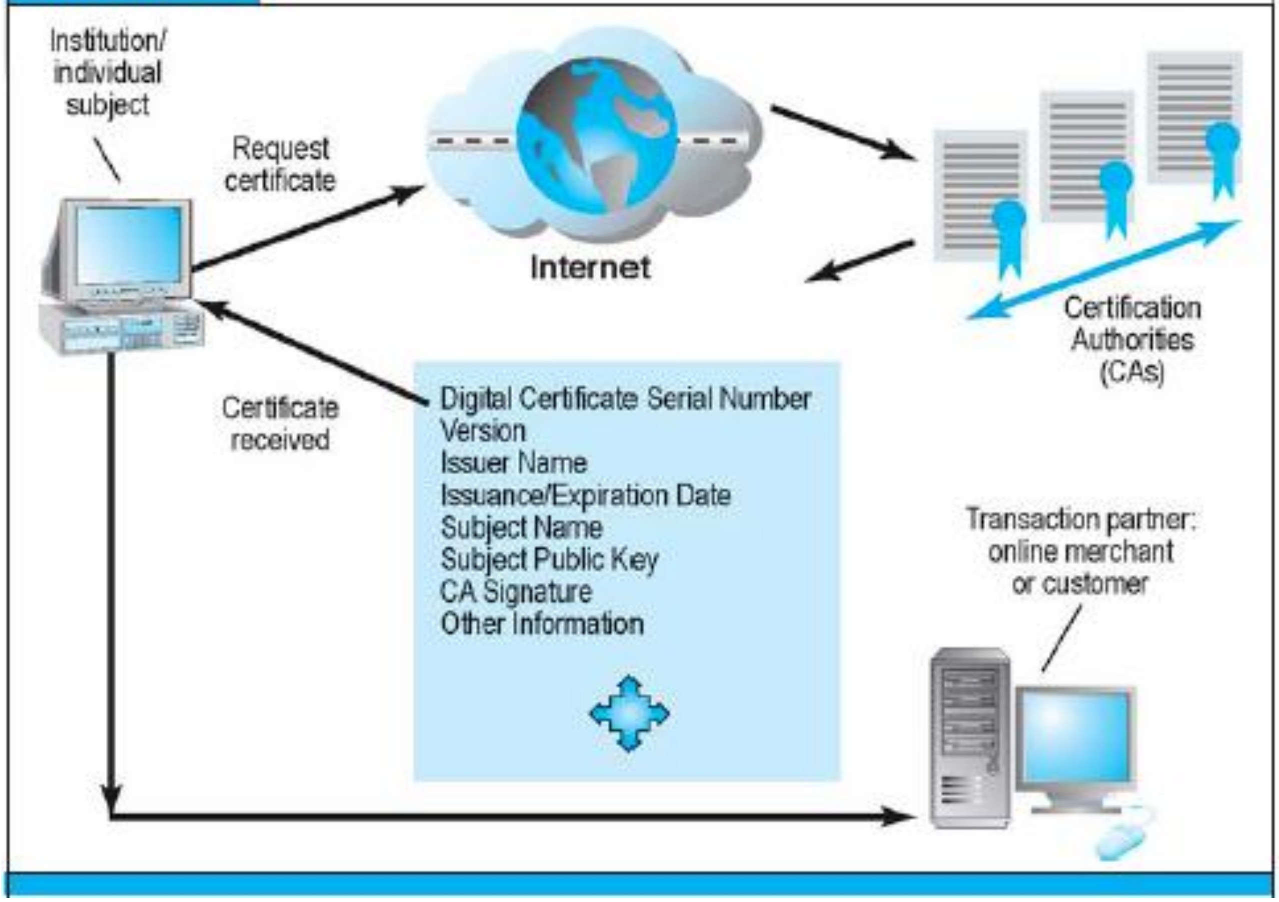
- An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

- An individual wishing to send an encrypted message applies for a digital certificate from a ***Certificate Authority (CA)***. that includes:

– Name of subject/company
– Subject’s public key
– Digital certificate serial number
– Expiration date
– Issuance date
– Digital signature of certification authority (trusted third party institution) that issues certificate
– Other identifying information

- **Public Key Infrastructure (PKI):** refers to the CAs and digital certificate procedures that are accepted by all parties

FIGURE 5.13 DIGITAL CERTIFICATES AND CERTIFICATION AUTHORITIES



- The user generates a public or private key pair and sends a request to CA with user’s public key.

- The CA verifies the information and issues certificate containing the user’s public key and other information. Finally CA creates message digest from certificate and sign with CA private key. The signed digest is called signed certificate.