S

SHA-1 Hash: Length, Collision Weakness, and Safer Replacements

SHA-1 produces a 160-bit or 40-hex-character hash, but practical collision attacks make it unsafe for signatures and other trust decisions. Learn when to migrate and what to use.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 SHA-1 facts
02 SHA-1 is hashing, not encryption
03 What is a collision?
04 Collision, preimage, and second-preimage attacks
05 Where SHA-1 is unsafe
06 Legacy uses and their limits
07 What to use instead
08 How to calculate a SHA-256 file hash
09 SHA-1 migration checklist
10 Frequently asked questions

SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function that converts input of any practical size into a fixed **160-bit digest**. The digest is commonly displayed as **40 hexadecimal characters**. The same input produces the same digest, while a small input change should produce a very different result.

SHA-1 is no longer suitable for digital signatures, certificates, or other uses that depend on collision resistance. Practical attacks can create two different inputs with the same SHA-1 hash.

01 SHA-1 facts

Property	SHA-1 value
Digest length	160 bits
Hexadecimal length	40 characters
Block size	512 bits
Designed for	Integrity and cryptographic applications available at the time of standardization
Current status	Deprecated or being phased out for security uses; collision resistance is broken

02 SHA-1 is hashing, not encryption

Encryption is designed to be reversed with the correct key. A hash function is one-way: it produces a digest used for comparison or as part of another security construction. There is no SHA-1 decryption operation.

However, one-way does not mean safe for passwords. Attackers can guess likely passwords, hash each guess, and compare results at high speed.

03 What is a collision?

A **collision** occurs when two different inputs produce the same hash. A secure cryptographic hash should make finding such a pair computationally infeasible. SHA-1 no longer provides the expected collision protection.

This matters when a hash is used to approve or sign content. If an attacker can construct a benign-looking file and a malicious file with the same digest, a signature or trust decision based on that digest may apply to the wrong content.

04 Collision, preimage, and second-preimage attacks

Attack goal	Meaning	SHA-1 relevance
Collision	Find any two different inputs with the same hash.	Practical attacks exist; this is the primary reason SHA-1 is retired.
Preimage	Given a hash, find an input that produces it.	Not the same as the demonstrated collision weakness.
Second preimage	Given one input, find a different input with the same hash.	Also distinct from finding any collision pair.

Do not interpret the distinction as permission to build new systems with SHA-1. Modern algorithms avoid the known collision problem and provide stronger security margins.

05 Where SHA-1 is unsafe

- Digital and document signatures.
- TLS and public-key certificates.
- Code signing and software-update trust.
- Timestamping and audit records that must resist deliberate forgery.

- Content-addressed security decisions in which an attacker controls input.
- New authentication and protocol designs.

06 Legacy uses and their limits

- **Accidental-corruption checks:** an old SHA-1 checksum can still detect many ordinary transfer errors, but SHA-256 should be published for new downloads because an attacker may manipulate content.
- **Legacy identifiers:** some systems use SHA-1-shaped values as non-security identifiers. Migration may require compatibility planning even when no trust decision relies on collision resistance.
- **HMAC-SHA-1:** keyed constructions do not map directly to an ordinary collision attack, but new designs should follow current standards and migrate to an approved modern option.
- **Verification of old signatures:** archives may need to validate historical material under a defined policy without allowing SHA-1 for new signatures.

07 What to use instead

Use case	Preferred approach
File checksum and general integrity	SHA-256 or SHA-512 from the SHA-2 family.
Alternative standardized hash family	SHA3-256 or another SHA-3 variant appropriate to the required output length.
Password storage	A password-hashing function such as Argon2id, scrypt, bcrypt, or PBKDF2 with a unique salt and suitable work factor.
Message authentication	An approved keyed construction such as HMAC with a modern hash, following the relevant protocol standard.

Do not choose an algorithm only by digest length. Protocol requirements, key management, parameters, implementation quality, and migration compatibility also matter.

08 How to calculate a SHA-256 file hash

- **Windows PowerShell:** `Get-FileHash .\file.iso -Algorithm SHA256`
- **macOS:** `shasum -a 256 file.iso`
- **Linux:** `sha256sum file.iso`

Compare the entire value with a checksum obtained through a trusted channel. A hash published beside a compromised download does not provide independent assurance.

09 SHA-1 migration checklist

1. Inventory certificates, signatures, repositories, APIs, database fields, scripts, and third-party integrations using SHA-1.
2. Separate security uses from non-security legacy identifiers.
3. Update producers before disabling consumers so new SHA-256 or SHA-3 values are available.
4. Use dual values only during a controlled compatibility period; do not treat the SHA-1 value as authoritative.
5. Replace certificates and signing workflows and test older clients.
6. Monitor for remaining SHA-1 generation and set a removal date.

10 Frequently asked questions

How long is a SHA-1 hash?

It is 160 bits, usually written as 40 hexadecimal characters or stored as 20 bytes.

Can SHA-1 be decrypted?

No. SHA-1 is a hash function, not encryption. Weak inputs such as passwords can still be discovered by guessing and comparing hashes.

Is SHA-1 safe for passwords?

No. SHA-1 is fast and does not provide the adaptive cost required for password storage. Use a dedicated salted password-hashing function with current parameters.

Is SHA-256 simply a longer SHA-1?

No. SHA-256 belongs to the SHA-2 family and has a different design as well as a 256-bit output. It is a common replacement, but applications should follow the relevant current standard rather than substitute names blindly.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com