[checksums]

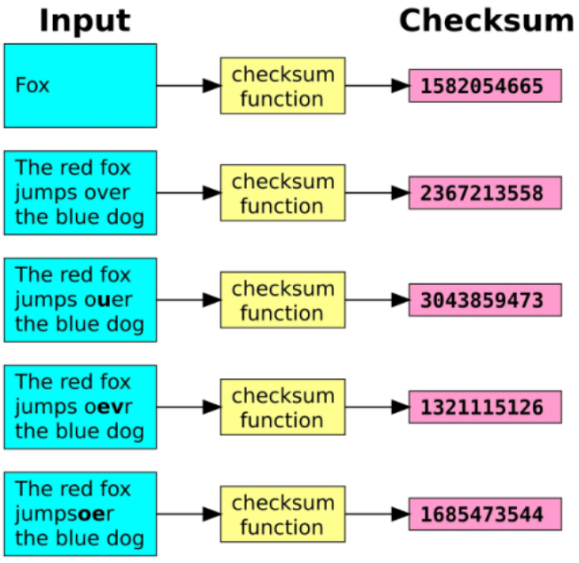
Used for Error Control in data

What is a Checksum?

A checksum is a **unique fingerprint** attached to the data before it's transmitted. When the data arrives at the recipient's end, the fingerprint is **recalculated** to ensure it matches the original one.

If the checksum of a piece of data matches the expected value, you can be confident that the data hasn't been modified or damaged.

Checksums are calculated by performing a mathematical operation on the data, such as adding up all the bytes or running it through a **cryptographic hash function**.



Credit: https://en.wikipedia.org/wiki/Checksum

How Does a Checksum Work?

The process of using a checksum for error detection is straightforward:

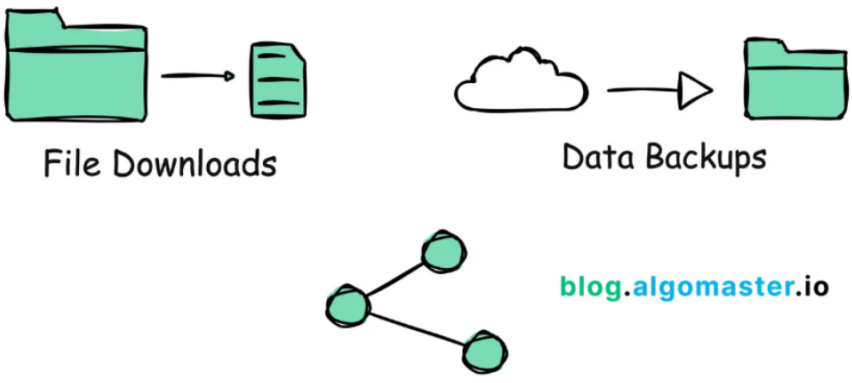
1. **Calculation:** Before sending or storing data, the original data is processed through a specific algorithm to produce a checksum value.
2. **Transmission/Storage:** The checksum is appended to the data and sent over the network or saved in storage.
3. **Verification:** Upon retrieval or reception, the checksum is recalculated using the same algorithm on the received data. This newly calculated checksum is compared with the original checksum.
4. **Error Detection:** If the two checksum values match, the data is considered intact. If they do not match, it indicates that the data has been altered or corrupted during transmission or storage.

Types of Checksums

There are several types of checksums, each with its own strengths and weaknesses. Here are a few of the most common:

- **Parity Bit:** A parity bit is a single bit that is added to a group of bits to make the total number of 1s either even (even parity) or odd (odd parity). While it can detect single bit errors, it fails if an even number of bits are flipped.
- **CRC (Cyclic Redundancy Check):** It works by treating the data as a large binary number and dividing it by a predetermined divisor. The remainder of this division becomes the checksum. CRCs are designed to detect common errors caused by noise in transmission channels.
- **Cryptographic Hash Functions:** These are one-way functions that generate a fixed-size hash value from the data. Popular examples include MD5, SHA-1, and SHA-256.

Real-World Applications of Checksums



- **File downloads**: Checksums verify that downloaded files are complete and uncorrupted.
- **Data backups**: Checksums ensure that backed-up data is accurate and trustworthy.
- **Network communication**: Checksums guarantee that data packets are transmitted correctly, preventing errors and corruption.

* Checksum is used at each layer like DLL, Transport layer even can be implemented in Application layer by application developer