**Experiment No. 6 Date:**

**TITLE: ERROR DETECTION AND CORRECTION**

**AIM**: To study error detection and correction methods like Hamming code.

**Theory:**

Hamming Codes:

Hamming codes are error detecting and self-correcting code developed by Richard Hamming. It is used to detect and correct single-bit errors and detect (but not correct) two-bit errors. The code uses parity bits placed at specific positions within the data bits to create a codeword. If a data bit is represented by positions that are powers of 2 (1, 2, 4, 8, etc.), then parity bits are calculated for overlapping groups of data bits. When a bit error occurs, the parity bits indicate the position of the corrupted bit, which can then be corrected.

They are commonly used in memory systems, satellite communication, and digital communication where single-bit errors are likely to occur.

Issues:

* Ineffective for burst errors (multiple-bit errors).
* Overhead increases with the number of parity bits added for larger data block.

Efficiency: It is eficient for single-bit error detection and correction but not suited for high-error environments.

### Cyclic Redundancy Check (CRC)

### CRC is an error-detecting technique used to detect errors during data transmission. It treats data as a binary number and divides it by a predetermined polynomial, resulting in a remainder (CRC value) that is appended to the data. During reception, the same division is performed to check if the data was altered.

### It is used in data transmission protocols like Ethernet, USB, and file transfer protocols to ensure data integrity.

Issues:

* It can detect burst errors but error correction is not possible.
* The efficiency depends on the choice of the polynomial used.

Efficiency: It is highly efficient for detecting errors, especially burst errors. It is commonly used in network communication and data storage systems.

Real-Time Use: It is used in network protocols (Ethernet, TCP/IP), storage devices (Hard Disks, SSDs), and file compression formats (ZIP, RAR).

Checksum:

A checksum is a basic error-detecting technique where the data is divided into equal-sized blocks. The blocks are summed using binary addition, and the resulting value is sent along with the data. The receiver repeats the addition and compares the result with the transmitted checksum.

It is used in simpler data transfer methods like UDP (User Datagram Protocol) and file transmission systems where high reliability is not required.

Issues:

* Ineffective against specific types of errors (e.g., if two bits are altered in a way that maintains the sum).
* Not suitable for high-reliability systems.

Efficiency: It has low computational overhead but limited reliability. It is useful for detecting random errors but not burst errors.

Real-Time Use: It is commonly used in UDP, TCP, and simple file transmission systems for basic error detection.