Advanced Hashing Cryptography Concepts

Dr. Dwayne Hodges, USA, (Ret.)

CISSP, CCISO, CEH, CNDA, ECES, SEC+ ITIL

Advanced Hashing Cryptography Concepts

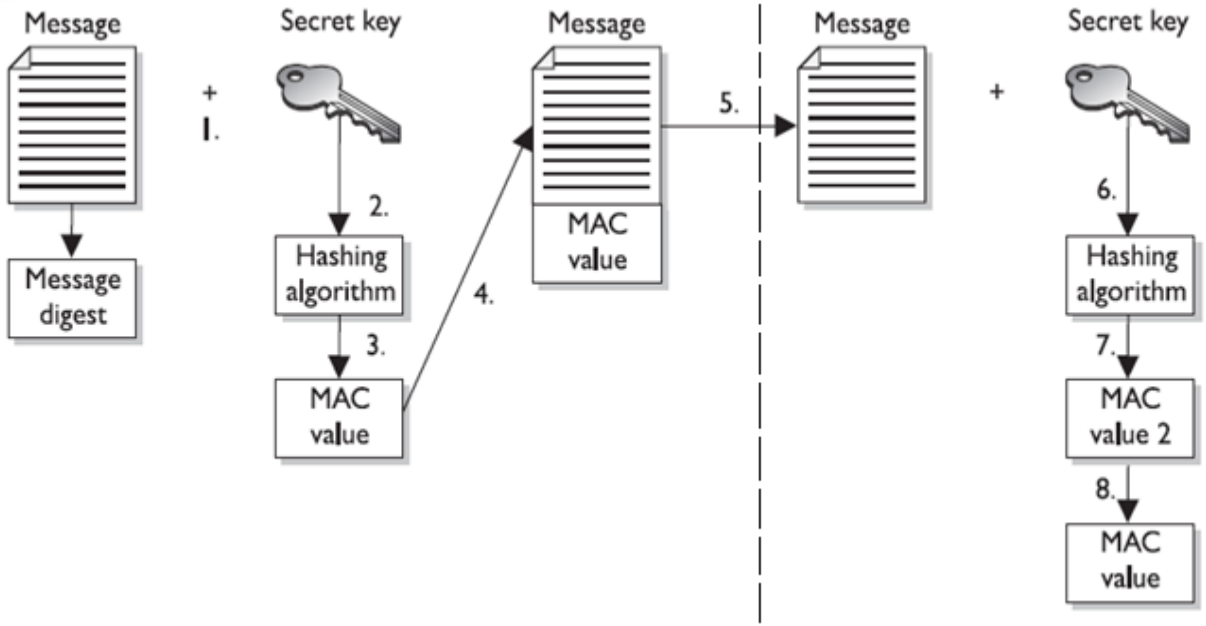
- Goals of Cryptography
  - Confidentiality
  - Integrity
  - Availability
  - Non-Repudiation

Advanced Hashing Cryptography Concepts

Algorithm that takes a variable-length input and generates a fixed-length output

- Footprint of data
- Proves integrity only
- Works best with with PKI for HMAC
- One-way function
- Non reversable
- Used to create checksums or message digests
- Ensures data integrity
- Collision resistance

Advanced Hashing Cryptography Concepts



Advanced Hashing Cryptography Concepts

Online MD5 Calculator - Dwayne Hodges loves Infromation Secuirty - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Online MD5 Calculator - Dwayne Hodge...

md5-online.tk/?q=Dwayne+Hodges+loves+Infromation+Secuirty+

WhiteSmoke US New Customized Web Search

Online MD5 Calculator

Welcome to Online **MD5 Calculator**. The purpose of this site is to allow fast and easy calculation of MD5 function for any input. **MD5** is cryptographic hash function. It converts input of arbitrary length into 128-bit hash value, represented as 32 hexadecimal digits.

MD5 is widely used for checksumming - calculating hash value of file content allows one to validate if it has been tampered with. It is also possible to use **MD5** to securely store passwords.

Enter plaintext: Go

Your plaintext: **Dwayne Hodges loves Infromation Secuirty**

MD5 hash: **627a1931abb8d091631d315eb80a2c66**

SHA1 hash: **961cf990a49636da3487772c697a3b62c8e2660e**

CRC32 checksum: **-1649329993**

ROT13 transform: **Qjnlar Ubqtrf ybirf Vasebzngvba Frphvegl**

Check also hashes for those values: Dwayne Hodges loves Infromation Secuirty A / Dwayne Hodges loves Infromation Secuirty B / Dwayne Hodges loves Infromation Secuirty C / Dwayne Hodges loves Infromation Secuirty D / Dwayne Hodges loves Infromation Secuirty E / Dwayne Hodges loves Infromation Secuirty F / Dwayne Hodges loves Infromation Secuirty G / Dwayne Hodges loves Infromation Secuirty H / Dwayne Hodges loves Infromation Secuirty I / Dwayne Hodges loves Infromation Secuirty J / Dwayne Hodges loves Infromation Secuirty K / Dwayne Hodges loves Infromation Secuirty L / Dwayne Hodges loves Infromation Secuirty M / Dwayne Hodges loves Infromation Secuirty N / Dwayne Hodges loves Infromation Secuirty O / Dwayne Hodges loves Infromation Secuirty P / Dwayne Hodges loves Infromation Secuirty Q / Dwayne Hodges loves Infromation Secuirty R / Dwayne Hodges loves Infromation Secuirty S / Dwayne Hodges loves Infromation Secuirty T / Dwayne Hodges loves Infromation Secuirty U / Dwayne Hodges loves Infromation Secuirty V / Dwayne Hodges loves Infromation Secuirty W / Dwayne Hodges loves Infromation Secuirty X / Dwayne Hodges loves Infromation Secuirty Y / Dwayne Hodges loves Infromation Secuirty Z / Dwayne Hodges loves Infromation Secuirty a / Dwayne Hodges loves Infromation Secuirty b / Dwayne Hodges loves Infromation Secuirty c / Dwayne Hodges loves Infromation Secuirty d / Dwayne Hodges loves Infromation Secuirty e / Dwayne Hodges loves Infromation Secuirty f / Dwayne Hodges loves Infromation Secuirty g / Dwayne Hodges loves Infromation Secuirty h / Dwayne Hodges loves Infromation Secuirty i / Dwayne Hodges loves Infromation Secuirty j / Dwayne Hodges loves Infromation Secuirty k / Dwayne Hodges loves Infromation Secuirty l / Dwayne Hodges loves Infromation Secuirty m / Dwayne Hodges loves Infromation Secuirty n / Dwayne Hodges loves Infromation Secuirty o / Dwayne Hodges loves Infromation Secuirty p / Dwayne Hodges loves Infromation Secuirty q / Dwayne Hodges loves Infromation Secuirty r / Dwayne Hodges loves Infromation Secuirty s / Dwayne Hodges loves Infromation Secuirty t / Dwayne Hodges loves Infromation Secuirty u / Dwayne Hodges loves Infromation Secuirty v / Dwayne Hodges loves Infromation Secuirty w / Dwayne Hodges loves Infromation Secuirty x / Dwayne Hodges loves Infromation Secuirty y / Dwayne Hodges loves Infromation Secuirty z / Dwayne Hodges loves Infromation Secuirty 0 / Dwayne Hodges loves Infromation Secuirty 1 / Dwayne Hodges loves Infromation Secuirty 2 / Dwayne Hodges loves Infromation Secuirty 3 / Dwayne Hodges loves Infromation Secuirty 4 / Dwayne Hodges loves Infromation Secuirty 5 / Dwayne Hodges loves Infromation Secuirty 6 / Dwayne Hodges loves Infromation Secuirty 7 / Dwayne Hodges loves Infromation Secuirty 8 / Dwayne Hodges loves Infromation Secuirty 9 / Dwayne Hodges loves Infromation Secuirty

Advanced Hashing Cryptography Concepts the “ Avalanche affect”

- Your plaintext: **dwayne hodges loves information security**
- MD5 hash: **86f088900260389e37cb7806b996dd6f**
- SHA1 hash: **34d742dcffc0a1e5c686def53d9d30e0c009d9e8**
- CRC32 checksum: **1053360939**
- ROT13 transform: **qjnlar ubqtrf ybirf vasbezngvba frphevg**

Love without the “s”

plaintext: **dwayne hodges love information security** MD5 hash: **81c09ae95680e3c5debcfac0072f4b52**

SHA1 hash: **cf9e66658b906731fb8e99a69b8b1ff27fd0aefa**

CRC32 checksum: **-95024785**

ROT13 transform: **qjnlar ubqtrf ybir vasbezngvba frphevgl**

Advanced Hashing Cryptography Concepts

Collisions

- Happen when an algorithm produce the same output or digest on two different inputs
- This is called a birthday attack
  - A paradox that with 23 people in the same room, two are likely to have the same birthday

Hash Function	Size
MD5	128
SHA0/1	160
SHA-2 256	224,256,384,512
SHA-3	224,256, 384, 512 (operations/internal structure different
FORK	256
Race Integrity Primitive Evaluation Message Digest (RIPEMD)	160
GOST (Russian National Standard)	256