## Section A

### Q1. Describe the term on information security.?

Ans - Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electronic one.

### Q2. Analyze the cyber terrorism and how to tackle risks of cyber-crime ?

Ans - Cyberterrorism refers to the use of technology and cyberspace to conduct acts of terrorism. It involves the deliberate exploitation of computer systems, networks, and information to cause harm or instill fear among individuals, organizations, or governments . To tackle cyber risks:

- Strengthen cybersecurity through measures like encryption and regular updates.
- Foster public-private collaboration for information sharing and resource allocation.

### Q3. Analyze the difference between E-mail spoofing and E-mail bombing ?

Ans- Email spoofing and email bombing are two different forms of malicious activities involving emails:

- **Email spoofing**: Email spoofing involves forging the email header to make it appear as if the email originated from a different source than it actually did. The sender's email address is manipulated, often to impersonate a trusted entity, in order to deceive the recipient.
- **Email bombing:** Email bombing refers to the act of overwhelming an individual's or organization's email account with a large volume of unwanted emails. This flood of emails can disrupt the normal functioning of the email server or cause inconvenience to the recipient.

### Q4. Analyze the difference between the computer forensics and cyber forensics ?

Ans- Computer forensics and cyber forensics are two related but distinct fields:

- **Computer forensics**: Computer forensics involves the investigation and analysis of digital devices such as computers, laptops, and storage media to gather evidence for legal purposes. It focuses on retrieving, preserving, and analyzing data from physical and logical storage devices.
- **Cyber forensics**: Cyber forensics, also known as digital forensics or network forensics, is a broader field that encompasses the investigation and analysis of digital evidence in networked environments. It involves the collection and analysis of data from network traffic, logs, servers, and other digital sources to investigate cybercrimes.

### Q5. Classify the different kinds of hackers ?

Ans -- Hackers can be classified into different categories based on their intentions and actions. Let's explain these categories to a baby:

- **White Hat Hackers:** These are the good guys! White hat hackers are like superheroes who use their skills to help protect computer systems and find security vulnerabilities.
- **Black Hat Hackers**: These are the bad guys! Black hat hackers use their skills for malicious purposes. They may break into computer systems to steal information, cause damage, or commit cybercrimes.
- **Gray Hat Hackers**: These hackers fall somewhere in between. They may hack into systems without permission, but they don't have harmful intentions.
- **Script Kiddies**: These are amateur hackers who don't have much technical knowledge.

### Q6. Classify the different types of digital evidence ?

- **Text Messages**: These are like digital conversations people have on their phones or computers.
- **Emails**: Emails are like digital letters that people send to each other.
- **Photos and Videos**: These are like digital pictures and movies.
- **Documents**: Digital documents are like digital papers or files that people create and save on their computers.

### Q7. Classify the types of IPR ?

- **Copyright:** Copyright is like a special protection for creative works, such as books, music, movies, and artwork.

- **Trademark:** A trademark is like a special sign or symbol that helps us recognize a particular product or brand. It can be a logo, a word, or a combination of both.
- **Patent:** A patent is like a special right given to inventors for their new and useful inventions.

**Q8. Define computer forensics ?**

Ans - Computer forensics is like being a detective for computers. When something goes wrong or there's a problem with a computer, computer forensics helps find out what happened and why. It's like looking for clues and evidence on the computer to solve a mystery. Computer forensics experts use special tools and techniques to investigate things like deleted files, internet history, and other digital traces. They help figure out if someone did something wrong or if something bad happened on the computer.

**Q9. Define copyright law. ?**

Ans - Copyright law is like a set of rules that protect the things people create. It means that when someone makes something like a book, a song, or a picture, they have the right to say how it can be used. It's like having a special ownership over their creation. Copyright law helps make sure that people who create things can decide if others can copy or use their work. It's important to respect copyright law and ask for permission before using someone else's creations.

**Q10. Define cyber law ?**

Ans - Cyber law is like a set of rules that help keep us safe when we use computers and the internet. It's like having special guidelines to make sure everyone behaves well online, just like we do in real life. Cyber law helps protect our personal information, like our names and addresses, from being shared without our permission. It also makes sure that people can't do mean or bad things to each other using computers, like bullying or stealing.

**Q11. Define cyber security. ?**

Ans - Cybersecurity is like having a special superhero shield to protect our computers, phones, and all the cool things we do online. It helps keep our information and secrets safe from bad guys who try to steal or do naughty things. Just like we lock the door to our house to keep it safe, cybersecurity helps lock our digital devices and keeps them safe from hackers and viruses.

**Q12. Define e-commerce in cyber platform ?**

Ans - E-commerce in the cyber platform is like a big online shopping mall where we can buy things using our computer or phone. It's a place where we can find lots of different stores and products without having to go to a physical store. We can browse through pictures and descriptions of things we want, like toys, clothes, or books, and then we can buy them with just a click! It's like having a magical shop that is always open, and we can shop from the comfort of our own home.

**Q13. Define intellectual property rights. ?**

Ans - Intellectual property rights (IPR) are like special protections for things that people create using their imagination and creativity. It's like having ownership over something you make, just like when you build a cool LEGO creation or draw a beautiful picture. IPR means that when someone creates something, like a story, a song, or a cool invention, they have the right to say how it can be used. It's like having a special ownership over your ideas and creations..

**Q14. Explain Botnets- a fuel for cybercrimes. ?**

Ans - Botnets are like groups of naughty robots that are controlled by bad guys. Just like we play with our toy robots and tell them what to do, bad guys create botnets by taking control of many computers and making them work together without the owners knowing. These naughty robots in a botnet can do bad things. They can spread viruses, steal information, or even attack other computers.

**Q15. Give few important rules of having good cyber ethics. ?**

Ans - Here are a few important rules for good cyber ethics explained in a layman way:

- Be Kind Online: Treat others on the internet the way you want to be treated.
- Respect Privacy: Don't share personal information about yourself or others without permission
- Be Honest: Don't lie or pretend to be someone you're not online.
- Give Credit: When you use someone else's work, like a picture or a quote, give them credit by mentioning their name .

**Q16. Illustrate the motives behind the cybercrimes. ?**

Ans - The motives behind cybercrimes can be explained in a very short way:

- Stealing: Bad guys want to take things that don't belong to them, like money or personal information.
- Causing Trouble: Some people enjoy causing mischief and making others unhappy or confused.
- Spying: Bad guys want to see what others are doing or saying without permission, like peeking into their private lives.
- Seeking Power: Some people want to gain control over others or feel powerful by manipulating technology or causing chaos.

**Q17. List out the key elements of information security. ?**

Ans - Here are the key elements of information security in very short terms:

- Confidentiality: Keeping information private and only accessible to authorized individuals.
- Integrity: Ensuring that information is accurate, complete, and trustworthy.
- Availability: Making sure information is accessible to authorized users when needed.
- Authentication: Verifying the identity of individuals or systems to prevent unauthorized access.

**Q18. List out the two approaches of ethics in cyber law ?**

Ans - The two approaches of ethics in cyber law can be summarized concisely:

- Deontological Approach: This approach focuses on following ethical rules and principles. It emphasizes moral duties and obligations, regardless of the consequences.
- Consequentialist Approach: This approach looks at the consequences or outcomes of actions to determine their ethical nature. It considers the overall impact and seeks to maximize positive outcomes while minimizing negative ones.

**Q19. Sketch the primary precaution steps after security attack?**

Ans - After a security attack, here are the primary precaution steps in very short terms:

1. Stay Calm 2.) Disconnect 3.) Notify an Adult 4.) Report 5.) Change Passwords 6.) Update Security Software 7.) Learn from the Experience.

**Q20. What is fair use in cyber space ?**

Ans - Fair use in cyber space means that you can use someone else's work, like a picture or a video, without getting permission, but only in certain cases. It's like borrowing a toy from a friend for a little while, as long as you use it for a good reason, like for education, criticism, or news reporting. Fair use allows us to share and use things in a fair and limited way, respecting the original creator's rights.

**SECTION B**

**Q21. What are the major cybercrimes that are done frequently in digital world ?**

**Ans -** In the digital world, there are major cybercrimes that happen frequently. Here are some of them explained in an easy and short way:

- Hacking: Bad guys try to break into computers or networks to steal information or cause harm, like sneaking into a secret hideout.
- Phishing: Tricky bad guys pretend to be someone else, like a friend or a company, to trick people into giving them personal information, like a secret password or a valuable treasure.
- Identity Theft: Bad guys steal someone's personal information, like their name and bank details, to pretend to be them and do bad things, like pretending to be a superhero but for the wrong reasons.
- Online Scams: Sneaky bad guys try to trick people into giving them money or valuable things, like pretending to sell something but never delivering it, just like selling a toy but never giving it to the buyer.
- Cyberbullying: Mean bad guys use the internet to bully or harass others, like saying mean things or spreading rumors, but doing it online instead of face-to-face.

**Q22. Analyse the best practices & challenges in cyber security. ?**

**Ans -** Best Practices in Cybersecurity (Layman Terms):

- Use Strong Passwords: Use passwords that are hard to guess, like a secret code, to protect your accounts.

- Keep Software Updated: Regularly update your devices and software to fix any security vulnerabilities, like getting a superhero upgrade for your computer.
- Be Cautious Online: Avoid clicking on suspicious links or downloading unknown files, just like avoiding unknown candies that may not be safe to eat.

Challenges in Cybersecurity:-
- Sophisticated Attacks: Bad guys are becoming smarter and using advanced techniques to carry out cyberattacks, like villains with new tricks up their sleeves.
- Human Error: People can unintentionally make mistakes, like clicking on harmful links or sharing sensitive information, which can lead to security breaches.
- Lack of Awareness: Many people may not be aware of the risks and best practices in cybersecurity, like not knowing about the dangers that exist in the digital world.

**Q23. Analyse the cyber terrorism and how to tackle risks of cybercrime. ?**

**Ans -** Cyber terrorism is when bad guys use computers and the internet to cause harm and create fear, just like villains who want to make people scared. They might try to attack important systems, like power plants or government websites, to disrupt things and make people feel unsafe.

Here are a few things they do to keep us safe:

- Building Strong Defences: They create strong walls and shields, like installing firewalls and antivirus software, to protect our devices and networks from cyber threats.
- Investigating and Catching Bad Guys: They work like detectives to find the bad guys behind cybercrimes and stop them from doing more harm.
- Educating and Raising Awareness: They teach us how to stay safe online, like telling us not to share personal information with strangers and to be careful when clicking on links or opening emails from unknown sources.
- Creating Rules and Laws: They help make rules and laws to punish cybercriminals and make the digital world a safer place for everyone.

**Q24. Analyse the various types of cyber-attacks. ?**

- Virus Attack: It's like a sneaky bug that gets into your computer and makes it sick. It can spread from one computer to another and cause a lot of trouble.
- Phishing Attack: Imagine someone pretending to be a friend and asking for your favorite toy. In the digital world, bad guys pretend to be someone else to trick you into sharing your personal information, like passwords or addresses.
- Denial-of-Service (DoS) Attack: It's like a big crowd of people blocking the entrance to a playground so no one can go in. In the digital world, bad guys send lots of requests to a website at once, making it crash and preventing others from using it.
- Ransomware Attack: It's like a digital kidnapper who locks up your favorite toy and asks for money to give it back. Bad guys use special software to encrypt your files, making them inaccessible until you pay a ransom.
- Social Engineering Attack: It's like someone using their charm or tricks to convince you to give them your toy. In the digital world, bad guys manipulate people into sharing sensitive information .

**Q25. Define Trojan horse. ?**

**Ans -** A Trojan horse is like a pretend toy that looks fun and nice, but it's actually sneaky and can cause trouble. It's like a toy robot that seems friendly, but when you turn it on, it starts doing things it's not supposed to. In the digital world, a Trojan horse is a special kind of computer program that pretends to be something good or interesting, like a game or a cute picture. But when you download or open it, it can do bad things to your computer or steal your information without you knowing.So, just like you wouldn't play with a toy that might hurt you, we need to be careful with things we download or open on our computers and make sure they are safe and trusted.

**Q26. Demonstrate about Encryption techniques ?**

**Ans -** Encryption is like turning your secret message into a secret code that only you and your friend can understand. It's like having a special language that no one else knows.When we use encryption, we take our message and use a special key to scramble the letters and numbers. It's like mixing up puzzle pieces. Only the person with the right key can unscramble the message and read it.So, if someone tries to peek at your secret message, all they see is a jumble of letters and numbers that make no sense. It keeps your message

safe and private, just like hiding a treasure in a secret box that only you and your friend can open.Encryption helps us protect our important information, like passwords or messages, from people who shouldn't see them. It's like having a secret code that keeps our secrets safe!

**Q27. Describe in detail about the ethical principles and its process of cyber ethics. ?**

**Ans -** Here are some ethical principles in cyber ethics explained in a short and simple way for a baby:

- Be Kind: Treat others online the way you want to be treated. Use nice words and don't say mean things to others. Just like you share your toys and play nicely with friends, we should be kind to others on the internet too.
- Be Honest: Always tell the truth and don't lie or pretend to be someone you're not. Just like you would tell the truth to your friends and family, we should be honest when using computers and the internet.
- Respect Others' Privacy: Everyone has the right to keep their personal information private. Don't share someone's secrets or personal things without their permission. Just like you respect someone's privacy by not peeking into their diary, we should respect others' privacy online too.
- Ask for Permission: Always ask for permission before using someone else's things, like pictures or words. Just like you would ask your friend if you can borrow their toy, we should ask for permission before using things on the internet that belong to someone else.
- Be Responsible: Take care of your own actions and think before you click or share things online. Don't do things that could hurt others or yourself. Just like you take care of your toys and make sure you don't break them, we should be responsible when using computers and the internet.

**Q28. Describe the detailed the phases of cyber forensics ?**

1. Collecting Evidence: Investigators gather clues and collect evidence, just like detectives collecting puzzle pieces. They look for things like pictures, messages, or logs on computers or devices.
2. Analyzing Evidence: Investigators carefully examine the evidence they collected. It's like putting the puzzle pieces together to see the bigger picture. They try to understand what happened and who might be responsible.
3. Identifying Suspects: Based on the evidence, investigators try to figure out who might have done the bad things. It's like finding the person who broke a toy or made a mess.
4. Tracking Digital Footprints: Investigators follow the "digital footprints" left by the bad guys. It's like following footprints in the sand to find out where someone went. They trace the actions of the suspects in the digital world.
5. Reporting Findings: Investigators write a report explaining what they found and share it with others, like teachers or parents. They help people understand what happened and what actions need to be taken.

**Q29. Describe the state the current young generation aware about the cyber technology. ?**

**Ans -** The current young generation is very familiar with cyber technology. They have grown up with computers, smartphones, and the internet. It's like they have always had these things as part of their lives, just like you have always had toys to play with.They know how to use apps, play games, and find information online. They are like little experts in the digital world! They can navigate websites, send messages, and even create their own videos or pictures.But it's also important for them to learn about the risks and be safe while using technology. Just like you need to be careful and not touch things that can hurt you, they need to be cautious about sharing personal information, talking to strangers online, or clicking on unknown links.Parents and grown-ups are there to guide and teach them about being responsible and making good choices in the digital world, just like they guide and teach you in the real world.So, the current young generation is very aware of cyber technology and they are growing up with amazing opportunities and new ways to learn and connect with others. They are like little digital superheroes!

**Q30. Discuss the technology development in cybercrime ?**

**Ans -** Technology development in cybercrime means that bad guys are using new and fancy tools to do bad things on computers and the internet. It's like they have new toys that help them do naughty things.Just like you have cool toys to play with, bad guys have special computer programs and tricks that they use to steal information or cause problems for others. They try to find ways to break into computers and do things they're not supposed to.But don't worry, there are good guys too! Just like superheroes, there are people called cybersecurity experts who work hard to stop the bad guys. They use their own clever tools and tricks to catch the bad guys and keep us safe.So, even though bad guys might have cool toys, the good guys are always working to outsmart them and protect us from their tricks. It's like a game of good versus bad in the digital world!

**Q31. Examine the difference between a virus and worm and explain in details ?**

**Ans -** A virus and a worm are both bad things in the computer world, but they are a little different.A virus is like a tiny bug that can make your computer sick. It gets inside your computer by attaching itself to other files, just like a bug sticks to your clothes. When you open those infected files, the virus starts causing trouble. It can make your computer slow, delete important things, or even make it stop working.A worm, on the other hand, is like a sneaky creature that can move around on its own. It doesn't need to attach itself to other files like a virus does. It can travel from one computer to another, like a little explorer. When it finds a new computer to visit, it copies itself and starts causing mischief. It can steal information or make the computer act strangely.

**Q32. Explain Denial of Service & DNS Spoofing ?**

**Ans -** Denial of Service and DNS Spoofing are two tricky things that can cause problems in the computer world, but let's break them down in simple terms for a baby:

1. Denial of Service: Imagine you have a toy that you love playing with, but suddenly someone takes it away and hides it from you. That's what happens with a Denial of Service attack. Bad guys try to overwhelm a website or a computer by sending too much information or requests all at once. It's like sending so many messages or requests that the computer gets confused and can't handle them all. This makes the website or computer stop working for a while, like when you can't play with your toy because it's taken away.
2. DNS Spoofing: Have you ever played a game of pretending to be someone else? That's what happens with DNS Spoofing. Every website has an address called a URL, and it's like the house number of a website. When you type a website's name, your computer asks a special server called DNS to find the correct address. But with DNS Spoofing, bad guys trick your computer into going to the wrong address. It's like someone tells you the wrong house number, and you end up going to the wrong friend's house instead of the right one.

**Q33. Illustrate the classification between cyber forensics and investigation. ?**

1. Cyber Forensics: Imagine you're playing with your favorite toy, but suddenly it breaks or stops working. What do you do? You become a detective and investigate what happened to your toy. Cyber forensics is like being a detective in the computer world. When something bad happens, experts use special tools and skills to collect clues, just like puzzle pieces, from computers and devices. They carefully analyze these clues to understand what happened and who might be responsible. It's like solving a mystery to find out the truth.
2. Investigation: Sometimes, when something naughty happens, like when you find your crayons scribbled on the walls, you want to find out who did it. That's where investigation comes in. Investigators ask questions and gather information to find the person who did something wrong. In the computer world, investigators use their skills and knowledge to track down the bad guys. They might talk to people, look at records, or even use special tools to find out who did the naughty things.

**Q34. Shortlist the characters of cyber criminals. ?**

1. Hackers: Hackers are like sneaky magicians who use their computer skills to break into other people's computers or websites. They can do things they're not supposed to, like stealing information or causing mischief. They try to find ways to get past security and access things that belong to others.
2. Phishers: Phishers are like tricky fishermen who use clever tactics to catch your personal information. They send messages or emails pretending to be someone else, like a friend or a company you know. They try to trick you into giving them your passwords, credit card numbers, or other private things.
3. Scammers: Scammers are like pretend friends who try to trick you into giving them money or valuable things. They might create fake websites or call you on the phone, pretending to offer something exciting or asking for your help. But their real intention is to deceive and take advantage of you.
4. Spammers: Spammers are like annoying bees that send lots of unwanted messages to your computer or email. They try to sell you things you don't need or send you messages that are not nice. Their goal is to get your attention and make you click on things you shouldn't.

**Q35. Summarize about the term CIA Traid and its fundamentals function.?**

**Ans -** The term "CIA Triad" refers to three important things that help keep information safe in the digital world. Let's understand it in simple terms:

1. Confidentiality: This is about keeping things a secret, just like when you have a surprise gift for someone and you don't want them to know what it is. In the digital world, it means protecting information so that only the right people can access it. For example, using a password to keep your tablet or computer locked and secure.
2. Integrity: This is about making sure things are accurate and not changed without permission, just like when you draw a beautiful picture and want it to stay the same. In the digital world, it means making sure that information doesn't get tampered with or altered by bad guys. For example, using special techniques to ensure that a message or a file hasn't been changed along the way.
3. Availability: This is about making sure things are accessible when you need them, just like having your favorite toy ready to play with. In the digital world, it means ensuring that information and services are available and can be accessed by the right people at the right time. For example, making sure a website is always up and running so that you can visit it whenever you want.

**Q36. Summarize the cyber defamation and discuss the major threats of cyber-crimes in current scenario on Business ?**

**Ans -** Cyber defamation is when someone says mean or untrue things about others on the internet. It's like spreading hurtful rumors or lies about someone using digital tools.

In the current business world, there are some major threats of cyber-crimes that can cause trouble:

1. Phishing: This is when bad guys try to trick businesses into giving away important information, like passwords or financial details. It's like pretending to be a customer or a trusted partner to gain access to sensitive information.
2. Data breaches: This happens when someone unauthorized gets into a company's computer systems and steals important data, like customer information or trade secrets. It's like a thief breaking into a company's vault and taking valuable things.
3. Ransomware: This is a type of attack where bad guys lock a company's computer files and demand money to release them. It's like someone putting a digital lock on a company's files and asking for a ransom to unlock them.
4. Business email compromise: This is when bad guys impersonate important people in a company, like the CEO or a manager, and trick employees into doing something harmful, like transferring money to the wrong account. It's like a pretend boss giving orders to do something wrong.

These cyber-crimes can harm businesses by causing financial losses, damaging reputations, and affecting customer trust. It's important for businesses to be aware of these threats and take precautions, like using strong passwords, training employees about cyber risks, and having good security measures in place.

**Q37. What are the types of cyber-attacks possible on mobile phones?**

**Ans -** There are several types of cyber-attacks that can happen on mobile phones. Let's learn about them in simple terms:

1. Malware: This is like a naughty software that can get into your phone and cause trouble. It can steal your personal information, make your phone slow, or even take control of it.
2. Phishing: This is when someone tries to trick you into sharing your personal information, like passwords or credit card details, by pretending to be someone else. They might send you fake messages or emails that look real.
3. Smishing: This is similar to phishing, but it happens through text messages (SMS). Bad guys might send you a text pretending to be from a bank or a company, asking for your personal information.
4. Wi-Fi Hacking: When you connect to public Wi-Fi networks, there's a risk that hackers might try to get into your phone and steal your information. They can set up fake Wi-Fi networks that look real to trick you.
5. App Vulnerabilities: Some apps on your phone might have weaknesses or security flaws that hackers can exploit. They can use these vulnerabilities to gain access to your personal data or control your phone.

**Q38. What do you understand by the salient features of Indian IT act?**

**Ans -** The Indian IT Act, also known as the Information Technology Act, has some important features that help regulate and protect digital activities in India. Let's understand them in simple terms:

1. Legal Recognition of Electronic Documents: The IT Act gives legal recognition to electronic documents, which means that electronic records and digital signatures are considered valid and enforceable, just like paper documents and physical signatures.
2. Cyber Crimes and Offenses: The Act defines various cyber crimes and offenses, such as unauthorized access, hacking, data theft, and spreading viruses or malware. It outlines penalties and punishments for those who commit such offenses.
3. Digital Signatures: The Act recognizes digital signatures as a way to authenticate and verify electronic documents. Digital signatures are like special codes or symbols that ensure the integrity and authenticity of electronic records.
4. Privacy and Data Protection: The IT Act includes provisions for protecting personal information and privacy in the digital realm. It lays down rules and regulations for the collection, use, and disclosure of personal data by individuals and organizations.
5. Cyber Security Measures: The Act establishes mechanisms for ensuring the security of computer systems and networks. It empowers the government and law enforcement agencies to take necessary steps to prevent and investigate cyber threats.

**Q39. What is Logic Bomb. ?**

**Ans -** A logic bomb is a type of malicious software that is like a hidden time bomb in a computer program. Let's understand it in simple terms:Imagine you have a special toy that has a secret code inside. When a certain condition is met, like a specific date or time, the toy will do something unexpected or bad. That's similar to how a logic bomb works.In the digital world, a logic bomb is like a secret code hidden in a computer program. It's set to activate and cause harm or do something bad when a specific condition is met. For example, it could be programmed to delete important files or cause the computer to stop working properly.The idea behind a logic bomb is to cause damage or disrupt things at a specific time or under certain circumstances. It's like a sneaky trick that waits quietly until it's time to create trouble.

**Q40. Write a note on cyber law and describes its advantages and disadvantages. ?**

**Ans -** Cyber law is a set of rules that help govern and regulate activities in the digital world. Here are its advantages and disadvantages, explained in simple terms:

**Advantages of Cyber Law:**

1. Protection against cybercrimes: Cyber law helps catch and punish people who commit cybercrimes like hacking, identity theft, and online fraud. It makes the internet a safer place.
2. Safeguarding personal information: Cyber law ensures that your personal information is protected online. It prevents unauthorized access and makes sure companies handle your data responsibly.
3. Protecting ideas and creations: Cyber law helps artists and inventors protect their work online. It stops others from stealing or copying their music, videos, or inventions without permission.

**Disadvantages of Cyber Law:**

1. Challenges in enforcing the law: Catching and punishing cybercriminals can be difficult, especially if they are in different countries. It's challenging to apply the law globally.
2. Evolving technology: Cyber law needs to keep up with rapidly advancing technology. New threats emerge as technology evolves, and updating the law can be a challenge.
3. Balancing privacy and security: Sometimes, cyber law may need to balance privacy and security concerns. It's important to find the right balance to protect people's privacy while ensuring security measures are in place.

**Section C**

**Q41. Elaborate phishing and explain the methods & counter measures of phishing. ?**

**Ans -** Phishing is a type of online scam where attackers try to trick you into revealing sensitive information like passwords, credit card numbers, or personal details. They usually do this by pretending to be a trustworthy entity, such as a bank, email provider, or online service.

Phishing methods can vary, but here are some common ones:

1. Email Phishing: Attackers send fake emails that appear to come from legitimate sources. These emails often contain urgent messages, asking you to click on a link or provide personal information.
2. Website Phishing: Attackers create fake websites that look identical to legitimate ones, tricking you into entering your login credentials or financial information.
3. Smishing: Attackers send fraudulent text messages that contain links or ask you to reply with personal information.

Countermeasures to protect yourself from phishing include:

1. Be vigilant: Be cautious of unsolicited emails or messages that ask for personal information. Avoid clicking on suspicious links or downloading attachments from unknown sources.
2. Verify the source: Double-check the sender's email address or the website URL to ensure they are legitimate. Pay attention to slight variations or misspellings.
3. Don't share sensitive information: Avoid sharing personal or financial information through email or text messages. Legitimate organizations usually don't request such information via these channels.
4. Keep software up to date: Regularly update your operating system, web browser, and antivirus software to patch any security vulnerabilities.
5. Enable multi-factor authentication (MFA): Use MFA whenever possible, which adds an extra layer of security by requiring you to provide a second form of verification, such as a code sent to your phone, in addition to your password.
6. Educate yourself: Stay informed about common phishing techniques and scams. Be aware of the latest phishing trends and learn how to spot warning signs.

**Q42. Describe criminalization of online speech and social media ?**

**Ans -** Criminalization of online speech refers to the process of making certain types of speech or expression on the internet illegal and punishable by law. This can include content shared on social media platforms.In simpler terms, when online speech is criminalized, there are laws in place that say you can get into trouble or face legal consequences for what you say or post online.The purpose of criminalizing online speech is to prevent harm, protect individuals' rights, and maintain a safe and respectful online environment. However, it can also raise concerns about freedom of expression and censorship.It's important to note that the specifics of what is considered illegal can vary from one country to another, as laws and regulations differ globally.To navigate this, it's crucial to familiarize yourself with the laws and guidelines regarding online speech in your country. Additionally, being respectful, mindful, and responsible in your online interactions can help avoid potential legal issues.

**Q43. Discuss the new trends in research on cybercrime and compare traditional criminal activity with cyber-crime ?**

**Ans -** In research on cybercrime, new trends focus on studying the latest methods used by criminals online. Researchers want to understand how cybercriminals operate, why they do what they do, and the impact of their actions.Comparing traditional criminal activity to cybercrime is like comparing crimes that happen in the physical world to crimes that occur in the digital world.Traditional criminal activity refers to crimes like theft or assault that happen offline, involving physical interactions and targeting individuals or property.Cybercrime involves criminal activities that happen online using computers or the internet. It includes things like hacking, stealing personal information, or spreading harmful software.The main difference is that traditional crimes happen in the physical world, while cybercrimes happen in the digital space. But both types of crimes can have serious consequences and harm people, organizations, and society.One important distinction is that cybercriminals can operate from anywhere and stay anonymous, making it harder to catch them. Cybercrimes can also affect people worldwide without the criminal needing to be physically present.Researchers are studying these differences and finding ways to prevent and fight cybercrime effectively. They want to develop strategies and technologies that improve cybersecurity, protect people's digital information, and make the online world safer for everyone.

**Q44. Elaborate the various legal provision in Indian perspective with the contemporary challenges of the cyber space ?**

**Ans -** In India, there are various legal provisions that deal with cybercrimes and govern activities in the digital world. These laws are designed to safeguard individuals, organizations, and the overall security of the

online space. However, there are contemporary challenges that need to be addressed. Let's explore this in simple terms:

1. Information Technology Act, 2000: This is the primary law that deals with cybercrimes in India. It defines offenses like hacking, identity theft, and data breaches, and provides legal measures to investigate and prosecute such crimes.**Contemporary challenge: The rapid advancement of technology has resulted in emerging cyber threats that require constant updates to the law to effectively tackle new forms of cybercrimes.
2. Indian Penal Code, 1860: While not specific to cybercrimes, the IPC includes provisions that can be applied to certain cyber offenses. For example, sections related to cheating, forgery, and defamation can be used to address online crimes as well.**Contemporary challenge: Traditional laws may not fully cover the complexities and nuances of cybercrimes, making it necessary to have specialized legislation.
3. Aadhaar Act, 2016: This act governs the use of the Aadhaar identification system in India, ensuring the security and privacy of individuals' biometric and demographic information.**Contemporary challenge: Safeguarding personal data and privacy in the digital age requires constant adaptation to evolving technology and sophisticated cyber threats.
4. Personal Data Protection Bill: This bill, currently in the drafting stage, aims to establish comprehensive data protection regulations in India. It seeks to protect individuals' personal data and regulate its processing by both government and private entities.**Contemporary challenge: Balancing the need for data protection while fostering innovation and digital economy growth is a complex task that requires careful deliberation.
5. Cyber Appellate Tribunal: It is an adjudicating body that deals with appeals against decisions made by the Controller of Certifying Authorities and other authorities under the IT Act.**Contemporary challenge: The need to establish specialized cybercrime courts or a dedicated judicial framework to handle cybercrime cases efficiently and expeditiously is an ongoing concern .

**Q45. Evaluate in details the public key functioning and protection provided by it under the electronic signature. ?**

**Ans -** Sure! Public key functioning and protection are essential components of electronic signatures. Here's a simplified explanation of how they work:

Public key functioning :-

- Public key: Imagine you have a box with two keys - a lock key and an unlock key. The lock key is your public key, which is freely available to anyone who wants to send you a secure message or verify your electronic signature.
- Private key: The unlock key is your private key, which you keep secret and only use to open messages or create electronic signatures.
- Encryption: When someone wants to send you a secure message or validate your electronic signature, they use your public key to encrypt the information. Once encrypted, only your private key can decrypt or unlock the message.
- Verification: To ensure the authenticity and integrity of an electronic signature, the recipient uses the sender's public key to verify that the signature matches the original message. If they match, it means the signature is valid and the message hasn't been tampered with.

Protection provided :-

- Security: The private key is kept secure and only accessible to the owner. It's important to protect the private key from unauthorized access or disclosure to maintain the integrity of the electronic signature.
- Authentication: Public key functioning allows for reliable authentication. By using the sender's public key, the recipient can verify the identity of the sender and ensure that the message or signature comes from the expected source.
- Integrity: Public key functioning helps ensure the integrity of the message or document. If anyone tries to tamper with the content, the verification process will fail, indicating that the message has been altered.

**Q46. Examine in detail about the mode and methods of committing cyber-crimes ?**

**Ans -** Cybercrimes encompass a range of illicit activities committed using computers, networks, or the internet. These crimes are perpetrated through various methods, each with its own approach and objective. Here are some common methods of committing cybercrimes:

- Hacking: Hackers use their technical expertise to exploit vulnerabilities in computer systems or networks. They gain unauthorized access to steal sensitive data, manipulate information, or disrupt operations.
- Malware Attacks: Cybercriminals create and distribute malicious software, such as viruses, worms, or ransomware. These programs infect computers and networks, enabling attackers to gain control, steal information, or extort money from victims.
- Identity Theft: Criminals engage in identity theft by unlawfully obtaining personal information, such as social security numbers, credit card details, or login credentials. They use this stolen data to assume someone else's identity, commit financial fraud, make unauthorized purchases, or gain access to sensitive accounts.
- Phishing: Phishing involves the use of deceptive emails, messages, or websites that appear legitimate to trick individuals into revealing their personal information. Attackers often impersonate trusted entities, such as banks or popular online services.
- Social Engineering: Social engineering is a manipulation technique where cybercriminals exploit human psychology to deceive individuals.
- Distributed Denial of Service (DDoS) Attacks: DDoS attacks aim to overwhelm a website or network by flooding it with an enormous amount of traffic. This flood of traffic makes the targeted service inaccessible to legitimate users..
- Online Scams: Cybercriminals create fraudulent websites, online marketplaces, or deceptive advertisements to deceive individuals.

**Q47. Explain difference between rights and responsibility in cyber world. ?**

**Ans -** In the cyber world, there is a distinction between rights and responsibilities. Here's a simplified explanation of the difference:

Rights: In the cyber world, rights refer to the entitlements and freedoms that individuals have while using digital platforms and engaging in online activities. These rights are similar to the rights we have in the physical world. For example:

- The right to privacy: The right to keep personal information secure and control who has access to it.
- Freedom of expression: The right to express opinions and thoughts freely online, within legal limits.
- Access to information: The right to access and seek information online, promoting knowledge and education.
- Intellectual property rights: The rights of creators and innovators to protect their original works, such as music, art, or inventions.

Responsibilities: On the other hand, responsibilities in the cyber world refer to the obligations and ethical considerations that individuals have while using digital platforms and engaging in online activities. Responsibilities help ensure a safe and respectful online environment. For example:

- Respect for others' rights: Respecting the privacy, opinions, and intellectual property of others.
- Online etiquette: Practicing good behavior, politeness, and respectful communication in online interactions.
- Cybersecurity: Taking measures to protect personal information, using strong passwords, and avoiding engaging in harmful activities.
- Digital literacy: Being responsible and informed users of technology, understanding the risks and consequences of online actions.

**Q48.Explain the information system resources and activities and what may be the reason of failure of it. ?**

**Ans -** Information system resources and activities refer to the components and processes involved in managing and utilizing information within an organization. Here's a simplified explanation:

Information System Resources:

- Hardware: Physical devices like computers, servers, and networking equipment that store and process data.

- Software: Programs and applications that enable various tasks, such as data management, communication, and analysis.
- People: Individuals who interact with the system, including users, administrators, and IT support staff.

Information System Activities:

- Data Input: Capturing and entering data into the system, often through forms, sensors, or manual input.
- Data Processing: Manipulating and analyzing data to derive insights, generate reports, or perform calculations.
- Data Storage: Storing and organizing data in databases or other storage systems to ensure easy retrieval and accessibility.
- Data Output: Presenting processed data in a usable format, such as reports, graphs, or visualizations.

Reasons for Failure: Several factors can contribute to the failure of information systems:-

- Technical Issues: Hardware or software malfunctions, system crashes, or compatibility problems that disrupt the functioning of the system.
- Human Error: Mistakes made during data entry, processing, or maintenance that result in incorrect or corrupted data.
- Security Breaches: Unauthorized access, data breaches, or cyberattacks that compromise the confidentiality, integrity, or availability of information.
- Lack of Training or User Awareness: Insufficient training or awareness among users can lead to improper system usage, errors, or vulnerabilities.

**Q49. Explain the liability aspects of the internet service provider as per the information technology act, 2000.?**

**Ans -** Under the Information Technology Act, 2000, internet service providers (ISPs) have certain liability aspects. Here's a simplified explanation of those aspects in layman terms:

- Safe Harbor Provision: The Information Technology Act provides a safe harbor provision for ISPs. This means that ISPs are not held legally responsible for the content transmitted or hosted by their users. They are considered intermediaries that facilitate the transmission of information.
- Limited Liability: ISPs are not liable for any illegal or harmful content shared or posted by their users unless they have specific knowledge of the content and fail to take action to remove or block it. However, ISPs have a duty to promptly remove or disable access to any illegal content upon receiving a complaint or notification.
- Obligations for Data Retention: ISPs may be required to retain certain user data for a specific period as prescribed by the government or regulatory authorities. This is to assist in investigations and enforcement of laws.
- Cooperation with Law Enforcement: ISPs are expected to cooperate with law enforcement agencies and provide assistance in their investigations. They may be required to disclose user information or assist in the identification of offenders involved in cybercrimes.
- Cybersecurity Measures: ISPs are expected to take reasonable security measures to protect the data and information transmitted through their networks. This includes implementing safeguards against unauthorized access, data breaches, and other security threats.

**Q50. How freedom of speech and expression performs in social media platforms?**

Ans - Freedom of speech and expression on social media platforms allows individuals to express their thoughts, opinions, and ideas publicly. Here's a simplified explanation of how it works:Social media platforms provide a space for people to share their views and engage in discussions with others. Users can post text, photos, videos, and other content to express themselves and communicate with a wide audience.However, there are some limitations to freedom of speech on social media platforms. The platforms have their own rules and guidelines that users must follow. These rules are in place to prevent harmful or illegal content, such as hate speech, threats, or harassment.If users violate these rules, their content may be flagged or removed by the platform, and they may face consequences like temporary or permanent suspension of their accounts.While social media platforms aim to balance freedom of speech with maintaining a safe and inclusive environment, there can be debates and controversies surrounding the enforcement of these rules. Platforms often face challenges in moderating content and addressing concerns related to misinformation, privacy, and the spread of harmful content.It's important for users to be aware of and respect the platform's guidelines while expressing themselves on social media. Responsible and respectful communication can help maintain a positive online community where diverse perspectives can be shared and heard.