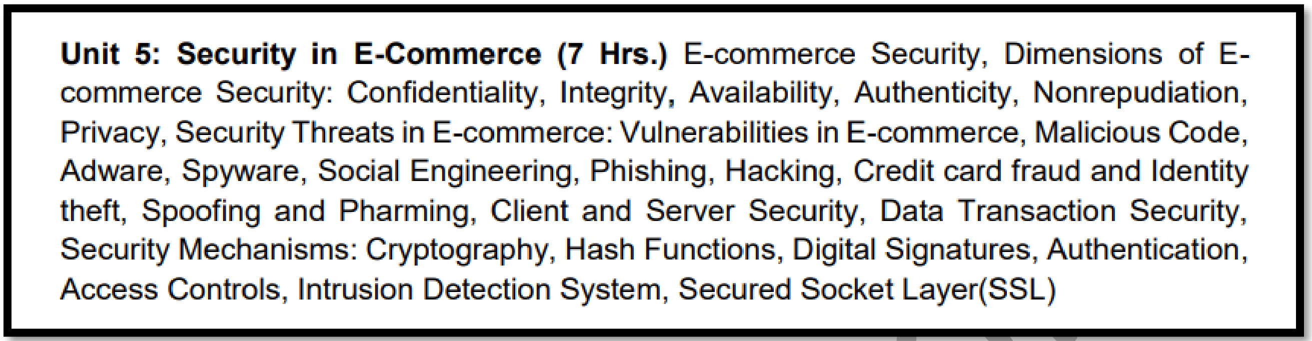
Unit-5

Security in E-Commerce



Unit 5: Security in E-Commerce (7 Hrs.) E-commerce Security, Dimensions of E-commerce Security: Confidentiality, Integrity, Availability, Authenticity, Nonrepudiation, Privacy, Security Threats in E-commerce: Vulnerabilities in E-commerce, Malicious Code, Adware, Spyware, Social Engineering, Phishing, Hacking, Credit card fraud and Identity theft, Spoofing and Pharming, Client and Server Security, Data Transaction Security, Security Mechanisms: Cryptography, Hash Functions, Digital Signatures, Authentication, Access Controls, Intrusion Detection System, Secured Socket Layer(SSL)

E-commerce Security: (page 242)

Internet and Web are increasingly vulnerable to large-scale attacks and potentially large-scale failure. Increasingly, these attacks are led by organized gangs of criminals operating globally—an unintended consequence of globalization. Anticipating and countering these attacks has proved a difficult task for both business and government organizations. However, there are several steps you can take to protect your websites, your mobile devices, and your personal information from routine security attacks.

For most law-abiding citizens, the Internet holds the promise of a huge and convenient global marketplace, providing access to people, goods, services, and businesses worldwide, all at a bargain price. For criminals, the Internet has created entirely new—and lucrative—ways to steal from the billions of Internet consumers. From products and services, to cash, to information, it's all there for the taking on the Internet. It's also less risky to steal online. Rather than rob a bank in person, the Internet makes it possible to rob people remotely and almost anonymously. Rather than steal a CD at a local record store, you can download the same music for free and almost without risk from the Internet. The potential for anonymity on the Internet cloaks many criminals in legitimate-looking identities, allowing them to place fraudulent orders with online merchants, steal information by intercepting e-mail, or simply shut down e-commerce sites by using software viruses and swarm attacks.

The actions of cybercriminals are costly for both businesses and consumers, who are then subjected to higher prices and additional security measures. The costs of malicious cyberactivity include not just the cost of the actual crime, but also the additional costs that are required to secure networks and recover from cyberattacks, the potential reputational damage to the affected company, as well as reduced trust in online activities, the loss of potentially sensitive business information, including intellectual property and confidential business information, and the cost of opportunities lost due to service disruptions.

Cybercrime is becoming a more significant problem for both organizations and consumers. Bot networks, DDoS attacks, Trojans, phishing, ransomware, data theft, identity fraud, credit card fraud, and spyware are just some of the threats that are making daily headlines.

Social networks also have had security breaches. But despite the increasing attention being paid to cybercrime, it is difficult to accurately estimate the actual amount of such crime, in part because many companies are hesitant to report it due to the fear of losing the trust of their customers. At present situation, cost to be safe is much higher than cost to run a business. Low-cost and readily available web attack kits enable hackers to create malware without having to write software from scratch. In addition, there has been a surge in polymorphic malware, which enables attackers to generate a unique version of the malware for each victim, making it much more difficult for pattern-matching software used by security firms to detect.

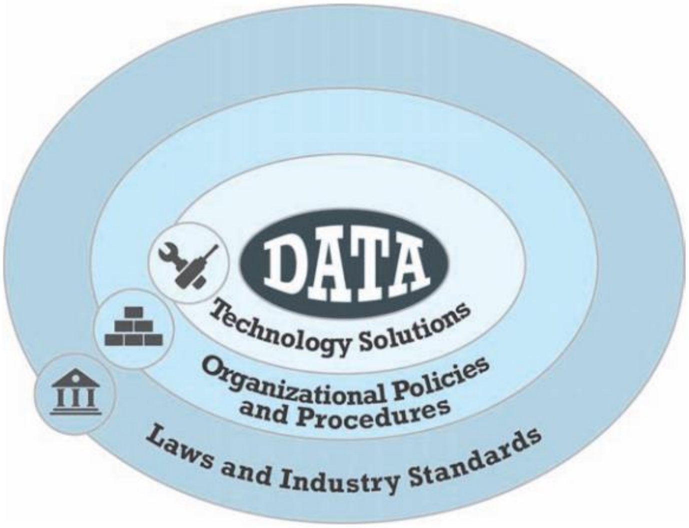
Online credit card fraud is one of the most high-profile forms of e-commerce crime. Although the average amount of credit card fraud loss experienced by any one individual is typically relatively small, the overall amount is substantial.

Good E-commerce Security:

What is a secure commercial transaction? Anytime you go into a marketplace you take risks, including the loss of privacy (information about what you purchased). Your prime risk as a consumer is that you do not get what you paid for. As a merchant in the market, your risk is that you don’t get paid for what you sell. Thieves take merchandise and then either walk off without paying anything, or pay you with a fraudulent instrument, stolen credit card, or forged currency.

E-commerce merchants and consumers face many of the same risks as participants in traditional commerce, Theft is theft, regardless of whether it is digital theft or traditional theft. all crimes in a traditional commercial environment—are also present in e-commerce. However, reducing risks in e-commerce is a complex process that involves new technologies, organizational policies and procedures, and new laws and industry standards that empower law enforcement officials to investigate and prosecute offenders.

The figure below, Illustrates the multi-layered nature of e-commerce security.


DATA
Technology Solutions
Organizational Policies and Procedures
Laws and Industry Standards

To achieve the highest degree of security possible, new technologies are available and should be used. But these technologies by themselves do not solve the problem. Organizational policies and procedures are required to ensure the technologies are not subverted. Finally, industry standards and government laws are required to enforce payment mechanisms, as well as to investigate and prosecute violators of laws designed to protect the transfer of property in commercial transactions.

The history of security in commercial transactions teaches that any security system can be broken if enough resources are put against it. Security is not absolute. In addition, perfect security of every item is not needed forever, especially in the information age. There is a time value to information—just as there is to money. Sometimes it is sufficient to protect a message for a few hours or days. Also, because security is costly, we always have to weigh the cost against the potential loss. Finally, we have also learned that security is a chain that breaks most often at the weakest link. Our locks are often much stronger than our management of the keys. We can conclude then that good e-commerce security requires a set of laws, procedures, policies, and technologies that, to the extent feasible, protect individuals and organizations from unexpected behavior in the e-commerce marketplace.

Dimensions of E-commerce Security:

There are six key dimensions to e-commerce security:

- Integrity
- Nonrepudiation
- Authenticity
- Confidentiality
- Privacy
- Availability

Integrity: refers to the ability to ensure that information being displayed on a website, or transmitted or received over the Internet, has not been altered in any way by an unauthorized party. For example, if an unauthorized person intercepts and changes the contents of an online communication, such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.

Nonrepudiation: refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions. For instance, the availability of free e-mail accounts with alias names makes it easy for a person to post comments or send a message and perhaps later deny doing so. Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so. In most cases, because merchants typically do not obtain a physical copy of a signature, the credit card issuer will side with the customer because the merchant has no legally valid proof that the customer ordered the merchandise.

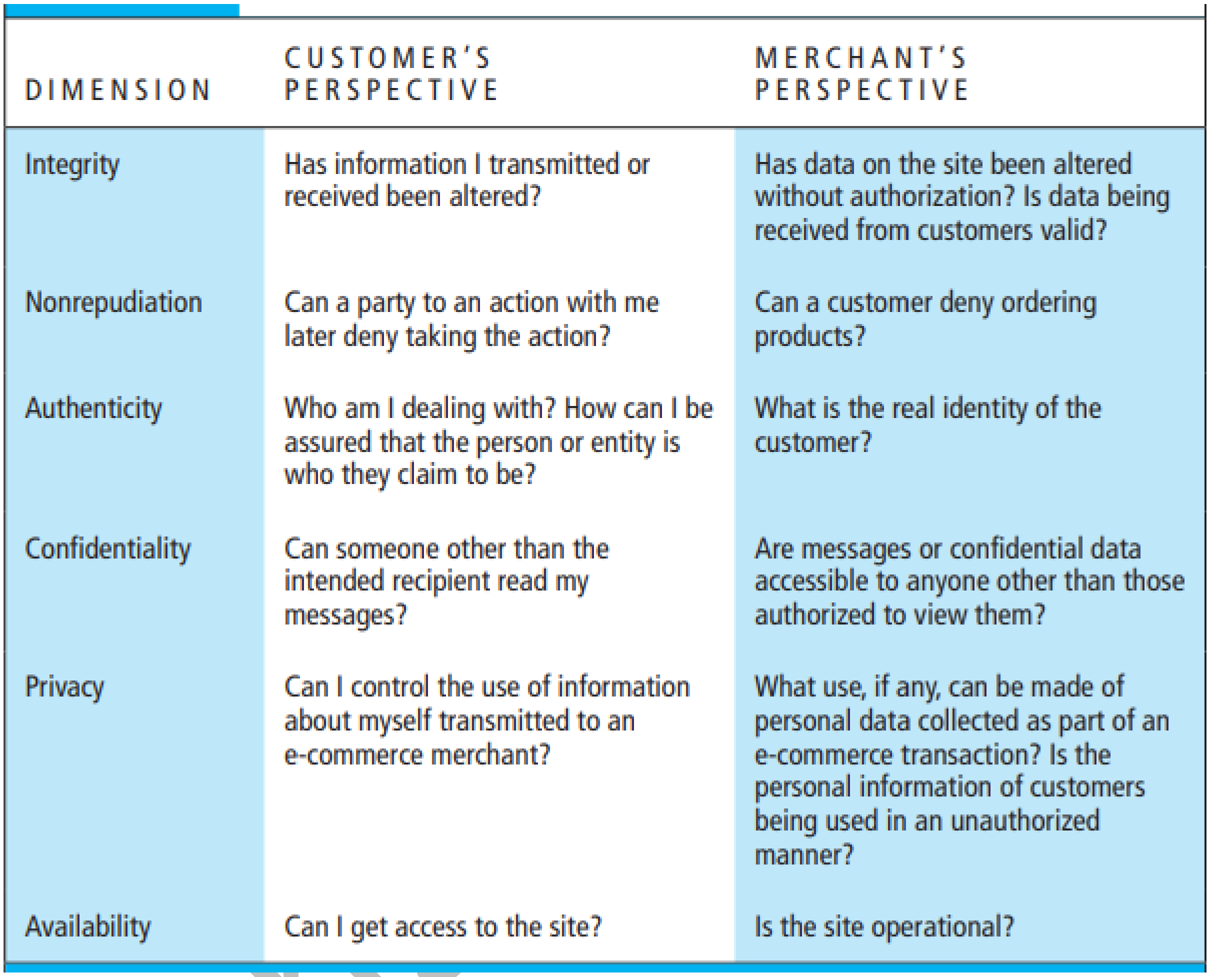
Authenticity: refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet. How does the customer know that the website operator is who it claims to be? How can the merchant be assured that the customer is really who she says she is? Someone who claims to be someone he is not is “spoofing” or misrepresenting himself.

Confidentiality: refers to the ability to ensure that messages and data are available only to those who are authorized to view them. In many cases, it is the part of security in e-commerce. E-commerce merchants have two concerns related to privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.

Privacy: Ability to control the use of information about oneself. E-commerce merchants have two concerns related to privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.

Availability: refers to the ability to ensure that an e-commerce site continues to function as intended.

Following table summarizes these dimensions from both the merchants' and customers' perspectives. E-commerce security is designed to protect these six dimensions. When any one of them is compromised, overall security suffers.



DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

Threats in the e-commerce environment:

From a technology perspective, there are three key points of vulnerability when dealing with e-commerce: the client, the server, and the communications pipeline.

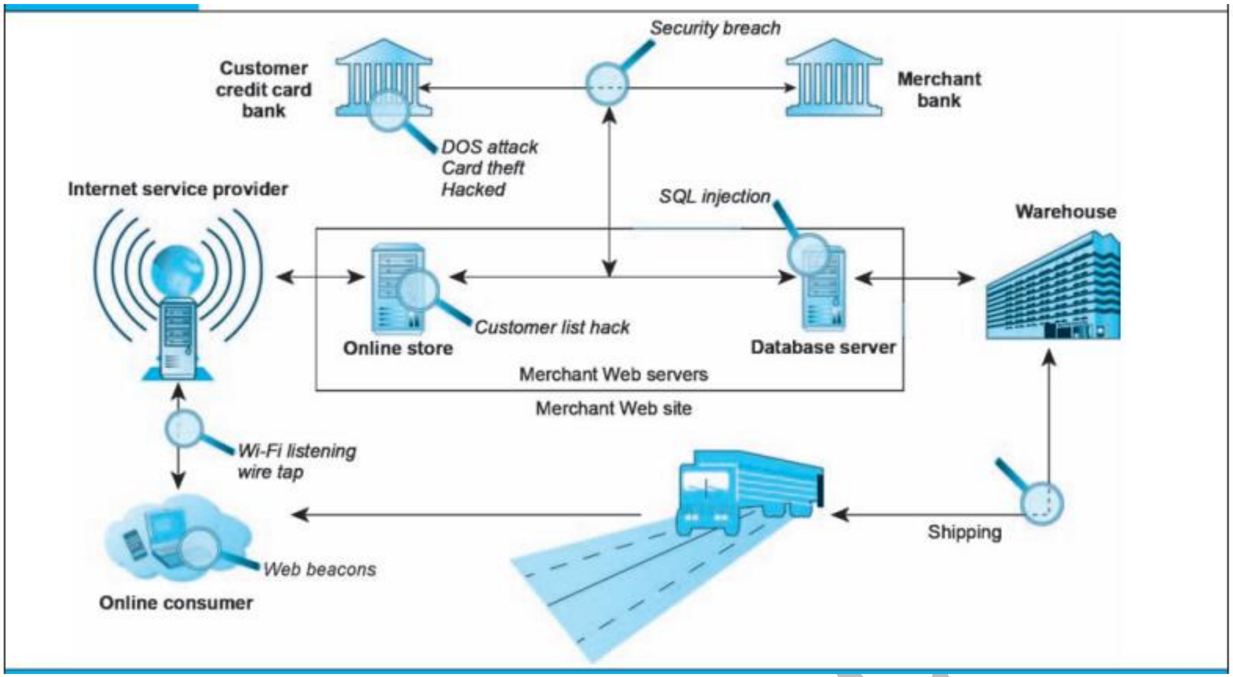


Fig: Vulnerable points in e-commerce transaction

There are three major vulnerable points in e-commerce transactions: Internet communications, servers, and clients. Above figure illustrates some of the things that can go wrong at each major vulnerability point in the transaction—over Internet communications channels, at the server level, and at the client level.

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

- Malicious Code
- Adware
- Spyware
- Social Engineering
- Phishing
- Hacking
- Credit card fraud
- Identity theft
- Spoofing
- Pharming

Read yourself the meaning of above listed terms. You can find in page 250 of your text book(2017 edition)

Client and Server Security:

Operating system features and anti-virus software can help further protect servers and clients from certain types of attacks.

Operating system security enhancement: The most obvious way to protect servers and clients is to take advantage of automatic computer security upgrades. The Microsoft, Apple, and Linux/Unix operating systems are continuously updated to patch vulnerabilities discovered by hackers. These patches are autonomic; that is, when using these operating systems on the Internet, you are prompted and informed that operating system enhancements are available. Users can easily download these security patches for free. The most commonly known worms and viruses can be prevented by simply keeping your server and client operating systems and applications up to date. In April 2014, Microsoft ended security support and updates for its Windows XP operating system. Despite this, many organizations continue to use XP-based systems, and as a result, many security experts anticipate a wave of strikes against such systems. Application vulnerabilities are fixed in the same manner. For instance, most popular Internet browsers are updated automatically with little user intervention.

Anti-Virus Software: The easiest and least-expensive way to prevent threats to system integrity is to install anti-virus software. Programs by Malwarebytes, McAfee, Symantec (Norton AntiVirus), and many others provide inexpensive tools to identify and eradicate the most common types of malicious code as they enter a computer, as well as destroy those already lurking on a hard drive. Anti-virus programs can be set up so that e-mail attachments are inspected before you click on them, and the attachments are eliminated if they contain a known virus or worm. It is not enough, however, to simply install the software once. Because new viruses are developed and released every day, daily routine updates are needed in order to prevent new threats from being loaded. Some premium-level anti-virus software is updated hourly. Anti-virus suite packages and stand-alone programs are available to eliminate intruders such as bot programs, adware, and other security risks. Such programs work much like anti-virus software in that they look for recognized hacker tools or signature actions of known intruders.

Data Transaction Security:

Because e-commerce transactions must flow over the public Internet, and therefore involve thousands of routers and servers through which the transaction packets flow, security experts believe the greatest security threats occur at the level of data transaction. This is very different from a private network where a dedicated communication line is established between two parties. A number of tools are available to protect the security of Internet communications, the most basic of which is message encryption.

Cryptography/Encryption: It is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is (a) to secure stored information and (b) to secure information transmission.

Encryption supports the six dimensions of e-commerce security:

- Message integrity—provides assurance that the message has not been altered.
- Nonrepudiation—prevents the user from denying he or she sent the message.
- Authentication—provides verification of the identity of the sender.
- Confidentiality—gives assurance that the message was not read by others.

This transformation of plain text to cipher text is accomplished by using a key or cipher. A key (or cipher) is any method for transforming plain text to cipher text. Encryption has been practiced since the earliest forms of writing and commercial transactions. Ancient Egyptian and Phoenician commercial records were encrypted using substitution and transposition ciphers.

In a substitution cipher, every occurrence of a given letter is replaced systematically by another letter. For instance, if we used the cipher "letter plus two"—meaning replace every letter in a word with a new letter two places forward—then the word "Hello" in plain text would be transformed into the following cipher text: "JGNNQ".

In a transposition cipher, the ordering of the letters in each word is changed in some systematic way. For example, making the text readable only in mirrors, the word "Hello" can be written backwards as "OLLEH".

Symmetric key cryptography: Symmetric Key Cryptography also known as Symmetric Encryption is when a secret key is leveraged for both encryption and decryption functions. This method is the opposite of Asymmetric Encryption where one key is used to encrypt and another is used to decrypt. In order to decipher (decrypt) these messages, the receiver would have to know the secret cipher that was used to encrypt the plain text. This is called symmetric key cryptography or secret key cryptography. In symmetric key cryptography, both the sender and the receiver use the same key to encrypt and decrypt the message. How do the sender and the receiver have the same key? They have to send it over some communication media or exchange the key in person. Symmetric key cryptography was used extensively throughout World War II and is still a part of Internet cryptography.

The possibilities for simple substitution and transposition ciphers are endless, but they all suffer from common flaws. First, in the digital age, computers are so powerful and fast that these ancient means of encryption can be broken quickly. Second, symmetric key cryptography requires that both parties share the same key. In order to share the same key, they must send the key over a presumably insecure medium where it could be stolen and used to decipher messages. If the secret key is lost or stolen, the entire encryption system fails. Third, in commercial use, where we are not all part of the same team, you would need a secret key for each of the parties with whom you transacted, that is, one key for the bank, another for the department store, and another for the government. In a large population of users, this could result in as many as n(n–1) keys. In a population of billions of Internet users, billions of keys would be needed to accommodate all e-commerce customers. Clearly this situation would be too unwieldy to work in practice.

Modern encryption systems are digital. The ciphers or keys used to transform plain text into cipher text are digital strings. Computers store text or other data as binary strings composed of 0s and 1s. For instance, the binary representation of the capital letter "A" in ASCII computer code is accomplished with eight binary digits (bits): 01000001. One way in which digital strings can be transformed into cipher text is by multiplying each letter by another binary number, say, an eight-bit key number 0101 0101. If we multiplied every digital character in our text messages by this eight-bit key and sent the encrypted message to a friend along with the secret eight-bit key, the friend could decode the message easily.

The strength of modern security protection is measured in terms of the length of the binary key used to encrypt the data. In the preceding example, the eight-bit key is easily deciphered because there are only 28 or 256 possibilities. If the intruder knows you are using an eight-bit key, then he or she could decode the message in a few seconds using a modern desktop PC just by using the brute force method of checking each of the 256 possible keys. For this reason, modern digital encryption systems use keys with 56, 128, 256, or 512 binary digits. With encryption keys of 512 digits, there are 2512 possibilities to check out. It is estimated that all the computers in the world would need to work for 10 years before stumbling upon the answer.

The Data Encryption Standard (DES) was developed by the National Security Agency (NSA) and IBM in the 1950s. DES uses a 56-bit encryption key. To cope with much faster computers, it has been improved by the Triple DES Encryption Algorithm (TDEA)—essentially encrypting the message three times, each with a separate key. Today, the most widely used symmetric key algorithm is Advanced Encryption Standard (AES), which offers key sizes of 128, 192, and 256 bits. AES had been considered to be relatively secure, but in 2011, researchers from Microsoft and a Belgian university announced that they had discovered a way to break the algorithm, and with this work, the "safety margin" of AES continues to erode. There are also many other symmetric key systems that are currently less widely used, with keys up to 2,048 bits.

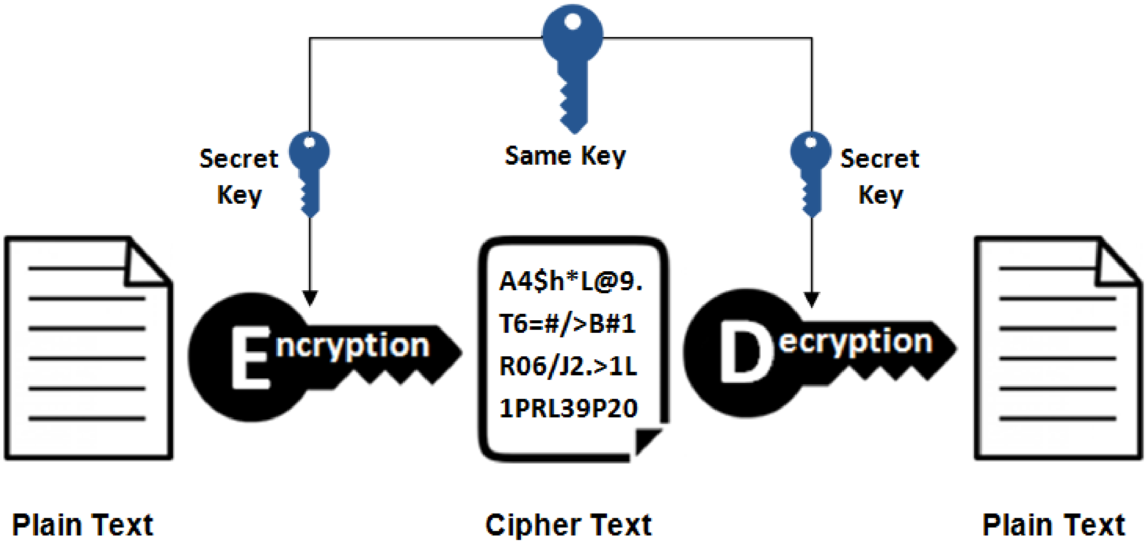


Fig: Symmetric key encryption

Public Key Cryptography: In 1976, a new way of encrypting messages called public key cryptography was invented by Whitfield Diffie and Martin Hellman. Public key cryptography (also referred to as asymmetric cryptography) solves the problem of exchanging keys. In this method, two mathematically related digital keys are used: a public key and a private key. The private key is kept secret by the owner, and the public key is widely disseminated. Both keys can be used to encrypt and decrypt a message. However, once the keys are used to encrypt a message, the same key cannot be used to unencrypt the message. The mathematical algorithms used to produce the keys are one-way functions. A one-way irreversible mathematical function is one in which, once the algorithm is applied, the input cannot be subsequently derived from the output. Most food recipes are like this. For instance, it is easy to make scrambled eggs, but impossible to retrieve whole eggs from the scrambled eggs. Public key cryptography is based on the idea of irreversible mathematical functions. The keys are sufficiently long (128, 256, and 512 bits) that it would take enormous computing power to derive one key from the other using the largest and fastest computers available.

The process of public key cryptography is illustrated in the following diagram:

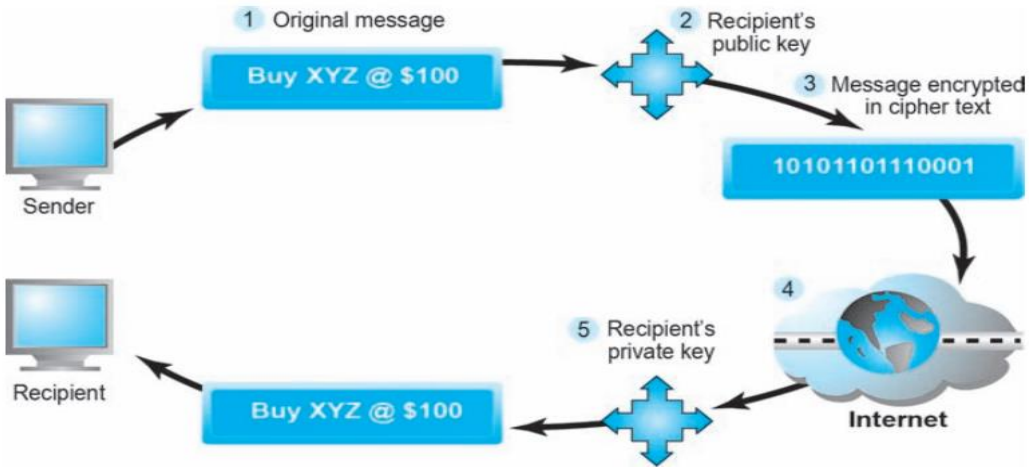
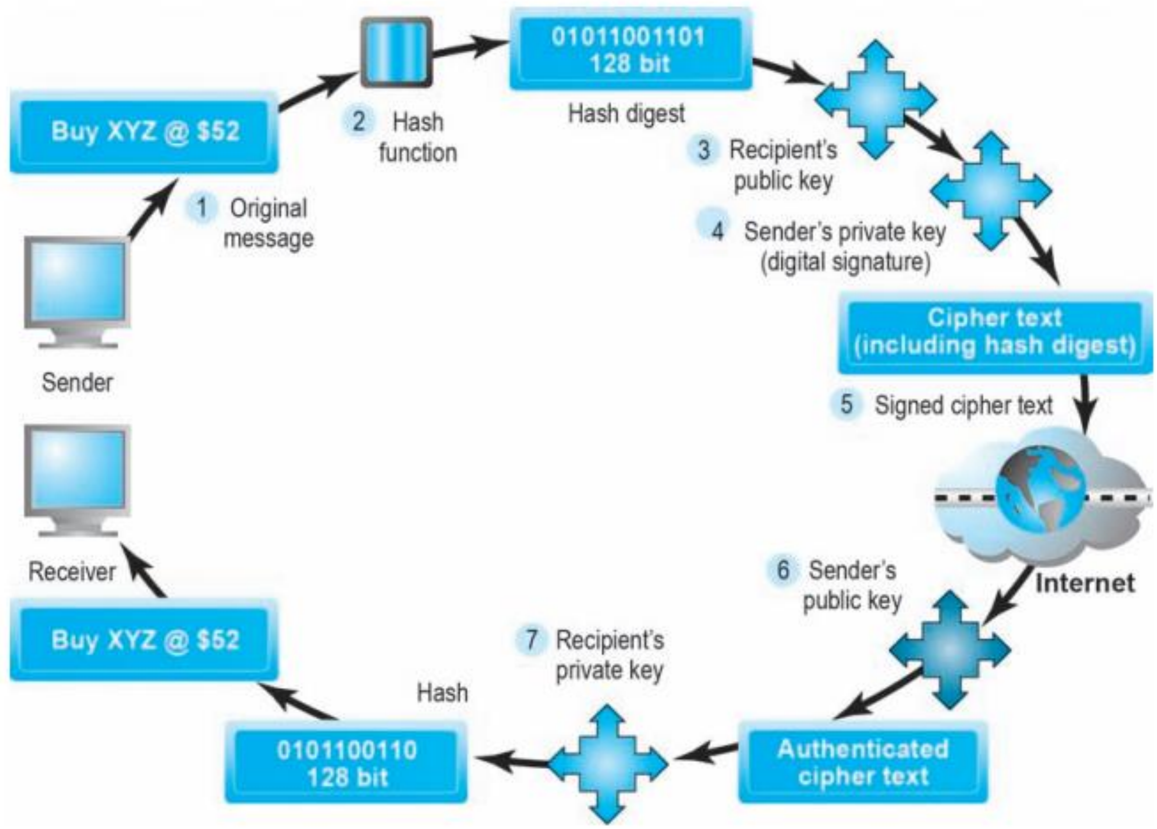


Fig: Public Key Cryptography (a simple case)

Hash Functions:

In public key cryptography, some elements of security are missing. Although we can be quite sure the message was not understood or read by a third party (message confidentiality), there is no guarantee the sender really is the sender; that is, there is no authentication of the sender. This means the sender could deny ever sending the message (repudiation). And there is no assurance the message was not altered somehow in transit. For example, the message "Buy Cisco @ $16" could have been accidentally or intentionally altered to read "Sell Cisco @ $16." This suggests a potential lack of integrity in the system.

A more sophisticated use of public key cryptography can achieve authentication, nonrepudiation, and integrity. Following figure illustrates this more powerful approach.



To check the integrity of a message and ensure it has not been altered in transit, a hash function is used first to create a digest of the message. A hash function is an algorithm that produces a fixed-length number called a hash or message digest. A hash function can be simple, and count the number of digital 1s in a message, or it can be more complex, and produce a 128-bit number that reflects the number of 0s and 1s, the number of 00s and 11s, and so on. Standard hash functions are available (MD4 and MD5 produce 128- and 160-bit hashes) (Stein, 1998). These more complex hash functions produce hashes or hash results that are unique to every message.

The results of applying the hash function are sent by the sender to the recipient. Upon receipt, the recipient applies the hash function to the received message and checks to verify the same result is produced. If so, the message has not been altered. The sender then encrypts both the hash result and the original message using the recipient's public key, producing a single block of cipher text.
One more step is required. To ensure the authenticity of the message and to

ensure nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender’s private key. This produces a digital signature (also called an e-signature) or “signed” cipher text that can be sent over the Internet.

A digital signature is a close parallel to a handwritten signature. Like a handwritten signature, a digital signature is unique—only one person presumably possesses the private key. When used with a hash function, the digital signature is even more unique than a handwritten signature. In addition to being exclusive to a particular individual, when used to sign a hashed document, the digital signature is also unique to the document, and changes for every document.

The recipient of this signed cipher text first uses the sender’s public key to authenticate the message. Once authenticated, the recipient uses his or her private key to obtain the hash result and original message. As a final step, the recipient applies the same hash function to the original text, and compares the result with the result sent by the sender. If the results are the same, the recipient now knows the message has not been changed during transmission. The message has integrity.

Early digital signature programs required the user to have a digital certificate, and were far too difficult for an individual to use. Newer programs are Internet-based and do not require users to install software, or understand digital certificate technology.

Digital Signatures:

To ensure the authenticity of the message and to ensure nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender’s private key. This produces a digital signature (also called an e-signature) or “signed” cipher text that can be sent over the Internet.

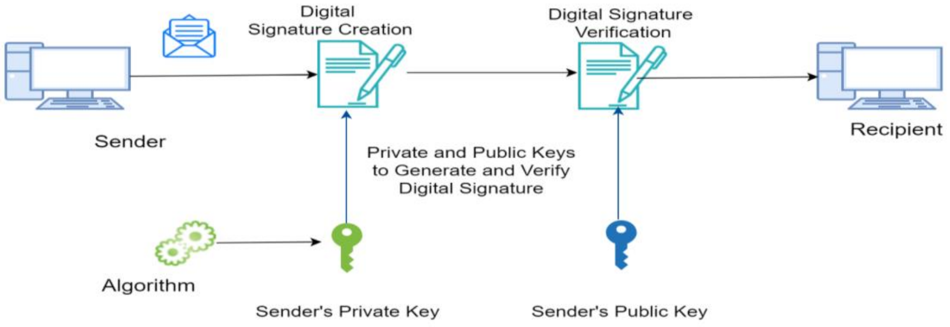


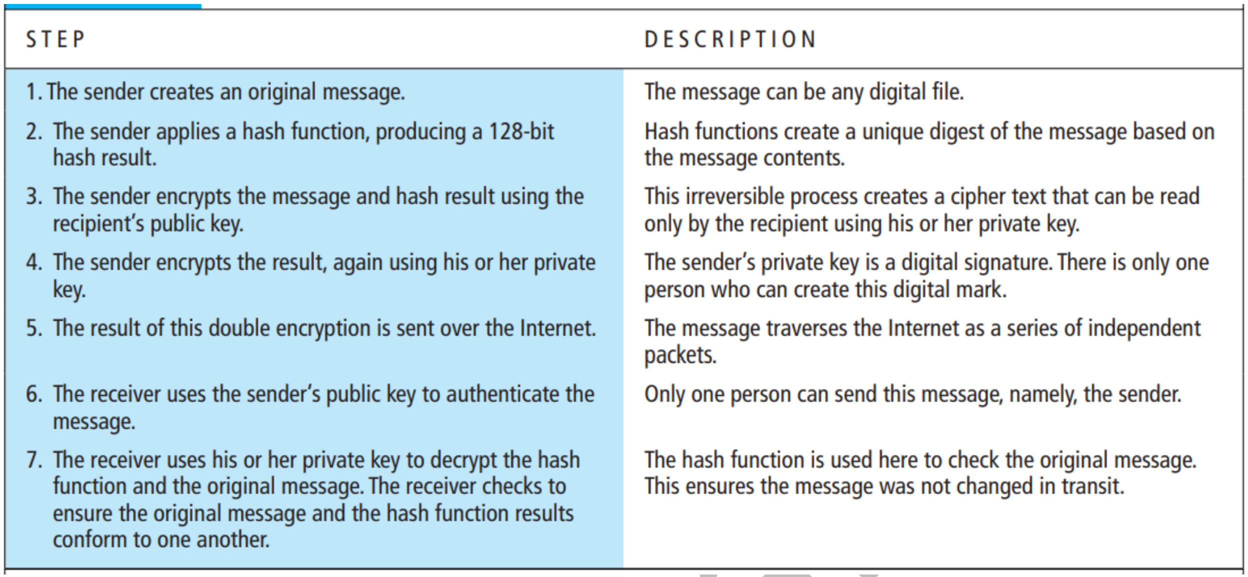
Fig: Digital Signature

A digital signature is a close parallel to a handwritten signature. Like a handwritten signature, a digital signature is unique—only one person presumably possesses the private key. When used with a hash function, the digital signature is even more unique than a handwritten signature. In addition to being exclusive to a particular individual, when used to sign a hashed document, the digital signature is also unique to the document, and changes for every document.

The recipient of this signed cipher text first uses the sender’s public key to authenticate the message. Once authenticated, the recipient uses his or her private key to obtain the hash result and original message. As a final step, the recipient applies the same hash function to the original text, and compares the result with the result sent by the sender. If the results are the same, the recipient now knows the message has not been changed during transmission. The message has integrity.

Early digital signature programs required the user to have a digital certificate, and were far too difficult for an individual to use. Newer programs are Internet-based and do not require users to install software, or understand digital certificate technology.

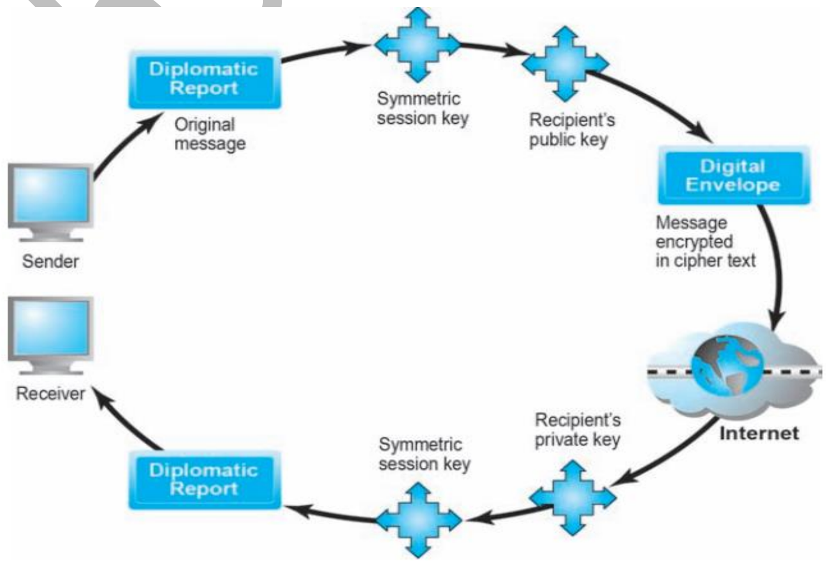
Following table contains the steps and description of public key cryptography with digital signature.



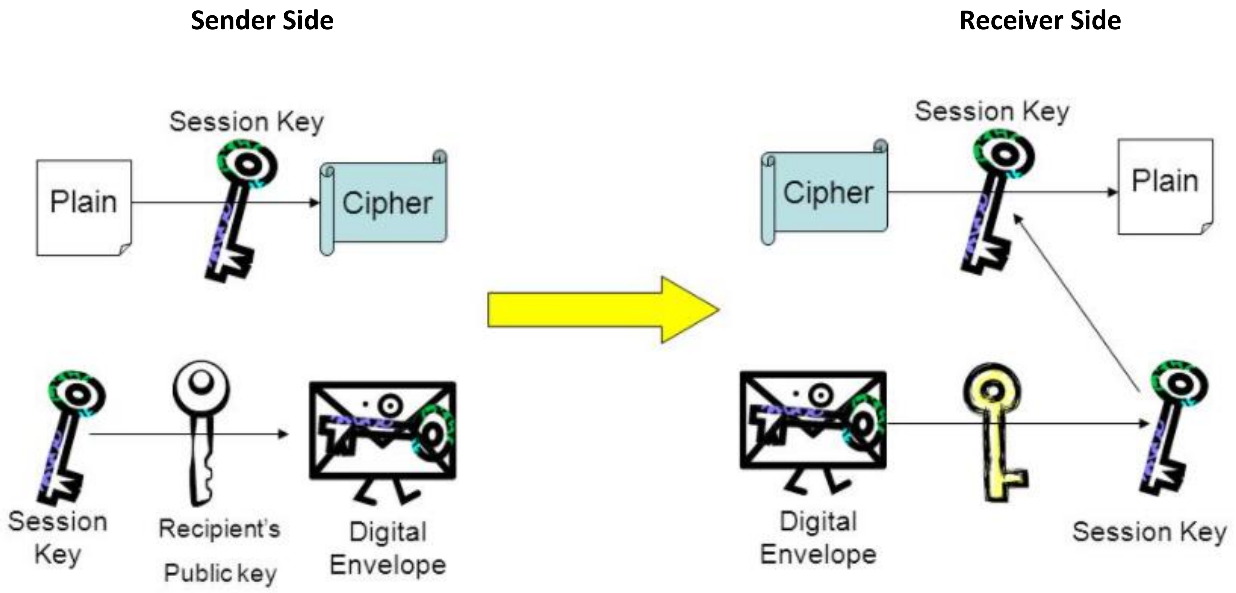
STEP	DESCRIPTION
1. The sender creates an original message.	The message can be any digital file.
2. The sender applies a hash function, producing a 128-bit hash result.	Hash functions create a unique digest of the message based on the message contents.
3. The sender encrypts the message and hash result using the recipient's public key.	This irreversible process creates a cipher text that can be read only by the recipient using his or her private key.
4. The sender encrypts the result, again using his or her private key.	The sender's private key is a digital signature. There is only one person who can create this digital mark.
5. The result of this double encryption is sent over the Internet.	The message traverses the Internet as a series of independent packets.
6. The receiver uses the sender's public key to authenticate the message.	Only one person can send this message, namely, the sender.
7. The receiver uses his or her private key to decrypt the hash function and the original message. The receiver checks to ensure the original message and the hash function results conform to one another.	The hash function is used here to check the original message. This ensures the message was not changed in transit.

Digital Envelop:

Public key cryptography is computationally slow. If one used 128- or 256-bit keys to encode large documents—such as this chapter or the entire book—significant declines in transmission speeds and increases in processing time would occur. Symmetric key cryptography is computationally faster, but as we pointed out previously, it has a weakness—namely, the symmetric key must be sent to the recipient over insecure transmission lines. One solution is to use the more efficient symmetric encryption and decryption for large documents, but public key cryptography to encrypt and send the symmetric key. This technique is called using a digital envelope.



Following diagram clearly explains the concept of digital envelop.



Authentication:

Authentication procedures include the use of digital signatures, certificates of authority, and PKI. Now that e-signatures have been given the same legal weight as an original pen-and-ink version, companies are in the process of devising ways to test and confirm a signer's identity. Companies frequently have signers type their full name and click on a button indicating their understanding that they have just signed a contract or document.

Authentication refers to the guarantee that the sender is the one who is claimed to be. In data transmission, authenticity is obtained due to the use of PKI. In PKI, authenticity is obtained due to the use of message encryption using the senders private key. Such message can be decrypted by the receiver using the sender's public key and hence verifies that the message was originally sent by the individual.

Access Control:

The security organization typically administers access controls, authentication procedures, and authorization policies. Access controls determine which outsiders and insiders can gain legitimate access to your networks. Outsider access controls include firewalls and proxy servers, while insider access controls typically consist of login procedures (usernames, passwords, and access codes).

Intrusion Detection System:

In addition to a firewall and proxy server, an intrusion detection and/or prevention system can be installed. An intrusion detection system (IDS) examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack. If it detects suspicious activity, the IDS will set off an alarm alerting administrator and log the event in a database. An IDS is useful for detecting malicious activity that a firewall might miss. An intrusion prevention system (IPS) has all the functionality of an IDS, with the additional ability to take steps to prevent and block suspicious activities. For instance, an IPS can terminate a session and reset a connection, block traffic from a suspicious IP address, or reconfigure firewall or router security controls.

Secured Socket Layer (SSL):

SSL stands for Secure Sockets Layer. At the core, this technology helps to secure an internet connection and protect any data that's transferred between a browser and a web server. If your customers input their private information on your website, then you need an SSL certificate for security. By encrypting and securing any data that passes through this connection you help to prevent any data theft or hacking. By encrypting and securing any data that passes through this connection, you help to prevent any data theft or hacking.

An SSL connection needs two systems in order to be active. Think a server and a website browser, or a server to server connection. With this connection, any data that's transferred between the two will actually be impossible to read. The encryption algorithms will scramble any data being sent over the connection, so if the information is compromised it'll be impossible to decipher.

In the past, SSL was commonly used to protect and secure sensitive information, like banking details, credit card numbers, and sensitive personal information. However, today with stricter privacy standards, almost every website can benefit from installing an SSL certificate to protect any user information.

But; SSL certificates can do a lot more than just give you a rankings and trust boost. Trust is so important on the Internet. Any site that acquires a reputation for unreliability, insecurity or dishonesty can expect to see traffic dwindle to zero. On the other hand, a site that can prove it takes security seriously can attract more visitors. That's always a good thing, whether your web site is for a nonprofit, small business, or eCommerce.

Surfers and online shoppers also increasingly recognize the on-screen presence of a small padlock icon or a website address that begins with "https://…" as signs that they can trust the site they're connecting to. That's SSL or 'secure sockets layer' in action.

Secure | https:// www.techsastra.com

he biggest reason websites use SSL is to protect sensitive information that's sent between computers and servers. If information like credit card numbers, passwords, and other personal information isn't encrypted this leaves it open for hackers to easily step in and steal the information. With the SSL certificate. your information is unreadable to anyone who attempts to steal it. The only people able to decipher it are the intended recipients at the other end of the connection. With an SSL certificate, your customers can do business with you knowing that their information is going to be safe from identity thieves and potential hackers.

>> How does SSL certificate work?

SSL operates between a visitor's browser and your site or application. It's an industry-standard mechanism that ensures the encryption of data being passed backward and forwards so that no unauthorized person can spy on the information and hack it. It also prevents cybercriminals from diverting visitor traffic to their own site using their own encryption and gaining access to your data that way. All major web browsers have SSL capability built in.

The process of enabling an SSL certificate on your site is quite simple. First, you'll install an SSL certificate on your server. A web browser will connect to your server, see the SSL certificate and initiate the SSL connection. This will then encrypt any information that passes between a browser and your server. The step can be listed as follows;

- An SSL handshake occurs once the web browser validates the presence of an SSL certificate on the server.

- The server then sends all of the necessary information including the type of SSL certificate present, the level of encryption to use, and more.
- If the SSL certificate is valid, then the secure connection begins.

All of this takes place instantly. It might seem fairly technical, but if you open up a website with an SSL certificate installed, you'll never even notice that the above steps occurred.

>> How to add SSL certificate to your site?

The approach you'll take to install an SSL certificate on your site depends upon the host you're using, and the type of site that you're running. Primarily, the way of including SSL in your site depends on your hosting service provider. You can activate SSL from hosting control panel. Now a days, many hosting plans offer free SSL certificates. Once you have your SSL certificate activated, you'll need to ensure that your domain redirects from the previous HTTP to the new HTTPS.

>> Why we should enable SSL?

- End-to-end encryption.
- Trust from the customers.
- Higher rank in search engines.

SSL certificate becomes very important if a site is made for any of the following;

- User can make online purchase.
- A membership site.
- Collecting user information.