[](https://ida.interchain.io/)

[Interchain Developer Academy](https://ida.interchain.io/)/[Interchain Developer Academy](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)



Search

[Interchain Developer Academy](https://ida.interchain.io/)[Interchain Developer Academy](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

Search



Filters

Interchain Developer Academy

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 0 - Getting Started](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Getting Started](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Blockchain 101](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Blockchain History](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Public and Managed Blockchains](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Consensus in Distributed Networks](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Cryptography](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Self-Assessment Quiz](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Go Introduction - First Steps](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Go Basics](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Go Interfaces](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Control Structures in Go](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Arrays and Slices in Go](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Standard Packages in Go](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Concurrency in Go](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Good-To-Know Dev Terms](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Docker Introduction](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 1 - Introduction to the Interchain](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Introduction to the Interchain](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Blockchain Technology and the Interchain](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[The Interchain Ecosystem](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Getting ATOM and Staking It](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[A Blockchain App Architecture](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Accounts](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Transactions](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Messages](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Modules](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Protobuf](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Multistore and Keepers](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[BaseApp](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Queries](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Events](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Context](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Testing](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Relaying with IBC](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Interchain Security](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Bridges](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Migrations](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 1 Quiz](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 2 - First Steps](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[First Steps](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Setup Your Work Environment](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Run a Node, API, and CLI](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Ignite CLI](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Exercise - Make a Checkers Blockchain](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Store Object](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Create Custom Messages](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Create and Save a Game Properly](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Add a Way to Make a Move](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Emit Game Information](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Record the Game Winner](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 2 Exercise](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 3 - Introduction to IBC and CosmJS](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Introduction to IBC and CosmJS](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[What is IBC?](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC/TAO - Connections (OPTIONAL)](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC/TAO - Channels (OPTIONAL)](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC/TAO - Clients (OPTIONAL)](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC Token Transfer](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Interchain Accounts (OPTIONAL)](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC Middleware (OPTIONAL)](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Create a Custom IBC Middleware (OPTIONAL)](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Integrate IBC Middleware Into a Chain (OPTIONAL)](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC Tooling](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[What is CosmJS?](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Your First CosmJS Actions](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Compose Complex Transactions](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Learn to Integrate Keplr](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Create Custom CosmJS Interfaces](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 4 - Ignite CLI and IBC Advanced](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Ignite CLI and IBC Advanced](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Keep an Up-To-Date Game Deadline](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Keep Track Of How Many Moves Have Been Played](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Put Your Games in Order](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Auto-Expiring Games](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Let Players Set a Wager](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Handle wager payments](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Integration tests](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Incentivize Players](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Help Find a Correct Move](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Play With Cross-Chain Tokens](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Understand IBC Denoms](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Go Relayer](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Hermes Relayer](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 5 - CosmJS Advanced](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[CosmJS Advanced](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Create Custom Objects](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Create Custom Messages](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Get an External GUI](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Integrate CosmJS and Keplr](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Backend Script for Game Indexing](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 6 - IBC Deep Dive](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC Deep Dive](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[IBC Application Developer Introduction](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Make a Module IBC-Enabled](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Adding Packet and Acknowledgment Data](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Extend the Checkers Game With a Leaderboard](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Create a Leaderboard Chain](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Week 7 - From Code to MVP to Production and Migrations](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[From Code to MVP to Production and Migrations](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Run in Production](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Prepare the Software to Run](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Prepare a Validator and Keys](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Prepare Where the Node Starts](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Prepare and Connect to Other Nodes](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Configure, Run, and Set Up a Service](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Prepare and Do Migrations](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Simulate Production in Docker](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Tally Player Info After Production](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Add a Leaderboard as a Module](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Migrate the Leaderboard Module After Production](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Simulate a Migration in Docker](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Final Exam](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[What's Next?](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

[Continue Your Interchain Journey](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html)

Docs Version Switcher

On this page

[Public and private keys](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#public-and-private-keys)

[Encrypt and decrypt](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#encrypt-and-decrypt)

[Sign and verify](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#sign-and-verify)

[Mix and match](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#mix-and-match)

[Is this science or magic?](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#is-this-science-or-magic)

[Key management and public key infrastructure](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#key-management-and-public-key-infrastructure)

[Cryptographic hash functions](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#cryptographic-hash-functions)

[A closer look at a hash function](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#a-closer-look-at-a-hash-function)

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#cryptographic-fundamentals-of-blockchain) **Cryptographic Fundamentals of Blockchain**

Modern cryptography leverages computer capabilities to make the power of certain mathematical functions available for practical use. Without modern cryptography, there would be no blockchain technology.

Therefore, anyone new to blockchains discovers frequent references to message signatures and other concepts related to cryptography. While this is not an extensive exploration of the topic and you will not deep dive into the mathematics, this section will demystify important concepts if they are new to you.

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#public-and-private-keys) Public and private keys

In public-key cryptographic systems, keys always **come in pairs** and offer various capabilities. The capabilities are based on cryptographic mathematics. As the name suggests, the **public key** is meant to be distributed while the **private key** is to be jealously guarded. Compare the key pairs to having your house address public but keeping the key to your house private.

The following example will help to better understand public/private keys, which you may know under the names:

* RSA
* PGP or GnuPG



Copy

// Create SECP256K1 private key with explicit parameters for backward compatibility

$ openssl ecparam -name secp256k1 -genkey -noout -out secp256k1-key.pem -param\_enc explicit

// Create public key

$ openssl ec -in secp256k1-key.pem -pubout -out secp256k1-key-pub.pem

// Show public key

$ openssl ec -in secp256k1-key-pub.pem -pubin -text -noout

// Create RSA private key

$ openssl genrsa -des3 -out rsa-key.pem 2048

Generating RSA private key, 2048 bit long modulus

.....................................................+++

...........+++

e is 65537 (0x10001)

Enter pass phrase for rsa-key.pem:

Verifying - Enter pass phrase for rsa-key.pem:

// Create public key

$ openssl rsa -in rsa-key.pem -outform PEM -pubout -out rsa-key-pub.pem

Enter pass phrase for rsa-key.pem:

writing RSA key

This is like a password that is used to encrypt your private key on disk. If the private key was not encrypted, it would be at greater risk of theft. Since you are just testing here, you can put in nothing or just a simple word. Still remember that whenever you create keys in the future, you need to protect them with a proper password.



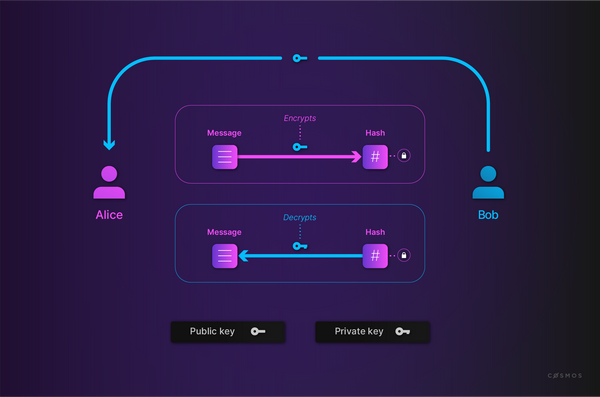
You may need openssl version 1.0 or a newer one.

Now take a look at scenarios in which public/private key pairs are useful.

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#encrypt-and-decrypt) Encrypt and decrypt

Alice wants to send a message to Bob that is meant for Bob's eyes only:

1. Bob gives Alice his public key.
2. Alice uses Bob's public key to encrypt the message.
3. Alice sends Bob the encrypted message.
4. Bob decrypts the message with his private key.



Now look at the senario code-wise. For example, try the following:



Copy

// Encrypt file

$ openssl pkeyutl -encrypt -pubin -inkey rsa-key-pub.pem -in helloworld.txt -out helloworld.enc

// Decrypt file

$ openssl pkeyutl -decrypt -inkey rsa-key.pem -in helloworld.enc -out helloworld2.txt

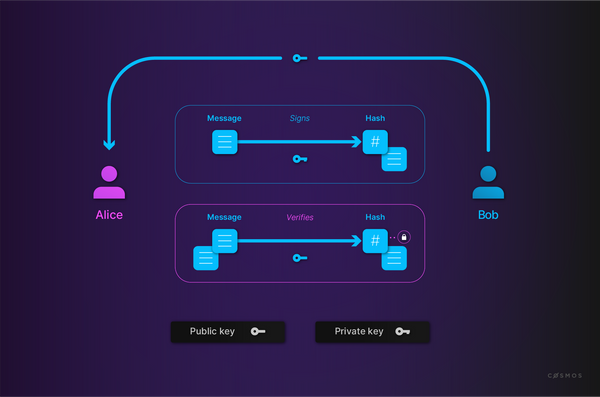


If you receive an error, try with openssl rsautl instead.

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#sign-and-verify) Sign and verify

Alice wants to make sure that Bob's public announcement is indeed from Bob:

1. Bob gives Alice his public key.
2. Bob signs his announcement with his private key.
3. Bob sends Alice his announcement and its signature.
4. Alice verifies the signature with Bob's public key.



Back to the code example:



Copy

# Sign file hash

$ openssl dgst -sha256 -sign secp256k1-key.pem -out helloworld-bin.sha256 helloworld.txt

# Encode signature in Base64

$ openssl base64 -in helloworld-bin.sha256 -out helloworld.sha256

# Decode signature form Base64

$ openssl base64 -d -in helloworld.sha256 -out helloworld-bin-decoded.sha256

# Verify signature

$ openssl dgst -sha256 -verify secp256k1-key-pub.pem -signature helloworld-bin-decoded.sha256 helloworld.txt

Which finally prints:



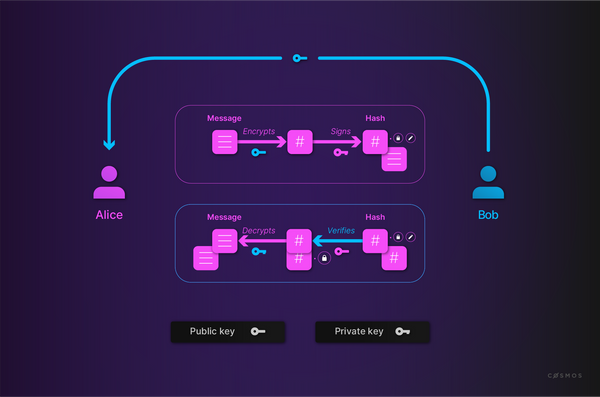
Copy

Verified OK

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#mix-and-match) Mix and match

It is possible to mix both conceptual ideas. For example:

1. Alice encrypts her message with Bob's public key.
2. Alice signs the encrypted file with her private key.
3. Upon reception, Bob verifies the signature with Alice's public key to make sure the file came from Alice.
4. Bob decrypts the file with his private key.



[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#is-this-science-or-magic) Is this science or magic?

If these examples seem counter-intuitive it means you sense the mathematical shadow of public-key encryption. You do not have to understand the mathematics behind it at a deep level, but you must understand the properties and implications of using public-key cryptography.

Given four keys (A, B, C, and D), we can encrypt a message with three keys (A, B, and C) such that the fourth key (in this case, D) is required to decrypt it and is very hard to guess or discover. So, if Alice knows her private key and her public key and she also knows Bob's public key, she can encrypt a message that can only be understood by someone who knows Bob's private key.

Similarly, given knowledge of public and private keys, one can generate a signature (i.e. a character string) so that someone with a copy of the message and the signature can independently determine the public key of the entity that signed the message, proving that the signer knows the corresponding private key.

It is then possible to proceed with the understanding that signed messages from Alice could only come from someone with knowledge of Alice's private key, and messages that are encrypted for Bob can only be deciphered by Bob.

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#key-management-and-public-key-infrastructure) Key management and public key infrastructure

If you look again at the Alice and Bob examples, you will notice that there is a vulnerability in "Bob gives Alice his public key". A malicious Charlie could intercept Bob's public key and pass on *his own* public key to Alice.

Key management and public key infrastructure (PKI) is an important aspect of cryptography that helps mitigate this risk.

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#cryptographic-hash-functions) Cryptographic hash functions

Blockchain technology relies heavily on hash functions, as they help establish the so-called "chain of blocks".

All cryptographic hash functions fulfill several properties:

* Converts an input (a.k.a. the message) into an output (a.k.a the hash).
* Does the conversion in a reasonable amount of time.
* It is practically impossible to re-generate the message out of the hash.
* The tiniest change in the message changes the hash beyond recognition.
* It is practically impossible to find two different messages with the same hash.

With such a function, you can:

* Prove that you have a message without disclosing the content of the message, for instance:
  + To prove you know your password.
  + To prove you previously wrote a message.
* Be confident that the message was not altered.
* Index your messages.

[#Copy link](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#a-closer-look-at-a-hash-function) A closer look at a hash function

MD5 is such a hash function:



Copy

$ echo "The quick brown fox jumps over the lazy dog" | md5

Which prints:



Copy

37c4b87edffc5d198ff5a185cee7ee09

On Linux, this is md5sum.

Now introduce a typo to see what happens (e.g. changing "jumps" to "jump"):



Copy

$ echo "The quick brown fox jump over the lazy dog" | md5

Which prints:



Copy

4ba496f4eec6ca17253cf8b7129e43be

Notice how the two hashes have nothing in common other than their length, but length is identical for all MD5 hashes so it reveals nothing about the input.



This provides a convenient example, but MD5 is no longer considered a hard-to-crack hash function. Bitcoin uses SHA-256. Ethereum uses Keccak-256and Keccak-512.



**Further readings**

* [The Mathematics of the RSA Public-Key Cryptosystem (opens new window)↗](https://www.nku.edu/~christensen/the%20mathematics%20of%20the%20RSA%20cryptosystem.pdf)
* [OSCDaily (2012): Encrypt & Decrypt Files from the Command Line with OpenSSL (opens new window)↗](http://osxdaily.com/2012/01/30/encrypt-and-decrypt-files-with-openssl/)
* [Zimuel, Enrico (2016): Sign and verify a file using an OpenSSL comand line tool (opens new window)↗](https://gist.github.com/ezimuel/3cb601853db6ebc4ee49)

synopsis

To summarize, this section has explored:

* How modern cryptography leverages computing to make complex mathematical functions useful on a practical level, providing the essential foundation for blockchain technology.
* How public/private key systems are used to encrypt and decrypt private messages across a public network, providing certainty to both parties that only the intended recipient can open them and that only the claimed sender can be the actual source.
* How cryptographic hash functions allow for such things as the one-way confirmation of data; for example, being able to check that a person has a particular piece of data *without the necessity of actually sharing that data as part of the check*.

previous

[](https://ida.interchain.io/ida-course/0-blockchain-basics/4-consensus.html)

**[Consensus in Distributed Networks](https://ida.interchain.io/ida-course/0-blockchain-basics/4-consensus.html)**

up next

**[Self-Assessment Quiz](https://ida.interchain.io/ida-course/0-blockchain-basics/6-quiz.html)**

[[](https://ida.interchain.io/ida-course/0-blockchain-basics/6-quiz.html)](https://ida.interchain.io/ida-course/0-blockchain-basics/6-quiz.html)

Rate this Page

icon smile

icon meh

icon frown

Would you like to add a message?

Submit

Thank you for your Feedback!

[](https://ida.interchain.io/ida-course/discord-info.html)

On this page

[Public and private keys](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#public-and-private-keys)

[Encrypt and decrypt](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#encrypt-and-decrypt)

[Sign and verify](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#sign-and-verify)

[Mix and match](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#mix-and-match)

[Is this science or magic?](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#is-this-science-or-magic)

[Key management and public key infrastructure](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#key-management-and-public-key-infrastructure)

[Cryptographic hash functions](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#cryptographic-hash-functions)

[A closer look at a hash function](https://ida.interchain.io/ida-course/0-blockchain-basics/5-crypto.html#a-closer-look-at-a-hash-function)

#### **Get Cosmos updates**

Unsubscribe at any time. [Privacy Policy↗](https://v1.cosmos.network/privacy)

     Next

Documentation

[Cosmos SDK](https://docs.cosmos.network/)[Cosmos Hub](https://hub.cosmos.network/)[CometBFT](https://docs.cometbft.com/)[IBC Protocol](https://ibc.cosmos.network/)

Community

[Interchain blog](https://blog.cosmos.network/)[Forum](https://forum.cosmos.network/)[Discord](https://discord.gg/cosmosnetwork)

Contributing

[Source code on GitHub](https://github.com/cosmos/sdk-tutorials)

[](https://ida.interchain.io/)

[Interchain Developer Academy](https://ida.interchain.io/)

**[](https://blog.cosmos.network/)[](https://twitter.com/cosmos)[](https://discord.gg/cosmosnetwork)[](https://www.linkedin.com/company/interchain-foundation/about/)[](https://reddit.com/r/cosmosnetwork)[](https://t.me/cosmosproject)[](https://www.youtube.com/c/CosmosProject)**



Dark mode

† This website is maintained by the Interchain Foundation (ICF). The contents and opinions of this website are those of the ICF. The ICF provides links to cryptocurrency exchanges as a service to the public. The ICF does not warrant that the information provided by these websites is correct, complete, and up-to-date. The ICF is not responsible for their content and expressly rejects any liability for damages of any kind resulting from the use, reference to, or reliance on any information contained within these websites.

Cosmos is a registered trademark of the [Interchain Foundation.](https://interchain.io/)[Privacy](https://v1.cosmos.network/privacy)