DIGITAL TECHNOLOGY NOTE FOR SS3
1ST TERM NOTE 2026

SCHEME OF WORK

1	Overview of Number Bases	• Review of Number Bases: • Conversion Between Number Bases • Basic Arithmetic in Number Bases:
2	Data Representation	• Definition of Data Representation • Methods of Data Representation: • Computer Character Sets
3	Security and Ethics I	• Sources of Security Breaches: • Preventive Measures:
4	Security and Ethics II	• Legal Issues in Computing: • Examples of Cybercrimes:
5	Wireless Network	• Types of Wireless Network • Advantages and Disadvantages of wireless network
6	Practical	• Practical on Microsoft Word and Excel Applications
7	Practical	• Practical on PowerPoint and Microsoft Access Applications
8	Practical	• Practical on CorelDraw Application
9	Revision	• Revision
10	Examination	

OVERVIEW OF NUMBER BASES

1. Review of number bases
2. Conversion in Number bases
3. Basic Arithmetic in number bases

Review of Number Bases

Most computer systems operates using binary logic. The binary number system works like the decimal number system except that the binary number systems uses base 2, and its digits are 0 and 1 while decimal system uses base 10 and its digits are from 0 – 9.

The common number systems used in computing are:

(i) Base 10 known as Decimal Number System

(ii) Base 2 known as Binary Number System

(iii) Base 8 known as Octal Number System

(iv) Base 16 known as Hexadecimal Number System

Binary Number System

The binary numeral system, or base-2 number system, represents numeric values using two symbols, 0 and 1.

Octal Number System

The octal numeral system is the base 8 number system, and uses the digits 0-7. Numerals can be made from binary numerals by grouping consecutive binary digits into group of three (starting from the right). For example, the binary representation for decimal 74 is 1001010, which can be grouped into (00)1 001 010. Therefore, the octal representation is 112.

Decimal Number System

the decimal numeral system (also called base ten or occasionally denary) has ten as its base. It is the most common notation and often refers to a base-10 positional notation.

Hexadecimal Number System

Hexadecimal (also base 16, or hex) is a positional numeral system with a base of 16, i.e. it uses sixteen distinct symbols, i.e. 0-9, A-F representing values 10-15.

CONVERSION IN NUMBER BASES

From Decimal to Other Bases

To convert from base 10 to any other base, simply divide the given number continuously by the number base being converted to, until its no longer divisible. Then the remainders are copied in **ascending order**.

Example 1: Convert 345_{10} to base 2

2	**345**		
2	172	R	1
2	86	R	0
2	43	R	0
2	21	R	1
2	10	R	1
2	5	R	0
2	2	R	1
2	1	R	0
	0	R	1

Therefore, $345_{10} = 101011001_2$

Example 2: Convert 2000_{10} to base 8

8	**2000**		
8	250	R	0
8	31	R	2
8	3	R	7
8	0	R	3

Therefore, $2000_{10} = 3720_8$

Conversion from Binary to Decimal

Example 1: Convert 101100101_2 to base 10

8 7 6 5 4 3 2 1 0 ⟶ place value

$1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1_2$ ⟶ binary digits

$= 1 \times 2^8 + 0 \times 2^7 + 1 \times 2^6 + 1 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$

$= 1 \times 256 + 1 \times 64 + 1 \times 32 + 1 \times 4 + 1 \times 1$

$= 256 + 64 + 32 + 4 + 1$

$= 357_{10}$

Conversion from Octal to Decimal

45_8 to base 10

$= 4 \times 8^1 + 5 \times 8^0$

$= 4 \times 8 + 5 \times 1$

$= 32 + 5$

$= 37_{10}$

Conversion from Hexadecimal to Binary

The hexadecimal number system (base 16) uses group of four bits, the table below can be used for conversions:

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

To convert D14B to binary:

D = 1101, 1 = 0001, 4 = 0100, B = 1011

When we put the pieces together, we get $D14B_{16} = 1101000101001011_2$

Basic Arithmetic in Number Bases

The rules for adding base 2 numbers are simple;

0 + 0 = 0

0 + 1 = 1

1 + 1 = 10

1 + 1 + 1 = 11

1 + 1 + 1 + 1 = 100

1 + 1 + 1 + 1 + 1 = 101

Example 1: Add the numbers 10101101 + 1011110
Example 2: 10001 – 100
Example 3: Add up $467_8 + 453_8$
Example 4: Compute $FAD_{16} – BED_{16}$

EXERCISE

1. Write short notes on the on the various number systems.

2. Convert the following numbers to the base indicated;
   (i) 49_{10} to base 8
   (ii) 101101_2 to decimal
   (iii) $FA6_{16}$ to binary

3. Solve the following;
   (i) AB + C
   (ii) Subtract 67_8 from 247_8

DATA REPRESENTATION

1. Definition Data Representation
2. Description of Data Representation Methods
3. Computer Character Sets

Definition of Data Representation
Data Representation is the way that the physical properties of a medium are used to represent data and the manner in which data is expressed symbolically by binary digits in a computer.

Description of Data Representation Methods
Data can be represented in the following ways:
Bits: A bit is simply a *1or a 0. A true or a false.* It is the most basic unit of data in a computer. It is also called machine language. A bit (also called binary) is the basic unit of information in computing and telecommunication. It is one of two possible distinct states.

BCD: BCD stands for binary coded decimal. It is a digital encoding method for numbers using decimal notations, with each decimal digit represented by its own binary sequence. In BCD, a numeral is usually represented by four bits which in general, represents the decimal range 0 through 9 to 00000000 through 00001001. BCD is a method of using binary digits to represent the decimal digits 0 through 9.

BCD	Decimal	BCD	Decimal	BCD	Decimal
0000	0	0011	3	0110	6
0001	1	0100	4	0111	7
0010	2	0101	5	1000	8

EBCDIC: Extended Binary Coded Decimal Interchange Code: Is an 8-bit character encoding used mainly on IBM mainframe and IBM midrange computer operating systems.
EBCDIC is a Character set that was developed before the ASCII (American Standard Code for Information Interchange, became commonly used. Both ASCII and EBCDIC are both 8-bit character set, unlike the BCD which is a 4-bit character set.

ASCII: The American Standard Code for Information Interchange (ASCII) is a character-encoding scheme based on the ordering of the English alphabet. ASCII codes represent text in computers, communication equipment, and other devices that use text. Most modern character-encoding schemes are based on ASCII, though they support many more characters than ASCII does.

Computer Character Sets
Each Character is stored in the computer as a byte. Since a byte consists of 8-bits, there are 28, or 256 possible combinations of bits within a byte, numbered from 0 to 255. There are two commonly used character sets that determine which particular pattern of bits will represent

which character. ASCII is used on most minicomputers and PCs, while EBCDIC is used on IBM, Mainframes.

EXERCISE

1. Discuss any three ways in which data can be represented.
2. What is the advantage of EBCDIC over BCD?
3. Give the full description of the words ‘ASCII’ and EBCDIC.
4. Which of the computer character set is most popular and why?

SECURITY AND ETHICS

1. Sources of Security Breaches
2. Preventive Measures Against Security Breaches
3. Legal Issues to be Considered When Using ICT

COMPUTER SECURITY

Computer security is the protection of *computer* systems and information from harm, theft, and unauthorized use.

Computer security can also be defined as controls that are **put** in place to provide confidentiality, integrity, and availability for all components of computer systems.

These components include data, software, hardware, and firmware.

Computer security allows you to use the computer while keeping it safe from threats. Computer Security allows an Organisation to carry out its mission by:

- Enabling people to carry out their jobs, education, and research.
- Supporting critical business process.
- Protecting personal and sensitive information.

SECURITY BREACH

A **security breach** is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying **security** mechanisms.

Security Breach can also be defined as an act of breaking security polices, practices or procedures.

When security in computer is breached, it may result in the damage of vital files, failure of certain computer hardware components

Sources of Security Breaches

1. **Virus:** A virus is a malicious piece of software, designed to spread and cause damage to programs and files on computers. Some viruses are merely annoying, displaying useless error messages. Other viruses can destroy your data and prevent your computer from working. Examples of virus are Trojan horse, worm etc.

(i) **Trojan horse:** This is a program that does not replicate or copy itself, but causes damage by tricking you into opening an infected file.

(ii) **Worm**: This is a program that copies itself specifically intended to be distributed to other computers, via email or network connections.

(iii) **Virus**: This is a program that replicates itself and infects another program by inserting or attaching itself, especially on files already present on the computer.

2. **Hackers**: Hackers are people who break into someone's personal online account without the permission to do so. Hackers have developed automated programs, such as "cracks." To break the passwords in files by raw brute force, trial and error techniques. Since it could take a month to crack well chosen passwords, some systems now use aging systems that require all users to set new passwords periodically.

3. **Poorly Implemented Policies or Lack of ICT Policy**: An ICT policy is a statement of what is allowed and what is not allowed as far as computers id concerned. If such policy is not there or if it is poorly implemented, there will be a problem because every computer user will be doing whatever he or she likes.

3. Lack of ICT Policy: When ICT security policies that controls the order in which the users should conduct themselves when using the ICT facilities do not exist due to ignorance or poor implementation, lawlessness will be in place and this can lead to security breach.

5. **Carelessness**: Most of the time, computer security is breached due to the careless behaviour of some organizations and individuals who do not exercise proper care in safeguarding data and information.

EXERCISE

1. Explain the term "sources of security breach"
2. What is a Trojan horse?

Preventive Measures Against Computer Security Breaches

Preventive measures against computer security breaches are as follows:

1. **Use of antivirus**: Antivirus programs are designed to detect and kill viruses. It is very necessary to buy and install antivirus software in your system. Update your computer regularly for protection against new viruses. Also scan your computer regularly.

2. **Use of firewall**: Firewall is a security arrangement of hardware and of software that prevents unauthorized access of data, information and storage media on the network. Firewall can also prevent problems, worms and hackers that may attack your system over the internet.

3. **Exercising care in giving out personal and vital information:** People steal personal or confidential information a lot. The use of usernames and passwords or biometric devices can help protect information stored on the computer located in the organization or one's premises.

4. **Encryption:** This is the process of converting readable data into unreadable characters with the aim of preventing unauthorized access. To read an encrypted data, one must have to decrypt or decipher it into readable form. The unencrypted readable data is known as Bold. While the encrypted unreadable data are known as Cipher text.

5. **Proper networked implementation and policy:** Effective management ensures that proper network implementation and good ICT policy are put in place. Some of the effective management strategies include the following;

(i) Restrict access to those staff who can be trusted

(ii) Educate staff on proper handling of electronic items and counter measures should be adopted.

(iii) Carry out effective staff supervision with a view of identifying those who are no longer trustworthy.

(iv) Rotate staff to check collusion and corrupt activities among them.

6. **Using sites with web certificates**: Your internet service provider can help with a list of certified websites so that you can know the sites to be avoided. Alternatively you can buy and register any of the packages like internet filter, surf watch, Cyber patrol, Web Tract, etc.

7. **Exercising care in opening e-mail attachments**: Spam is an electronic mail or junk newsgroup posting mainly for the purpose of advertising for some products or services. It can be a nuisance and a waste of time. It can also distribute virus. Hence care should be adequately taken when opening e-mails.

EXERCISE

1. State 5 preventive measures when using a computer**.**
2. What is Spam mail
3. What is an internet filter?

Legal Issues to be Considered When Using ICT

Legal issues have documented definitions (laws) with specific consequences if the laws are broken.

Examples of Legal Issues in computing

1. Criminal statures
2. Cybercrime like Identity theft, hacking and Internet fraud

3. Piracy
4. Federal and state regulations
5. Commonly accepted professional practices
6. Unauthorized access
7. Sabotage and destruction of data
8. Theft of commercial software

SOME IMPORTANT LEGAL ISSUES TO BE CONSIDERED WHEN USING THE ICT;

Copyright: This is the legal right given to the only producer or seller of a creative work, such as textbook, a piece of music, a painting or a computer program.

Ownership Right: The originator of any textbook, images, audio and video programs has the ownership rights to such programs. If you want to copy and use any of the programs, you must accord the originator the due respect and recognition of obtaining permission.

Piracy: This is an illegal copying for personal use, sale or distribution of software, books, tapes, video, etc. This is a serious offence and the offender must be punished by the law.

Cybercrimes: This is an online or internet-based illegal act. Once a thief has the computer, he or she can access any document or information that is in the computer.

Hacking: This is gaining unauthorized access to the computer resources with the intention to cause harm. Hackers breach the security of computer systems owned by banks, and government agencies just to commit fraud.

Exercise

1. Define the term ‘hacking’.
2. Explain 5 legal issues to be considered when making use of software.
3. State 5 ways in which the internet can be abused.

WIRELESS NETWORKS

Introduction

Wireless networks allow devices to communicate without physical cables.
Utilize radio frequency (RF) signals to transmit data.
Common in homes, businesses, and public spaces.

Wireless Network

TYPES OF WIRELESS NETWORKS

1. Wireless Personal Area Network (WPAN)

Short-range networks (e.g., Bluetooth).
Connects personal devices like smartphones, headphones, and wearables.

2. Wireless Local Area Network (WLAN)

Covers a limited area like a home, school, or office.
Example: Wi-Fi networks.

3. Wireless Metropolitan Area Network (WMAN)

Spans a city or large campus.
Example: WiMAX.

4. Wireless Wide Area Network (WWAN)

Covers large geographic areas.
Example: 3G, 4G, 5G networks.

Key Technologies

Wi-Fi (IEEE 802.11): Most common WLAN technology.
Bluetooth: Short-range communication for personal devices.
Cellular Networks: 3G, 4G LTE, 5G for mobile communication.
WiMAX: Wireless broadband for metropolitan areas.
Zigbee & Z-Wave: Low-power protocols for IoT devices.

Components of Wireless Networks
Wireless Access Point (WAP): Central device that connects wireless devices to wired network.
Wireless Client Devices: Laptops, smartphones, tablets, IoT devices.
Antennas: Transmit and receive RF signals.

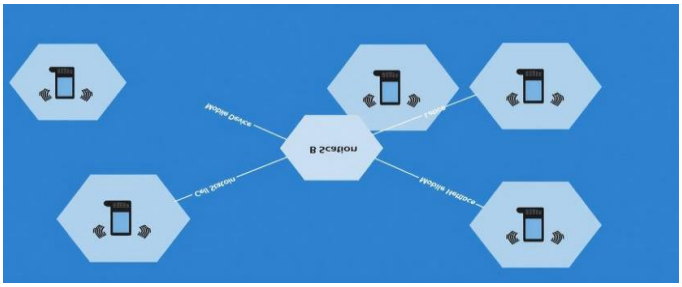
Advantages

1. Mobility and Flexibility: Users can move freely within the coverage area while maintaining network connectivity.
2. Easy Installation and Expansion: Wireless networks require less cabling, making setup quicker and easier to expand or reconfigure.
3. Cost-Effective: Reduces the need for extensive cabling and infrastructure, lowering installation and maintenance costs.
4. Convenience: Enables connection of multiple devices without physical constraints, ideal for dynamic environments.
5. Scalability: Easily accommodates new devices and users without significant hardware changes.

Disadvantages

1. Security Risks: Wireless networks are more vulnerable to unauthorized access and hacking if not properly secured.
2. Limited Range: Signal strength decreases with distance, limiting the coverage area.
3. Interference: Wireless signals can be disrupted by other electronic devices, obstacles, or physical barriers.
4. Lower Speed and Bandwidth: Wireless networks generally offer lower data transfer speeds compared to wired networks.
5. Reliability Issues: Wireless connections can be less stable and more prone to disruptions than wired connections.

Cellular Network:
A cellular network is a wireless communication system that divides a geographic area into smaller regions called cells. Each cell has its own base station that connects mobile devices within its area to the broader network. This architecture allows multiple users to share the same spectrum efficiently, enabling continuous communication even while moving between cells. Cellular networks support various services like voice calls, SMS, and mobile internet, and are the foundation of modern mobile communication systems such as 3G, 4G, and 5G.



CELLULAR NETWORK

SECURITY IN WIRELESS NETWORKS

- WEP (Wired Equivalent Privacy): Outdated, insecure.
- WPA/WPA2/WPA3: Improved security protocols.
- Use of strong passwords, encryption, and VPNs.
- Regular firmware updates.

WIRELESS SECURITY

Introduction to Wireless Security

Wireless networks use radio signals to connect devices, making them vulnerable to unauthorized access.
Security is crucial to protect data, privacy, and network integrity.

Common Wireless Security Threats

1. Eavesdropping: Unauthorized interception of data.
2. Unauthorized Access: Gaining access without permission.
3. Man-in-the-Middle Attacks: Intercepting and altering communication.
4. Rogue Access Points: Fake access points to trap users.
5. Denial of Service (DoS): Disrupting network availability.
6. Packet Sniffing: Capturing network traffic for malicious purposes.

Wireless Security Protocols

- WEP (Wired Equivalent Privacy): Older, insecure protocol; vulnerable to attacks.
- WPA (Wi-Fi Protected Access): Improved security over WEP, uses TKIP.
- WPA2: Current standard, uses AES encryption for stronger security.
- WPA3: Latest standard, provides enhanced security features like individualized data encryption.

Security Best Practices

- Change default SSID and passwords.
- Use strong, complex passwords.
- Implement WPA3 encryption where possible.
- Enable network encryption.
- Disable WPS (Wi-Fi Protected Setup) to prevent vulnerabilities.
- Regularly update firmware and security patches.
- Use MAC address filtering (though not foolproof).
- Enable guest networks for visitors.
- Turn off the network when not in use.

Additional Security Measures

1. Use VPNs for secure remote access.
2. Implement Network Access Control (NAC).
3. Enable firewalls and intrusion detection systems.
4. Limit signal range to reduce outside access.
5. Monitor network activity for suspicious behavior.

Conclusion

Wireless security is an ongoing process that requires regular updates and vigilance.
Combining strong encryption, secure configurations, and user awareness is key to protecting wireless networks.

Challenges

i. Signal interference from other devices.
ii. Network congestion.
iii. Ensuring security and privacy.

Future Trends

- ❖ 5G networks for faster, more reliable wireless connectivity.
- ❖ Integration with IoT for smart cities and homes.
- ❖ Enhanced security protocols and AI-driven network management

EXERCISE

1. Explain the main security challenges faced by wireless networks. What are the most effective strategies and protocols to protect wireless communications from unauthorized access and cyber threats?

2. Compare and contrast the different types of wireless networks, such as WLAN, WWAN, PAN, and WPAN. Discuss their typical use cases, advantages, and limitations.

3. Analyze the role of encryption and authentication protocols in ensuring the security of wireless networks. How do protocols like WPA2 and WPA3 enhance data protection compared to earlier standards?