#### **SS3 2ND TERM NOTES**

#### **Topic: Data Representation**

#### **Objectives**

By the end of the lesson, students should be able to:

1. Define data representation.
2. Explain the concept and importance of data representation.
3. Describe various methods of data representation.
4. Identify character sets used in data representation.



#### 

**Definition**

Data representation refers to the methods used to encode ( convert information or data into a different format ), store, and process information in a computer system using binary formats (a way of representing data using only two symbols: 0 and 1).

**Data Representation Methods**

Computers represent data using binary digits (bits), which are 0s and 1s.

These are combined in various ways to represent different types of data. These combinations are called **Character Set**.

**A character set** is a defined list of characters that a computer recognizes, along with their corresponding binary codes.

Common data representation/ character set include:

1. **Bits (Binary Digits)**:

The smallest unit of data in a computer, representing either 0 or 1.

1. **BCD (Binary-Coded Decimal)**:

Represents each decimal digit (0-9) with its binary equivalent.

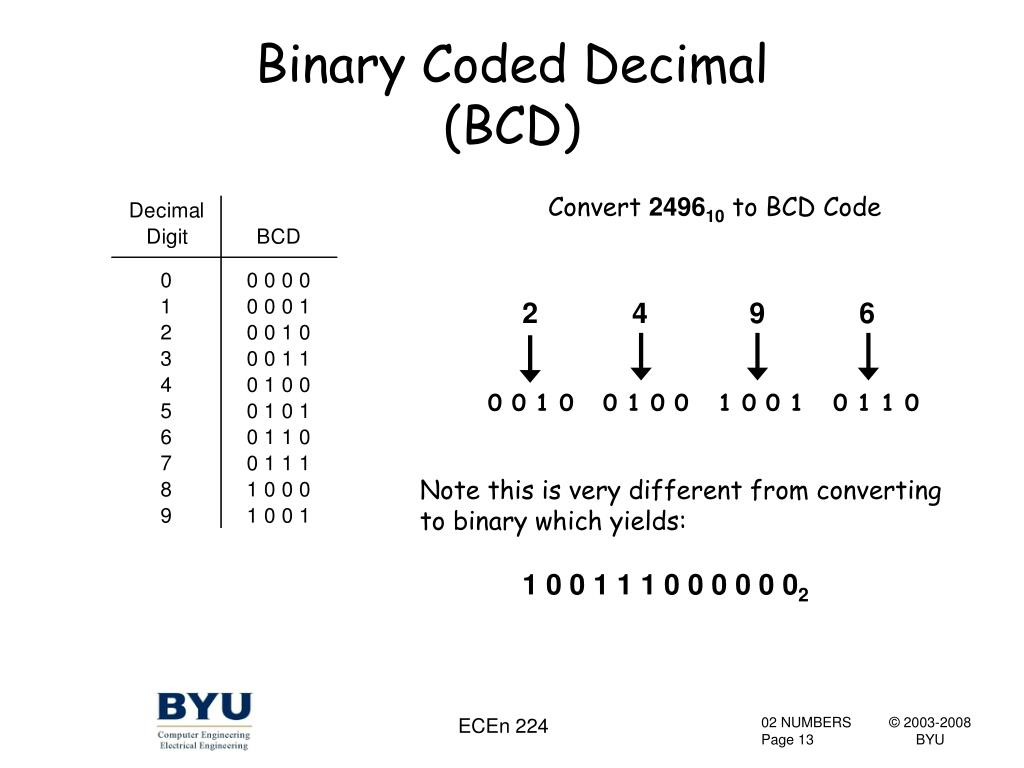
It translates each decimal digit into its own binary language and then puts them together.

Example: Decimal 45 is represented as 0100 0101 in BCD.

For the decimal number **45**:

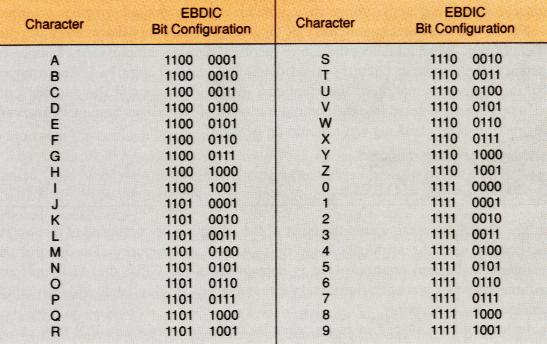
1. **4** in decimal is represented as **0100** in binary.
2. **5** in decimal is represented as **0101** in binary.

So, when you combine these binary sequences, you get **0100 0101** for the decimal number **45** in BCD.



3. **EBCDIC (Extended Binary Coded Decimal Interchange Code)**:

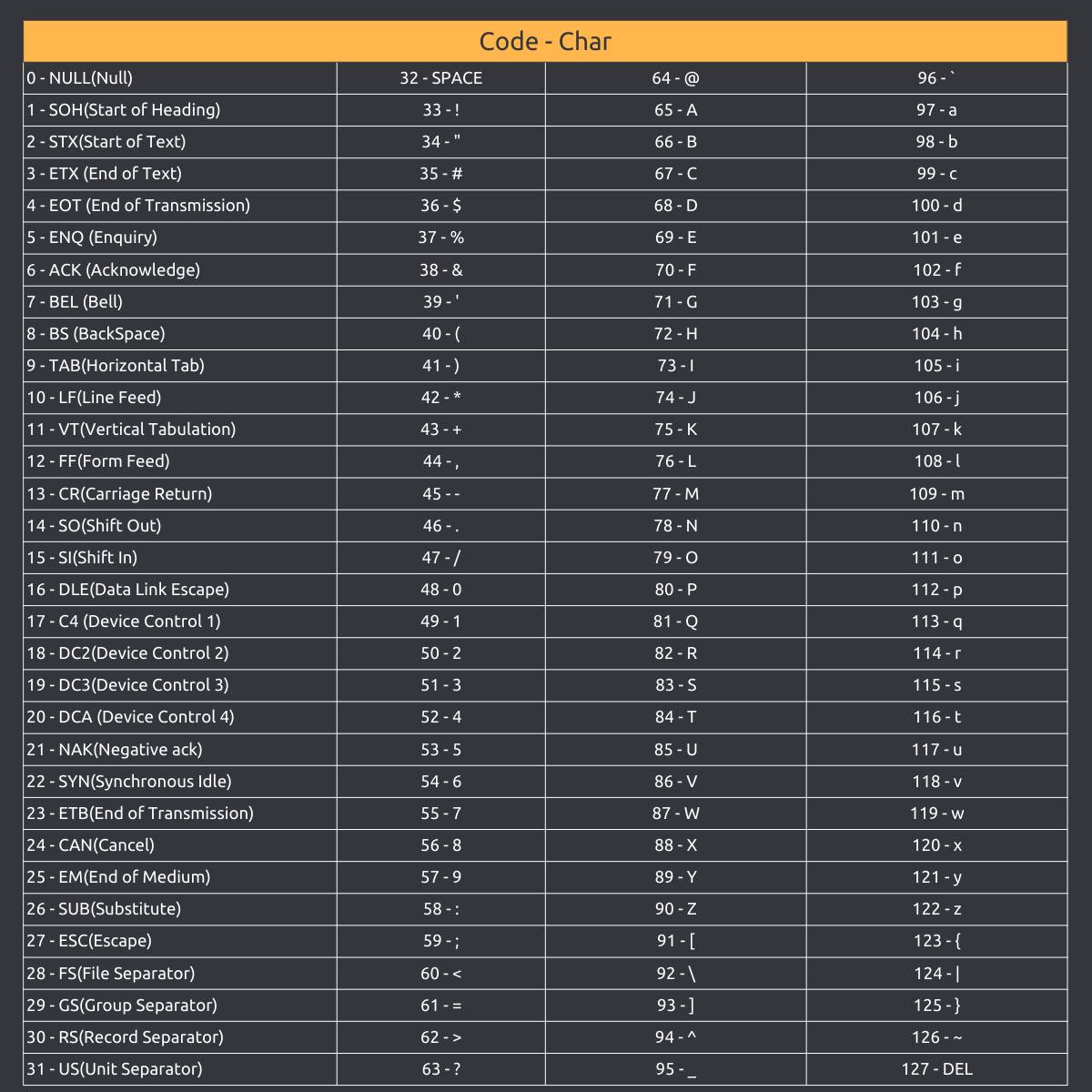
is an 8-bit character encoding system used primarily on IBM mainframe computers. It is used to represent alphanumeric characters, punctuation marks, and control characters.



**4. ASCII (American Standard Code for Information Interchange)**:

Uses 7 or 8 bits to represent text characters.

**Example**: The character "A" is represented as 65 in decimal or 01000001 in binary.



**5. Unicode:** Unicode is a universal character encoding standard that provides a unique number for every character, regardless of the platform, program, or language.

It uses 8, 16 or 32 bits

It was developed to address the limitations of earlier encoding systems like ASCII, which could only represent a limited set of characters.

Eg. Emojis and language symbols such as Chinese, Arabic, Korean etc.



#### **Assignment**

Create a table showing at least five characters and their binary equivalents in ASCII.

**WEEK 2-4**

**Topic:** Computer Security and Ethics

**Instructional Objectives:** By the end of the lesson, students should be able to:

1. Define security and ethics in the context of ICT.
2. Identify sources of security breaches.
3. Explain the concepts of viruses, worms, and Trojan horses.
4. Describe the impact of poorly implemented or lack of ICT policies.



#### **Introduction**

**Computer Security** is protecting computer systems and data from unauthorized access and threats.

**Ethics** is a set of moral principles that govern responsible use of ICT.

#### **Sources of Security Breaches**

Security breaches occur due to various factors, including:

1. **Malware (Malicious Software):** Programs designed to harm or exploit computers.
2. **Phishing Attacks:** Fraudulent attempts to obtain sensitive information.
3. **Weak Passwords:** Easily guessable or reused passwords.
4. **Poor Network Security:** Unprotected networks.
5. **Human Error:** Accidental data leakage or mismanagement.
6. **Poorly implemented or lack of ICT Policy:** ICT Policy is a set of guidelines for managing ICT systems securely.

#### **Impacts of Poor or Lack of ICT Policy:**

Increased vulnerability to attacks.

Data breaches and financial loss.

Reduced trust in organizational systems.

1. **Carelessness:** giving out personal and vital information on the internet without careful screening.

#### **Types of Malware**

1. **Virus:**
   * Attaches itself to files or programs.
   * Can spread when infected files are opened.
   * Causes damage by deleting files or corrupting data.
2. **Worm:**
   * Self-replicates and spreads without human action.
   * Consumes system resources and slows down networks.
3. **Trojan Horse:**
   * Disguised as legitimate software.
   * Allows unauthorized access to a computer.

4. **Ransomware**: This type of malware encrypts a victim's files and demands a ransom for the decryption key.

**5. Spyware**: Spyware secretly monitors user activity and collects sensitive information, such as passwords and credit card details.

**6. Adware**: Adware displays unwanted advertisements on the user's device, often leading to a degraded user experience.

**Preventive Measures**

Ways to protect computers and personal data from cyber threats include:

1. **Use strong passwords** and enable multi-factor authentication.
2. **Install antivirus software** and keep it updated.
3. **Regular data backup** to avoid loss of information.
4. **Avoid clicking on unknown links** to prevent phishing attacks.
5. **Use firewalls** to filter network traffic.

**Legal Issues in Cybersecurity**

1. **Data Protection Laws** – Laws that regulate how personal information is stored and shared.
2. **Intellectual Property Rights** – Protects software, music, books, and inventions from illegal copying.
3. **Cybercrime Laws** – Laws that punish hacking, identity theft, fraud, and cyberbullying.

**Web Content Ethics**

1. **Responsible Web Use:** Ensuring that shared information is accurate and ethical.
2. **Inappropriate Content:** Includes hate speech, misinformation, and illegal activities.
3. **Cyberbullying and Online Harassment:** The use of digital platforms to threaten or intimidate others.

**Piracy**

Piracy is the illegal copying, distribution, or use of software, music, movies, and books.

Common types of piracy include software piracy, music piracy, and movie piracy.

**Preventive measures:** Purchasing licensed software and using legal streaming services.

**Cybercrime and Hacking**

**Cybercrime** refers to crimes committed using computers or the internet. Examples include identity theft, online scams, and ransomware attacks.

**Hacking** is unauthorized access to computer systems. Types of hackers:

* + **White Hat Hackers:** Ethical hackers who help improve security.
  + **Black Hat Hackers:** Criminal hackers who steal or damage data.
  + **Grey Hat Hackers:** Hackers who exploit vulnerabilities without permission but do not have criminal intent.

**Conclusion:**

Understanding security and ethics in computing helps protect individuals and organizations from cyber threats while promoting responsible use of technology.

**Homework Assignment**

1. Research and explain at least three ways to prevent hacking.
2. Write a short essay on the impact of cybercrime in modern society.