COMPUTER SCIENCE

Grade: XI

INFORMATION SECURITY AND CYBER LAW

REFERENCE NOTE

Unit Wise Important Questions for Computer Science XI

Unit 8- Information Security and Cyber Law

1) ***What do you mean by Information Security? Explain.***
2) ***What is computer ethics? Explain.***
3) Explain the terms of software piracy, Plagiarism and Pornography.
4) ***What is digital divide? What is its effects on modern society?***
5) ***What is cyber-crime? Explain its different forms.***
6) Write Short notes on:
   a) Cyber Law b) Computer Virus c) Digital Signature d***) Malware*** ***e) Cryptography***

Unit 8- Information Security and Cyber Law

8.1 Digital Society and Computer ethics

Digital Society:

Digital Society is an interdisciplinary research area and a kind of progressive society that has been formed as a result of adaptation as well as integration of advanced technologies into the society and culture. *Digital Society deals with the highly advanced telecommunications and wireless connectivity systems and solutions.* The latest Digital Society includes Internet of Things (IoT), 5G, Cloud Computing, Big Data, Human Computer Interaction and so on.

Some of the benefits of Digital Society are:

a. Social connectivity
b. Communication Speed
c. versatile working
d. Learning Opportunities
e. Entertainment.

ICT (Information Communication Technology)

Information System is, which is used to communicate through any medium or by using technology, is called information communication technology. Information Communication Technology (ICT) literally used to clarify its meaning, which refers to the merging of telephone networks with computer networks. Information Technology (IT) is the study, design, development, implementation, support or management of information systems.

Social Impact of the ICT

POSITIVE Impact of ICT:

- Create opportunity for technical employment:
- E-Commerce
- Fast and Cheap Communication
- Education
- Health Care
- Multimedia Presentation

NEGATIVE Impact of ICT:

- Number of Employment Opportunity will Reduced
- Health Problem
- Money Theft
- Digital Divide
- Possibility of Leakage, hacked and Disclosure of Personal Information
- Pornography

Digital Divide:

Digital Divide refers to the gap between individuals, households, business and geographic areas at different socio- economic levels with regard with the opportunity to access Information and Communication Technology (ICT) in the Internet using computers and many other mobile computing devices such as tablet PC, PDA, mobile etc.

Computer Ethics:

The word 'ethics' means 'moral' beliefs and rules about right and wrong. Thus, computer ethics also refers to the responsible use of computers and computer networks. It is a branch of practical. Ethics deals with placing a value on acts according to whether they are good or bad.

Commandments:

1. Do not use a computer to harm other people
2. Do not interfere with other people's computer work
3. Do not snoop or view around in other people's files
4. Do not use a computer to steal
5. Do not use or copy software for which you have not paid
6. Do not use other people's computer resources without authorization
7. Think about the social consequences of the program you write Use a computer in ways that show consideration and respect

Objectives of Computer Ethics

1. To ensure the privacy and safety of computer users.
2. To help people use the computer in the right ways.
3. To guarantee that works done by someone did not declare by other people.

8.2 Concept of Information Security

Information security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information is anything that holds value for its receiver. Information Security programs are built around 3 objectives, commonly known as CIA (Confidentiality, Integrity, Availability).

Confidentiality:

Confidentiality refers to protecting information from disclosure. Information should not be revealed to unauthorized users.

Integrity:

Integrity refers to ensuring that the data or information is not corrupted or modified by unauthorized users.

Availability:

Availability of data or information means that the data or information is available for use whenever required. This essentially means placing security system in order to prevent the destruction or theft of information.

- **Network Security:**

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure.

- **Security Threat:**

Security threat is a possible danger that might exploit vulnerabilities in a computer system to breach security and thus cause possible harms. Vulnerability is a weakness of flaw in a computer system that can be exploited by a threat. **Types of security threats**

1. ***Interception:*** *It refers to the situation that an unauthorized party has gained access to a service or data.*
2. ***Interruption:*** *It refers to the situation in which services or data become unavailable, unusable, destroyed, and so on.*
3. ***Modification:*** *It involve unauthorized changing of data or tampering with a service so that it no longer adheres to its original specifications.*

4. ***Fabrication:*** *It refers to the situation in which additional data or activities are generated that would normally not exist.*

❖ **Security Threat:**

An attack is an attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset.

i. ***Passive attack:*** An attack that attempts to learn or make use of information from the system but does not affect system resources.

ii. ***Active attack:*** An attack that attempts to alter system resources or affect their operation.

❖ **Security Services:**

Security services is a services provided by a layer of communicating open systems, Which ensures adequate security of the systems or of data transfers.

Types of Security Services.

i. Authentication:

ii. Authorization:

iii. Data confidentiality:

iv. Data integrity:

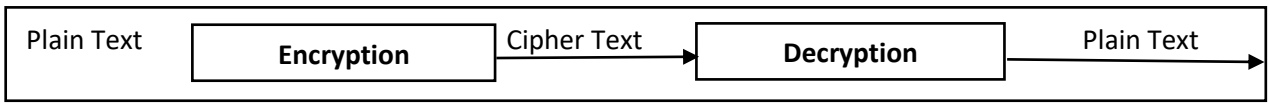
v. Non- repudiation:

❖ **Cryptography:**

Cryptography is the science of providing security for information. Cryptography means secret writing and is the art and science of information hiding.

Cryptography was mostly referred to as encryption and decryption. **Encryption** is the mechanism to convert the readable *plaintext* into unreadable text by using some algorithm and key.

Decryption is the opposite or reverse process of encryption. It converts *cipher text* back to the *plaintext* by using some algorithm or key. Alternatively the term *encode* and *decode* or *encipher* and *decipher* are used instead of ***encrypting*** and ***decrypting***.



8.3 Cyber-Crime:

Cyber-crime refers to the use of computer technology for illegal purposes or for unauthorized access of a computer system where the intent is to damage, delete or alter the data present in the computer. There are many types of cyber-crimes committed. Some of them are discussed below: ***Types of cyber-crime***

1. **Cyber stalking:** Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, group, or organization.
2. **Cyber terrorism:** Cyber terrorism is a terrorist activity intended to damage or disrupt vital computer systems. Cyber theft Cyber theft is the act of using an internet to steal someone's property or to interfere with someone's use and enjoyment of property.
3. **Hacking:** Hacking is the process of exploiting vulnerabilities to gain unauthorized access to systems or resources.
4. **Phishing:** Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
5. **Computer Virus:** Computer virus is a computer program that can replicate themselves and harm the computer systems on a network without the knowledge of the system users.
6. **Identity Theft:** Identity theft is the crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity to make transactions or purchases.
7. **Software piracy**: Software piracy is the illegal copying, distribution, or use of software.

8. **Cyber contraband:** Cyber contraband is the process of transferring illegal items through the internet (such as encryption technology) that is barred in some locations.
9. **Cyber extortion:** A crime involving an attack or threat of an attack coupled with the demand for money to stop the attack. Example, Ransomware attack.
10. ***Exit Scam:*** The dark web, not surprisingly, has given rise to the digital version of an old crime.
11. ***Cyberespionage:*** A crime involving a cybercriminal who attack into systems or networks to gain access to confidential information held by a government or other organization. Example, CCTV, Webcams, e-mails etc.
12. ***Crypto jacking:*** An attack that uses scripts to mine cryptocurrencies within browsers without the user's consent.

8.4 Malicious Software and Spam

Malicious software, commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, Trojans etc.

Computer viruses are the programs or malware which are loaded onto your computer by 'mean' people, without your knowledge. These viruses replicate relentlessly and infect computer programs. They might even delete or corrupt your computer data or erase your hard disk too. These virus programs are placed into commonly used programs. So, when those programs are run, the attached virus infects the executable program or file.

Symptoms of Virus:

- Slowing down of the speed of the computer.
- Change in files' extension.
- A long time in the loading of a program.
- Showing of unusual error message on the screen.
- System data corruption.
- Memory space reduction in a computer.
- Inaccessibility to the location of files.

Prevention of Virus:

- Password protection should be employed.
- Execute familiar programs only as to their origin. Programs sent by e-mail should always be suspicious.
- Load software only from original CDs or disks instead of pirated or copied ones.
- Check all shareware and free programs downloaded from online services with a virus checking program.
- Computer uploads and "system configuration" changes should be always performed by the computer owner.
- Purchase or download an anti-virus program that runs as you boot or work on your computer. Also, update it frequently.

Types of Viruses

1. **Trojan Horse:** Appearing as a useful and desired function, a Trojan Horse program neither replicates nor copies itself, but causes damages and compromises the security of a computer. This virus program may arrive in the form of software of some sort or a joke program that must send by someone or carried by another program.

2. **Worm:** It is a program that copies and facilitates self-distribution from one disk drive to another or by copying itself using e-mail or any other transport mechanism.
3. **Macro Virus:** These viruses infect documents such as MS Excel or MS Word and other similar documents. These viruses use another application's macro programming language to distribute themselves.
4. **Boot sector Virus:** Normally, spread by floppy disks, this virus attaches itself to the 1st part of the hard disk which is read by the computer upon boot up.
5. **Polymorphic Virus:** A Polymorphic Virus is a very sophisticated virus program as it not only replicates itself by creating multiple files itself but also changes its digital signature each time it replicates.
6. **Memory Resident Virus:** This virus is initiated from a virus within the computer and they stay in a computer's volatile memory (RAM) after its initiating program closes.

8.5 Prevention of Cyber Crime:

Prevention is always better than cure. It is always better to take certain precautions while accessing the Internet.

a. Prevent cyber stalking and avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.

b. Avoid sending any photographs online, particularly to strangers and chat friends. There have been incidents of misusing photographs.

c. Use latest and updated antivirus software to guard against virus attacks.

d. Keep back up volumes so that one may not suffer data loss in case of virus contamination.

e. To guard against frauds, never send you credit card number to any site that is not secure.

f. Web servers running public sites should be separated and protected from internal corporate network.

Technical solutions

If correctly installed, the following can help to block attacks:

- Firewalls:
- Software Solution:
- Authentication
- Hardware Cryptography
- Patches

8.6 Intellectual Properties Right

Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his/her creation for a certain period of time.

The term intellectual property refers broadly to a distinct types of the creations of the human mind such as musical, literary, photographic and artistic works; discovers and inventions; and words, phrases , symbols and designs etc.

Intellectual property rights protect the interests of creators by giving them property rights over their creations.

Common types of intellectual property rights include

- Copyrights
- Trademarks
- Patents
- Industrial Design Rights etc.

Privacy and Anonymity

Privacy: Privacy is the concept for the protection of user's data which is not be examined or viewed by anyone else without his/her permissions. Privacy is the ability to control particular information. Many people use the term to mean universal internet privacy.

Various types of personal information often come under privacy concerns. Some of them are as follows.

i) Financial privacy
ii) Internet Privacy
iii) Medical Privacy
iv) Political privacy

Anonymity: Anonymity is derived from the Greek word anonymia which means 'without a name' or 'nameless'. In general, anonymity typically refers to the state of an individual personal identity or personally identifiable information being publicly unknown or hidden.

8.7 Concept of Digital Signature

Digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Digital signatures do this by generating a unique hash of the message or document and encrypting it using the sender's private key. The hash generated is unique to the message or document, and changing any part of it will completely change the hash.

Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery and tampering.

Digital signatures increase the transparency of online interactions and develop trust between customers, business partners and vendors. Digital signatures work by proving that a digital message or document was not modified intentionally or unintentionally-from the time it was signed.

8.8 Concept of Cyber law in Nepal:

Cyber law:

Cyber law is commonly known as the law of the internet. It governs the legal issues of cyberspace. The term that cyberspace is not only restricted to the internet. It is a very wide term that includes:

- Computer
- Computers networks
- The internet
- Data
- Software etc.

What Cyber law deals with? Or Area of Cyber Law

- Electronic and Digital Signatures
- Computer Crime
- Intellectual Property
- Data Protection and Privacy
- Tale-communication laws.

8.9 ICT Policy in Nepal:

Cyber Law of Nepal

Cyber law of Nepal commonly known as the Electronic Transaction and Digital Signature Act-Ordinance was enacted in Nepal in 2061 BS (2004).

The cyber law in Nepal was formulated after making a thorough discussion of the IT Acts already implemented in other countries. It was formulated mainly to legalize the different trading activities through the global computer network and to give a boost to the e-governance activities.

The Act is divided into 12 sections and 80 clauses with detailed information on role rights of regulator, certification, authority, customer, government and all the concerned stakeholders. It has also established a separate judicial bodies-IT Tribunal and Appellate Tribunal to look into all cases related to computer and cybercrimes.

The three members' tribunal will be headed by the district court judge or legal officers of equivalent status. It contains a strong provision of punishment against cyber-crimes according to the nature of the crime.

The different cyber mentioned in the law include hacking, damage to computer source code, breach of privacy and faking digital signatures. As per the provisions of law, the government is fully authorized to punish cyber criminals - both an individual and an institution with imprisonment and fine.

The major interesting aspects of the act are listed below:

a. A controller of public key certifying authorities has been appointed by the Government. This office will recognize certifying authorities who will have the authority to issue public key certificates and verify digital signatures.

b. To facilitate electronic filing of documents with the Government agencies and to promote efficient delivery of Government services by means of reliable electronic records.

c. Provides a legal framework to facilitate and safeguard electronic transactions in the electronic medium.

d. Provides a detailed provisions for the Controller of Certifying Authorities to regulate Certifying Authorities. e. Provides provision of an Appellate Judicial body to listen to complaints, cases and cyber related crime.

e. Provides punishment to a hacker who

i. Downloads, copies or extracts data from a database without permission of the owner.
ii. Introduce computer virus into any computer or computer network.
iii. Damages programs or data residing in a computer or network or illegally copies them.
iv. Disrupts a computer or network.
v. Provides legal status for various banking transactions through electronic media, which will be instrumental in boosting economic activities throughout the world via Internet.
vi. Provides legal status to digital signatures sent through the electronic media, which would be an important provision to introduce e-banking.

- **This policy** is intended to create foundational groundwork for an overarching vision of “Digital Nepal”. As per this vision, Information and Communication Technology will be a key driving force in transforming Nepali society into knowledge and information based society and strengthening Nepal’s pursuit of equality and sustainable growth by leveraging Information and communication technology.
- This policy is primarily designed to guide and mainstream the use of ICTs in all sectors of the Nepalese economy within the overall context of socio-economic development and poverty reduction agenda pursued by the country.

- Infrastructural synergies shall be promoted while upgrading existing and developing new infrastructure such as roads and electric power and facilitating cost effective roll-out of telecommunications and broadband infrastructure aimed at supporting the goals of the policy.
- Nepal will continue to uphold the principle of freedom of expression on the Internet and net neutrality.
- The policy intends to promote platform neutral services in e-governance.

❖ **Vision:** To transform Nepal into an information and knowledge-based society and economy.

❖ **Mission:** To create conditions for the intensified development and growth of ICT sector as a key driver for Nepal's sustainable development and poverty reduction strategies.

❖ **Objectives of National Information and Communication Technology Policy**

a. To empower and facilitate Nepal's participation in the Global Knowledge Society.
b. To transform Government service delivery regime by promoting transparency, efficiency, inclusiveness and participation through effective utilization of information and communication technologies
c. To promote ICT to further productivity among the sectors that is key drivers of the national economy.
d. To foster efficient, inter-operable, secure, reliable and sustainable national ICT infrastructure in alignment with grass-root needs, and compliant with regional and international standards
e. To promote research and innovation on the role of ICT on the resilience of low-income communities amid potential environmental, economic and social shocks.

❖ **Strategies**

The following information technology strategies shall be adopted to accomplish the above mentioned objectives through rapid development and extension of information technology in a fair and competitive manner.

a. Digital literacy will be encouraged as a basic requirement for employment and promotion in all sectors
b. ICT awareness programmers will be developed among all citizens and ICT as an alternative career path will be promoted for youths and women
c. E-Learning systems will be promoted to extend the reach of educational services including teachers training programs
d. The integration of computer skills into the teaching and learning process at primary, high school and tertiary levels will be promoted and facilitated
e. Special tax instruments and incentives to promote the development of the local ICT production and services industry will be developed and implemented
f. Specific measures will be taken to promote, stimulate and support the development of innovative local content and applications
g. The use of social media will be promoted to drive inclusion and participation in governance h. Establish monetary and fiscal policy measures to ensure consumer confidence in E-Commerce.

The End