Message Integrity

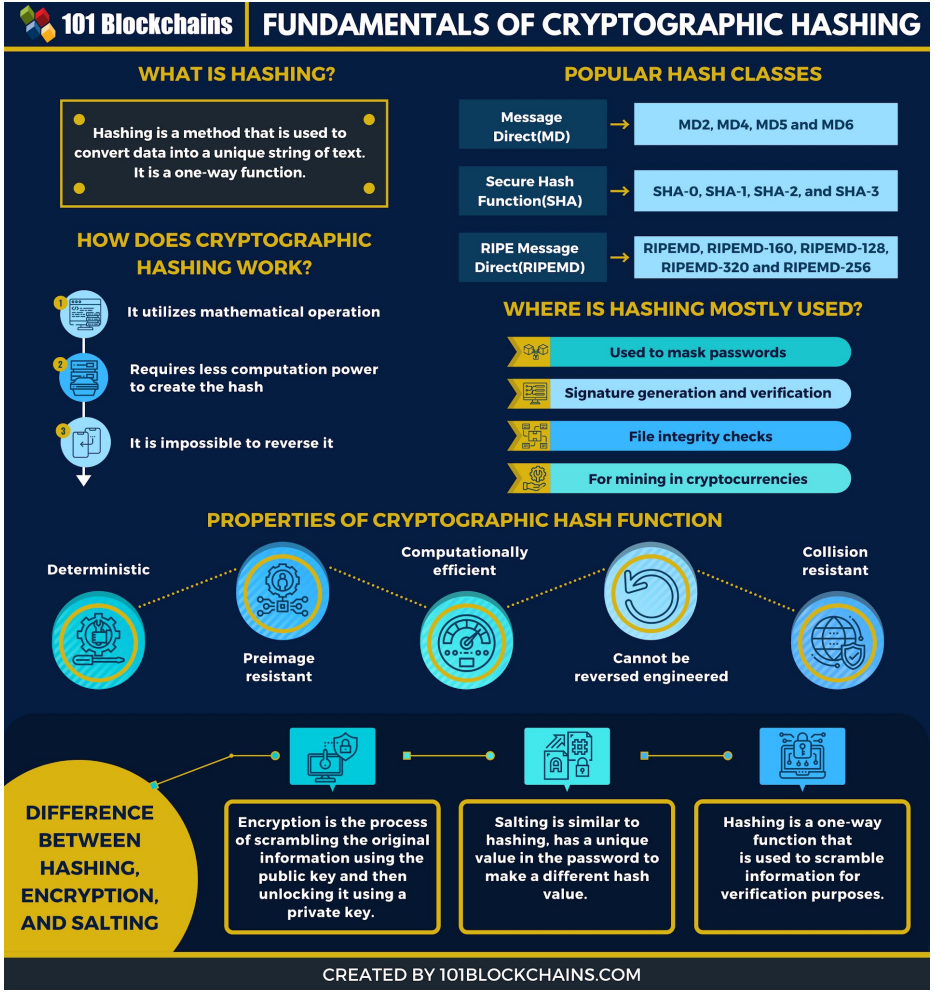
Devharsh Trivedi

Index

Introduction

Cryptographic primitive Security Goal	Hash	MAC	Digital signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudiation	No	No	Yes
Kind of keys	none	symmetric keys	asymmetric keys

Hash


101 Blockchains
FUNDAMENTALS OF CRYPTOGRAPHIC HASHING
WHAT IS HASHING?
Hashing is a method that is used to convert data into a unique string of text. It is a one-way function.
POPULAR HASH CLASSES
Message Direct(MD)
MD2, MD4, MD5 and MD6
Secure Hash Function(SHA)
SHA-0, SHA-1, SHA-2, and SHA-3
RIPE Message Direct(RIPEMD)
RIPEMD, RIPEMD-160, RIPEMD-128, RIPEMD-320 and RIPEMD-256
HOW DOES CRYPTOGRAPHIC HASHING WORK?
1
It utilizes mathematical operation
2
Requires less computation power to create the hash
3
It is impossible to reverse it
WHERE IS HASHING MOSTLY USED?
Used to mask passwords
Signature generation and verification
File integrity checks
For mining in cryptocurrencies
PROPERTIES OF CRYPTOGRAPHIC HASH FUNCTION
Deterministic
Preimage resistant
Computationally efficient
Cannot be reversed engineered
Collision resistant
DIFFERENCE BETWEEN HASHING, ENCRYPTION, AND SALTING
Encryption is the process of scrambling the original information using the public key and then unlocking it using a private key.
Salting is similar to hashing, has a unique value in the password to make a different hash value.
Hashing is a one-way function that is used to scramble information for verification purposes.
CREATED BY 101BLOCKCHAINS.COM

Hash : Demo

- https://www.pelock.com/products/hash-calculator
- https://docs.oracle.com/javase/8/docs/api/java/security/MessageDigest.html
- Hash.java

- https://www.iusmentis.com/technology/hashfunctions/md5/
- MD5_impl.java

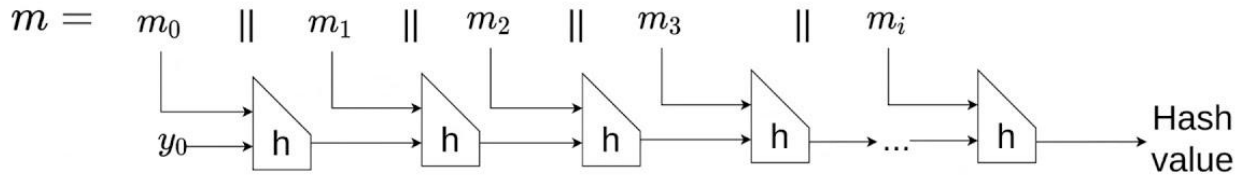
Length Extension Attack

CYBER CAMPUS NRW

cry.college

MD

In a Merkle-Damgard system, the hash value is the last chaining value:



if we have a hash value, we can just “continue” the computation.

Length Extension Attack : Demo

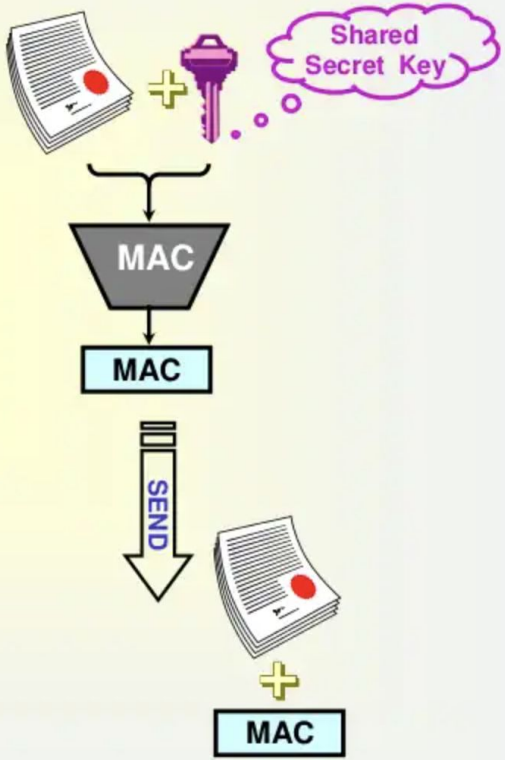
- MD5(secretdata) = 6036708eba0d11f6ef52ad44e8b74d5b
- "secret" = secret
- "data" = data
- 80 00 00 ... — The 46 bytes of padding, starting with 0x80
- 50 00 00 00 00 00 00 00 — The bit length in little endian

- https://cryptii.com/pipes/md5-hash
- hash_extension_1.c
- hash_extension_2.c

MAC

Message Authentication Codes (MACs)

- **MAC**
  - ✓ Generate a fixed length MAC for an arbitrary length message
  - ✓ A keyed hash function
  - ✓ Message origin authentication
  - ✓ Message integrity
  - ✓ Entity authentication
  - ✓ Transaction authentication
- **Constructions**
  - ✓ Keyed hash: HMAC, KMAC
  - ✓ Block cipher: CBC-MAC
  - ✓ Dedicated MAC: MAA, UMAC

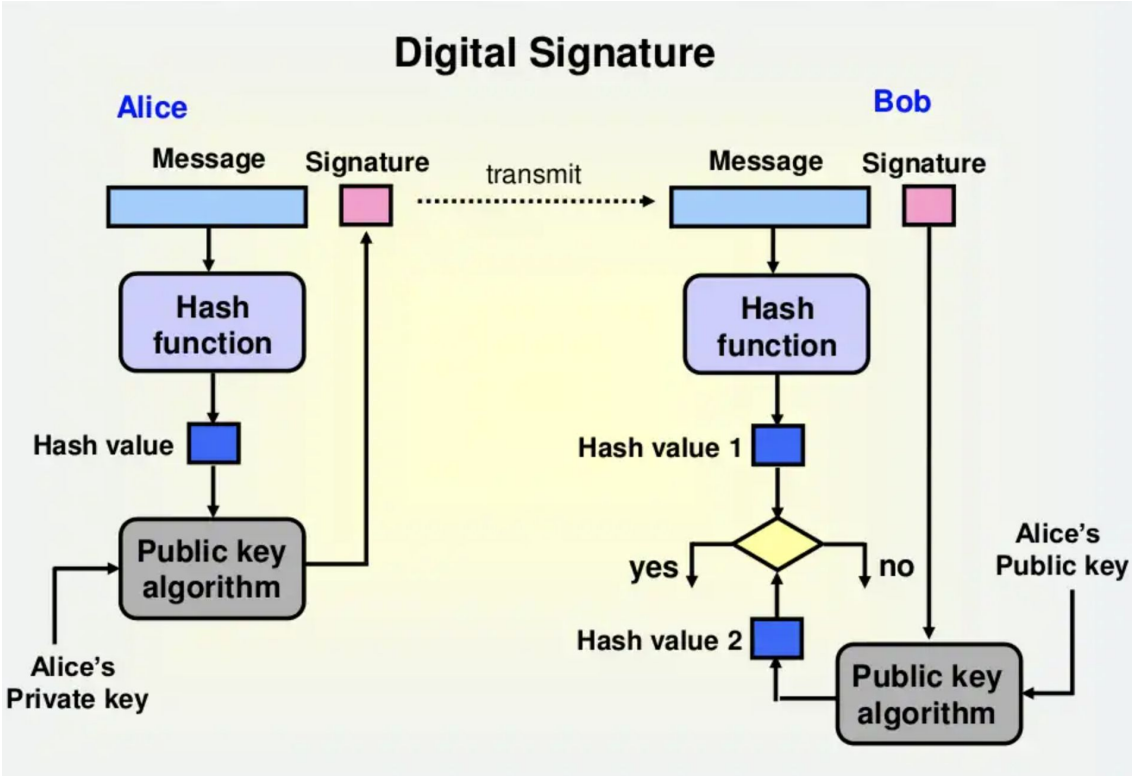


MAC : Demo

- https://cryptopp.com/wiki/Category:MAC
- https://www.apriorit.com/images/articles/Top_7_Methods_of_Data_Encryption_in_Android_Applications/figure-6.jpg

- HMAC.java
- https://docs.microsoft.com/en-us/dotnet/api/javax.crypto.mac?view=xamarin-android-sdk-9
- https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html#Mac

Digital Signature



Digital Signature : Demo

- GenerateDigitalSignature.java

Resources

- https://www.cryptologie.net/article/389/a-hash-function-does-not-provide-integrity/
- https://101blockchains.com/cryptographic-hashing/
- https://www.youtube.com/watch?v=QLSlKxAQD8I
- https://blog.skullsecurity.org/2012/everything-you-need-to-know-about-hash-length-extension-attacks
- https://www.coursera.org/learn/crypto/lecture/LbrG3/introduction
- https://www.slideshare.net/HarryPotter40/hash-function-61328365