Online Security and Payment System

❖ E-Commerce Security Environment

- Ecommerce security is a set of protocols that safely guide ecommerce transactions. Stringent security requirements must be in place to protect companies from threats like credit card fraud.
- Cybercrime is become more significant problem for both organization and consumers.
- **Reporting issues**
  2012 survey: Average annualized cost of cybercrime was $8.9 million/year
- **Underground economy marketplace**:
  Stolen information stored on underground economy servers. finding these servers is difficult for average users

❖ What Is Good E-commerce Security?

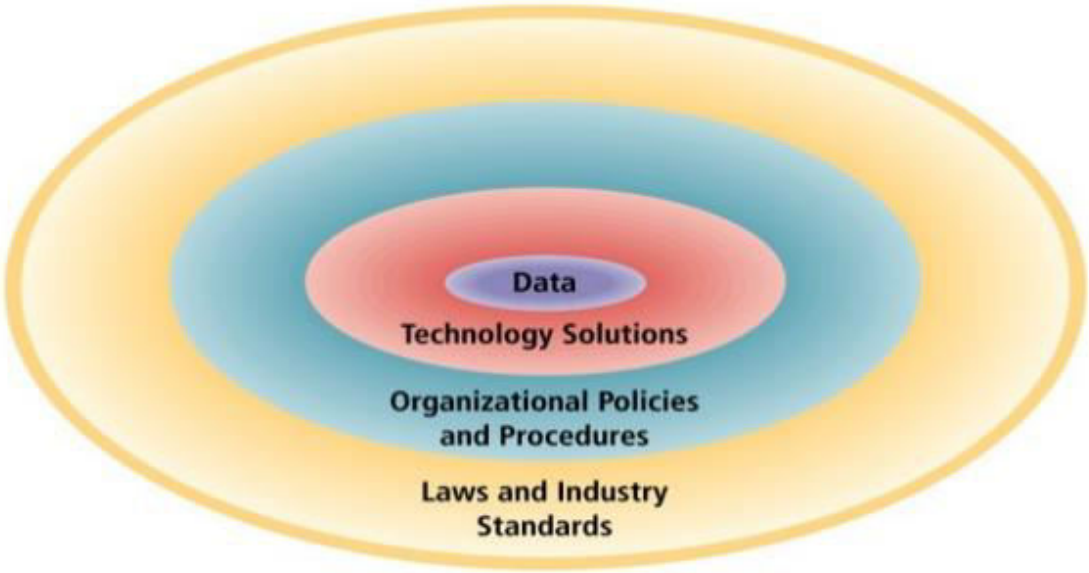
- **To achieve highest degree of security**

New technologies Organizational policies and procedures
Industry standards and government laws

- **Other factors**

Time value of money Cost of security vs. potential loss
Security often breaks at weakest link

The E-commerce Security Environment



❖ Dimensions of E-commerce Security

1) Integrity

- The ability to ensure that information being displayed on a web site or transmitted or received over the internet has not been altered in any way by an unauthorized party

2) Nonrepudiation

- The ability to ensure that e-commerce participants do not deny (i.e. repudiate) their online actions.

3) Authenticity

- The ability to identify the identity of a person or entity with whom you are dealing in the internet

4) Confidentiality

- The ability to ensure that messages and data are available only to those who are authorized to view them.

5) Privacy

- The ability to control the use of information about oneself.

6) Availability

- The ability to ensure that an e-commerce site continues to function as intended

❖ The tension between security and other values

1. Security vs. ease of use:

- There are tensions b/w security and ease of use. When traditional merchants are so fearful of robbers,the same can be true on the web.

- The more security measures added, the more difficult a site is to use, and the slower it becomes. Digital security is purchased at the price of slowing down processes.

- Too much security can harm profitability, while not enough security can potentially put you out of business. The more

security measures added, the more difficult a site is to use, and the slower it becomes

2. Security vs. Public Safety and The Criminal uses of the Internet

- There is also an expected tension b/w the desires of individuals to hide their identity and the needs of public officials to maintain public safety than can threatened by criminals or terrorists.

- Use of technology by criminals to plan crimes or threaten nation- state. Terrorists are also fond users of the Internet and have been for many years.

- Encrypted files sent via e – mail were used by Ramsey Yousef – a member of the Al Qaeda responsible for bombing the World Trade Center in 1993, as American Says. Encrypted files used to hide plans for bombing 11 U.S. airliners.

❖ 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.

9. Poorly designed server and client software

- Many security threats prey on poorly designed server and client software, sometimes in the operating system and sometimes in the application software, including browsers.

- The very design of the personal computer includes many open communication ports that can be used, and indeed are designed to be used, by external computers to send and receive messages. The port typically attacked is TCP port 445.

- May client computer didn't install antivirus program or didn't enable firewall.May be many unwanted programs are in browsers.

❖ 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:

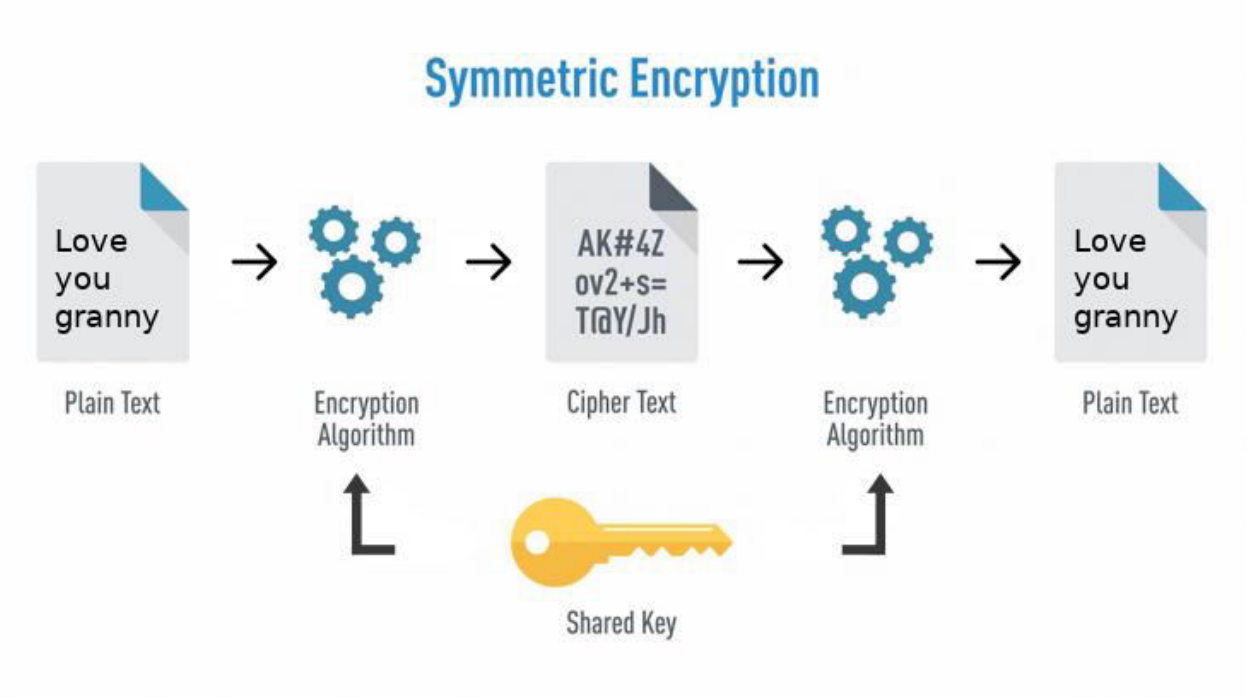
  Message integrity

  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.

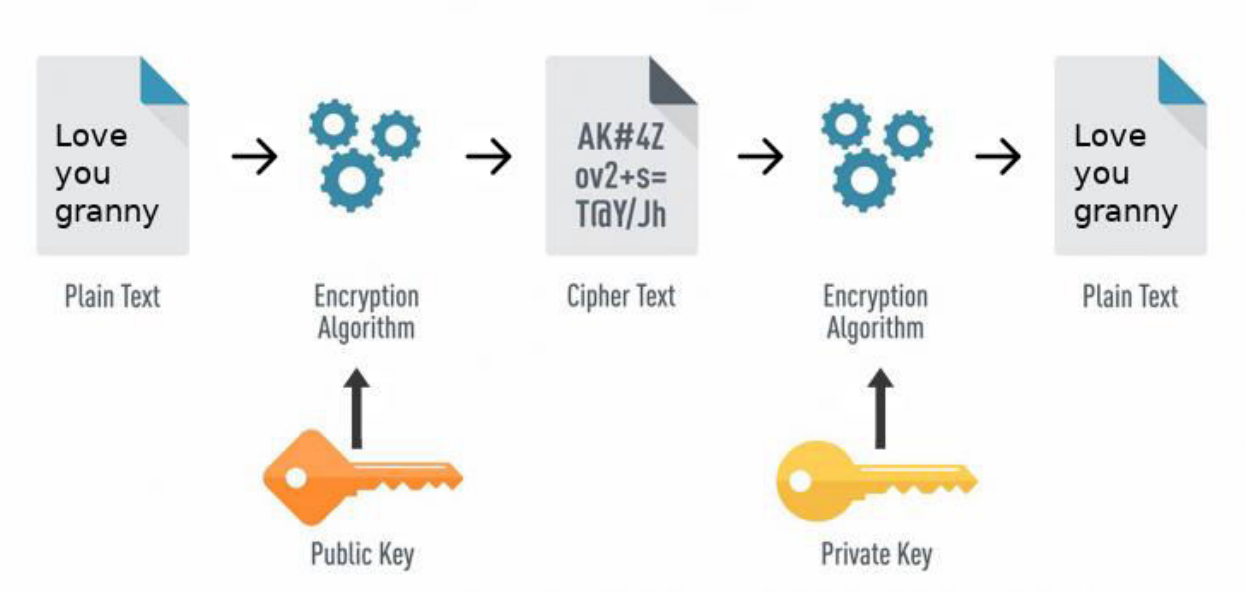
- DES has since been replaced by the **Advanced Encryption Standard (AES),** which uses 128-, 192- or 256-bit keys. Most people believe that AES will be a sufficient encryption standard for a long time coming

2. Public Key Encryption

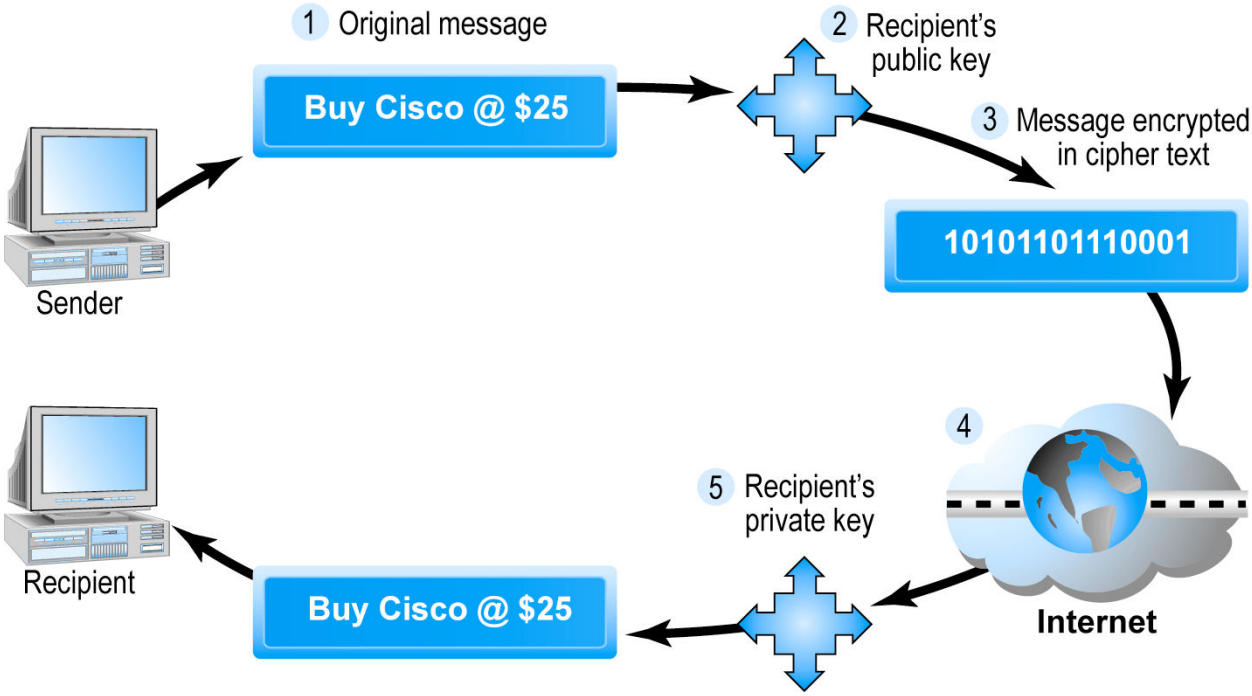
- Solves symmetric key encryption problem of having to exchange secret key.

- 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

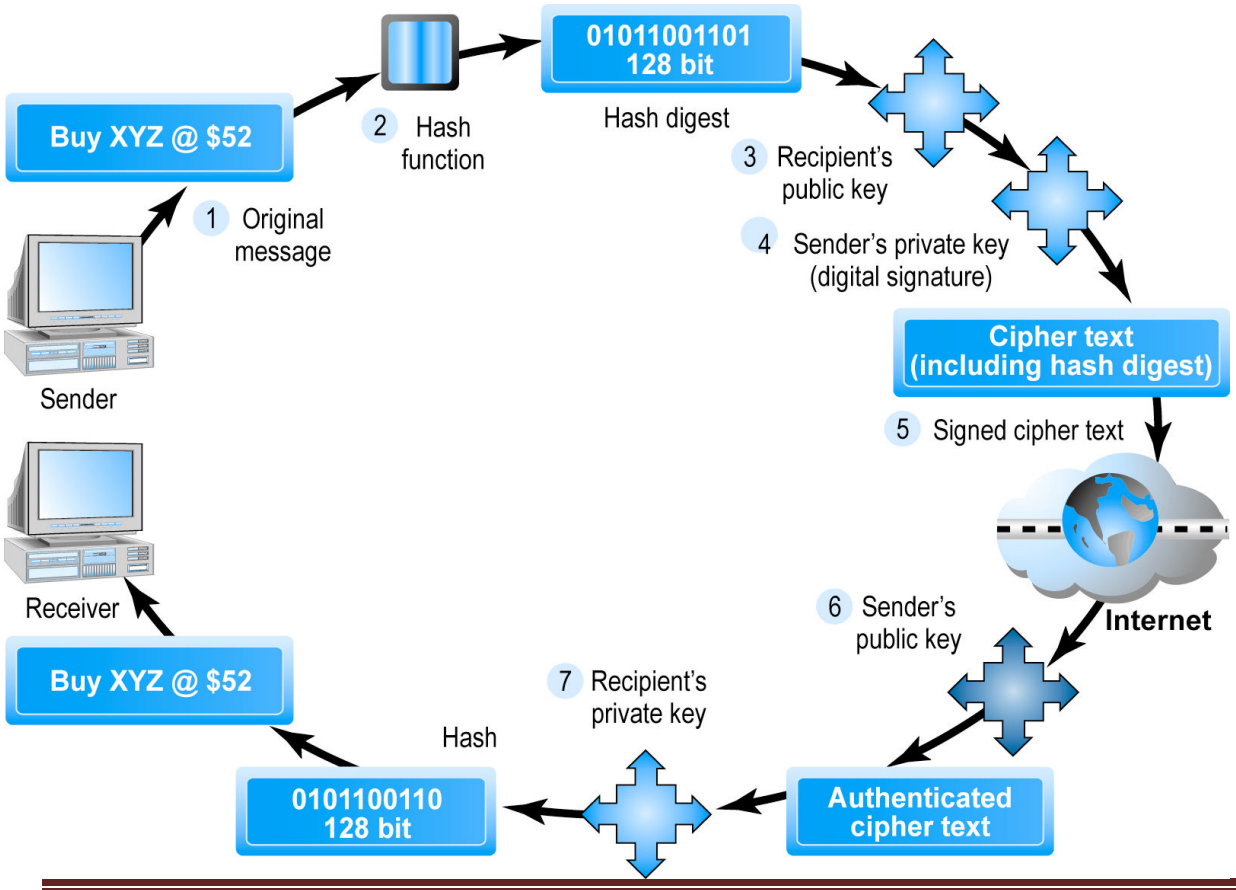


- For example, sender uses recipient's public key to encrypt message recipient uses his/her private key to decrypt it



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.

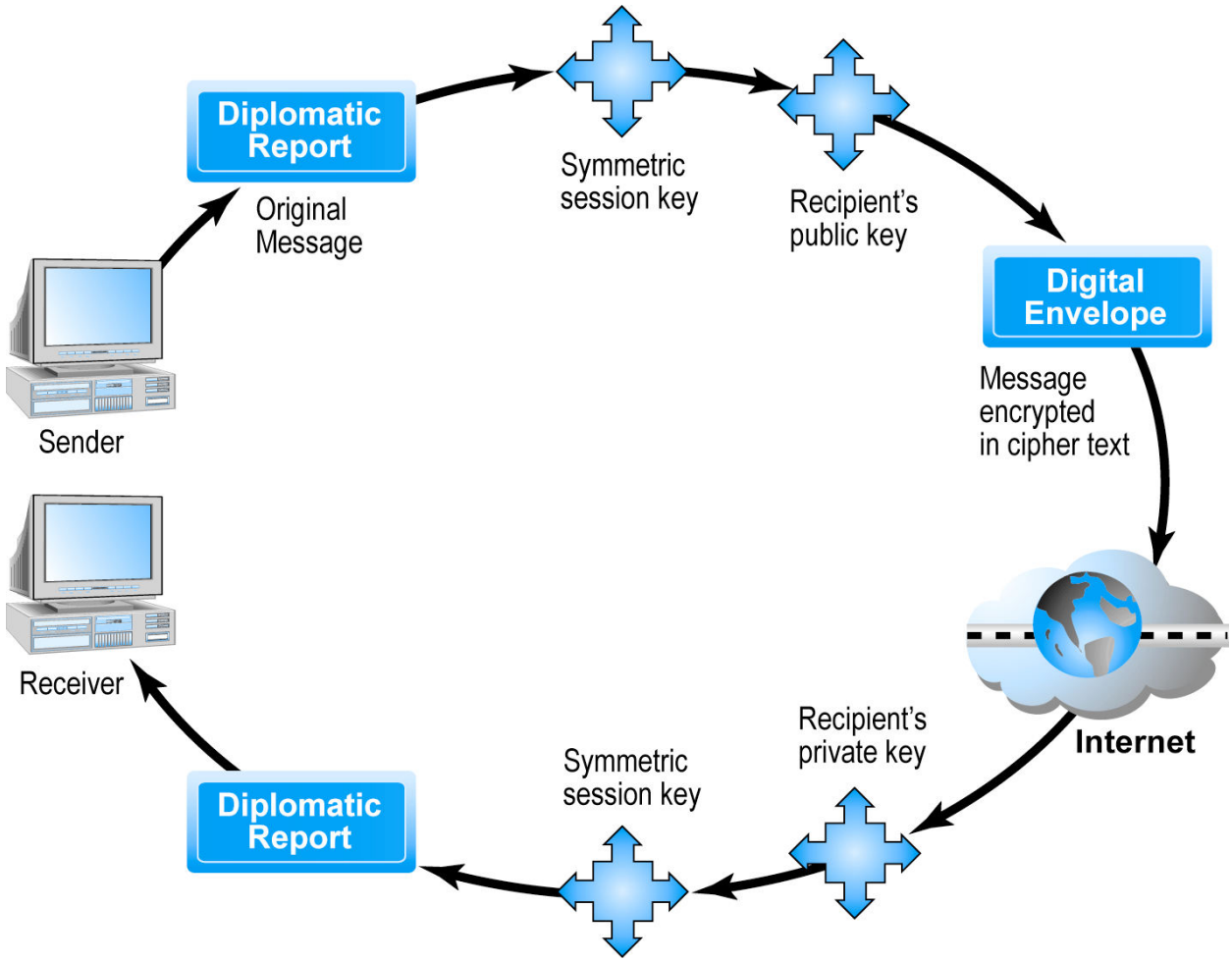
4. Digital Envelopes

- 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.



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