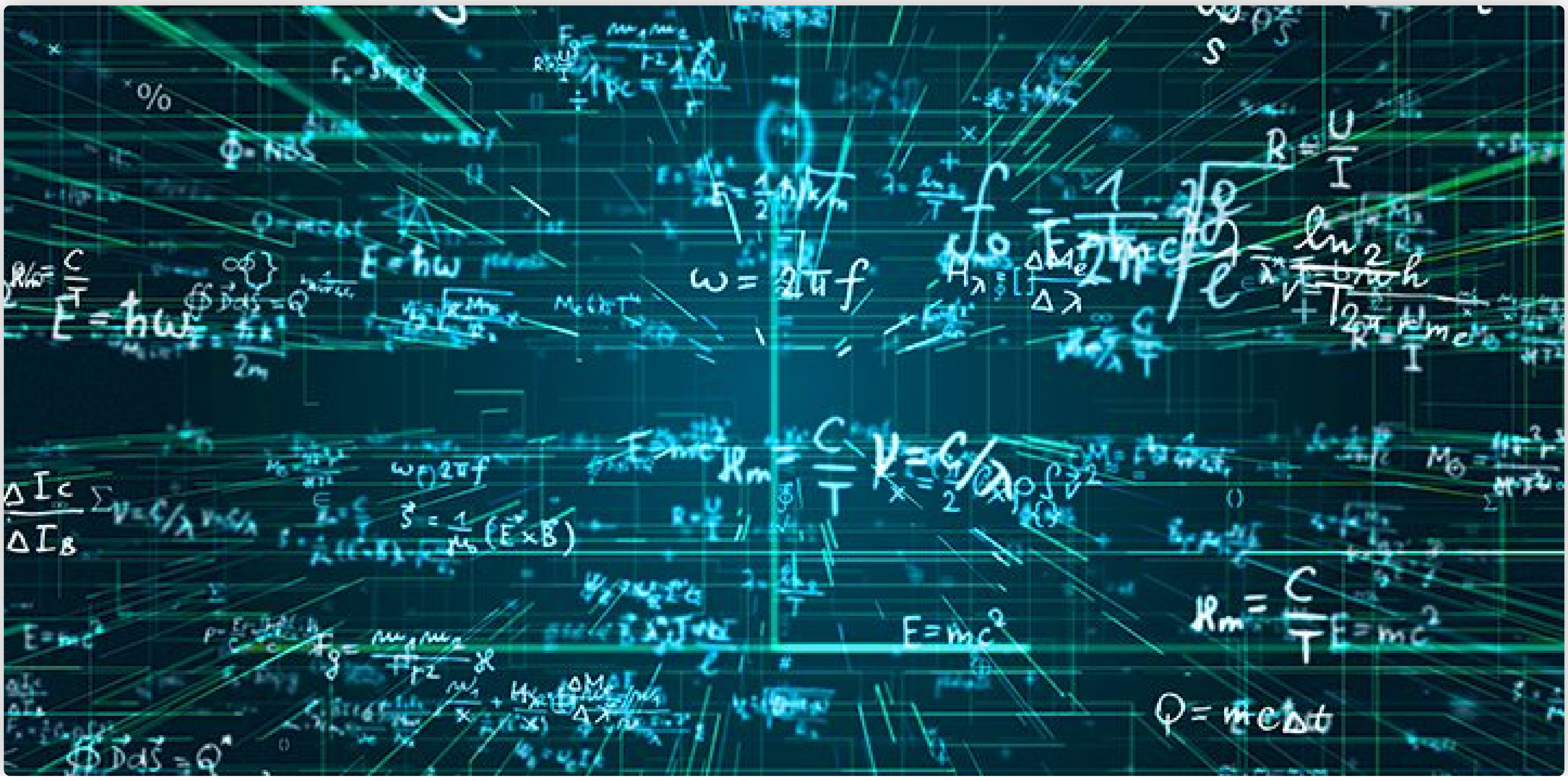
SHA-256 Algorithm Overview

By N-able
12th September, 2019

Security



Encryption is a critical part of modern computer security. Encryption algorithms like AES 256 and PGP are used to scramble data while in transit and unscramble it when it reaches the legitimate destination. But what happens when you need to scramble data in a way that's impossible to unscramble? That's where hashing comes in. This article will examine SHA-256, a widely used hash function, and its role in contemporary cybersecurity.

What is SHA-256?

The SHA-256 algorithm is one flavor of SHA-2 (Secure Hash Algorithm 2), which was created by the National Security Agency in 2001 as a successor to SHA-1. SHA-256 is a patented cryptographic hash function that outputs a value that is 256 bits long.

What is hashing? In encryption, data is transformed into a secure format that is unreadable unless the recipient has a key. In its encrypted form, the data may be of unlimited size, often just as long as when unencrypted. In hashing, by contrast, data of arbitrary size is mapped to data of fixed size. For example, a 512-bit string of data would be transformed into a 256-bit string through SHA-256 hashing.

In cryptographic hashing, the hashed data is modified in a way that makes it completely unreadable. It would be virtually impossible to convert the 256-bit hash mentioned above back to its original 512-bit form. So why would you want to create a scrambled message that can't be recovered? The most common reason is to verify the content of data that must be kept secret. For example, hashing is used to verify the integrity of secure messages and files. The hash code of a secure file can be posted publicly so users who download the file can confirm they have an authentic version without the contents of the file being revealed. Hashes are similarly used to verify digital signatures.

Password verification is a particularly important application for cryptographic hashing. Storing users' passwords in a plain-text document is a recipe for disaster; any hacker that manages to access the document would discover a treasure trove of unprotected passwords. That's why it's more secure to store the hash values of passwords instead. When a user enters a password, the hash value is calculated and then compared with the table. If it matches one of the saved hashes, it's a valid password and the user can be permitted access.

What role does SHA-256 hashing play in cybersecurity? SHA-256 is used in some of the most popular authentication and encryption protocols, including SSL, TLS, IPsec, SSH, and PGP. In Unix and Linux, SHA-256 is used for secure password hashing. Cryptocurrencies such as Bitcoin use SHA-256 for verifying transactions.

How secure is SHA-256?

SHA-256 is one of the most secure hashing functions on the market. The US government requires its agencies to protect certain sensitive information using SHA-256. While the exact details of how SHA-256 works are classified, we know that it is built with a Merkle-Damgård structure derived from a one-way compression function itself created with the Davies-Meyer structure from a specialized block cipher.

Three properties make SHA-256 this secure. First, it is almost impossible to reconstruct the initial data from the hash value. A brute-force attack would need to make 2^{256} attempts to generate the initial data. Second, having two messages with the same hash value (called a collision) is extremely unlikely. With 2^{256} possible hash values (more than the number of atoms in the known universe), the likelihood of two being the same is infinitesimally, unimaginably small. Finally, a minor change to the original data alters the hash value so much that it's not apparent the new hash value is derived from similar data; this is known as the avalanche effect.

Interested in learning more about how to securely back up your servers and critical applications? Explore our product suite to see how you can be prepared for potential disasters.

Blog

30th June, 2021

5 reasons why your telemarketing strategy isn’t working

Looking to get your sales pipeline running properly? Don’t be tempted to think cold calling is outdated and redundant, says Stefanie Hammond.

Read more ›

Blog

29th June, 2021

The Top 7 Risks of Bring Your Own Device (BYOD) MSPs Should Remember

BYOD is on the rise—find out what this means for MSPs and read about the risks your MSP should be aware of.

Read more ›

Video

N-able RMM: A Lightweight Desktop Management Software

Find out moreRelated ProductRMMOffer out-of-the-box monitoring, management, patching, and automation on Day 1. Simplify operations and business growth. Find out more

View Resource ›

Blog

24th June, 2021

What’s new in the Automation Cookbook

In this article, we'll cover some of the most recent policies from the Automation Cookbook. Unless specified, all scripts will work with both N-central and RMM.

Read more ›

Product Information

Integrated Endpoint Detection and Response (EDR) in RMM FAQ

With cybercriminals finding new angles to exploit businesses every day, it’s important to stay on top of threats—and keep your customers protected. N-able™ RMM now includes integrated Endpoint Detection and...

View Resource ›

Event

7th July, 2021

RMM Automation

Join head automation nerd, Marc-Andre Tanguay and ask him for help automating whatever you need! Marc will walk you through some recently added automation policies and will help you build...

Read more ›

Products

N-central

RMM

Backup

EDR

Mail Assure

Passportal

MSP Manager

Take Control

Features

About us

Leadership

News & Press

Careers

Investors

Why N-able

Integrations

Contact us

Get started

English Legal → Privacy → Cookies Settings