

Checksum

Definition

A checksum is an error-detection method in which the transmitter computes a numerical value according to the number of set or unset bits in a message and sends it along with each message frame. At the receiver end, the same checksum function (formula) is applied to the message frame to retrieve the numerical value. If the received checksum value matches the sent value, the transmission is considered to be successful and error-free.

A checksum may also be known as a hash sum.

A mismatched checksum shows that the entire message has not been transmitted. TCP/IP and User Datagram Protocol (UDP) provide a checksum count as one of their services.

The procedure of generating checksums from messages is called a checksum function and is performed using a checksum algorithm. Efficient checksum algorithms produce different results with large probabilities if messages are corrupted. Parity bits and check digits are special checksum cases suitable for tiny blocks of data. Certain error-correcting codes based on checksums are even capable of recovering the original data.

The most commonly-used checksum tools include:

- "cksum" - Unix commands generating 32-bit cyclic redundancy check (CRC) and byte count for an input file
- "md5sum" - Unix command generating Message-Digest Algorithm 5 (MD5) sum
- "jdigest" - Java GUI tool generating MD5 and Secure Hash Algorithm (SHA) sums
- "Jacksum" - Java application programming interface that incorporates numerous checksum implementations and permits any number of extensions
- "jcksum" - Java libraries used to calculate checksum using different algorithms