Khatam Blockchain Lab

Basic Cryptography for Blockchain

Mohammad Tehrani

Faculty at Computer School at Khatam Univ.

matehrani

- **Steganography**

  concealing a msg in another msg without attracting attention

- **Cryptography**

  Secure communication in presence of third party

Khatam Blockchain Lab

Kirchhoff's principle

1) The system must be practically, if not mathematically, indecipherable.
2) It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.
3) Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents.
4) It must be applicable to telegraphic correspondence.
5) Apparatus and documents must be portable, and its usage and function must not require the concourse of several people.
6) Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

Khatam Blockchain Lab

Cryptography

- **Unkeyed**

  Cryptographic Hash function

- **Keyed**

  Symmetric-key algorithms

  Asymmetric-key algorithms

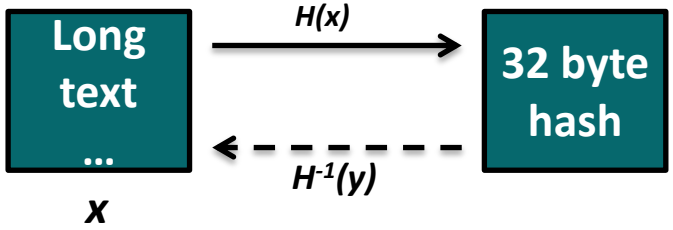
Cryptographic hash functions

- Any input string → Fix length string
- Always the same for the same input
- Small change in input →Large change in output
- Fast computation

Khatam Blockchain Lab

Cryptographic hash functions

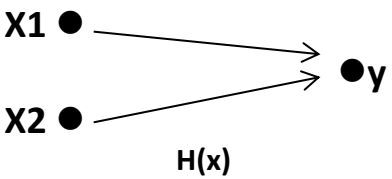
- Assume ***H(x)*** is a cryptographic hash function
- Fast computable
- ***H(x)*** is a **one-way** mathematical functions
- Finding the $H^{-1}(y)$ is computationally hard



Khatam Blockchain Lab

Cryptographic hash functions

Collision resistance



Given the **X1** it is computationally hard to find **X2**

Random looking

Small perturbation in **x** leads to big and random looking changes in **H(x)**

Fixed size output

It means that collision do exists.

- Bitcoin uses **SHA256** as its cryptographic hash function.

Khatam Blockchain Lab

Cryptographic hash functions
Collision resistance

- **Weak collision resistance**

  given an input, it is computationally infeasible to find another input with the same hash

- **Strong collision resistance**

  It is computationally infeasible to find two input that result in the same hash

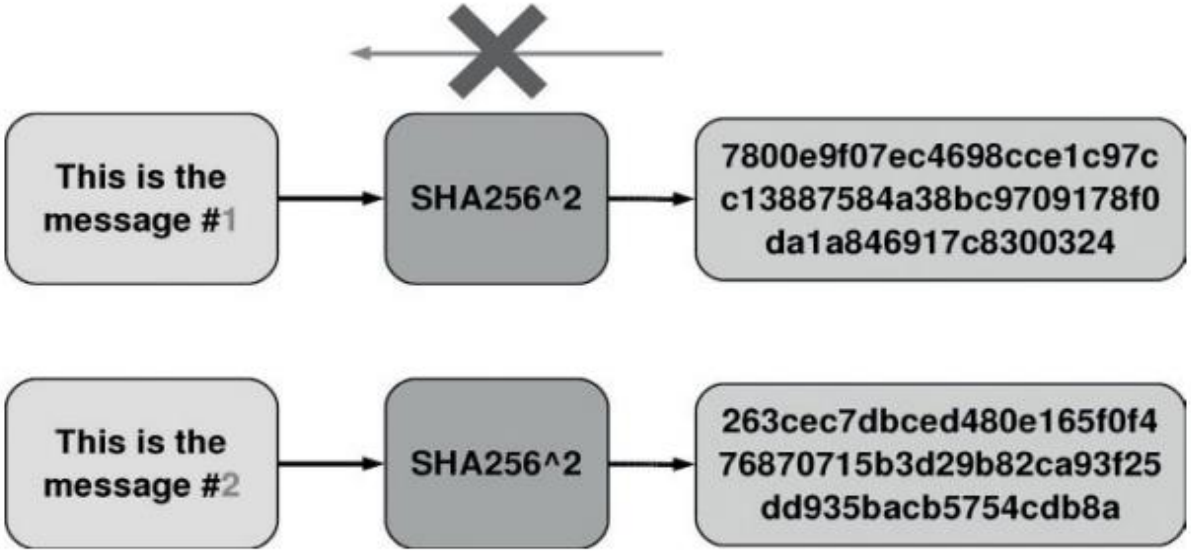
Khatam Blockchain Lab

Hash finger print

- Using **collision resistance** and **random looking** property one can use hash as **finger print.**
- No one have found two different files with same **SHA256.**
- We can assume hash of a file is a **unique property** of it.

Khatam Blockchain Lab

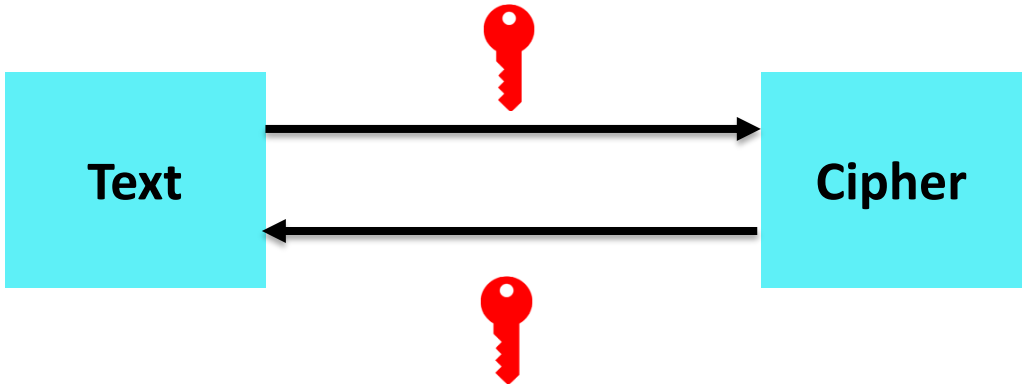
Bitcoin hash functions



Bitcoin uses SHA256^2 for proof of work

Khatam Blockchain Lab

Symmetric-key cryptography



Bitcoin uses AES-256 for storing private keys in wallet

Khatam Blockchain Lab

Asymmetric-key Cryptography (Public-key)

- Key distribution problem

  when two people use symmetric, they must share the same key.

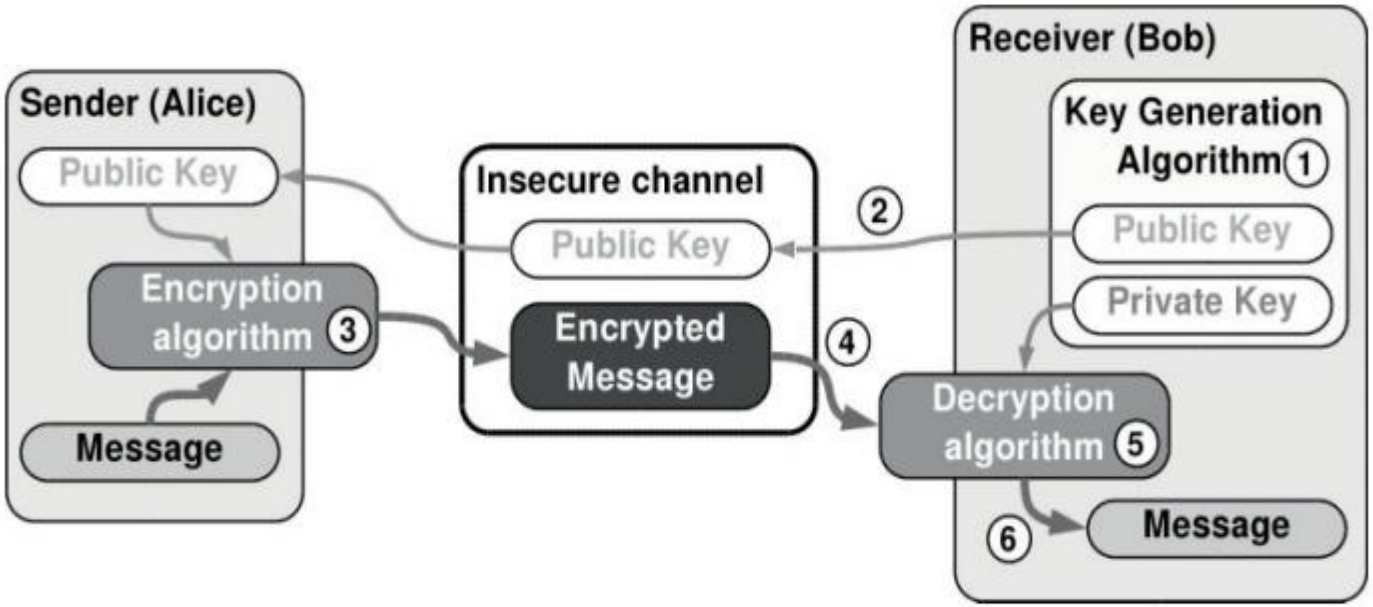
- Public-private key pair

  private: to unlock the safe

  Public : to lock the safe

Khatam Blockchain Lab

Asymmetric-key Cryptography (Public-key)



Khatam Blockchain Lab

Digital Signature

- Everyone have a singing key (aka. Secret key) and a verifier key (aka. Public key).
- Generation a pair of key is easy.
- Finding singing key from verifier key is computationally hard. **As hard as impossible!**

Signing key

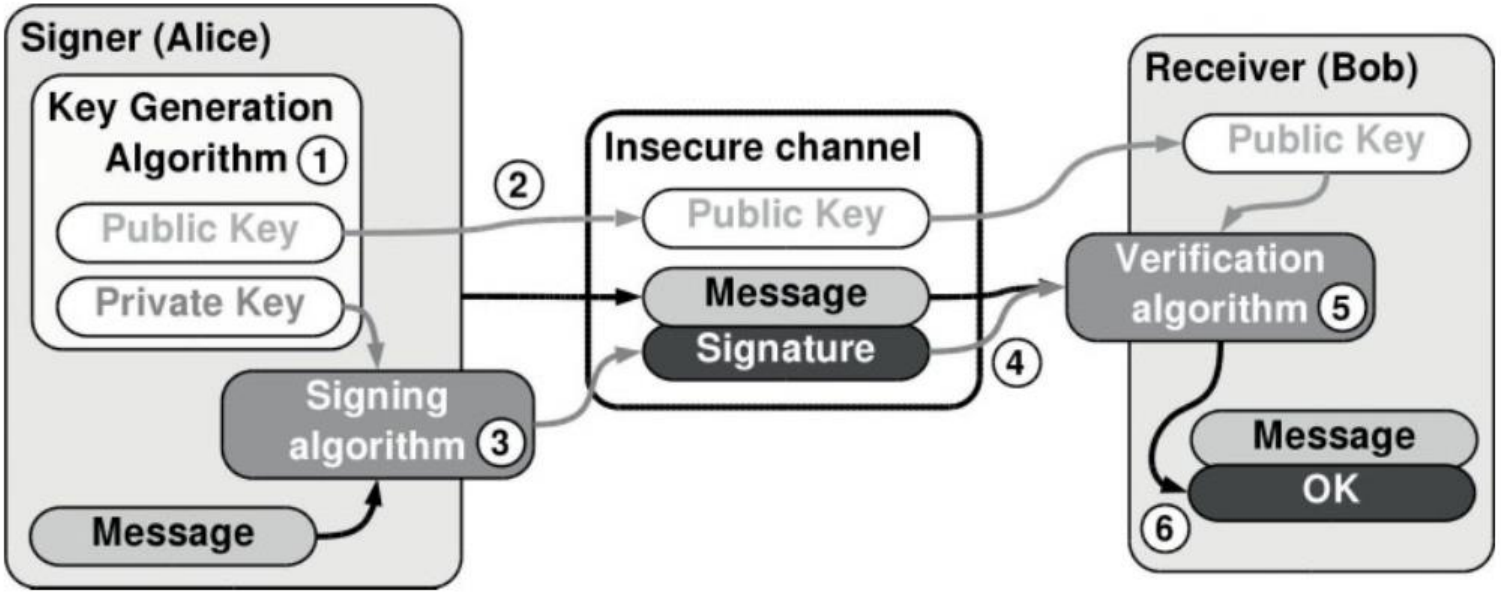
Verifier key

Digital Signature

- Everyone announce her/his verifier key to public, similar to **card number.**
- Bitcoin addresses obtained from verifier key.
- Signing key is secret, similar to **password.**

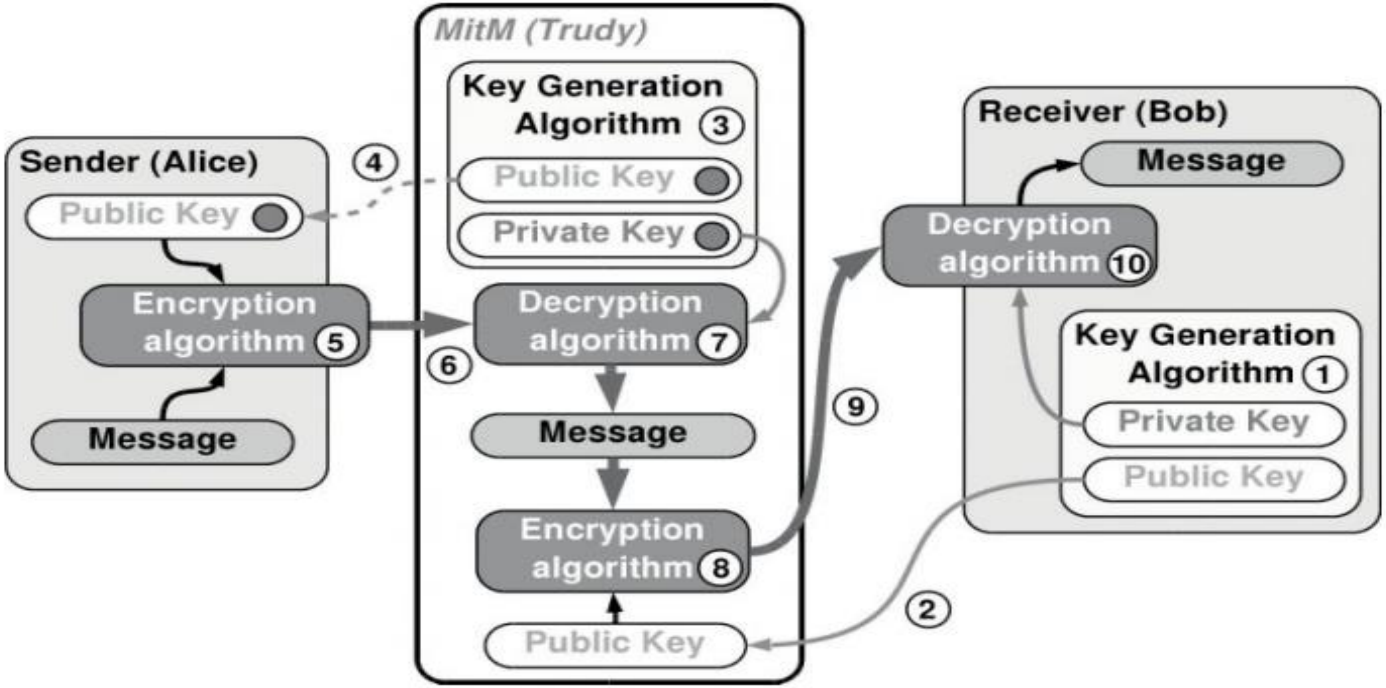
Khatam Blockchain Lab

Digital Signature



Khatam Blockchain Lab

Man-in-the-middle attack



To avoid man-in-the-middle

- Interchange keys using a **different channel**
- **Web of trust**: user sign the public keys of other user they know
- **Public key Infrastructure** (PKI) & Certificate Authority(CA)

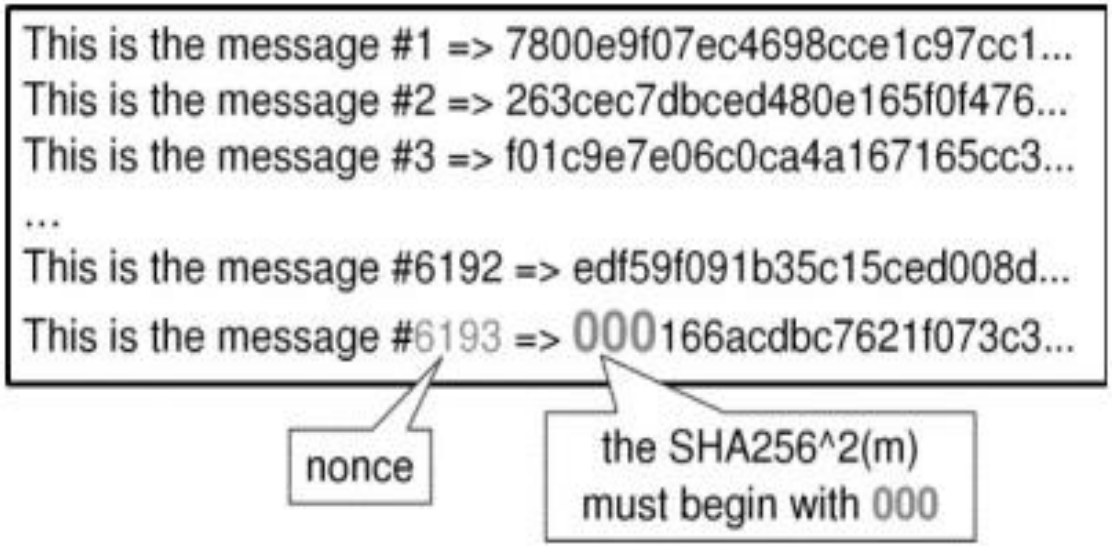
DoS attack

How to avoid DoS attack?

- Sync: challenge-response (CAPTCHA)
- Async: solution-verification (partial hash inversion)

To avoid DoS attack

- Partial hash inversion proof of work



Khatam Blockchain Lab

Bitcoin Address generation