system. The main functions of an

output, storage and control at work place.

Q.2 ***What is an information system ? Explain the importance and basics of information systems.***

Ans. : Information systems comprise hardware, software, data, applications, communication and people, help an organization to better manage and secure its critical corporate, customer and employee data. An information system is a set of interrelated components that collect, process, store or distribute information to support decision making and control in an organization.

Information systems also improve integration and work processes the benefits go on and on. Its objective is to monitor and document the operations of other systems, which we can call target systems. For example, production activities would be the target system for a production scheduling information system, human resources would be the target system of a human resource information system and so on. Every reactive system may have a subsystem that can be considered as an information system whose objective is to monitor and control such a system.

The main functions of an information system may be input, processing, output, storage and control at work place. Therefore information system is a system comprises people, machines and/or methods organized to collect, process, store or disseminate data that represent user information. The emergence of a global economy, transformation of industrial economies, transformation of the business enterprise and the emergence of digital firm make information systems essential in business today. Information system is a foundation for conducting business today. In many businesses, survival and the ability to achieve strategic business goals is difficult without wide use of information technology. There are six reasons behind the importance of businesses use information system :

1. Operational excellence.
2. New products, services, and business models.
3. Customer and supplier intimacy.
4. Improved decision making.
5. Competitive advantage.
6. Survival.

(Important Questions asked in UPTU and Other Universities Exams)

Q.1 *Why do organizations need information systems ?*

Ans. : Computers are essential today. Information is the lifeblood of any organization. Damaged or lost data can cause disruptions in normal business activities leading to financial losses, law suits, etc. Information systems comprise hardware, software, data, applications, communication and people, help an organization to better manage and secure its critical corporate, customer and employee data. Information systems also improve integration and work processes, the benefits go on and on. We check our email with it, find answers to questions, watch media, bank and more using computers. Therefore we need systems that can organize, and serve information when people around the world request it.

For example, production activities would be the target system for a production scheduling information system, human resources would be the target system of a human resource information system and so on. We could say that every reactive system may have a subsystem that can be considered as an information system whose objective is to monitor and control such a system. The main functions of an information system may be input, processing, output, storage and control at work place.

integrating web

Q.6 *What are information system threats and attacks ?*

Ans. : In particular, those engaged in e-business, it is vital to be aware from online threats while using the internet to access information about business related links, business partners and customers relate to different organizations. Today's mostly all business organizations have information systems that use integrated technologies as intranets, extranets or internet access to communicate and transmit information to take rapid business decisions. Under these states, threats from outside the organizations must be attended because of harms from non secured information system in an organization.

Security threats depend on four main sources that are :

Human error - Leak or expose of secret information.

Computer crime- A person intends to be malicious and starts to steal information from sites or cause damage to computer network. Example : Cyber crime through fraud through electronic transfers of money by victim.

Natural calamities/ disasters - In the form of natural calamities, war, home riots etc.

Failure of hardware/software - Like server down or malfunctioning, software fault or error etc.

Some security threats come into the system due to abuse of computers mostly in computer networks that are impersonation (enjoy the person privilege by another unauthentic person), logic bombs, viruses, DoS attacks, spoofing, data leakage, wiretapping, theft through mobile devices etc.

Example : The flooding attacks in the mail server with many messages so that it gets chocked. So these types of attacks qualify as information based attack. Information based attacks are setting of revenge websites and distribute false information that attacks can affect the goodwill of the esteemed organization. The network based attacks are hacking of computer system, insertion of DoS attacks as well as spreading malicious code such as viruses.

Security threats related to computer/ cyber crime or maltreatment occurs from system, which are :

1) Impersonation : Enjoys the privileges of a legal user to gain access of the system by identifying oneself as another person after having defeated to identified and authentication controls of the system.

2) Logic bomb : Unauthorized instructions which stay dormant until a specific event occurs at which they bring into effect of unauthorized act.

3) Trojan horse : Conceal within an unauthorized program as a set of instructions that will cause unauthorized act.

4) Computer viruses and worms : Segment of code that perform malicious acts and replicate copies of these programs into the system that makes impact on our programs and systems.

   Worms (Write Once Read Many) are independent programs transmit copies of themselves through telecommunication networks.

5) Spoofing : Configuring a computer system to masquerade (impersonate) as another system over the network in order to get unauthorized access to the resources of the system being mimicked.

6) Zapping : Using a system's program that can bypass regular system controls to perform unauthorized acts.

1) Physical threats

2) Accidental error

3) Unauthorized access

4) Malicious misuse

5) Malware

1) Physical threat

Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software, theft of the computer system, vandalism, natural disaster such as flood, fire, war, earthquakes etc. Acts of terrorism such as the attack on the world trade centre is also one of the major threats to computer which can be classified as physical threat. Another good example of a physical threat to computer system is the flooding of the city during which valuable information was lost and billions of computer data were destroyed.

2) Accidental error

This is an important security issue which computer security experts should always put into consideration when designing security measures for a system. Accidental errors could occur at any time in a computer system but having proper checks in place is the major concern of the designer. Accidental error includes corruption of data caused by programming error, user or operator error.

3) Unauthorized access

This also poses a great security threats to the computer system due to unauthorized person's having access to the system. Not only this, information can be accessed via a remote system in the process of being transmitted from one point to the other via network media which includes wired and wireless media. Considering an example of an organization in which a member of staff at a particular level of hierarchy within the establishment is only allowed access to specific area according to the policy of the organization. If this employee by other means gain access to the restricted data area on the computer, this can be termed an unauthorized access.

4) Malicious misuse

Any form of tampering of the computer system which includes penetration, viruses and any form of illegal alteration of the computer system which also includes the generation of illegal codes to alter the standard codes within the system can be termed as malicious misuse. This could also lead to a great financial loss and should be prevented in all cases.

5) Malware

You can inadvertently leave your information system open to malware such as Trojans, rootkits and trapdoors if you do not ensure its various data access points. For example, DHCP servers do not have strong security by default. They will assign any computer an IP address that requests it. Malware was listed as the second highest ranked development.

compliance assistance for mobile solutions.

2.2.1 Security and Mobility

The mobility of users and data introduces, therefore, security problems from the point of view of the location of a user and the secrecy and authenticity of the data exchanged. A user on a mobile wireless network may choose, for example, to have the information concerning his existence treated as being confidential. That is a user may choose to remain anonymous to the majority of other users on the network, with the exception of a select number with whom the user often interacts.

Another potential security problem lies in the possibility of information leakage, through the inference made by an attacker masquerading as a mobile support station, who may issue a number of queries to the database at the user's home node or to database at other nodes, with the aim of deducing parts of the user's profile containing the patterns and history of the user's movements. Related to the management of these databases is the issue of replication of certain parameters and user profiles with the aim of replicating the environments surrounding the user. Thus, as the user roams across zones, the user must not experience degradation in the access and latency times. In general, as sensitive data is replicated across several sites, the security risks are also increased due to the multiplication of the points of attack.

Therefore the mobility introduces a number of issues or problems. For example :

Address migration : This consequence of mobility and several techniques such as selective broadcast, central services, home bases and forwarding pointers may provide solutions.

Location-dependent information : Information needed to configure a computer, such as the local name server, available printers, time zone, etc., is location dependent. Mechanisms are needed for obtaining configuration data appropriate to each location.

Privacy : Answering dynamic location queries requires knowing the location of other mobile users. Such information should be protected against misuse and this can be achieved by denying users the availability to know other users' location.

Inter-realm support : Designing distributed services to support the mobile user. Provide authentication, accounting and management over a wide area and across organizations.

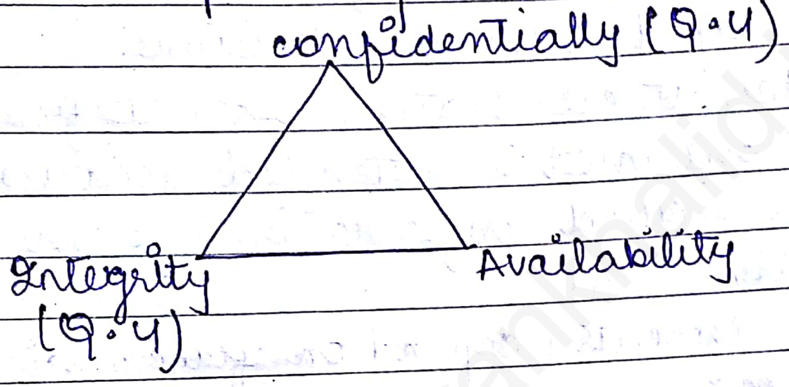
Technical Challenges

...ity. On the

5. Explain the basic three pillas of Information security?

5. Information security means protecting information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. The common goals of IS are to protect the confidentially, integrity & availability of Infor^n^.

Basic three pillars of IS:-



Availability / Accessibility :-

For any information system to serve its purpose, the information must be available when it is needed. The concept of availability ensures the reliable and timely access to information or computing resources by the user. This means that th computing systems used to store and process the information, the security controls used to protect i and the communication channels used to access it must be functioning correctly. High availabilit

a) Integrity :-

Integrity refers to the trustworthiness of information resources. It includes the concept of "data integrity"- namely, that data have not been changed inappropriately, whether by accident or delliberately malign activity. It also includes "origin" or "source" integrity"- that is, that the data actually came from the person or entity you think it did, rather than an imposter. The term Integrity is used frequently when considering information security as it is represents one of the primary indicators of security.

The Integrity of data is not only whether the data is 'correct', but whether it canbe trusted & relied upon. For example, making copies say by e-mailing a file of a sensitive document, threatens both confidentiality & the Integrity of the information. Because of making one or more copies, the data is then at risk of change or modification. So we say that data integrity is violated when a message is actively modified in transit. In Information security, integrity means that data cannot be modified undetectably.

b) confidentiality :-

Assurance of information is shared only among authorized persons or organizations. confidentiality refers to limiting information access and disclosure to authorized users - "the right people" - and preventing access by or disclosure to unauthorized ones - "the wrong people".

violate of confidentiality can occur when data is not handled in a manner adequate to safeguard the confidentiality of the information concerned.

The classification of the information should determine its confidentiality and hence the appropriate safeguards. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction network. The system efforts to enforce confidentiality by encrypting the card number during transmission, by limiting the places that is in databases, log files, backups printed receipts etc, and by restricting access to the places where it is stored. If an un-authorized party obtains the card number in any way, violate of confidentiality has occurred.

c) Security and Access control :-

Access to protected information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the info^n must also be authorized. This requires that mechanisms be in place to control the access to protected information.

Access control mechanisms are built start with identification and authentication.

Identification:- Is an assertion of who someone is or what something is. If a person makes the statement "Hello, my name is John Doe" they are making a claim of who they are. However, their claim may or may not be true. Before John Doe canbe granted access to protected information it will be necessary to verify that the person claiming to be John Doe really is John Doe.

Authentication :- Is the act of verifying a claim of identify. The bank teller asks to see a photo ID, so he hands the teller his driver's license. The bank teller checks the license to make sure it has John Doe printed on it & compares the photograph on the license against the person claiming to be John Doe. If the photo and name match the person, then the teller has authenticated that he claimed to be.

req... payee obtains a guarantee on the payme... is able to authorize and check for availability of funds in the payer's account.

3.5.2.1 Electronic or Digital Cash

This combines computerized convenience with security and privacy that improve upon paper cash. Cash is still the dominant form of payment as : the consumer still mistrusts the banks. The non-cash transactions are inefficiently cleared. In addition, due to negative real interests rates on bank deposits. Now we will enumerate some qualities of cash :

a. Cash is a legal tender i.e. payee is obligatory to take it.

b. It is negotiable i.e. can be given or traded to someone else.

c. It is a bearer instrument i.e. possession is proof of ownership.

d. It can be held and used by anyone, even those without a bank certificate.

e. It places no risk on part of acceptor.

E-cash combines computerized convenience with security and privacy that improve upon paper cash. The e-cash system also includes setup protocols : system setup, payer setup and payee setup which performs system initialization functions, namely creating and publishing public keys and opening payer and payee bank accounts. E-cash allows person to pay for goods or services by transmitting a number from his computer subsystem to the merchant computer system. One key feature of digital cash is that it's anonymous and reusable just like real cash.

Basic model of e-cash system : An anonymous off-line e-cash consists of three probabilistic, polynomial-bounded parties, a bank B, payer P, and payee R, and three main sub protocols : withdrawal, payment and deposit. Payer and payee maintain their accounts with the bank. The payer withdraws electronic coins from their account with the bank, by performing a withdrawal protocol over an authenticated channel. The payer spends coins by participating in a payment protocol with the payee over an anonymous channel. In effect, the payee performs a deposit protocol, to deposit the coins into their account. The e-cash system also includes setup protocols : system setup, payer setup and payee setup which performs system initialization functions, namely creating and publishing public keys and opening payer and payee bank accounts.

3.5.2.2 Electronic Cheques

The electronic cheques are modeled on paper checks, except that they are initiated electronically. They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account. They are delivered either by direct transmission using telephone lines or by public networks such as the Internet.

Benefits of electronic cheques :

- o Well suited for clearing micro payments. Conventional cryptography of e-cheques makes them easier to process than systems based on public key cryptography (like digital cash).
- o They can serve corporate markets. Firms can use them in more cost-effective manner.
- o They create float and the availability of float is an important requirement of commerce.

3.5.2.3 Credit Card

A credit card is a payment card issued to users as a system of payment. It allows the cardholder to pay for goods and services based on the holder's promise to pay for them. Credit cards are issued by financial institutions which allow making a purchase up to a certain limit or credit. Most of the credit card companies recognize the shopping malls or shops etc from where the items are purchased. Payments of these items are paid by the credit card company on user's behalf.

A credit card allows you to borrow money when making purchases. The money isn't directly debited from your bank account at the time of purchase; instead, you are sent a bill every month for the sum total of your purchases. If you plan to borrow using your credit card, you also need to understand the terms and, in particular, the way interest charges are computed.

A credit card is different from a charge card : a charge card requires the balance to be paid in full each month. In contrast, credit cards allow the consumers a continuing balance of debt, subject to interest being charged. A credit card also differs from a cash card, which can be used like currency by the owner of the card.

Secured credit cards

A secured credit card is a type of credit card secured by a deposit account owned by the cardholder. Typically, the cardholder must deposit between 100 % and 200 % of the total amount of credit desired. Thus if the cardholder puts down ₹ 1000, they will be given credit in the range of ₹ 500-1000. In some cases, credit card issuers will offer incentives even on their secured card portfolios. In these cases, the deposit required may

2. What is the biomatrics? How cana bio-matrics to be used for access control?

2. Biometrics :

→ The term biometrics comes from Greek word Bios means life and metrics mea measure.

→ It is well known that the human uses intutive way of body characteristics such as face, voice etc to recognize Eac other.

→ Biometrics is used as one of the method for physical access control. Biometrics dat have characteristics w/c are so unique to a person & embedded with a person that

It can't be lost, stolen and copied.

Biometrics : Access control :-

→ Biometric identifiers are the distinctive, measurable characteristics used to label & describe individuals.

→ Biometrics access control systems consist of a reader or scanning device, software that converts the gathered information into digital form and a database that stores the information for comparison with previous records.

→ A physiological biometric would identify by one's voice, DNA, hand print or behaviou

→ Biometrics Access control systems consist of a readers, or scanning devices, can scan for a fingerprint, hand geometry, signature, iris/retina, facial recognition, voice print and even DNA.

→ This technology canbe used for a number o applications including time and attendance reporting, building access control, verification of signatures, point-of-sale identity verification, process control security and cellular phone security.

Q.1 *Give the security threats to e-commerce.*

Ans. : Most businesses that make online presence have experienced some kind of security threat to their business. Since the internet is the public system in which every transaction can be tracked, logged, monitored and stored in many locations. So it is important for business to understand possible security threats for their business.

In a typical e-commerce experience, a shopper proceeds to a Web site to browse a catalog and make a purchase. This simple activity illustrates the four major players in e-commerce security. One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit. As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors. The software vendor is the last of the three legitimate players. The attacker is the player whose goal is to exploit the other three players for illegitimate gains.

The vulnerability of a system exists at the entry and exit points within the system. E-commerce system with several points that the attacker can target :

i) Shopper

ii) Shopper' computer

iii) Network connection between shopper and Web site's server

iv) Web site's server

v) Software vendor

vi) Tricking the shopper

There are many threats to E-commerce that may come from source within organization or through external world. The following are the security threats categorized as internal and external threats :

i) Unauthorized internal users accessed confidential information by breaking or stealing password for the purpose of committing fraud.

ii) Weak access point in information infrastructure security exposed organization information and threats towards trade.

iii) Partners, brokers and consultants take privileges of even limited access to important systems.

iv) Management that underlines or not well known the importance of security is the great risk for e-commerce conducts business.

v) User's mentality towards internet security is changing due to sales of antivirus software.

down so nobody can walk off with them.

Q.4 *Write short notes on i) B2B E-commerce ii) B2C E-commerce iii) C2C E-commerce*

Ans. : E-commerce is the purpose of internet and the web to conduct business but when we concentrate on commercial deals among organizations and individuals demanding selective information systems under the guarantee of the firm it accepts the form of e-business.

Types of E-commerce: E-commerce can be broken into four main categories: B2B, B2C, C2B, and C2C :

1. **Business to Business E-commerce (B2B E-commerce)** : In this type of ecommerce, both participants are businesses. As a result, the volume and value of B2B e-commerce can be huge. B2B stands for Business to Business. It consists of largest form of e-commerce. This model defines that buyer and seller are two different entities. It is similar to manufacturer issuing goods to the retailer or wholesaler. An example of business to business e-commerce could be a manufacturer of gadgets sourcing components online. Dell deals with computers and other associated accessories online but it does not make all those products. So, in manage to deal those products, first step is to purchases them from unlike businesses i.e. the producers of those products.

2. **Business to Consumer E-commerce (B2C E-commerce)** : B2C stands for Business to Consumer as the name suggests. It is the model taking businesses and consumers interaction. Online business sells to individuals. The basic concept of this model is to sell the product online to the consumers. B2C is the indirect trade between the company and consumers. It provides direct selling online. For example : if you want to sell goods and services to customer so that anybody can purchase any products directly from supplier's website. Directly interact with the customers is the main difference with other business model. As B2B it manages directly relationship with consumers, B2C supply chains normally deal with business that are related to the customer. Amazon.com pops up in most discussions about e-commerce. Elimination of the need for physical stores is the biggest rationale for business to consumer e-commerce. But the complexity and cost of logistics can be a barrier to B2C e-commerce growth.

3. **Consumer to Consumer E-commerce (C2C E-commerce)**: The moment you think of C2C e-commerce eBay.com comes to mind. Though there is no major parties needed but the parties will not fulfill the transactions without the program. That is because it is the most popular platform that enables consumers to sell to other consumers. Since eBay.com is a business, this form of

e-commerce could also be called C2B2C e-commerce (consumer to business to consumer e-commerce). It helps the online dealing of goods or services among people.

Q.5 *What are the problems with traditional payment system as compared to electronic payment systems ?*

Ans. : Traditional or conventional instruments of payments such as demand draft, checks, credit notes are not fit for e-commerce. Conventional instruments are too slow to be processed and the overheads of processing of such instrument may be high.

These methods have several shortcomings :

i) Checks and cash cannot be exchanged in real time.

ii) The overhead of cash system do not support low value transactions (micropayments).

iii) Traditional system do not support individual to individual payment transactions.

iv) Traditional methods adopt very timeconsuming process.

v) These methods are not able to assure the validity of financial transaction.

In e-commerce, the challenges of payment transactions were initially underrated but now the business via the internet and mobile has so far dominated by the e-methods of e-commerce payment systems. As compared to traditional system, electronic payment is a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender.

Electronic payments involve a payer and a payee. A payer (buyer or customer), is an entity who makes a payment. A payee (seller or merchant), is an entity who receives a payment. The main purpose of an electronic payment protocols is to transfer monetary value from the payer to the payee. The process also involves a financial institution (or bank). Secure user friendly and low priced innovative e-payment solutions are urgently required to boost international oriented e-commerce to boost trade.

There are three common electronic payment instruments, namely e-cash, e-cheque and cards.

E-cash combines computerized convenience with security and privacy that improve upon paper cash. The e-cash system also includes setup protocols : system setup, payer setup and payee setup. E-cash allows person to pay for goods or services by transmitting a number from his computer subsystem to the merchant computer system.

Electronic cheques are modeled on paper checks, except that they are initiated electronically. They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account. They are delivered either by direct transmission using telephone lines or by public networks such as the internet.

Q.7 ***What is Electronic Data Interchange (EDI) ? Also give its benefits.***

Ans. : Electronic Data Interchange (EDI) is the structured transmission of data between organizations by electronic means, which is used to transfer electronic documents or business data from one computer system to another computer system, i.e. from one trading partner to another trading partner without human intervention. It is more than mere e-mail; for instance, organizations might replace bills and even cheques with appropriate EDI messages. It also refers specifically to a family of standards. EDI documents use specific computer record formats that are based on widely accepted standards. However, each firm will use the flexibility allowed by the standards in a unique way that fits their business needs.

The acts of controlling, directing, guiding, influencing and standardizing the conduct, actions and solutions associated with the discipline (i.e. enterprise capability) known as Electronic Data Interchange (EDI) Management

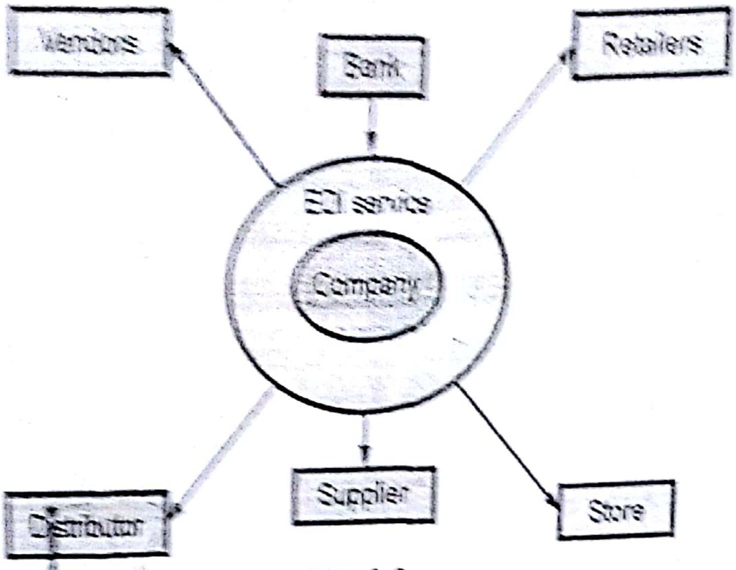


Fig. 3.2

The above diagram shows a company and its various partner companies like as vendors, banks, retailers, distributers, suppliers and warehouses.

Benefits of EDI

The EDI process provides many benefits. By moving from a paper-based exchange of business document to one that is electronic, businesses enjoy major benefits such as reduced cost, increased processing speed, reduced errors and improved relationships with business partners. From a financial perspective alone, there are impressive benefits from implementing EDI with your trading partners and each additional document that you implement can increase that savings. But cost savings is far from the only benefit of using EDI.

Here are the top five key benefits or reasons why businesses adopt EDI.

1) *Remove document re-keying* : By removing the manual keying of key business documents such as orders, invoices, acknowledgments and dispatch Notes your company can benefit significantly by *reduced labor cost, eliminate of human keying errors, faster document processing, instant document retrieval etc.*

2) *Eliminate paper* : Paper-based trading relationships have some inherent disadvantages when compared with their electronic trading equivalents that are *Stationery and printer consumable costs, Document storage costs lost documents, postage costs etc.*

3) *Reduce lead times and stockholding* : Electronic trading documents can be delivered far more quickly than their paper counterparts, thus the turnaround time from order to delivery can be reduced. By using EDI for forecasting and planning, companies are able to get forward warning of likely orders and to plan their production and stock levels accordingly. Companies receiving advanced shipping notes or acknowledgments know in advance. Integrating electronic documents means they can be processed much faster, again reducing lead times and speed up payments.

4) *Increase quality of the trading relationship* : Electronic trading accurate documents when printed are much easier to read than copies faxed on multi-part stationery by

4.1 Purpose of Cryptography

Cryptography is the science of writing in secret code and is an ancient art. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet.

Cryptography can be used to provide :

- Confidentiality - ensure data is read only by authorized parties,
- Data integrity - ensure data wasn't altered between sender and recipient,
- Authentication - ensure data originated from a particular party.

A cryptographic system (or a cipher system) is a method of hiding data so that only certain people can view it. Cryptography is the practice of creating and using cryptographic systems. Cryptanalysis is the science of analyzing and reverse engineering cryptographic systems. The original data is called plaintext. The protected data is called ciphertext. Encryption is a procedure to convert plaintext into ciphertext. Decryption is a procedure to convert ciphertext into plaintext. A cryptographic system typically consists of algorithms, keys, and key management facilities. The steps of this process are following :

1. The sender converts the plaintext message to ciphertext. This part of the process is called encryption (sometimes encipherment).
2. The ciphertext is transmitted to the receiver.
3. The receiver converts the ciphertext message back to its plaintext form. This part of the process is called decryption (sometimes decipherment).

The conversion involves a sequence of mathematical operations that change the appearance of the message during transmission but do not affect the content. Cryptographic techniques can ensure confidentiality and protect messages against unauthorized viewing (eavesdropping), because an encrypted message is not understandable. Digital signatures, which provide an assurance of message integrity, use encryption techniques.

Within the context of any application-to-application communication, there are some specific security requirements, including :

- Authentication : The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based.)

turn (usually) be decrypted into usable plaintext.

4.2.1 Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. They are to be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms are :

a. Secret Key Cryptography (SKC) : Uses a single key for both encryption and decryption.

b. Public Key Cryptography (PKC) : Uses one key for encryption and another for decryption.

c. Hash Functions : Uses a mathematical transformation to irreversibly "encrypt" information.

4.2.1.1 Secret Key Cryptography

With *secret key cryptography*, a single key is used for both encryption and decryption. As shown in Fig. 4.2.1, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called *symmetric encryption*.

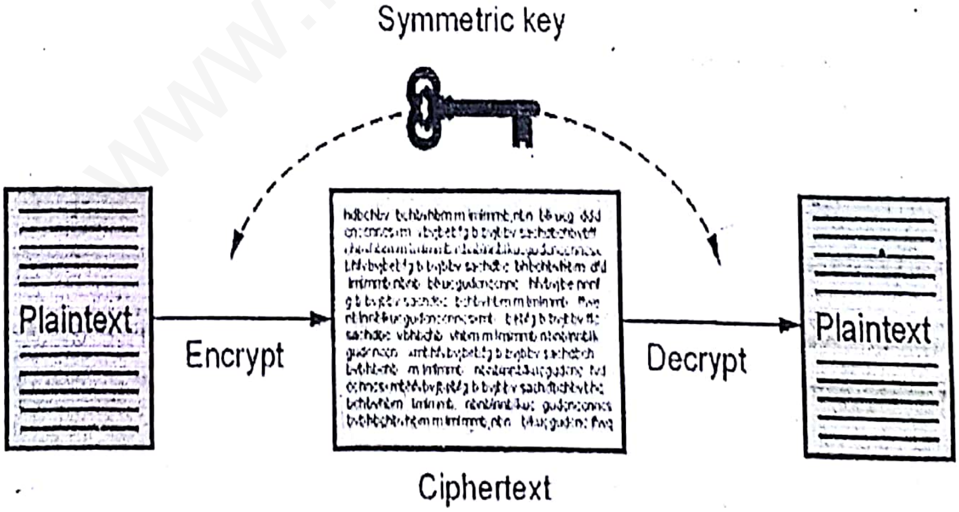


Fig. 4.2.1 Secret Key Cryptography

4.2.1.2 Public Key Cryptography

Public-key cryptography is also called asymmetric cryptography. It uses a secret key that must be kept from unauthorized users and a public key that can be made public to anyone. Both the public key and the private key are mathematically linked; data encrypted with the public key can be decrypted only by the private key, and data signed with the private key can only be verified with the public key. The public key can be published to anyone. Both keys are unique to the communication session.

1. Each system generates a pair of keys.
2. Each system publishes its encryption key (public key) keeping its companion key private.
3. If A wishes to send a message to B it encrypts the message using B's public key.
4. When B receives the message, it decrypts the message using its private key. No one else can decrypt the message because only B knows its private key.

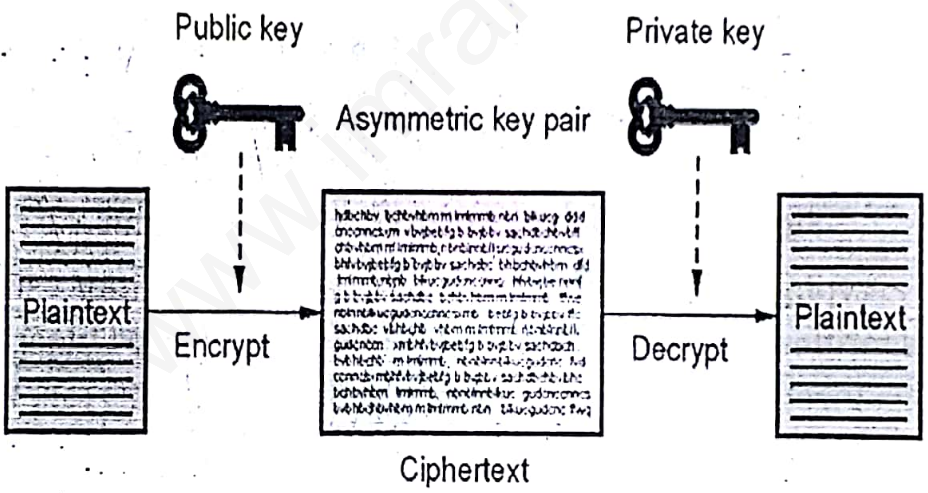


Fig. 4.2.2 Public Key Cryptography

Fig. 4.2.2 shows plaintext encrypted with the receiver's public key and decrypted with the receiver's private key. Only the intended receiver holds the private key for decrypting the ciphertext. Note that the sender can also encrypt messages with a private key, which allows anyone that holds the sender's public key to decrypt the message, with the assurance that the message must have come from the sender.

4.2.2 Difference between Symmetric vs. Asymmetric Encryption (Private Key vs. Public Key)

Symmetric, or private-key, encryption (also known as conventional encryption) is based on a secret key that is shared by both communicating parties. The sending party uses the secret key as part of the mathematical operation to encrypt (or encipher) plain text to cipher text. The receiving party uses the same secret key to decrypt (or decipher) the cipher text to plain text. Examples of symmetric encryption schemes are the RSA RC4 algorithm (which provides the basis for Microsoft Point-to-Point Encryption (MPPE), Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), and the Skipjack encryption technology proposed by the United States government (and implemented in the clipper chip).

Asymmetric, or public-key, encryption uses two different keys for each user : One is a private key known only to this one user; the other is a corresponding public key, which is accessible to anyone. The private and public keys are mathematically related by the encryption algorithm. One key is used for encryption and the other for decryption, depending on the nature of the communication service being implemented. In addition, public key encryption technologies allow digital signatures to be placed on messages. A digital signature uses the sender's private key to encrypt some portion of the message. When the message is received, the receiver uses the sender's public key to decipher the digital signature to verify the sender's identity.

covered, and how users must authenticate.

4.5 Digital Signature and Verification

A digital signature certificate, like hand written signature, establishes the identity of the sender filing the documents through internet which sender can not revoke or deny. Accordingly, digital signature certificate is a digital equivalent of a hand written signature which has an extra data attached electronically to any message or a document. Digital signature also ensures that no alterations are made to the data once the document has been digitally signed. A DSC is normally valid for 1 or 2 years, after which it can be renewed.

Digital signature certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as a proof of identity of an individual for a certain purpose; for example a driver's license identifies someone who can legally drive in a particular country. Likewise, a digital certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally.

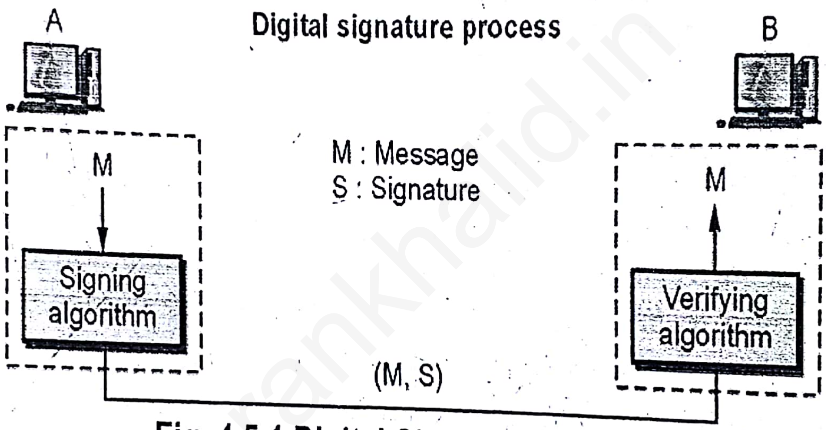


Fig. 4.5.1 Digital Signature Process

Digital signature is a mechanism by which a message is authenticated i.e. proving that a message is effectively coming from a given sender, much like a signature on a paper document. For instance, suppose that A wants to digitally sign a message to B. To do so, A uses her private-key to encrypt the message; A then sends the message along with her public-key (typically, the public key is attached to the signed message). Since A's public-key is the only key that can decrypt that message, a successful decryption constitutes a digital signature verification, and meaning that there is no doubt that it is A's private key that encrypted the message.

...olutions. ...gnature ...list of licensed CAs along with ...ilable on www.mca.gov.in. You may obtain your DSC

4.5.1 Digital Signatures : Integrity in Public Cryptographic Key Systems

Integrity is guaranteed in public-key systems by using *digital signatures*. A digital signature is a piece of data which is attached to a message and which can be used to find out if the message was tampered with during the conversation (e.g. through the intervention of a malicious user). The digital signature is attached to the message, and sent to the receiver. The receiver then does the following :

a) Using the sender's public key decrypts the digital signature to obtain the message digest generated by the sender.

b) Uses the same message digest algorithm used by the sender to generate a message digest of the received message.

c) Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver). If they are not exactly the same, the message has been tampered with by a third party. We can be sure that the digital signature was sent by the sender (and not by a malicious user) because only the sender's public key can decrypt the digital signature (which was encrypted by the sender's private key; remember that what one key encrypts, the other one decrypts, and vice versa). If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

privacy, another layer of encryption/decryption must be applied.

4.6 Fingerprints

Fingerprints are created by applying a cryptographic hash function to a public key. Since fingerprints are shorter than the keys they refer to, they can be used to simplify certain key management tasks. A fingerprinting algorithm is a procedure that maps an arbitrarily large data item (such as computer file) to a much shorter bit string, its fingerprint, that uniquely identifies the original data for all practical purposes just as human fingerprints uniquely identify people for practical purposes. This fingerprint may be used for data de-duplication purposes.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

A *public key fingerprint* is typically created through the following steps :

1. A public key (additional data) is encoded into a sequence of bytes. To ensure that the same fingerprint can be recreated later, the encoding must be deterministic, and any additional data must be exchanged and stored alongside the public key. The additional data is typically information which anyone using the public key should be aware of. Examples of additional data include : Which protocol versions the key should be used with (case of PGP fingerprints); and the name of the key holder (case of X.509 trust anchor fingerprints, where the additional data consists of an X.509 self-signed certificate).
2. The data produced in the previous step is hashed with a cryptographic hash function such as MD5 or SHA-1.
3. If desired, the hash function output can be truncated to provide a shorter, more convenient fingerprint.

When a public key is received over an untrusted channel, such as the Internet, the recipient often wishes to authenticate the public key. Fingerprints can help accomplish this, since their small size allows them to be passed over trusted channels where public keys won't easily fit.

4.7 Firewalls

asseoti

Firewalls make it possible to filter incoming and outgoing traffic that flows through your system. A firewall can use one or more sets of "rules" to inspect the network packets as they come in or go out of your network connections and either allows the traffic through or blocks it. The rules of a firewall can inspect one or more characteristics of the packets, including but not limited to the protocol type, the source or destination host address, and the source or destination port.

Firewalls can greatly enhance the security of a host or a network. They can be used to do one or more of the following things :

- To protect and insulate the applications, services and machines of your internal network from unwanted traffic coming in from the public Internet.
- To limit or disable access from hosts of the internal network to services of the public Internet.
- To support network address translation (NAT), which allows your internal network to use private IP addresses and share a single connection to the public Internet (either with a single IP address or by a shared pool of automatically assigned public addresses).

4.7.1 Types of Firewalls

Conceptually, there are two types of firewalls :

1. Network layer firewalls
2. Application layer firewalls

1. Network layer firewalls

These generally make their decisions based on the source, destination addresses and ports in individual IP packets. A simple router is the ``traditional'' network layer firewall, since it is not able to make particularly sophisticated decisions about what a packet is actually talking to or where it actually came from. Modern network layer firewalls have become increasingly sophisticated, and now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. One thing that's an important distinction about many network layer firewalls is that they route traffic directly though them, so to use one you either need to have a validly assigned IP address block or to use a ``private internet'' address block. Network layer firewalls tend to be very fast and tend to be very transparent to users.

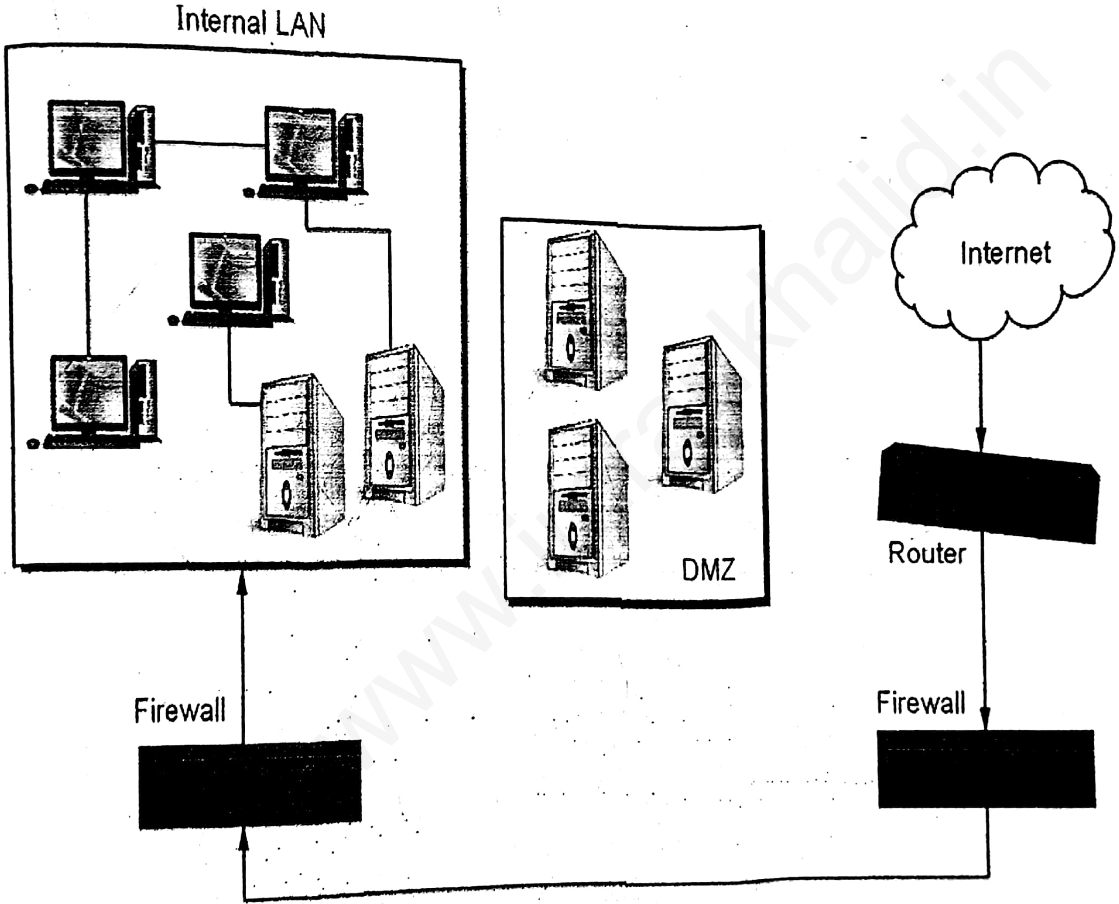
2. Application layer firewalls

These generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform elaborate logging and auditing of traffic passing through them. Since the proxy applications are software components running on the firewall, it is a good place to do lots of logging and access control. Application layer ternet interface to allow the passing of tunnel maintenance traffic and tunneled data to the VPN server. Additional filters can allow the passing of traffic to Web servers, FTP servers, and other types of servers on the DMZ.

Q.10 *What is the concept of demilitarized zone (DMZ) ?*

Ans. : The area separated between the two firewalls is called DMZ. Basically, a DMZ is a sub network that is located neither inside the internal network nor outside as part of the Internet. Technically, a demilitarized area is any area where access is controlled but not prevented by firewall technology. A DMZ can lie between two firewalls. Alternatively, a DMZ can also be off from a separate segment from one firewall. In either case, the types of access to and from DMZ servers are controlled and should be limited to a small group of users or network.

DMZ servers can provide additional functionalities in e-coomerce servers, web servers and FTP servers.



The demilitarized zone (DMZ)

Q. 11 *Discuss how network security matters in the modern digital world, in which today's* content. By combining Steganography and Cryptography one can achieve better security.

Q.9 *Explain the VPN architecture and discuss how can implement firewall with advantages of VPN.*

Ans. : A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet to provide remote offices or individual users with secure access to their organization's network. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking.

VPNs are primarily used to extend an enterprise's internal private network i.e. intranet across un-trusted public networks. They provide the capability to secure convey information across the public network into corporate network. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost.

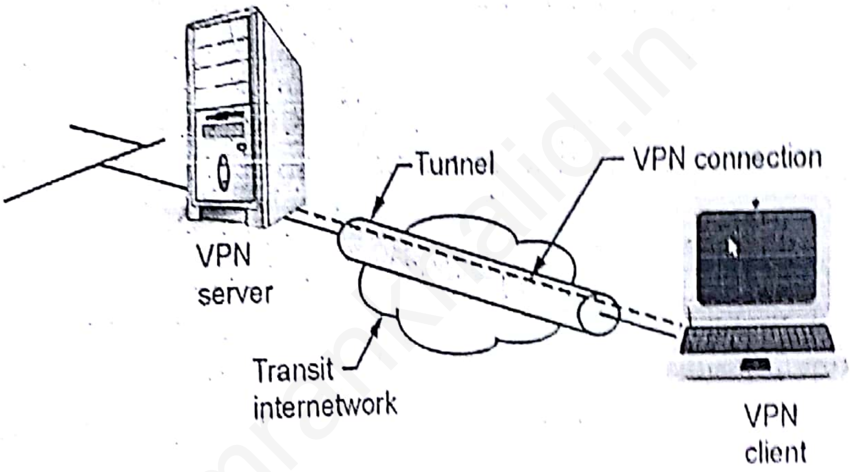


Fig. 5.1 Virtual private network connection

VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations; where workers must be able to connect to central resources and must be able to communicate with each other.

Therefore, a VPN solution should provide at least all of the following :

- *User Authentication* : The solution must verify the VPN client's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.
- *Address Management* : The solution must assign a VPN client's address on the intranet and ensure that private addresses are kept private.
- *Data Encryption* : Data carried on the public network must be rendered unreadable to unauthorized clients on the network.
- *Key Management* : The solution must generate and refresh encryption keys for the client and the server.

- Common law.

6.3.1 IPR

Intellectual Property Rights are legal rights, which result from intellectual activity in industrial, scientific, literary and artistic fields. These rights are safeguard creators and other producers of intellectual goods and services by granting them certain time-limited rights to control their use. Protected IP rights like other property can be a matter of trade, which can be owned, sold or bought. These are intangible and no exhausted consumption.

The importance of intellectual property in India is well established at all levels- statutory, administrative and judicial. India ratified the agreement establishing the World Trade Organization (WTO). This Agreement, inter-alia, contains an Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS) which came into force from 1st January 1995. It lays down minimum standards for protection and enforcement of intellectual property rights in member countries which are required to promote effective and adequate protection of intellectual property rights with a view to reducing distortions and impediments to international trade. The obligations under the TRIPS Agreement relate to provision of minimum standard of protection within the member countries legal systems and practices.

The Agreement provides for norms and standards in respect of following areas of intellectual property

- Patents
- Trade marks
- Copyrights
- Geographical indications
- Industrial designs

6.3.2 Patent Law

A patent is an exclusive right granted for an invention, which is a product or a process that provides a new way of doing something, or offers a new technical solution to a problem. It provides protection for the invention to the owner of the patent. The protection is granted for a limited period, i.e. 20 years. Patent protection means that the invention cannot be commercially made, used, distributed or sold without the patent owner's consent.

A patent owner has the right to decide who may - or may not - use the patented invention for the period in which the invention is protected. The patent owner may give permission to, or license, other parties to use the invention on mutually agreed terms. The owner may also sell the right to the invention to someone else, who will then become the new owner of the patent. Once a patent expires, the protection ends, and an invention enters the public domain, that is, the owner no longer holds exclusive rights to the invention, which becomes available to commercial exploitation by others.

All patent owners are obliged, in return for patent protection, to publicly disclose information on their invention in order to enrich the total body of technical knowledge in the world. Such an ever-increasing body of public knowledge promotes further creativity and innovation in others. In this way, patents provide not only protection for the owner but valuable information and inspiration for future generations of researchers and inventors. General Principles governing the Patent System in India and further details can be viewed at DIP and P website at http://ipindia.nic.in/ipr/patent/patents.htm

The basic obligation in the area of patents is that, invention in all branches of technology whether products or processes shall be patentable if they meet the three tests of being new involving an inventive step and being capable of industrial application. In addition to the general security exemption which applied to the entire TRIPS Agreement, specific exclusions are permissible from the scope of patentability of inventions, the prevention of whose commercial exploitation is necessary to protect public order or morality, human, animal, plant life or health or to avoid serious prejudice to the environment. Further, members may also exclude from patentability of diagnostic, therapeutic and surgical methods of the treatment of human and animals and plants and animal other than micro-organisms and essentially biological processes for the production of plants and animals.

The TRIPS Agreement provides for a minimum term of protection of 20 years counted from the date of filing.

The Patents (Amendment) Rules 2006.

6.3.3 Trademarks

A trademark is a distinctive sign that identifies certain goods or services as those produced or provided by a specific person or enterprise. It may be one or a combination of words, letters, and numerals. They may consist of drawings, symbols, three-dimensional signs such as the shape and packaging of goods, audible signs such as music or vocal sounds, fragrances, or colors used as distinguishing features. It provides protection to the owner of the mark by ensuring the exclusive right to use it to identify goods or services, or to authorize another to use it in return for payment. It helps consumers identify and purchase a product or service because its nature and quality, indicated by its unique trademark, meets their needs. Registration of trademark is prima facie proof of its ownership giving statutory right to the proprietor. Trademark rights may be held in perpetuity. The initial term of registration is for 10 years; thereafter it may be renewed from time to time. General Principles governing the Trademarks System in India and further details can be viewed at DIP and P website at http://ipindia.nic.in/tmr_new/default.htm

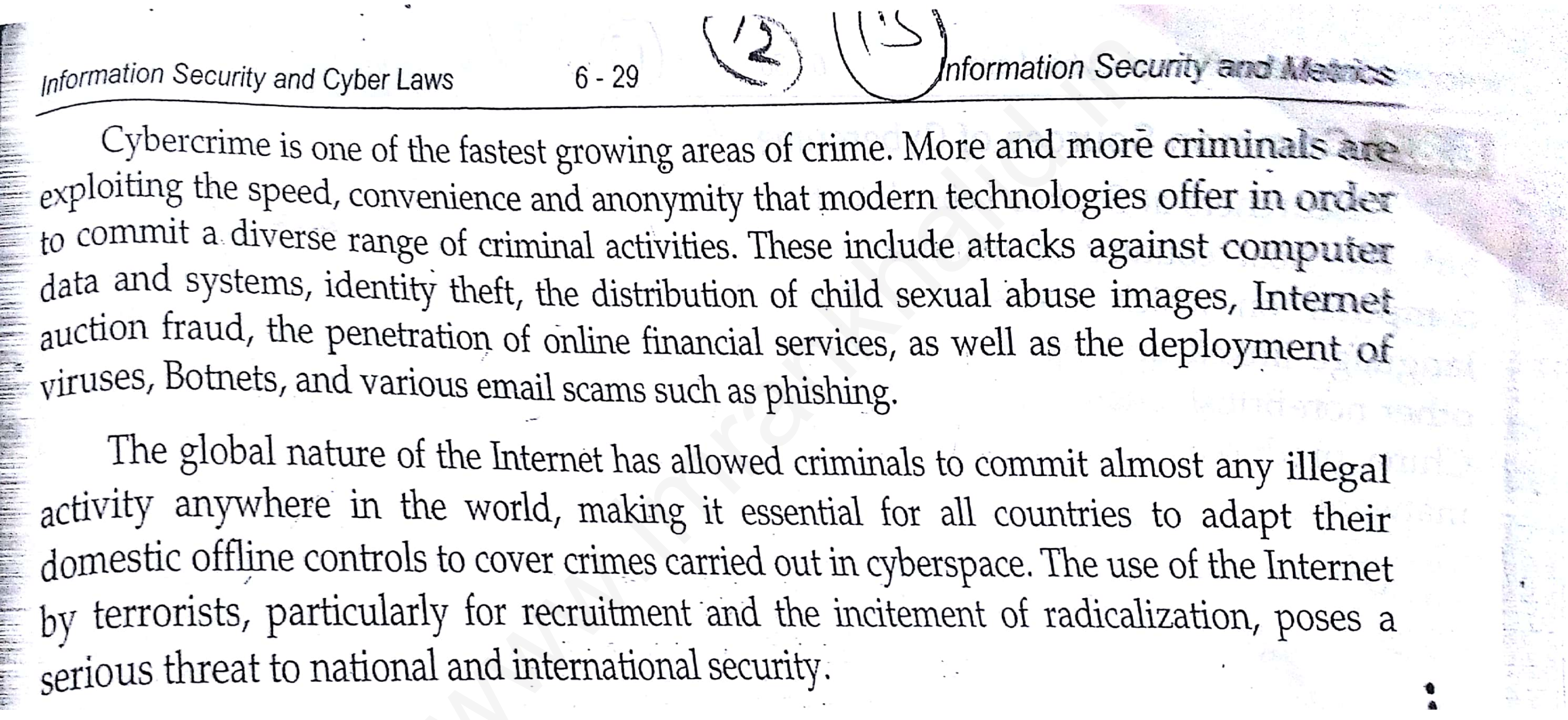
Trademarks have been defined as any sign, or any combination of signs capable of distinguishing the goods or services of one undertaking from those of other undertakings. Such distinguishing marks constitute protectable subject matter under the provisions of the TRIPS Agreement. The Agreement provides that initial registration and each renewal of registration shall be for a term of not less than 7 years and the registration shall be renewable indefinitely. Compulsory licensing of trademarks is not permitted.

Keeping in view the changes in trade and commercial practices, globalization of trade, need for simplification and harmonization of trade marks registration systems etc., a comprehensive review of the Trade and Merchandise Marks Act, 1958 was made and a Bill to repeal and replace the 1958 Act has since been passed by Parliament and notified in the Gazette on 30.12.1999. This Act not only makes Trade Marks Law, TRIPS compatibility but also harmonizes it with international systems and practices. Work is underway to bring the law into force.

out of reach for on-premise installations.

6.8 Overview of Cyber Crimes and Cyber Crime Types ✓

Computer crime is known by lots of different names, including cybercrime, e-crime, or electronic crime. All of these are crimes where computers or networks are used or attacked. These electronic crimes are being used to steal identities and huge sums of money. Many traditional crimes such as theft, blackmail, forgery, embezzlement and fraud today are all conducted on the internet. An Introduction Computer or Internet Crime is where the target or source of crime is either computer or network of computers termed as Internet. Cyber Criminals feel safe to commit crimes from the privacy of their homes. There are more cyber criminals than cyber cops need to develop laws to combat latest technologies.



Cybercrime is one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities. These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, Internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, Botnets, and various email scams such as phishing.

The global nature of the Internet has allowed criminals to commit almost any illegal activity anywhere in the world, making it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace. The use of the Internet by terrorists, particularly for recruitment and the incitement of radicalization, poses a serious threat to national and international security.

Contributor- Nashra Anjum(3 Times Topper)
Website- http://www.diplomacs.com