Cryptographic Checksum

Return to Glossary

Cryptographic Checksum is generated by a Cryptographic Algorithm, a **Cryptographic Checksum** is a mathematical value assigned to a file sent through a network for verifying that the data contained in that file is unchanged. The algorithm performs numerous mathematical operations to create a hash value, or fixed string of digits. This hash value is then used as a Checksum to confirm that the sent file was not changed by an attacker.

A hash value remains unchanged from the time it is created and is considered an “electronic fingerprint” of a file. A **Cryptographic Checksum** is assigned to a file and is used to verify that the data in that file has not been tampered with or manipulated, possibly by a malicious entity.

Cryptographic Checksums provide the basis of modern cryptography, particularly for signing and Encryption, Digital Signature, email certificates and website certificates. They are also known as message authentication codes, integrity check values, modification detection codes or message integrity codes.

Source: https://www.techtarget.com/searchsecurity/definition/cryptographic-checksum