Cyber Crimes and Laws PYQ 2017

Q1 a Explain the different kinds of cybercrimes?

Ans. Cybercrime refers to criminal activities that are committed using digital technology or the internet. There are several different types of cybercrimes, including:

Hacking: Unauthorized access to someone's computer system or network with the intent to gain information, disrupt operations, or cause damage.

Example: A hacker gaining unauthorized access to a company's database and stealing sensitive customer information.

Phishing: A method used to trick individuals into revealing their personal information, such as usernames, passwords, and credit card numbers, by pretending to be a trustworthy entity.

Example: Sending a fake email claiming to be from a bank, asking the recipient to click on a link and provide their login credentials.

Malware: Malicious software that is designed to infiltrate, damage, or gain unauthorized access to a computer system or network. This includes viruses, worms, and ransomware.

Example: Installing a virus on a victim's computer that steals their personal information and sends it to the attacker.

Identity theft: Stealing someone's personal information, such as their name, address, social security number, and financial details, with the intent to commit fraud or other illegal activities.

Example: Using someone's stolen credit card information to make unauthorized purchases online.

Cyber stalking: Harassing or threatening someone online, often through social media, emails, or other forms of digital communication.

Example: Sending repeated threatening messages to someone on social media or through email.

Online fraud: Using deception to obtain money or assets from individuals or organizations through fraudulent online schemes.

Example: Setting up a fake online investment scheme and convincing victims to invest money, only to disappear with the funds.

Cyberbullying: Using technology to intimidate, harass, or harm individuals, often through social media, text messages, or emails.

Example: Sending threatening messages to a person through social media platforms with the intent to harm their reputation or cause emotional distress.

Distributed Denial of Service (DDoS) attacks: Overwhelming a website or network with traffic from multiple sources to disrupt its normal functioning and deny access to legitimate users.

Example: Flooding a website with traffic from multiple sources to bring it down and make it inaccessible to users.

These are just some examples of the different types of cybercrimes that can occur in today's digital world. It's important to stay vigilant and take necessary measures to protect oneself and organizations from cyber threats.

Q1 b What is cyber security? Describe the major steps that should be taken to ensure cyber security.

Ans. Cybersecurity refers to the practice of protecting computers, servers, networks, software, data, and other digital assets from unauthorized access, use, or damage. It involves implementing measures and safeguards to prevent, detect, respond to, and recover from cyber threats and attacks.

The major steps that should be taken to ensure cybersecurity include:

Risk Assessment: Identify and assess potential cybersecurity risks and vulnerabilities in your systems, networks, and data. Conduct regular risk assessments to understand the potential impact of cyber threats on your organization.

Implement Strong Authentication: Use strong, unique passwords for all accounts and enable multi-factor authentication (MFA) wherever possible to add an additional layer of security. Avoid using default or easily guessable passwords.

Keep Software and Systems Updated: Keep all software, operating systems, and devices up-to-date with the latest security patches and updates. This helps to address known vulnerabilities and protect against known exploits.

Use Firewalls and Antivirus Software: Deploy firewalls to protect your networks from unauthorized access and use antivirus software to detect and remove malware.

Regularly Back Up Data: Regularly back up critical data and systems to a secure offsite location. This ensures that you can restore your data in case of a security breach or data loss event.

Educate Users: Train employees and users about safe online practices, such as not clicking on suspicious links or downloading unknown attachments, being cautious with emails from unknown sources, and reporting any suspicious activity to IT or security personnel.

Control Access: Limit access to sensitive data and systems to only authorized personnel. Use role-based access control (RBAC) and grant permissions based on the principle of least privilege, giving users only the access they need to perform their job responsibilities.

Regular Monitoring and Auditing: Implement monitoring and auditing mechanisms to detect and respond to security incidents in real-time. Regularly review logs, system activities, and other security metrics to identify any anomalies or potential security breaches.

Incident Response Plan: Develop and implement an incident response plan that outlines the steps to be taken in case of a cybersecurity incident. This includes procedures for detecting, containing, mitigating, and recovering from security breaches.

Regular Security Awareness Training: Conduct regular cybersecurity awareness training for employees to keep them updated with the latest threats, best practices, and policies.

Engage Security Experts: Consider engaging cybersecurity experts or partnering with a managed security services provider (MSSP) to augment your organization's cybersecurity capabilities and stay protected against evolving threats.

Implementing these steps can help organizations establish a strong cybersecurity posture and mitigate the risk of cyber threats and attacks. It's important to continuously monitor and update cybersecurity measures to adapt to changing threats and technologies.

OR

Q1 a What are the domain name disputes? Explain the different kinds of domain name disputes and remedies available to settle them.

Ans. Domain name disputes refer to conflicts or disagreements that arise between parties over the ownership, use, or control of a particular domain name on the internet. Domain names are unique and human-readable addresses used to identify websites on the internet, and they are registered and managed by domain name registrars.

There are several different types of domain name disputes, including:

Cybersquatting: This occurs when a person or entity registers a domain name with the intention of profiting from the goodwill associated with a trademark or brand owned by another party. For example, registering a domain name that closely resembles a well-known brand, such as "go0gle.com" instead of "google.com".

Typosquatting: This involves registering domain names that are intentionally misspelled versions of popular brands or trademarks, with the intention of redirecting users to another website or gaining unauthorized access to user information.

Domain Name Hijacking: This occurs when someone wrongfully transfers or gains control of a domain name that rightfully belongs to another party, often through fraudulent means or unauthorized access to the domain registrar's account.

Trademark Infringement: This occurs when a domain name registered by one party infringes upon the trademark rights of another party, causing confusion among consumers and diluting the value of the trademark.

To settle domain name disputes, there are several remedies available, including:

Domain Name Dispute Resolution Policy (UDRP): This is a process established by the Internet Corporation for Assigned Names and Numbers (ICANN) that provides a relatively quick and cost-effective way to resolve domain name disputes without going to court. The UDRP allows trademark owners to file complaints against domain name registrants for abusive or bad faith registrations. If the complaint is successful, the domain name may be transferred or canceled.

Court Litigation: Parties can also resolve domain name disputes through legal proceedings in court, typically by filing a trademark infringement lawsuit or a claim for cybersquatting or domain name

hijacking. Court litigation can be more complex, time-consuming, and costly compared to the UDRP process, but it provides an avenue for resolving disputes based on established trademark laws and legal principles.

Negotiation and Settlement: Parties involved in a domain name dispute can also choose to negotiate and settle the dispute outside of court through mediation, arbitration, or other alternative dispute resolution methods. This may involve reaching a mutually agreeable resolution, such as transferring the domain name to the rightful owner, modifying the domain name, or other forms of compensation or resolution.

Domain Name Recovery: In cases where a domain name has been wrongfully transferred or hijacked, the rightful owner may seek recovery of the domain name through legal or administrative means, such as filing a complaint with the domain registrar, law enforcement agencies, or other relevant authorities.

It's important to note that the specific process and remedies for settling domain name disputes may vary depending on the applicable laws, domain name registrar policies, and other factors. It's advisable to seek legal counsel or consult the relevant dispute resolution procedures for the specific domain name dispute at hand.

Q1 b Explain the various effects of cybercrimes.

Ans. Cybercrimes can have various effects on individuals, organizations, and society as a whole. Some of the key effects of cybercrimes include:

Financial Loss: Cybercrimes can result in significant financial losses for individuals and organizations. This can include theft of financial information, unauthorized access to bank accounts, credit card fraud, ransomware attacks, and other forms of online fraud or extortion. Financial losses can be devastating, resulting in direct monetary damages and potential long-term financial repercussions.

Data Breaches and Information Loss: Cybercrimes can lead to data breaches, where sensitive or confidential information is accessed, stolen, or leaked. This can include personal information, business data, intellectual property, trade secrets, and other valuable information. Data breaches can result in reputational damage, legal liabilities, regulatory fines, and loss of competitive advantage.

Reputational Damage: Cybercrimes can damage the reputation of individuals, organizations, and even entire industries. Breaches of customer data, privacy violations, or public exposure of confidential information can erode trust and credibility, leading to loss of customers, partners, investors, and other stakeholders.

Disruption of Operations: Cybercrimes can disrupt the normal operations of organizations, including their IT systems, networks, websites, and online services. This can result in downtime, loss of productivity, and increased costs associated with incident response, recovery, and remediation efforts.

Legal and Regulatory Consequences: Cybercrimes can have legal and regulatory consequences, including potential lawsuits, fines, penalties, and other legal liabilities. Organizations may be held accountable for failing to protect sensitive information or comply with relevant data protection laws, industry regulations, or contractual obligations.

Personal and Psychological Impact: Cybercrimes can have a personal and psychological impact on individuals who fall victim to online harassment, stalking, identity theft, or other forms of cyber-attacks. This can lead to emotional distress, anxiety, and loss of privacy, and may require extensive efforts to restore one's personal and online reputation.

Societal Impact: Cybercrimes can have broader societal impacts, including erosion of public trust in online platforms and services, damage to critical infrastructure, disruption of public services, and increased costs for law enforcement and government agencies in investigating and prosecuting cybercriminals.

Overall, cybercrimes can have wide-ranging effects on individuals, organizations, and society, encompassing financial, operational, reputational, legal, personal, and societal consequences. It underscores the importance of robust cybersecurity measures, vigilant online behavior, and effective cybercrime prevention and response strategies to mitigate the risks and impacts of cybercrimes.

Q2 a Define E-Contract. What are the essentials of E-Contract? Explain the different kinds of E-Contract?

Ans. E-Contract, also known as electronic contract, refers to a legally binding agreement formed electronically, typically through the internet or other electronic means. E-Contracts are governed by the same principles of contract law as traditional paper-based contracts, but they are formed, executed, and stored electronically.

The essentials of an E-Contract include:

Offer and Acceptance: Like traditional contracts, an E-Contract must involve a clear offer by one party and a clear acceptance of that offer by another party. The offer and acceptance must be communicated electronically and must be capable of being understood by both parties.

Intention to Create Legal Relations: There must be an intention by the parties to create a legally binding contract. This means that the parties must intend to be legally bound by the terms and conditions of the E-Contract.

Consideration: Like traditional contracts, an E-Contract must involve consideration, which refers to something of value exchanged between the parties, such as goods, services, or money.

Capacity: The parties entering into an E-Contract must have the legal capacity to do so. This means that they must be of legal age, mentally competent, and not under any legal disability that would prevent them from entering into a contract.

Consent: The parties must freely and voluntarily consent to the terms and conditions of the E-Contract. This includes understanding and agreeing to the terms of the contract, including any applicable terms of service, privacy policies, or other contractual terms.

Legality: The subject matter of the E-Contract must be legal and not involve any illegal or prohibited activities.

Different kinds of E-Contracts include:

Click-Wrap Agreements: These are E-Contracts where the user must click on an "I Agree" button or similar mechanism to indicate acceptance of the terms and conditions. Click-wrap agreements are commonly used in online transactions, such as software license agreements, online terms of service, and other digital agreements.

Browse-Wrap Agreements: These are E-Contracts where the terms and conditions are typically posted on a website, and the user's use of the website or online services is deemed as acceptance of those terms. Browse-wrap agreements are usually displayed as hyperlinks or disclaimers on web pages and may not require an explicit action from the user to indicate acceptance.

Email Agreements: These are E-Contracts formed through email exchanges between parties. Email agreements can be legally binding, provided they meet the essential elements of a contract, including offer, acceptance, consideration, and intention to create legal relations.

Online Marketplaces: E-Contracts can be formed on online marketplaces, such as e-commerce platforms, where buyers and sellers agree to terms and conditions for the purchase and sale of goods or services.

Mobile App Agreements: E-Contracts can also be formed through mobile apps, where users agree to terms and conditions when downloading or using an app.

It is important to note that the legality and enforceability of E-Contracts may vary depending on the jurisdiction and applicable laws. It is advisable to seek legal advice when entering into or forming E-Contracts to ensure compliance with relevant laws and regulations.

Q2 b Internet is a boon in today's world however, it has certain disadvantages. Comment.

Ans. The internet has undoubtedly revolutionized the way we live, work, communicate, and access information. It has brought about numerous advantages and opportunities, but it also has its share of disadvantages. Some of the disadvantages of the internet include:

Privacy and Security Concerns: The internet has raised significant concerns about privacy and security. Cybercrime, data breaches, identity theft, and online scams are prevalent, and users' personal and sensitive information can be compromised.

Online Harassment and Cyberbullying: The anonymity of the internet can lead to online harassment, cyberbullying, and trolling, which can have serious psychological and emotional impacts on individuals, especially vulnerable groups such as children, teenagers, and marginalized communities.

Misinformation and Fake News: The internet has facilitated the spread of misinformation, fake news, and propaganda, leading to the erosion of trust in traditional media and the proliferation of misinformation that can have social, political, and economic consequences.

Addiction and Overdependence: The internet can be addictive, leading to issues such as internet addiction, social media addiction, and online gaming addiction, which can negatively impact mental health, relationships, and overall well-being. Moreover, overdependence on the internet for various activities can also lead to a loss of offline social interactions and real-world skills.

Online Content and Accessibility: The internet is flooded with vast amounts of content, ranging from useful and educational to misleading or harmful. It can be challenging to filter and verify the

accuracy of information, leading to potential misinformation or misinterpretation. Additionally, not everyone has equal access to the internet, which can result in a digital divide and limit opportunities for marginalized communities.

Cybersecurity Threats: The internet is constantly under the threat of cyber attacks, including viruses, malware, ransomware, and other cyber threats, which can cause financial losses, disruption of services, and compromise of sensitive information.

Social and Ethical Concerns: The internet has raised significant social and ethical concerns, including issues related to online hate speech, discrimination, censorship, surveillance, and the ethical implications of emerging technologies such as artificial intelligence, internet of things (IoT), and big data.

In conclusion, while the internet has brought numerous advantages and opportunities, it also has its share of disadvantages and challenges that need to be addressed to ensure a safe, secure, and responsible use of the internet in today's world. It is important for individuals, organizations, and policymakers to be vigilant and proactive in addressing these concerns and promoting responsible internet usage.

OR

Q2 a What are the objectives of IT Act 2000? What are the exclusions from the Act?

Ans. The Information Technology (IT) Act 2000, also known as the Cyber Law of India, was enacted with the objectives of providing legal recognition to electronic transactions, facilitating e-governance, ensuring data security, and preventing cybercrimes. The main objectives of the IT Act 2000 are as follows:

Legal Recognition of Electronic Transactions: The IT Act 2000 provides legal recognition to electronic transactions, electronic records, and digital signatures, making them legally valid and enforceable in courts of law. This helps in promoting e-commerce, e-governance, and other electronic transactions.

Facilitating E-Governance: The IT Act 2000 aims to facilitate e-governance by providing legal recognition to electronic records and digital signatures in government transactions, promoting the use of digital signatures for authentication and verification, and promoting the use of electronic documents in government processes.

Data Security and Privacy: The IT Act 2000 aims to ensure data security and privacy by prescribing security practices and procedures for handling sensitive information, protecting against unauthorized access, and providing provisions for punishment of unauthorized access, data theft, and data breaches.

Prevention of Cybercrimes: The IT Act 2000 aims to prevent cybercrimes by providing legal provisions for offenses such as hacking, phishing, identity theft, cyber stalking, cyber fraud, and other cyber offenses, and prescribing penalties for these offenses.

Regulation of Digital Signatures: The IT Act 2000 provides for the regulation of digital signatures, including their legal recognition, certification, and verification, to ensure their integrity and authenticity in electronic transactions.

Establishment of Cyber Appellate Tribunal: The IT Act 2000 establishes the Cyber Appellate Tribunal, which serves as a specialized forum for hearing appeals against the orders of the Adjudicating Officer under the Act.

Exclusions from the IT Act 2000:

The IT Act 2000 has certain exclusions, which include:

Negotiable Instruments and Power of Attorney: The IT Act 2000 does not apply to negotiable instruments, such as checks, promissory notes, and bills of exchange, and power of attorney, as these are governed by other laws in India.

Electronic Records and Digital Signatures under Other Laws: The IT Act 2000 does not apply to electronic records and digital signatures that are governed by other laws in India, such as the Indian Evidence Act, the Indian Penal Code, and the Companies Act.

Physical Signatures: The IT Act 2000 does not affect the validity of physical signatures on paper documents, as it primarily deals with the legal recognition and regulation of electronic records and digital signatures.

It is important to note that the IT Act 2000 has been amended multiple times to keep pace with the changing technological landscape and evolving cyber threats, and it is advisable to consult the latest version of the Act and seek legal advice for specific legal interpretations and implications.

Q2 b Describe E-Form. What advantages it has in comparison to paper form?

Ans. An E-Form, short for Electronic Form, is a digital or electronic document that is used to collect, store, and process information electronically. E-Forms are typically used in various digital platforms, such as websites, online applications, mobile apps, and other electronic systems, for data collection, data entry, and information processing purposes.

Advantages of E-Forms compared to paper forms:

Efficiency and Speed: E-Forms enable faster and more efficient data collection and processing compared to traditional paper forms. Electronic data entry eliminates the need for manual data entry, reduces the chances of errors and duplication, and streamlines the overall process, saving time and resources.

Accessibility and Convenience: E-Forms can be accessed and filled out from anywhere at any time, as long as there is an internet connection. This makes it convenient for users to submit information and complete forms remotely without the need for physical presence or paper documents.

Cost-effective and Environmentally Friendly: E-Forms eliminate the need for printing, storing, and managing paper forms, which can result in cost savings on printing, storage, and transportation. Additionally, E-Forms are environmentally friendly as they reduce paper consumption and waste, contributing to sustainability efforts.

Accuracy and Data Validation: E-Forms can include data validation features, such as required fields, data formats, and validation rules, which help ensure data accuracy and consistency. This reduces the

chances of errors, incomplete or inconsistent data, and improves the quality of collected information.

Data Security and Privacy: E-Forms can be designed with built-in security features, such as encryption, access controls, and user authentication, to protect sensitive information. This helps ensure data security and privacy, which is crucial for maintaining confidentiality and complying with data protection regulations.

Integration and Automation: E-Forms can be integrated with other digital systems, databases, or workflows, enabling automated data processing, validation, and integration with other business processes. This improves data integration and workflow efficiency, reducing manual efforts and errors.

Enhanced User Experience: E-Forms can provide a better user experience with features such as user-friendly interfaces, auto-fill options, and interactive elements, making it easier and more convenient for users to complete and submit forms.

Overall, E-Forms offer several advantages over traditional paper forms, including increased efficiency, accessibility, cost savings, data accuracy, security, and user experience, making them a preferred choice for many organizations in the digital era.

Q3 a What is Digital Signature? Explain the process of creation and verification of Digital Signature.

Ans. A digital signature is a cryptographic technique used to authenticate the integrity and authenticity of digital documents, messages, or transactions. It is a unique digital representation of a person or entity that can be attached to an electronic document, verifying its origin and ensuring that it has not been tampered with.

The process of creating and verifying a digital signature typically involves the following steps:

Creation of Digital Signature:

Step 1: Message Digest Calculation - The sender creates a hash or message digest of the electronic document using a secure hash function. This produces a fixed-size string of characters that is unique to the content of the document.

Step 2: Private Key Encryption - The sender then encrypts the message digest using their private key, which is a part of their digital certificate. This creates the digital signature.

Step 3: Attaching Digital Signature - The digital signature is then attached to the electronic document, along with the sender's public key, digital certificate, and other relevant information.

Verification of Digital Signature:

Step 1: Extracting Message Digest - The receiver extracts the message digest from the electronic document and calculates the hash value using the same secure hash function as the sender.

Step 2: Decryption with Public Key - The receiver then decrypts the digital signature using the sender's public key, which is obtained from the sender's digital certificate.

Step 3: Comparison of Message Digests - The receiver compares the calculated message digest with the decrypted message digest. If they match, it indicates that the document has not been tampered with during transmission and that the digital signature is valid.

Step 4: Certificate Verification - The receiver also verifies the authenticity and validity of the sender's digital certificate, which contains their public key, by checking the certificate against a trusted Certificate Authority (CA).

If the message digests match, the digital signature is valid, and the sender's digital certificate is trusted, then the document is considered authentic and has not been tampered with.

Digital signatures provide several benefits, including authenticity, integrity, non-repudiation, and security, making them a widely used technique in various digital transactions, contracts, and communications where verification of document authenticity is critical.

Q3 b Describe the rules laid down in IT Act regarding attribution and acknowledgement of receipt of E-records.

Ans. The Information Technology (IT) Act, 2000, is an Indian legislation that governs electronic transactions and communication, including the attribution and acknowledgement of receipt of electronic records. The Act includes specific provisions related to these aspects, which are as follows:

Attribution of electronic records (Section 3): According to the IT Act, an electronic record shall be deemed to be attributed to the originator if it was sent by the originator himself/herself or by an automated system programmed by or on behalf of the originator to operate automatically. This means that an electronic record is legally attributed to the person or entity that has sent it or authorized an automated system to send it.

Acknowledgement of receipt of electronic records (Section 13): The IT Act lays down the rules for acknowledging the receipt of electronic records. If the originator has not stipulated any particular method of acknowledgement, an acknowledgement of receipt may be implied if the electronic record has been received by the addressee and he/she has had the opportunity to access the record. However, mere silence or inaction does not constitute an acknowledgement of receipt.

Time and place of dispatch and receipt of electronic records (Section 12): The IT Act establishes that the time of dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator. Similarly, the time of receipt of an electronic record is when it is capable of being retrieved and processed by the addressee.

These rules laid down in the IT Act regarding the attribution and acknowledgement of receipt of electronic records provide legal recognition and validity to electronic transactions and communications, ensuring that electronic records are legally attributed to their originators and that the receipt of electronic records is duly acknowledged in a legally recognized manner.

OR

Q3 a What do you understand by the term E-Governance? Explain the provisions of IT Act that facilitate E-Governance.

Ans. E-Governance, or electronic governance, refers to the use of information and communication technologies (ICTs) by governments to transform their processes, systems, and service delivery to citizens, businesses, and other stakeholders. E-Governance aims to enhance transparency, efficiency, effectiveness, and accessibility in governance, leading to better service delivery and improved citizen engagement.

The Information Technology (IT) Act, 2000, of India includes provisions that facilitate E-Governance. **Some of the key provisions are:**

Legal recognition of electronic records (Section 4): The IT Act grants legal recognition to electronic records, including electronic documents, digital signatures, and electronic contracts. This enables government agencies to use electronic records in their transactions and communications, eliminating the need for physical paper-based records.

Use of digital signatures (Section 5): The IT Act recognizes digital signatures as a valid means of signing electronic records. This allows government agencies to use digital signatures for authentication and verification of electronic records, such as digital signatures on digital documents or online forms.

Electronic delivery of services (Section 6A): The IT Act allows the government to prescribe rules for electronic delivery of services, which enables government agencies to provide services online, such as e-filing of taxes, online payment of bills, and online application and processing of government permits, licenses, and certificates.

Facilitation of electronic filing and record keeping (Section 10A): The IT Act allows government agencies to prescribe rules for electronic filing and record keeping, which enables government departments and agencies to maintain electronic records, including documents, reports, and records, in digital format, instead of physical paper-based records.

Authentication of electronic records (Section 11): The IT Act provides for the use of electronic signatures, digital signatures, or any other method of authentication as a means to establish the authenticity of electronic records. This enables government agencies to verify the authenticity of electronic records used in E-Governance processes.

Time and place of dispatch and receipt of electronic records (Section 12): The IT Act establishes the time and place of dispatch and receipt of electronic records, which enables government agencies to determine the legal validity of electronic records in E-Governance transactions.

These provisions of the IT Act facilitate the use of electronic records, digital signatures, and other ICTs in E-Governance processes, enabling government agencies to leverage technology for efficient, transparent, and citizen-centric service delivery.

Q3 b Compare E-Signature with Digital Signature.

Ans. E-Signature and Digital Signature are two terms often used interchangeably, but they have distinct differences. Here's a comparison:

E-Signature:

E-Signature refers to an electronic signature that is used to sign a document or record electronically.

E-Signatures can take various forms, such as scanned images of physical signatures, typed names, checkboxes, or other digital markers.

E-Signatures are commonly used for informal and low-risk transactions, such as signing contracts, agreements, or other documents in everyday business or personal transactions.

E-Signatures do not typically involve the use of digital certificates or cryptographic methods for signing and verification.

E-Signatures may not be as secure or legally binding as Digital Signatures, as they may be susceptible to forgery or repudiation.

Digital Signature:

Digital Signature refers to a specific type of electronic signature that uses cryptographic methods to provide a high level of security, authenticity, and integrity to a document or record.

Digital Signatures involve the use of a digital certificate, which is issued by a trusted Certificate Authority (CA), to verify the identity of the signer and ensure the integrity of the signed document.

Digital Signatures use public key infrastructure (PKI) technology, where the signer has a private key for signing the document, and the recipient has a corresponding public key for verification.

Digital Signatures provide a higher level of security and legal validity, as they are difficult to forge or repudiate, and they can be verified by third parties.

Digital Signatures are commonly used for formal and high-stakes transactions, such as signing legal documents, financial contracts, or other sensitive records that require a higher level of security and trust.

In summary, while E-Signatures are more commonly used for everyday transactions and may not provide the same level of security and legal validity as Digital Signatures, Digital Signatures are a more robust and secure method for signing and verifying electronic records, especially in formal or high-stakes scenarios.

Q4 a Describe the provisions relating to issue, suspension and revocation of Digital Signature Certificate as per IT Act.

Ans. As per the Information Technology (IT) Act, 2000 in India, the provisions relating to issue, suspension, and revocation of Digital Signature Certificate (DSC) are outlined as follows:

Issue of Digital Signature Certificate:

a. Digital Signature Certificate can be issued by a Certifying Authority (CA) only after verifying the identity of the applicant as per the guidelines prescribed by the Controller of Certifying Authorities (CCA).

b. The DSC is issued with a validity period mentioned in the certificate, which may not exceed two years.

Suspension of Digital Signature Certificate:

a. The CCA or any officer authorized by it has the power to suspend a DSC if it is found that the certificate holder has contravened any provision of the IT Act or its rules.

b. The suspension of DSC can be done for a temporary period pending an inquiry or investigation.

Revocation of Digital Signature Certificate:

a. The CCA or any officer authorized by it has the power to revoke a DSC if it is found that the certificate holder has contravened any provision of the IT Act or its rules.

b. The revocation of DSC can be done if the certificate holder requests for revocation or if the certificate holder ceases to exist, or if the certificate has expired, or if the certificate has been compromised or is suspected to be compromised.

c. The revoked DSC is included in the Certificate Revocation List (CRL) maintained by the CA, and the same is published on the CCA's website.

It's important to note that the IT Act and its rules prescribe guidelines and procedures for the issue, suspension, and revocation of Digital Signature Certificates to ensure the integrity, authenticity, and security of electronic records and transactions in the digital ecosystem. These provisions aim to prevent misuse, fraud, or unauthorized access to DSCs and maintain trust and reliability in the use of digital signatures for various online transactions.

Q4 b Define Certifying Authority and describe the duties performed by it.

Ans. Certifying Authority (CA) is an entity that issues, suspends, or revokes Digital Signature Certificates (DSCs) under the provisions of the Information Technology (IT) Act, 2000 in India. The CA acts as a trusted third party that verifies the identity of individuals, organizations, or entities applying for DSCs and issues them after due authentication. The duties performed by a Certifying Authority include:

Issuing Digital Signature Certificates (DSCs): The primary function of a Certifying Authority is to issue DSCs to individuals or organizations after verifying their identity as per the guidelines prescribed by the Controller of Certifying Authorities (CCA). The CA ensures that the DSCs are issued only to genuine entities and are valid for the specified period mentioned in the certificate.

Maintaining Certificate Revocation List (CRL): The Certifying Authority maintains a Certificate Revocation List (CRL) that contains information about the revoked or suspended DSCs. The CRL is published on the website of the CCA and is regularly updated to provide information to users about the status of DSCs.

Suspension and Revocation of DSCs: The CA has the authority to suspend or revoke a DSC if it is found that the certificate holder has contravened any provision of the IT Act or its rules, or if the certificate holder requests for suspension or revocation, or if the certificate has expired or is compromised. The CA follows the procedures prescribed by the IT Act and its rules for suspension or revocation of DSCs.

Ensuring Security and Integrity of DSCs: The Certifying Authority is responsible for maintaining the security and integrity of the DSCs issued by it. The CA must ensure that the private key associated with the DSC is kept secure and not disclosed to unauthorized entities. The CA must also ensure that the DSCs are tamper-proof and issued using secure cryptographic algorithms.

Compliance with Guidelines and Regulations: The Certifying Authority must comply with the guidelines, rules, and regulations prescribed by the CCA and other regulatory authorities. The CA must follow the security standards, audit requirements, and other guidelines to ensure the trustworthiness and reliability of the DSCs issued by it.

Providing Technical Support and Assistance: The Certifying Authority may be required to provide technical support and assistance to users of DSCs, including guidance on the installation, configuration, and usage of DSCs in different applications and environments.

Overall, the Certifying Authority plays a crucial role in ensuring the integrity, authenticity, and security of digital signatures and certificates, and upholding the trust and reliability of electronic transactions in the digital ecosystem.

OR

Q4 a Explain the penalties and compensation available under IT Act to provide legal protection to the owner of computer resources against cybercrime.

Ans. The Information Technology (IT) Act, 2000 in India provides legal protection to the owners of computer resources against cybercrime by specifying penalties and compensation for various offenses. The penalties and compensation provisions under the IT Act are as follows:

Penalties for unauthorized access and hacking: Section 43 of the IT Act specifies that if a person accesses or secures access to a computer resource without authorization, or downloads, copies, or extracts data from a computer resource without permission, he/she shall be liable to pay damages by way of compensation to the owner of the computer resource. The compensation amount can be up to INR 1 crore (10 million) or more, depending on the severity of the offense.

Penalties for computer-related offenses: Section 66 of the IT Act specifies that if a person commits any offense such as hacking, introducing malware or virus, tampering with computer source code, identity theft, etc., he/she shall be punishable with imprisonment for a term which may extend up to three years, or with fine which may extend up to INR 5 lakh (500,000), or with both.

Compensation for unauthorized interception, monitoring, or data theft: Section 43A of the IT Act specifies that if a person, without permission, intercepts, monitors, or steals data from any computer

resource, he/she shall be liable to pay damages by way of compensation to the person affected. The compensation amount can be up to INR 5 crore (50 million) or more, depending on the severity of the offense.

Compensation for failure to protect data: Section 43A of the IT Act also specifies that if a body corporate, possessing, dealing, or handling any sensitive personal data, fails to protect such data and causes wrongful loss or gain to any person, it shall be liable to pay damages by way of compensation to the person affected. The compensation amount can be up to INR 5 crore (50 million) or more, depending on the severity of the offense.

Penalties for cyber terrorism: Section 66F of the IT Act specifies that if a person engages in any act of cyber terrorism, which includes causing disruption to essential services, damaging critical infrastructure, or spreading panic among the public, he/she shall be punishable with imprisonment for a term which may extend to life imprisonment, along with a fine.

It is important to note that the penalties and compensation provisions under the IT Act may vary depending on the specific offense committed, and the severity of the offense. These provisions are aimed at providing legal protection to the owners of computer resources and victims of cybercrime, and to deter cybercriminal activities in the digital ecosystem.

Q4 b Define Subscriber and describe his duties as per IT Act.

Ans. In the context of the Information Technology (IT) Act, 2000 in India, a "subscriber" refers to a person who has been assigned a unique identification by a "Certifying Authority" for the purpose of obtaining a Digital Signature Certificate (DSC) or an Electronic Authentication Technique (EAT). The subscriber is the person who holds the DSC or uses the EAT for electronic transactions and communications.

As per the IT Act, a subscriber has certain duties, which include:

Generating key pair: A subscriber is required to generate a pair of cryptographic keys, known as the public key and the private key, for the purpose of creating a digital signature or using an EAT. The subscriber must take reasonable care to ensure the security and secrecy of the private key, as it is the key used for creating the digital signature or authenticating electronic records.

Secure storage of private key: The subscriber is responsible for securely storing the private key associated with the DSC or EAT to prevent unauthorized access, use, or disclosure of the private key. The private key should be kept confidential and not shared with others.

Avoiding unauthorized use: The subscriber is responsible for ensuring that the DSC or EAT is not used by any unauthorized person for creating digital signatures or authenticating electronic records. The subscriber should take necessary precautions to prevent any misuse of the DSC or EAT.

Reporting loss or compromise of private key: In case of loss, theft, compromise, or unauthorized use of the private key associated with the DSC or EAT, the subscriber is required to report the same to the respective Certifying Authority as soon as possible. This is to ensure that appropriate action can be taken to prevent any misuse of the DSC or EAT.

Compliance with Certifying Authority's rules: The subscriber is required to comply with the rules, regulations, and guidelines laid down by the Certifying Authority regarding the use and management

of the DSC or EAT. This includes following the procedures for obtaining, renewing, revoking, or suspending the DSC or EAT, as specified by the Certifying Authority.

Non-repudiation of electronic records: The subscriber is bound by the digital signatures or EATs created using the DSC or EAT, and cannot repudiate the authenticity or integrity of electronic records signed or authenticated by them using the DSC or EAT.

It is important for subscribers to understand their duties and responsibilities as per the IT Act to ensure the secure and lawful use of digital signatures or EATs, and to maintain the integrity and confidentiality of their private keys.

Q5. Write notes on the following:

(i) Cyber Forensic

(il) Cyber Space Jurisdiction

(iii)Encryption and Decryption

Ans. (i) Cyber Forensics: Cyber forensics, also known as digital forensics, is the process of collecting, analyzing, and preserving digital evidence in order to investigate and prevent cybercrime. It involves the application of forensic techniques to digital devices, networks, and digital data to uncover evidence of cybercrimes, such as hacking, data breaches, cyber fraud, and other cyber-related offenses.

Some key points about cyber forensics are:

Collection of digital evidence: Cyber forensic experts use various tools and techniques to collect digital evidence from devices such as computers, smartphones, servers, and networks. This includes recovering deleted files, analyzing log files, capturing network traffic, and other methods to collect data for forensic analysis.

Analysis of digital evidence: Cyber forensic experts analyze the collected digital evidence to extract relevant information, reconstruct events, and identify the perpetrator of cybercrimes. This may involve activities such as data recovery, data discovery, data analysis, and data interpretation to reconstruct the sequence of events and establish a chain of custody for the evidence.

Preservation of digital evidence: Cyber forensic experts ensure that the collected digital evidence is preserved in a forensically sound manner to maintain its integrity and admissibility in court. This involves using proper techniques for evidence handling, storage, and preservation to prevent tampering or alteration of the evidence.

(ii) Cyber Space Jurisdiction: Cyber space jurisdiction refers to the legal authority of a country or jurisdiction over activities that occur in the virtual realm of the internet. It involves the determination of which laws and regulations apply to various cyber-related activities, including online transactions, cybercrimes, data breaches, and other cyber-related legal matters.

Some key points about cyber space jurisdiction are:

Territoriality principle: The territoriality principle states that a country's laws apply to activities that occur within its physical territory. However, in cyberspace, the territoriality principle can be complex, as cyber activities can transcend geographical boundaries, making it challenging to determine the appropriate jurisdiction for legal matters.

National laws and regulations: Different countries have their own laws and regulations related to cyber activities, including cybercrime laws, data protection laws, and other relevant regulations. These laws can vary from country to country, and they may have extraterritorial jurisdiction, meaning that they can apply to activities that occur outside of their physical territory.

International treaties and agreements: Some countries have signed international treaties and agreements related to cyber space jurisdiction to establish common rules and principles for addressing cyber-related legal matters. Examples include the Budapest Convention on Cybercrime, which aims to facilitate international cooperation in investigating and prosecuting cybercrimes, and the General Data Protection Regulation (GDPR) of the European Union, which has extraterritorial application for data protection in the EU.

(iii) Encryption and Decryption:

Encryption is the process of converting data into a coded form that is unreadable without a key or password, in order to protect the confidentiality and integrity of data. Decryption is the process of converting encrypted data back into its original, readable form using the key or password.

Some key points about encryption and decryption are:

Encryption algorithms: Encryption uses mathematical algorithms to scramble data into a ciphertext that is unreadable without the appropriate key or password. There are various types of encryption algorithms, including symmetric encryption, asymmetric encryption, and hashing algorithms.

Symmetric encryption: In symmetric encryption, the same key is used for both encryption and decryption. This means that the sender and receiver need to share the same secret key in order to encrypt and decrypt messages. Examples of symmetric encryption algorithms include Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

Asymmetric encryption: In asymmetric encryption, also known as public-key cryptography, different keys are used for encryption and decryption. This means that the sender and receiver have a pair of keys, a public key and a private key. The public key is used for encryption, while the private key is used for decryption. Messages encrypted with the public key can only be decrypted with the corresponding private key, providing a higher level of security. Examples of asymmetric encryption algorithms include RSA, DSA, and Elliptic Curve Cryptography (ECC).

Hashing algorithms: Hashing is a one-way process of converting data into a fixed-length string of characters, typically a hexadecimal value, which represents a unique fingerprint of the original data. Hashing algorithms are commonly used for data integrity and password storage. However, unlike encryption, hashing is irreversible, meaning that the original data cannot be retrieved from the hash value.

Importance of encryption and decryption: Encryption and decryption play a crucial role in securing data and communications over the internet. They provide confidentiality, integrity, and authentication of data, ensuring that only authorized parties can access and read the data. Encryption is widely used for securing sensitive information, such as financial transactions, personal

data, and confidential communications, in order to protect against unauthorized access, data breaches, and cyber attacks.

It's worth noting that while encryption provides a high level of security, it is not foolproof, and vulnerabilities or weaknesses in encryption algorithms or implementation can potentially be exploited by skilled hackers or attackers. Therefore, it's important to use strong encryption methods, keep encryption keys secure, and regularly update and patch encryption software to maintain the highest level of security in the digital environment.

OR

Q5 a Differentiate between :

(i) Cyber crime and Conventionai crime

(in) Private key and Public key

(iii) Cyber contravention and cyber offence

Ans. (i) Cyber crime vs Conventional crime:

Cyber crime refers to illegal activities committed using digital technologies, such as computers, networks, and the internet. It includes activities such as hacking, identity theft, phishing, ransomware attacks, online fraud, and spreading malware or viruses. Cyber crime is typically committed against digital systems or data, and its impact can be widespread, affecting individuals, organizations, and even nations.

Conventional crime, on the other hand, refers to illegal activities that are committed using traditional methods, such as physical force, violence, theft, fraud, or vandalism. Conventional crime typically involves tangible or physical targets, such as people, property, or possessions, and is governed by the laws of the physical world.

(ii) Private key vs Public key:

Private key, also known as a secret key or symmetric key, is a cryptographic key that is used in symmetric encryption algorithms, where the same key is used for both encryption and decryption. The private key is kept secret by the owner and is used to encrypt and decrypt messages or data. Since the same key is used for both encryption and decryption, it is essential to keep the private key secure and protect it from unauthorized access.

Public key, also known as an asymmetric key, is a cryptographic key that is used in asymmetric encryption algorithms, where a pair of keys, a public key, and a private key, are used for encryption and decryption. The public key is made available to the public and can be freely shared, while the private key is kept secret by the owner. Messages or data encrypted with the public key can only be decrypted with the corresponding private key, providing a higher level of security and enabling secure communication between parties.

(iii) Cyber contravention vs Cyber offence:

Cyber contravention refers to the violation of rules, regulations, or guidelines related to the use of information and communication technologies (ICT), including computers, networks, and the internet. It may involve activities such as unauthorized access to computer systems, misuse of data or resources, circumvention of security measures, or non-compliance with ICT policies or guidelines.

Cyber offence, on the other hand, refers to illegal activities committed using digital technologies, such as cyber crime. It includes activities such as hacking, spreading malware or viruses, identity theft, online fraud, cyber stalking, cyber terrorism, and other illegal acts that are specifically prohibited by law and can result in criminal charges and legal consequences. Cyber offences are typically governed by specific cybercrime laws and regulations in different jurisdictions.

Q5 b Briefly discuss the following:

(i) Punishment for sending offensive messages

(ii) Punishment for disclosure of information in breach of lawful contract

Ans. (i) Punishment for sending offensive messages:

Sending offensive messages is considered a cybercrime and can have legal consequences under the IT Act or other relevant laws in different jurisdictions. The punishment for sending offensive messages may vary depending on the severity of the offense and the specific laws in place. In many countries, sending offensive messages with an intent to harass, intimidate, threaten, defame, or offend others online may be punishable by fines, imprisonment, or both.

For example, under the IT Act of India, Section 66A (which has been struck down by the Supreme Court of India as unconstitutional), previously criminalized sending offensive messages online and could result in imprisonment for up to three years and a fine. However, it's important to note that the legal landscape may change over time, and it's always advisable to consult the latest laws and regulations in your specific jurisdiction for accurate and up-to-date information.

(ii) Punishment for disclosure of information in breach of lawful contract:

Disclosure of information in breach of a lawful contract can also have legal consequences, depending on the nature of the breach, the terms of the contract, and the applicable laws in the jurisdiction. In general, breaching a lawful contract may result in civil liabilities, such as monetary damages, restitution, or specific performance, rather than criminal penalties.

For example, if a party discloses confidential information in violation of a non-disclosure agreement (NDA) or breaches a contract that contains clauses prohibiting the disclosure of certain information, the aggrieved party may be entitled to seek legal remedies through civil courts, such as compensation for damages incurred as a result of the breach.

It's important to note that the specific punishments or legal consequences for the breach of a lawful contract may vary depending on the laws in place, the terms of the contract, and the jurisdiction where the contract is governed. Therefore, it's advisable to seek legal advice and consult relevant

laws and regulations to understand the specific implications of breaching a lawful contract in your jurisdiction.