MCS-215: Security and Cyber Laws
Guess Paper-I

Q. Explain how spyware harm security.

Ans. Spyware is a type of malicious software -- or malware -- that is installed on a computing device without the end user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms or external users. Any software can be classified as spyware if it is downloaded without the user's authorization. Spyware is controversial because, even when it is installed for relatively innocuous reasons, it can violate the end user's privacy and has the potential to be abused. Spyware is one of the most common threats to internet users. Once installed, it monitors internet activity, tracks login credentials and spies on sensitive information. The primary goal of spyware is usually to obtain credit card numbers, banking information and passwords. Spyware can be difficult to detect; often, the first indication a user has that a computing device has been infected with spyware is a noticeable reduction in processor or network connection speeds and -- in the case of mobile devices -- data usage and battery life. Antispyware tools can be used to prevent or remove spyware. Antispyware tools can either provide real-time protection by scanning network data and blocking malicious data, or they can detect and remove spyware already on a system by executing scans.

A Spyware is generally classified into adware, tracking cookies, system monitors and Trojans. The most common way for a spyware to get into the computer is through freeware and shareware as a bundled hidden component. Once a spyware gets successfully installed, it starts sending the data from that computer in the background to some other place.

These days spywares are usually used to give popup advertisements based on user habits and search history. But when a spyware is used maliciously, it is hidden in the system files of the computer and difficult to differentiate. One of the simplest and most popular, yet dangerous are Key loggers. It is used to record the keystrokes which could be fatal as it can record passwords, credit card information etc. In some shared networks and corporate computers, it is also intentionally installed to track user activities. Presence of spyware in a computer can create a lot of other troubles as spyware intended to monitor the computer can change user preferences, permissions and also administrative rights, resulting in users being locked out of their own computer and in some cases, can also result in full data losses. Spyware running in the background can also amount to increased number of processes and result in frequent crashes. It also often slows down a computer. Best way to remain protected is to use good Antivirus/Antispyware software. More importantly, be careful while installing freeware applications by properly removing the unnecessarily checked options by default. Spyware can affect any personal computer (PC) or Mac, as well as iOS or Android devices. While the Windows operating system (OS) is more likely to fall prey to an infiltration, hackers are getting better at finding ways into Apple's OS as well. Some of the most common ways for computers to become infected include the following:

- pirating media, including games, videos and music;
- downloading materials from unreliable or unknown sources;
- accepting a pop-up advertisement or prompt without reading the content; and
- Accepting and opening email attachments from unrecognized senders.

In its least damaging form, spyware exists as an application that starts up as soon as the device is turned on and continues to run in the background. Its presence will steal random access memory (RAM) and processor power and could generate infinite pop-up ads, effectively slowing down the web browser until it becomes unusable. Spyware may also reset the browser's homepage to open to an ad every time or redirect web searches and control the provided results, making the search engine useless. Additionally, spyware can change the computer's dynamically link libraries (DLLs) -- which are used to connect to the internet -- resulting in connectivity failures that can be hard to diagnose. At its most damaging, spyware will track web browsing history and record words, passwords and other private information, such as credit card numbers or banking records. All of this information can be gathered and used for identity theft. Spyware can also secretly make changes to a device's firewall

settings, reconfiguring the security settings to allow in even more malware. Some forms of spyware can even identify when the device is trying to remove it from the Windows registry and will intercept all attempts to do.

Q. What is digital security? Write some pros. and cons. of Digital Security.

Ans. Digital security is a broader term which encompasses within itself protection of online identity data assets Technology with the use of various tools like software, Web Services, biometrics, firewalls, proxies, vulnerability scanner, instant message or telephone encryption tools etc. Digital security provides protection against cyber-attacks unauthorized access, online malicious activities etc.

The 3 pillars of digital security are:

(1) Confidentiality
(2) Integrity
(3) Availability

The basic essence of these principles is that the information which is private should be shared with the least amount of people to keep it more secure, the information provided should not be modified or corrupted and lastly, that the information provided should work effectively and efficiently at all times. The OECD Recommendation and its companion documents were published in 2015 which provides guidance for all stakeholders on cyber security aspects. The Organization for Economic Cooperation and Development (OECD) helps in facilitating information, data and is progressing to eradicate poverty and inequality by bringing forefront solutions for the benefit of the world. The OECD Working Party on Security and Privacy in the Digital Economy (SPDE) develops public policy analysis and high-level recommendations to help governments and other stakeholders to ensure that digital security and privacy protection foster the development of the digital economy.

Digital Security Pros:

- It helps in protecting personal information stored in devices.
- Suspicious or unauthorized access to devices can be blocked through digital security and thus preventing possible harm.
- Security based on biometrics is capable of providing a higher degree of protection against attacks as it's difficult to steal biometric information.
- Digital security enables oneself to fearlessly communicate, transact, and work etc. in online mode.
- Protects the computer from crashing or slowing down and thus protects business, transactions, communication etc. happening over computer, network or system.
- Digital security thus may help in fostering the economy of the State as it cuts down on many costs.

Digital Security Cons:

- Availing services or procuring tools for digital security can be a costly affair.
- Web services or tools may or may not be compatible with the device of the user.
- Digital security services or tools may be difficult to configure at times and needs to be updated regularly
- Services or tools may slow down functioning of user's device or at times may intervene even normal functioning of another programme

Q. Write some various phishing techniques used by attackers and how to prevent from it.

Ans. Various phishing techniques used by attackers:

- Embedding a link in an email that redirects your employee to an unsecure website that requests sensitive information
- Installing a Trojan via a malicious email attachment or ad which will allow the intruder to exploit loopholes and obtain sensitive information
- Spoofing the sender address in an email to appear as a reputable source and request sensitive information

- Attempting to obtain company information over the phone by impersonating a known company vendor or IT department.

Steps from prevention:

- Educate your employees and conduct training sessions with mock phishing scenarios.
- Deploy a SPAM filter that detects viruses, blank senders, etc.
- Keep all systems current with the latest security patches and updates.
- Install an antivirus solution, schedule signature updates, and monitor the antivirus status on all equipment.
- Develop a security policy that includes but isn't limited to password expiration and complexity.
- Deploy a web filter to block malicious websites.
- Encrypt all sensitive company information.
- Convert HTML email into text only email messages or disable HTML email messages.
- Require encryption for employees that are telecommuting.

Q. Explain Cyber Security Intrusion Detection.

Ans. Intrusion detection systems monitor traffic and generate alerts in the case of suspicious activity tending to harm the cyber security. However, some intrusion detection systems are capable of even prevention of cyber threats. Such intrusion systems may be network, host, hybrid, application, protocol based and method of detection may be signature based or anomaly based. Signature based intrusion detection system detects intrusions based on patterns or already known malicious instruction sequence. Anomaly based systems rely on trustful activity model with the use of machine learning and anything dissimilar from the model is alerted as suspicious. With the rise of IOT based environment use of such intrusion detection systems have grown multi fold.(Elrawy, M., Awad, A. & Hamed, H, 2018) Intrusion detection systems can help in ensuring IT related regulatory compliance, maintain security standards, and raises alarms against malwares like spywares, keyloggers, unauthorized clients, unintentional accidental leakage etc., and measure the cyber-attacks in number and forms/types, increase efficacy. However, such detection systems are susceptible to few flaws like it has been witnessed that such systems often raise false alarms, unable to avid encrypted packets, they need to be continually updated and generally should be looked after by an expert engineer. Strong Passwords, Firewalls, Encryption, Digital Signature, Clipper Chip, Routers/Gateways, Free software programs like security administrator tool, COPS, Omni Guard and Net probe which can identify any obstacle in the security mechanism and can be adopted to be safe at all times.

Q. Discuss about the tips and tricks to prevent Cryptojacking.

Ans. Although it's difficult to detect when your computer system has been compromised by cryptojacking, there are some preventative measures you can take to protect your computer and networking systems and your own crypto-assets:

Train Your IT Team: Your IT team should be trained to understand and detect cryptojacking. They should be well aware of the first signs of an attack and take immediate steps to investigate further.

Educate Your Employees: IT teams need to rely on employees to let them know when computers are running slowly or overheating. Employees also need to be educated in cybersecurity, such as not clicking on links in emails that execute cryptojacking code and only downloading from trusted links. The same rule applies for personal email on your own devices.

Use Anti-Cryptomining Extensions: Cryptojacking scripts are often deployed in web browsers. Use browser extensions to block cryptominers across the web such as minerBlock, No Coin, and Anti Miner.

Use Ad-Blockers: Web ads are common places for cryptojacking scripts to be embedded. Using an ad-blocker can both detect and block malicious cryptomining code.

Disable JavaScript: When browsing online, disabling JavaScript can prevent cryptojacking code from infecting your computer. Keep in mind that disabling JavaScript will block many of the functions you need when browsing.

Q. Briefly discuss about the infrastructure of DSE.

Ans. A DSE is data standard encryption in cryptography. Development in PKI occurred in the early 1970s at the British intelligence agency GCHQ where James Ellis and Clifford Cocks made popular development for PKI. The sole purpose of PKI is to facilitate the best secure electronic transfer of information for digital activities. It is an arrangement that binds public keys with respective identities of entities. The binding is established through a process of registration and issuance of certificates at and by a Certificate authority (CA).

The deployment of PKI may be delegated by a CA to assure valid and correct registration, which is called registration Authority (RA). The Internet Engineering Task Force's RFC 3647 defines an RA. So, the RA is responsible for accepting request for digital certificates and authenticating the entity requested by the user. The most unique feature of PKI is that it uses a pair of keys to achieve the secured digital communication by comprising both private and public keys.

Data Encryption Standard is a encryption algorithm which uses symmetric keys for cipher encryption. It uses 56 bits (+8 parity bits) in 16 rounds having a block size of 64 bits. It has been designed by IBM team and adopted by national Institute of standards of Technology (NIST). It was first published in 1975 (federal Register standardized in 1977. Its structure is Balanced Feistel Network and its successors are Triple DES, G-DES, DES-X, LOKO89 and ICE. Though DES is no longer NIST's federal standard, it does not mean that it is no longer in use. Triple DES is still used today and it is considered a legacy encryption algorithm. But in practice, PKI has overcome the DES for ensuring digital communication system. The main disadvantage of Public Key Infrastructure is that one of the keys i.e., public key is in a public domain and is therefore, likely to be misused. It is rarely seen that cryptographic schemes are compromised due to weakness in their design but very often it is compromised due to the poor key management. The same can be achieved by keeping private keys secret throughout.

Q. What is pseudorandom numbers and sequences?

Ans. Random number generation is an important primitive in many cryptographic mechanisms. For example, keys for encryption transformations need to be generated in a manner which is unpredictable to an adversary. Generating a random key typically involves the selection of random numbers or bit sequences. Random number generation presents challenging issues.

Often in cryptographic applications, one of the following steps must be performed:

- From a finite set of elements, select an element at random.
- From the set of all sequences (strings) of length over some finite alphabet of symbols, select a sequence at random.
- Generate a random sequence (string) of symbols of length over a set of symbols.

A Pseudo Random Number Generator: It refers to an algorithm that utilities mathematical formulation to create series of random numbers. They produce a series of numbers assessing the properties of random numbers. With the arrival of technology, computer programmers acknowledged the requirement for a way of announcing unpredictability into a computer program. In spite of this, unexpected as it may seem, it is tough to get a computer to do something by chance as computer trails the specified instructions unseeingly and is therefore totally foresee able. It is not possible to create truly random numbers from deterministic thing like computers so this is a method expounded to generate random numbers using a computer. Some of the advantages are that this system is efficient as it can create number in a short span of time, easy to determine if replaying the same sequence of numbers again at a later stage and lastly are periodic i.e., that the sequence will eventually repeat itself.

MCS-215: Security and Cyber Laws
Guess Paper-II

Q. What is steganography? How it is beneficial for us?

Ans. It is one of the techniques of hiding secret data within a non-secret, ordinary file or manages to avoid being deleted. It will be decoded at the station. In modern digital steganography, data is first encrypted or obfuscated in some other way and then inserted, using a special algorithm, into data that is part of a particular file format such as JPEG image, audio or video file. The secret message can be embedded into ordinary data files in many different ways. One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file. By applying, the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has noise patterns of regular, unencrypted data.

It can be divided into following five types:

- Text Steganography
- Image Steganography
- Video Steganography
- Audio Steganography
- Network Steganography

The benefit of this method is that the data is extra and twice as safe i.e., that first that it is out of sight and the second is that it is encrypted. Because of this process, it becomes challenging for the person to first locate or trace the data and then encrypt it. Some of the well-known uses of stego around the world include: Head of the messenger was shaved and a tattoo was done on the head and after the hair grew back, the messenger was sent and the recipient again shaved the hair to read the tattooed message, U.S. Marine Corps Navaho code talkers of WWII, Disappearing ink and microdots, Osama bin Laden's pre-recorded videos that are re-played on TV stations around the world contain hidden messages, September 11 attacks in New York City, Washington, D.C. (Gary C. Kessler, 2001, p.1)

Q. What are the basic advantages and disadvantages of Asymmetric Key?

Ans. A computing environment that is secure would not be complete without considering encryption technology. By definition, encryption pertains to the method of obscuring the meaning of certain pieces of message or information through encoding them it in a way that it can be decoded, read and understood only by the people intended to receive them. In simple terms, it is the method of encoding data to prevent unauthorized individuals from viewing and modifying it.

Protecting information by using simple codes can be traced back to the 5th century BC, and as time goes by, the method has become more secure but complex. After all, it is done to better provide high security levels for communication networks, stored files, emails and other types of data that require protection. Together with symmetric encryption, another type is asymmetric encryption (also known as public key encryption), which is a technique of encrypting messages that uses two keys, namely the private and the public keys. In this method, textual data will be treated as a huge number that is raised to the power of second huge number and divided by a third huge number to produce a remainder. As for the remainder, it will be converted back into text to be able to produce encrypted messages. The private key is kept secret and is used to decrypt received messages, while the public key is made publicly available and is used to encrypt messages by an individual who wants to send messages to someone whom the key belongs to.

Pros of Asymmetric Encryption

- **It allows message authentication:** As public key encryption allows using digital signatures, message recipients will be able to verify messages to be truly coming from a particular sender.
- **It is convenient:** Asymmetric encryption solves the problem of distributing keys for encryption, with everyone publishing their public keys, while private keys being kept secret.

- **It allows for non-repudiation:** Digitally signed messages are like physically signed documents. Basically, it is like acknowledging a message, and therefore, the sender will not be able to deny it.
- **It detects tampering:** With digital signatures in public key encryption, message recipients can detect if a message was altered in transit.

Cons of Asymmetric Encryption

- **It is a slow process:** Public key encryption in this method is slow compared with symmetric encryption, which means that it is not suitable for decrypting bulk messages.
- **Its public keys are not authenticated:** Basically, no one absolutely knows that a public key belongs to the individual it specifies, which means that users will have to verify that their public keys truly belong to them.
- **It risks loss of private key, which may be irreparable:** When you lose your private key, your received messages will not be decrypted.
- **It risks widespread security compromise:** If your private key is identified by an attacker, all of your messages can be read by him/her.

To determine whether asymmetric encryption is a more secure solution for your communication needs, you should first understand its pros and cons. It is even recommended to use such method in conjunction with symmetric encryption.

Q. Write the comparison between Electronic Signature and Digital Signature.

Ans. People authenticate other people by recognizing their faces, voices and handwriting. Signatures on letterhead paper handle proof of signing raised seals and so on. Handwriting, paper, and ink experts can usually detect tampering. But none of these options are available electronically. That's why the concept of Digital signature came into existence to authenticate electronic documents. A Digital Signature is a technique by which it is possible to secure electronic information in such a way that the originator of the information, as well as the integrity of the information, can be verified. This procedure of guaranteeing the origin and the integrity of the information is also called Authentication.

The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature. For a computerised message system to replace the physical transport of paper and ink documents handwritten signatures have to be replaced by Digital Signatures. Basically what is needed, is a system by which one party can send a "signed" message to another party in such a way that

- The receiver can verify the claimed identity of the sender.
- The sender cannot repudiate the contents of the message.
- The receiver cannot possibly have concocted the message himself/ herself.

A digital signature is only a technique that can be used for different authentication purposes. For an E-record, it comes functionally very close to the traditional hand-written signatures. The user himself/ herself can generate key pair by using specific crypto software. Now Microsoft IE and Netscape, allow the user to create his/ her own key pair. Here, the most important thing is how can the user be sure that public keys belong to his/ her partner only? In this case, a third party (TTP) will guarantee the relationship between the identity and the public keys. The TTP are popularly called Certified Authorities (CAs).

Digital Certificate: These certificates are provided by CAs to authenticate that a particular site is globally secured. There are so many reputed CAs all over the world. Some of them are Very Sign from USA and Thawte Consulting from South Africa. Popular India CAs are SafeScrypt Ltd, TCS, IDRBT, MTNL Ltd and NIC. Digital certificates contain the following: Issuer, Issued to, organization name, organization unit, validity, Version, Public Keys, Thumbprint, algorithms etc. Secure Socket Layer (SSL) is the widely used protocol for digital certificates. The Uniform Resource Locator (URL) starts with "https" instead of "http" and are secured by SSL. At the bottom of the window, a lock symbol appears for SSL. Generally, 128 bits SSL are used.40 bits SSL are also available.

Section 2 (ta) of Information Technology Act, 2000 had defined electronic signatures as: "Authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature."
This definition has made the Act technologically neutral as it recognizes both digital and electronic signatures. It is important to note that electronic signatures are not safe as they are not encrypted and are likely to be tampered unlike that of digital signatures which includes private key and public key for encryption and decryption.
Some of the commonly used electronic signatures are email signatures, web based signatures, digitized image of a signature. Therefore, it is advised that digital signatures should be used as they are more secure and have more legal weightage.
Electronic Signatures has no expiry or validity period unlike a digital signature which is valid up to a maximum of three years.
Electronic Signatures are used for verifying a document unlike digital signatures which is used for securing a document.
Section 2(1) (p) of Information Technology Act, 2000 had defined digital signatures as: "Authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature."
Digital signatures are widely used for personal use, signing tenders, bidding, e-filing for ROC or income tax or for GST.
It follows an approach of using hash function i.e., usage of private key and a public key which is a two way protection system.
The process involves obtaining a digital signature certificate from a certifying authority which are set up and controlled by the mechanisms and law of the country. In order to transmit the message, public key and private key is used to encrypt and decrypt the message.

Q. Briefly elaborate the difference between authentication and authorization.
Ans. Authentication is a term which is used (and often abused) in a very broad sense. By itself, it has little meaning other than to convey the idea that some means has been provided to guarantee that entities are who they claim to be, or that information has not been manipulated by unauthorized parties. Authentication is specific to the security objective which one is trying to achieve. Examples of specific objectives include access control. The host countries might not permit secrecy on the channel; one or both countries might want the ability to monitor all communications. Jack and Bond, however, would like to be assured of the identity of each other, and of the integrity and origin of the information they send and receive. Authentication is one of the most important of all information security objectives. Until the mid 1970s it was generally believed that secrecy and authentication were intrinsically connected. With the discovery of hash functions and digital signatures, it was realized that secrecy and authentication were truly separate and independent information security objectives. It may at first not seem important to separate the two but there are situations where it is not only useful but essential. For example, if a two-party communication between Jack and Bond is to take place where Jack is in one country and Bond in another, the host countries might not permit secrecy on the channel; one or both countries might want the ability to monitor all communications. Jack and Bond, however, would like to be assured of the identity of each other, and of the integrity and origin of the information they send and receive.
The preceding scenario illustrates several independent aspects of authentication. If Jack and Bond desire assurance of each other's identity, there are two possibilities to consider.
1) Jack and Bond could be communicating with no appreciable time delay. That is, they are both active in the communication in "real time".
2) Jack or Bond could be exchanging messages with some delay. That is, messages might be routed through various networks, stored, and forwarded at some later time. In the first instance Jack and Bond would want to verify identities in real time. This might be accomplished by Jack sending Bond some challenge, to which Bond is the only entity which can respond correctly. Bond could perform a

similar action to identify Jack. This type of authentication is commonly referred to as entity authentication or more simply phrase challenge for identification.
For the second possibility, it is not convenient to challenge and await response, and moreover the communication path may be only in one direction. Different techniques are now required to authenticate the originator of the message. This form of authentication is called data origin authentication.
Thus, Data origin authentication or message authentication techniques provide to one for originality. 13 In the authentication process, verification of users is done and determines whether the person is a user or not while in the authorization process validation of users is done wherein determination is done as to whether the user has requisite permission to access the data or the information. Authentication is done prior to authorization process. The process of authentication requires user's login details while authorization only requires user's privilege or security levels.

Q. What do you mean by Good Hash Function?
Ans. A good hash function should have the following properties:

- **Efficiently computable.**
- **Should uniformly distribute the keys (Each table position equally likely for each key)**

For phone numbers, a bad hash function is to take the first three digits. A better function is considered the last three digits. Please note that this may not be the best hash function. There may be better ways. In practice, we can often employ ***heuristic techniques*** to create a hash function that performs well. Qualitative information about the distribution of the keys may be useful in this design process. In general, a hash function should depend on every single bit of the key, so that two keys that differ in only one bit or one group of bits (regardless of whether the group is at the beginning, end, or middle of the key or present throughout the key) hash into different values. Thus, a hash function that simply extracts a portion of a key is not suitable. Similarly, if two keys are simply digited or character permutations of each other *(such as 139 and 319)*, they should also hash into different values.
The two heuristic methods are ***hashing by division*** and ***hashing by multiplication*** which are as follows:
The mod method: In this method for creating hash functions, we map a key into one of the slots of table by taking the remainder of key divided by table size. That is, the hash function is

- Since it requires only a single division operation, hashing by division is quite fast.
- When using the division method, we usually avoid certain values of table size like table size should not be a power of a number suppose **r**, since if ***table_size = r^p***, then h(key) is just the p lowest-order bits of key. Unless we know that all low-order p-bit patterns are equally likely, we are better off designing the hash function to depend on all the bits of the key.
- It has been found that the best results with the division method are achieved when the table size is prime. However, even if table_size is prime, an additional restriction is called for. If **r** is the number of possible character codes on an computer, and if **table_size** is a prime such that r % table_size equal 1, then hash function **h(key) = key % table_size** is simply the *sum of the binary representation of the characters* in the key mod table_size.
- Suppose **r** = 256 and **table_size** = 17, in which r % table_size i.e. 256 % 17 = 1.
- So for **key = 37599**, its hash is

The multiplication method:

- In multiplication method, we multiply the key **k** by a constant real number **c** in the range **0 < c < 1** and extract the *fractional part of* ***k * c***.
- Then we multiply this value by table_size **m** and take the floor of the result. It can be represented as:
- where the function **floor(x)**, available in standard library *math.h*, yields the integer part of the real number x, and **frac(x)** yields the fractional part. **[frac(x) = x – floor(x)]**

- An advantage of the multiplication method is that the value of *m is not critical*, we typically choose it to be a power of 2 (**$m = 2^p$** for some integer **p**), since we can then easily implement the function on most computers
- Suppose that the word size of the machine is **w** bits and that key fits into a single word.
- We restrict **c** to be a fraction of the form **$s / (2^w)$**, where s is an integer in the range **$0 < s < 2^w$**.
- Referring to figure, we first multiply key by the w-bit integer **$s = c * 2^w$**. The result is a 2w-bit value

Q. Briefly describe trusted third parties and public key certificates

Ans. A TTP is said to be unconditionally trusted if it is trusted on all matters. For example, it may have access to the secret and private keys of users, as well as be charged with the association of public keys to identifiers.

Various third party services require different types of trust and competency in the third party. For example, a third party possessing secret decryption keys (or entity authentication keys) must be trusted not to disclose encrypted information (or impersonate users). A third party required (only) to bind an encryption public key to an identity must still be trusted not to create false associations and thereafter impersonate an entity. In general, three levels of trust in a third party T responsible for certifying credentials for users may be distinguished. Level 1: T knows each user's secret key. Level 2: T does not know users' secret keys, but can create false credentials without detection. Level 3: T does not know users' secret keys, and generation of false credentials is detectable.

A TTP is said to be functionally trusted if the entity is assumed to be honest and fair but it does not have access to the secret or private keys of users.

Public-key certificates: The distribution of public keys is generally easier than that of symmetric keys, since secrecy is not required. However, the integrity (authenticity) of public keys is critical.

Primary advantages offered by public-key (vs symmetric-key) techniques for applications related to key management include:

- Simplified key management. To encrypt data for another party, only the encryption public key of that party need be obtained. This simplifies key management as only authenticity of public keys is required, not their secrecy. The situation is analogous for other types of public-key pairs, e.g., signature key pairs.
- On-line trusted server not required. Public-key techniques allow a trusted on-line server to be replaced by a trusted off-line server plus any means for delivering authentic public keys (e.g., public-key certificates and a public database provided by an un-trusted on-line server). For applications where an on-line trusted server is not mandatory, this may make the system more amenable to scaling, to support very large numbers of users.
- Enhanced functionality. Public-key cryptography offers functionality which typically cannot be provided cost-effectively by symmetric techniques (without additional online trusted third parties or customized secure hardware). The most notable such features are non-repudiation of digital signatures, and true (single-source) data origin authentication.

A public-key certificate consists of a data part and a signature part. The data part consists of the name of an entity, the public key corresponding to that entity, possibly additional relevant information (e.g., the entity's street or network address, a validity period for the public key, and various other attributes). The signature part consists of the signature of a TTP over the data part.

Q. In which situation Database security is necessary?

Ans. Database security is necessary in the following situations:

- Theft and fraud
- Loss of availability of data
- Loss of confidentiality
- Loss of data privacy

- Loss of data integrity

The situations given above are the most likely to be exposed to date security threats and are required to be protected so that the chances of losses in this regard can be significantly reduced. It is noteworthy that these situations often cause cumulative losses due to inter dependencies and hence a loss due to one situation can affect multiple areas in the same organisation. The purpose of data protection (also known as information privacy and data privacy) is to define when and under what circumstances data can be safely put to use.

Q. What are the Challenges in Data Management?

Ans. Most of the challenges in data management today stem from the faster pace of business and the increasing proliferation of data. The ever-expanding variety, velocity, and volume of data available to organizations is pushing them to seek more-effective management tools to keep up. Some of the top challenges organizations face include the following:

Lack of data insight: Data from an increasing number and variety of sources such as sensors, smart devices, social media, and video cameras is being collected and stored. But none of that data is useful if the organization doesn't know what data it has, where it is, and how to use it. Data management so

Difficulty maintaining data-management performance levels: Organizations are capturing, storing, and using more data all the time. To maintain peak response times across this expanding tier, organizations need to continuously monitor the type of questions the database is answering and change the indexes as the queries change—without affecting performance.

Challenges complying with changing data requirements: Compliance regulations are complex and multijurisdictional, and they change constantly. Organizations need to be able to easily review their data and identify anything that falls under new or modified requirements. In particular, personally identifiable information (PII) must be detected, tracked, and monitored for compliance with increasingly strict global privacy regulations. Institutions need scale and performance to deliver meaningful insights in a timely manner.

Need to easily process and convert data: Collecting and identifying the data itself doesn't provide any value—the organization needs to process it. If it takes a lot of time and effort to convert the data into what they need for analysis, that analysis won't happen. As a result, the potential value of that data is lost.

Constant need to store data effectively: In the new world of data management, organizations store data in multiple systems, including data warehouses and unstructured data lakes that store any data in any format in a single repository. An organization's data scientists need a way to quickly and easily transform data from its original format into the shape, format, or model they need it to be in for a wide array of analyses.

Demand to continually optimize IT agility and costs: With the availability of cloud data management systems, organizations can now choose whether keep and analyze data in on-premises environments, in the cloud, or in a hybrid mixture of the two. IT organizations need to evaluate the level of identicality between on-premises and cloud environments in order to maintain maximum IT agility and lower costs.

Q. Discuss in brief about availability and integrity.

Ans. Integrity measures protect information from unauthorized alteration. These measures provide assurance in the accuracy and completeness of data. The need to protect information includes both data that is stored on systems and data that is transmitted between systems such as email. In maintaining integrity, it is not only necessary to control access at the system level, but to further ensure that system users are only able to alter information that they are legitimately authorized to alter.

As with confidentiality protection, the protection of data integrity extends beyond intentional breaches. Effective integrity countermeasures must also protect against unintentional alteration, such as user errors or data loss that is a result of a system malfunction.

Q. Discuss about the terms 'computer' and 'internet'.

Ans. The computer is the foundation of the entire virtual world and is now extensively used both personally and professionally in all walks of life. As the technology related to computers is constantly developing, the methods to secure data within the computers is not necessarily progressing a same pace. The computer In turn has given rise of many other forms of communication which includes the mobile.

A computer in layman terms is essentially a machine that was primarily used for calculations. Over the years, the use of a computer has grown two-fold; it not only helps in storing work related information but also has the capacity to transfer communication from one system to another with the help of the Internet. Computers today have reduced complicated jobs into much simpler tasks. For example, one can write a letter in a word document, edit it, spell check, print copied and also send it to someone across the world in a mere matter of seconds. These activities of simply even writing a letter would have taken someone days, to do before the advent of computers.

In other words, a computer simply is an information processor in a way that it takes whatever raw information or data which is fed by a human and stores that information, then proceeds to decrypt the information entered and consequently provide the result in the form of an output. The work of a computer is nothing without a computer program. We can see various computer programmes on a computer we rely on like Microsoft Word, Excel, etc. used for carrying out day to day activities at all spheres of life.

The Internet is an international network of computer systems that has evolved over the last decade. Currently, the Internet interconnects several thousand individual networks that connect over a million computers. The Internet today has become the electronic backbone for computer research, development and user communities. Similar issues of data security which affect the computer and mobile also affect the Internet.

Merriam-Webster's dictionary defines Internet as an electronic communications network that connects computer networks and organizational computer facilities around the world. There are various devices that help facilitate connections with people around the world with the help of a network. These multiple interconnected networks form the Internet.

Q. Describe in brief the various security measures.

Ans. Various security measures:

- **Access security:** By restricting access of users who have been granted access to information, thereby results in monitoring who all have access to a particular data. Therefore, in cases of data theft, sifting through the timelines of access granted to users can be easier to track down the culprit.
- **Data encryption:** Data when kept unencrypted leads to misuse of personal data by cybercriminals. Therefore, data has to be encrypted by usage of unique encryption codes, so as to avoid leakage of vital information stored in databases. When data has been encrypted and only the user has access to such a data has the decryption code, results in prevention of data theft.
- **Email security:** It is a form of procedure to protect an email account and the contents on an email account from unauthorised access. Therefore, measures like strong email passwords, end-to-end encryption of emails or messages that are sent from one person to another result in prevention of misuse of data, as emails are a popular forum for hackers to spread malware, spam and phishing attacks. For example- end-to-end encryption used by WhatsApp.
- **Risk-assessment analysis:** Organizations have to take a proactive approach while dealing with information security concerns. The main of conducting a risk assessment is to identify the risks pertaining to information stored in an organizations system. By conducting risk assessment analysis, an organization can understand and assess internal and external risks to their security, confidentiality and personal information stored in various storage media like laptops and portable devices.

- **Monitor effectiveness:** It is critical for an organization to verify security programs established and to establish if such security programs manage cyber security measures implemented for safeguarding an organization's information or data. This is done through regular tests and monitoring of information security programs annually or quarterly helps to assess the number of attacks made to an organizations data.
- **Third party issues:** Website's play a major role while showcasing an organization's success. Therefore, they implement third party tools to make their websites' more interactive and user-friendly and offer smooth connectivity for user interaction. These third-party tools help in generating revenue for an organization's website. Therefore, an organization has to undertake to ensure that all reasonable steps have been taken prior to giving access to third party service providers and that such third-party service providers apply the stringiest security measures.
- **Strong firewall:** Firewall of a system is part of such system's cyber security measure. A firewall enables to protect a system from internet traffic and services it is exposed to. These services are accessed by everyone who uses an internet. Therefore, firewalls enable to control who gains access to an organization's system like insider attacks which may originate from within a network used by an organization. Antiviruses are for files and firewalls are needed to protect from unauthorised access or usage of network. A firewall simply helps to control Internet traffic that is generated by using a network for work.
- **Antivirus protection:** An antivirus protection can be gained in the form of antivirus software. This software is a program designed to avoid, detect and deal with cyber security threats that an organization may face. The process of an antivirus is to run background scans on a system to detect and restrict unauthorised access in the forms of malware and to protect a system from vulnerabilities it may face. These solutions are extremely important for data security and must be installed on computer systems. These antivirus protections are available not only for laptops and computers but also for mobile devices and help to fight unwanted threats to files and data.
- **Back-up regularly:** A data security is meant for protecting information stored on a system from unauthorised access, destruction of such information and includes network security. Therefore, to avoid loss of data, data should be regularly be stored and kept somewhere safe where it cannot be accessed or violated by anyone. Further, the securing of such data helps in preventing accidental modification to data, theft of data, breach of confidentiality agreements and avoid release of data prior to its verification and authentication.

Q. Write six principles of security management.

Ans. Security management means minimizing the interruption of business activities and reducing the vulnerability to various attacks. Security bargains with distinctive trust aspects of information. Data security includes engineering where an incorporated permutation of appliances, arrangements and resolutions, software, surveillance, and vulnerability scans work together. Security is not just restricted to computer systems; it applies to all perspectives of securing data or information, in whatever structure. Security is accomplished utilizing a few methodologies at the same time or utilized in blend with one another.

There are six principles of security management:

(1) **Availability:** The continuous accessibility of systems tends to procedures, policies and controls which are used to ensure prompt access to data for authorized customers. This purpose secures against deliberate or inadvertent endeavours to refute legitimate costumers' access to data.

(2) **Integrity of data or systems:** System and data integrity is linked to the procedures, policies and controls which are used to guarantee that data has not been modified in an

unconstitutional way and that systems are liberated from illicit manipulation that would compromise precision, comprehensiveness and consistency.

(3) **Confidentiality of data or systems:** Confidentiality covers the procedures, policies and controls which are utilized to secure data of customers and the organization against illicit access or use.

(4) **Accountability:** Accountability incorporates the procedures, policies and controls essential to follow activities to their source. Accountability specifically underpins nonrepudiation, anticipation, infringement, deterrence, security checking, recuperation and legitimate tolerability of records.

(5) **Assurance:** Assurance addresses the procedures, strategies and controls which are used to create certainty that specialized and equipped security measures are working as anticipated.

(6) **Privacy:** It centers on the constitutional rights of people, the motivation behind data assortment and processing, security predilection and the manner in which organizations administer individual's data. It focuses on how to gather, process, offer, document and erase the information/data as per the law.

MCS-215: Security and Cyber Laws
Guess Paper-III

Q. What is Cybersquatting?

Ans. Cybersquatting is the practice by means of which a person or legal entity books up the trade mark, business name or service mark of another as his own domain name for the purpose of holding on to it and thereafter selling the same domain name to the other person for valuable premium and consideration. Cyber squatters book up domain names of important brands in the hope of earning quick millions.

The practice that's come to be known as cybersquatting originated at a time when most businesses were not savvy about the commercial opportunities on the Internet. Some entrepreneurial souls registered the names of well-known companies as domain names, with the intent of selling the names back to the companies when they finally woke up. Panasonic, Fry's Electronics, Hertz and Avon were among the "victims" of cyber squatters. Opportunities for cyber squatters are rapidly diminishing, because most businesses now know that nailing down domain names is a high priority. The practice that's come to be known as cybersquatting originated at a time when most businesses were not savvy about the commercial opportunities on the Internet. Some entrepreneurial souls registered the names of well-known companies as domain names, with the intent of selling the names back to the companies when they finally woke up. Panasonic, Fry's Electronics, Hertz and Avon were among the "victims" of cyber squatters. Opportunities for cyber squatters are rapidly diminishing, because most businesses now know that nailing down domain names is a high priority.

Q. Explain the meaning of Cyber Terrorism.

Ans. Cyber Terrorism denotes unlawful attacks and threats of attack against computers, network and information stored therein to intimidate or coerce a government or its people for propagating hidden political or unlawful social and religious motives. These attacks could result in violence against persons or property or cause public unrest. Few examples could be explosions, plane crashes and severe economic losses. Terrorists are known to use internet to prepare schemes, raise funds and spread cyber terrorism. For instance Ramzi Yousef who was a key person behind World Trade Centre attack had detailed schemes to destroy United States airliners encrypted files in his laptop computer. A website known as shows tips for hacking the pentagon. Cyber warfare is another area of concern. Cyber espionage methods seek to gain information about the enemy and attacks by destroying his information system and safe guarding one's own system from a counter attack. Several states in USA have addressed terrorism in state criminal codes, including statutes that address terroristic activities and threats. But at least three states- California, Georgia, and Pennsylvania – have laws specifically aimed at electronic terroristic threats or acts.

Cyber terrorism can include direct attacks on networks, computer systems, computer programs, and data, which may result in potentially disastrous consequences like shutting down vital infrastructure facilities such as power stations. Nearly every state has statutes banning hacking and unauthorized access, and at least sixteen states ban unleashing harmful computer viruses and contaminants. In India, Cyber terrorism has a stringent punishment of imprisonment of ten years or life imprisonment as per the IT Act,2000.

Q. What is hacking? Whether it is challenge to digital security?

Ans. Hacking attacks are one of the most common security challenges that both individuals and companies face in keeping their information secure. Whether it's getting access to passwords, credit cards, or other sensitive information, hackers are using email, social media, phone calls, and any form of communication they can to steal valuable data. Businesses, of course, are a particularly worthwhile target. not having the right tools in place and failing to train employees on their role in information security employees possess credentials and overall knowledge that is critical to the success of a breach

of the company's security. One of the ways in which an intruder obtains this protected information is via phishing. The purpose of phishing is to collect sensitive information with the intention of using that information to gain access to otherwise protected data, networks, etc. A phisher's success is contingent upon establishing trust with its victims. We live in a digital age, and gathering information has become much easier as we are well beyond the dumpster diving days.

Q. Explain the meaning and concept of web based Cryptojacking.

Ans. Cryptojacking is malicious crypto mining that happens when cybercriminals hack into both business and personal computers, laptops, and mobile devices to install software. This software uses the computer's power and resources to mine for crypto currencies or steal cryptocurrency wallets owned by unsuspec ting victims. The code is easy to deploy, runs in the background, and is difficult to detect.

With just a few lines of code, hackers can hijack the resources of any computer and leave unsuspecting victims with slower computer response times, increased processor usage, overheating computer devices, and higher electricity bills. Hackers use these resources to both steal cryptocurrency from other digital wallets and to allow hijacked computers to do the work so they can mine valuable coins. The core idea behind crypto jacking is that hackers use business and personal computer and device resources to do their mining work for them. Cybercriminals siphon the currency they either earn or steal into their own digital wallet by using these hijacked computers. These hijacked computers are compromised by a slowing down of CPU function and using more electricity for processing file-based crypto jacking, malware is downloaded and runs an executable file that spreads a crypto mining script throughout the IT infrastructure. One of the most common ways that crypto jacking occurs is by using malicious emails. An email is sent containing an attachment or link that looks legitimate. When a user clicks on the attachment or link, code is executed that downloads the crypto mining script onto the computer. This script works in the background without the user's knowledge**.** Browser-Based attacks can take place directly within a web browser, using IT infrastructure to mine for cryptocurrency. Hackers create a cryptomining script using a programming language and then embed that script into numerous websites. The script is run automatically, with code being downloaded onto the users' computer. These malicious scripts can be embedded in ads and vulnerable and out of date WordPress plugins. Cryptojacking can also happen through a supply chain attack, where cryptomining code compromises JavaScript libraries when hackers use cloud cryptojacking, they search through an organization's files and code for API keys to access their cloud services. Once access is gained, hackers siphon unlimited CPU resources for cryptomining, resulting in a huge increase in account costs. Using this method, hackers can significantly accelerate their efforts of cryptojacking to illicitly mine for currency.

Q. What do you mean by hack prevention function?

Ans. A hack function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called hash-values.

The most common cryptographic uses of hash functions are with digital signatures and for data integrity. With digital signatures, a long message is usually hashed (using a publicly available hash function) and only the hash-value is signed. The party receiving the message then hashes the received message and verifies that the received signature is correct for this hash-value. This saves both time and space compared to signing the message directly, which would typically involve splitting the message into appropriate-sized blocks and signing each block individually. Note here that the inability to find two messages with the same hash-value is a security requirement, since otherwise, the signature on one message hash-value would be the same as that on another, allowing a signer to sign one message and at a later point in time claim to have signed another hack functions may be used for data integrity as follows. The hash-value corresponding to a particular input is computed at some point in time. The integrity of this hash-value is protected in some manner. At a subsequent point in time, to verify that the input data has not been altered, the hash-value is recomputed using

the input at hand, and compared for equality with the original hash-value. Specific applications include virus protection and software distribution a third application of hash functions is their use in protocols involving prior commitments, including some digital signature schemes and identification protocols.

Hack functions as discussed above are typically publicly known and involve no secret keys. When used to detect whether the message input has been altered, they are called modification detection codes (MDCs). Related to these are hash functions which involve a secret key, and provide data origin authentication as well as data integrity; these are called message authentication codes.

Some of the popular hack prevention functions include:

- Message Digest is a 128-bit hash function which gives confidence about veracity of transmitted file. But it is no longer in practice as there were successful collisions i.e., analytical attack in 2004.
- Secure Hash Functions family consists of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3. The latest is Keccak algorithm which was chosen by NIST in October 2012 as the new SHA-3 standard which offers many benefits, such as efficient performance and good resistance for attacks.
- The RIPEMD is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was devised by open research community and generally known as a family of European hash functions.
- Whirlpool is a 512-bit hash function which has stemmed from the revised edition of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.

Q. Discuss about the procedure for adjudication under the Information Technology Act, 2000.

Ans. Section 43 to 45 of Information Technology Act, 2000 provides for the instances where the wrong doer is liable to pay damages by way of compensation to the effected party. Section 66 of Information Technology Act, 2000 however provides that if any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Section 43 of Information Technology Act, 2000 provides that any person who without permission of the owner or any other person who is in charge of a computer, computer system or computer network commits the following acts shall be liable to pay damages:

- Accesses or secures access;
- downloads, copies or extracts any data, computer data base or information;
- introduces or causes to be introduced any computer contaminant or computer virus;

"Computer contaminant‖ means any set of computer instructions that are designed–

(a) to modify, destroy, record, transmit data or program residing within a computer, computer system or computer network; or (b) by any means to usurp the normal operation of the computer, computer system, or computer network; (iii) —computer virus‖ means any computer instruction, information, data or program that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a program, data or instruction is executed or some other event takes place in that computer resource;" (d) damages or causes to be damaged data, computer data base or any other programs; (iv) of this section provides, " damage‖ means to destroy, alter, delete, add, modify or rearrange any computer resource by any means." (e) disrupts or causes disruption; (f) denies or causes the denial of access to any person authorised to access by any means; (g) provides any assistance to any person to facilitate access in contravention of the provisions of this Act, rules or regulations made there under; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating; (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with

an intention to cause damage;] [(v) —computer source code‖ means the listing of program, computer commands, design and layout and program analysis of computer resource in any form.]

Section 43A of Information Technology Act, 2000 provides for the liability for Compensation of a body corporate for failure to protect data. Explanation to this section defines a body corporate as: "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; The explanation also defines reasonable security practices and procedures as, "security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

Section 44 of Information Technology Act, 2000 provides for penalty for failure to furnish information, return, etc "If any person who is required under this Act or any rules or regulations made there under to– (a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure; (b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues; (c) maintain books of account or records, fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues."

Section 45 of Information Technology Act, 2000 provides for the residuary penalty. Contravention of any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided. The maximum penalty in such cases is 25000 rupees.

Adjudication: Section 46 provides for the adjudication of disputes for awarding compensation. It authorizes the Central Government to appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry. This officer shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore. a reasonable opportunity for making representation in the matter and on such inquiry must be given.

Where it accedes 05 (five) crore, The jurisdiction shall vest with the competent civil court:

- All proceedings before adjudicating officer shall be deemed to be judicial proceedings within the meaning of sections 193 and 228 of the Indian Penal Code, 1860;
- It shall be deemed to be a civil court for the purposes of sections 345 and 346 of the Code of Criminal Procedure, 1973;
- It shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code, 1908. No person shall be eligible to be appointed as an adjudicating officer if he does not possesses such experience in the field of Information Technology and legal or judicial experience which is explicitly prescribed by the Central Government.

Appellate Tribunal An appeal tribunal is a special court or committee that is formed to reconsider a decision made by another court or committee.

Section 48 provides that from coming into force of the Finance Act, 2017 Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997), shall be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under this Act.

Section 57 provides the procedure for appeal. Any person aggrieved by an order made by controller or an adjudicating officer under this Act may prefer an appeal to a Appellate Tribunal having jurisdiction in the matter. However no appeal shall lie to the Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties. Every appeal shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or the

adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed: Provided that Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.
The appeal shall be dealt with as expeditiously as possible and endeavor shall be made to dispose of the appeal finally within six months from the date of receipt of the appeal.
Section 58 provides that Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, it shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely:–

- Summoning and enforcing the attendance of any person and examining him on oath;
- Requiring the discovery and production of documents or other electronic records;
- Receiving evidence on affidavits;
- Issuing commissions for the examination of witnesses or documents;
- Reviewing its decisions;
- Dismissing an application for default or deciding it ex parte;
- Any other matter which may be prescribed.

Section 62 provides for the appeal to high court. Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order on any question of fact or law arising out of such order: Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

Q. Differentiate between Deductive and Inductive Method.
Ans. Deductive method: Deductive method is also termed as a 'top-down' approach or method of explanation/verification. It mainly involves testing of a theory. Based on a theory, hypothesis (es) are formulated, that are then tested in order to validate or invalidate the theory. The focus on this method could be on cause and effect relationship between the variables. Deductive methods mainly rely on the quantitative approach to research, though in certain situations qualitative approach may also be employed. Deductive method is more structured as there is a clear and specific aim that us to be achieved and is less time consuming when compared to inductive method. In deductive method, a larger sample size is taken in order to facilitate generalisation of the results.
Inductive method: Inductive method is also termed as 'bottom-up' approach or method of discovery. It mainly involves deriving a new theory. This method usually starts with a research question that is aimed to specify the scope of the research. The method mainly involves exploration of a novel phenomenon/ event or studying the phenomenon. event from a new perspective. In doing so inductive method may make use of qualitative methods of research. Inductive method is less structured and more time consuming when compared with deductive method. Inductive method is less concerned with generalisation and focuses on comprehending the context of the research.

Q. How the issue of jurisdiction of Indian courts with respect to offences committed outside India has been dealt with by the IT Act?
Ans. For the purpose of conducting cyber-crime investigation, essential special skills and technical tools are required without which the investigation is next to impossible. After commencement of the Information Technology Act, 2000, some provisions of Criminal Procedure Code, 1973 and the Evidence Act, 1872 have been duly amended. Along with these, certain new rules and regulations had been enforced by the Indian legislative system to meet the need of cyber-crime investigation.
Section 75 deal with the issue of jurisdiction with respect to cybercrimes. As we know, cybercrime knows no boundary. A person sitting in one country can commit offences having its consequences in

another country. Section 75 provides that if any person have committed an offence, or contravention committed outside India, and if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India, then the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

Section 76 provides that any computer, computer system, floppies, compact disks, tape drives, or any other accessories related thereto, in respect of which any provision of this Act, rules, orders, or regulations made there under has been, or is being contravened, shall be liable to confiscation. However, if it is proved that such resources were not used in committing fraud then only person in default will be arrested.

Section 77 provides that compensation, penalties or confiscation shall not interfere with other punishment.

Section 77A deals with compounding of offences. A court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding 03 (three) years has been provided, under this Act:

Provided that the court shall not compound such offence where the accused is, by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the court shall not compound any offence where such offence affects the socio economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

Section 77B provides that offences with three years' imprisonment shall be bailable.

Section 78 deals with the power to investigate. It provides that a police officer not below the rank of inspector shall investigate any offence under this Act.

Section 80 deals with the power of police officer and other officers to enter, search etc. It provides that any police officer, not below the rank of a inspector, or any other officer of the Central Government or a State Government authorised by the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act. Where any person is arrested by an officer other than a police officer, such officer shall, without unnecessary delay, take or send the person arrested before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

Q. Explain the need for regulation of cyberspace.

Ans. The following reasons can be cited in favor of proposition:

(1) The most visible and readily sensational concern is about the use of internet particularly for the distribution of obscene, indecent and pornographic content. The use of internet for child pornography and child sexual abuse and the relative ease with which the same may be accessed calls for strict regulation.

(2) The challenge that Cyberspace is posing to traditional notions of jurisdiction and regulation is another factor. The increasing business transaction from tangible assets to intangible assets like Intellectual Property has converted Cyberspace from being a mere info space into important commercial space. The attempt to extend and then protect intellectual property rights online will drive much of the regulatory agenda and produce many technical methods of enforcement.

(3) With the inventions of new technologies, the media has enhanced the possibility of invasion of the privacy of individual and bringing it into the public domain. The major area of concern where some sort of regulation is desirable is data protection and data privacy so that industry, public administrators, netizens, and academics can have confidence as on-line user.

(4) Encryption is the process of converting a message or document into a form which hides the content of the communication from the eyes of an eavesdropping third party and needs to

be decrypted if its content is to be read. New cryptographic techniques (cryptography is the process used to encode/encrypt electronic information) are commonly cracked in a relatively short time by computational force or by other analytical means. Therefore, another area in which regulation has assumed importance is in the debate over whether the public should be permitted to use 'cryptography' or not.

(5) Internet has emerged as the 'media of the people' as the internet spreads fast there were changes in the press environment that was centered on mass media. Unlike as in the established press, there is no editor in the Internet. In the press and publication environment, editors check the truthfulness of facts and circulate them once the artistic values are confirmed. On the internet however, people themselves produce and circulate what they want to say and this direct way of communication on internet has caused many social debates. Therefore, the future of Cyberspace content demands the reconciliation of the two views of freedom of expression and concern for community standards.

(6) Another concern is that, money laundering, be 'serious crime' becomes much simpler through the use of net. The person may use a name and an electronic address, but there are no mechanisms to prove the association of a person with an identity so that a person can be restricted to a single identity or identity can be restricted to a single person. Viruses, rumor-mongering, hate-mail and mail box bombardment are all describable phenomena and because of the fear of retribution all are more likely to use fake identity or may be anonymous mailers rather then a readily identifiable person. Therefore, Cyberspace needs to be regulated to curb this phenomenon. Please answer the following to check your progress.

Q. List the specific legislation in different countries to regulate cyber space.

Ans. Communications Decency Act 1996 (CDA) The Section 502 of the CDA amended sections 223(a) and (d) of Title 47 of the United States Code ('USC'). It prohibits the making and transmission of obscene or 'indecent' material to a minor by means of a telecommunications device, and the use of an interactive computer service to send or display 'patently offensive' material to minors. The provisions also prohibited a person from knowingly permitting a telecommunications facility under that person's control to be used to commit these offences. However Supreme Court in American Civil Liberties Union v, Janet Reno, Attorney General of the United States; American Library Association, Inc. v, United States Department of Justice (the 'CDA Case', 1997) declared unconstitutional the above two statutory provisions as a violation of both freedom of speech and personal privacy. COPPA In 1998 US Congress enacted Children Online Privacy Protection Act (COPPA) which necessitated the federal trade commission to release and implement regulations concerning children's online privacy. The Rule applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose personal information from children, operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13, websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children. The implementation of the Act was prohibited in the case of Aschcroft vs American Civil Liberties Union (2004) as it was likely to fail the "strict scrutiny" test due to the fact that it was not closely customized i.e., it prohibited online publishers from publishing some stuff that adults had a right to gain access to and since it did not utilize the minimum restrictive means feasible to safeguard children.

CIPA In 2000, Children Internet Protection Act (CIPA) was passed. This Act requires the schools and libraries to install filters on computers used by minors and adults.

Uniform Computer Information Transaction Act, 2000 (UCITA) According to UCITA, for a transaction to be 'Computer Information Transaction', the main focus of the transaction must be acquiring the computer information, access to it, or its use and not a mere incident of another transaction. The act applies to contracts for the development or creation of computer information,

such as software development contracts and contracts to create a computer database. This Act does not apply to many cases in which one person provides information to another person for another transaction such as making an employment or loan application. The state of Maryland was the first state in which UCITA became effective. (FindLaw Attorney Writers, 2017, p.1). The Gramm-Leach-Bliley Act (GLB Act or GLBA) or Financial Modernization Act of 1999. It is a United States federal law that calls for financial institutions to clarify how they share and keep their customers confidential information private. (Federal Trade Commission, p.1).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that necessitated the formation of national standards to protect the patient's sensitive health information from being revealed without the permission from the patient or without the knowledge of the patient. (Public Health Professionals Gateway, 2018, p.1).

The Fair Credit Reporting Act, 1970 was the first federal law to regulate the use of personal information by private businesses

The other cyber security laws to strengthen the domain in the US:

- Consumer Privacy Protection Act, 2017 aims at assuring the safety of personal information of users, to circumvent identity theft, to inform its citizens and organizations concerning security violations and to put a stop to the mishandling of sensitive user information. (Gov track, 2017, p.1)
- Cyber security Information Sharing Act (CISA) is a proposed legislation that will permit United States government agencies and non-government agencies to dole out information with each other as they examine and scrutinize cyber attacks. (Thomas F. Duffy, Chair, 2016, p.1)
- Cyber security Enhancement Act of 2014 was signed into law on December 18, 2014. It provides an ongoing, voluntary public-private partnership to develop, enhance and upgrade and develop cyber security and boost cyber security research and development, workforce development and education and public awareness and preparedness.

European Union: The approach of a large majority of (perhaps all) European Union Member States in dealing with illegal and harmful content on the Internet appears to be in accord with the1996 recommendations of the European Commission advocating the use of filtering software and rating systems, and an encouragement of self-regulation of access providers. In these countries, laws regarding material that is illegal offline, such as child pornography and racist material, also apply to Internet content. With regard to material unsuitable for children, the EU Safer Internet Action Plan covering the period 1999-2002 has a budget of 25 million euro and has three main action lines;

- Creating a safer environment through promotion of hotlines, encouragement of self-regulation and codes of conduct,
- Developing filtering and rating systems, facilitation of international agreement on rating systems,
- **Awareness:** Making parents, teachers and children aware of the potential of the Internet and its drawbacks, overall co-ordination and exchange of experience.

The word 'cyber security', from the viewpoint of European Union, involves a blend of cyber resilience, cybercrime, cyber defence, (strictly) cyber security and global cyberspace concerns. It is noteworthy that while the two EU Cyber security approaches pursued the adoption of various legislative measures regarding cyber security, they put forward policy objectives which later resulted in legislation, namely the Network and Information Security Directive and the Cyber security Act (came into force on 27th June 2019.) which further sheds light on the job and order of the European Union Agency for Network and Information Security (ENISA). Building on this observation, it is proposed that the cyber security area recuperates itself by both law and policy measures. Policy measures from various policy areas eventually led to changes and adjustments in various EU legal frameworks and vice versa. "The EU General Data Protection Regulation (GDPR), which governs how personal data of individuals in the EU may be processed and transferred, went into effect on May 25, 2018. GDPR is a comprehensive privacy legislation that applies across sectors and to

companies of all sizes. It replaces the Data Protection Directive 1995/46. The overall objectives of the measures are the same – laying down the rules for the protection of personal data and for the movement of data".

United Kingdom: In September 1996, UK Government issued R3 Safety-Net action plan (now Internet Watch Foundation, IWF), developed by UK ISP trade associations and where it is agreed by Government involve industry for establishment of complaints hotline and related take-down procedures for illegal Internet content, primarily child pornography. In February 2002, the IWF announced that it would henceforth also deal with "criminally racist content".

Related Legislation in UK

- The Computer Misuse Act, 1990 is an" Act to make provision for securing computer material against unauthorised access or modification; and for connected purpose".
- Electronic Communications Act, 2000 to facilitate the use of electronic communications and electronic data storage. 3) Data Protection Act 2018 (DPA 2018) superseded Data Protection Act, 1998 and supplements the EU General Data Protection Regulation (GDPR). The act makes "provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes."

National Cyber Security Centre (NCSC), UK – In 2016, CESG (the information assurance arm of GCHQ), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure were merged to form National Cyber Security Centre. It provides a single point of contact for SMEs, larger organisations, government agencies, the general public and departments and also works in collaboration with other law enforcement, defence, the UK's intelligence and security agencies and international partners.

Q. Explain the relationship between in lining and framing.

Ans. The Linking, In-lining and framing have become so common since in linking person is providing link and is not making any copies of material available online but the link here allows visitors to bypass information and advertisements at the relevant home page, inclining allows display of graphics on other website and framing often used in conjunction with inclining give picture to picture image and the user can surf directly to the information contained in another site without visiting its home page that may leads to copyright or trademark infringement since it may cause loss of income to businesses; create confusion among the users that the sites endorse each other or are associated with each other which might not be correct and lead to confusion as to original source and loss of reputation and goodwill of the original information holder/ businesses. ""Linking" allows a Web site user to visit another location on the Internet. By simply clicking on a "live" word or image in one Web page, the user can view another Web page elsewhere in the world, or simply elsewhere on the same server as the original page. This technique is what gives the Web its unique communicative power. At the same time, however, linking may undermine the rights or interests of the owner of the page that is linked to. Suppose, for example, that X sets up a homepage for her site. On the homepage she places some advertisements, from which she hopes to make some money. The homepage also contains links to various subordinate pages, which contain content that X believes consumers wish to see. Y then creates his own Web site, which contains links to X's subordinate pages. The net result is that visitors to Y's site will be able to gain access to X's material, without ever seeing X's advertisements. This type of activity is called "deep linking.""

Inlining: "Inlining" is the process of displaying a graphic file on one website that originates at another. For example, inlining occurs if a user at site A can, without leaving site A, view a "cartoon of the day" featured on site B. IMG links -- a special type of link -- can be used to display graphic files on one site that are stored on another". Kelly v. Arriba Soft Corp,2003, a federal court of appeals ruled that it was not an infringement to provide inlined links to "thumbnail" reproductions (here an image search engine called ditto.com used inline links to reproduce full-size photographic images from a

photographer's website) based on fair use principles but there was no clarity as to whether inlined links to full-sized reproductions constitute an infringement and are not automatically excused as a fair use. In Perfect 10, Inc. v. Amazon.com, Inc. ,2007, a federal court of appeal again permitted the use of inlined links (reproductions of images from an adult men's magazine website) for thumbnail reproductions.

Framing: "Framing" is the process of allowing a user to view the contents of one website while it is framed by information from another site, similar to the "picture-in-picture" feature offered on some televisions. Framing may trigger a dispute under copyright and trademark law theories, because a framed site arguably alters the appearance of the content and creates the impression that its owner endorses or voluntarily chooses to associate with the framer".

In Futuredontics Inc. v. Applied Anagramic Inc, 2007, A district court ruled that the addition of the reproduced Web pages within a "frame" by dental website containing contents of other website detailing Applied Anagramic as well as its trademark and links to all of its Web pages leads to modification in the appearance of the linked site and such modifications could, without authorization, amount to infringement of derivative work. To avoid linking, framing, and in lining violations one must seek permission from original owner of content / information /graphics to for deep linking, in lining, pulling full size images and framing graphic links comprising trademarks that tends to side step the linked site's home page and need to sign a linking agreement that give them right to display the Link and trademarks or images in the Link at their Site. In case one could not obtain the required permission from the linked site, disclaimer clearly and prominently displayed and stating the source of information can reduce the liability or unauthorized use and compensatory damage.