NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 07: Basic Cryptographic Primitives - V

CONCEPTS COVERED

- RSA Encryption and Decryption
- Digital Signature
- Hashing and Digital Signature

KEYWORDS

- RSA
- Digital Signature

RSA Encryption and Decryption

- Let be the integer representation of a message .
- **Encryption with public key**
- **Decryption with private key**

RSA Encryption and Decryption - Example

Key Selection

- Select 2 prime numbers: $p=17$, $q=11$
- Calculate $n=pq=17\times11=187$
- Calculate $\phi(n)=(p-1)(q-1)=16\times10=160$
- Select e such that e is relatively prime to $\phi(n)=160$ and less than $\phi(n)$; Let $e=7$
- Determine d such that $d.e \equiv 1 \bmod 160$ and $d<160$; Can determine $d = 23$ since $23\times7 = 161 = 1\times160+1$

RSA Encryption and Decryption - Example

Encryption of Plaintext M = 88

- $C=88^7 \bmod 187$
- $= [(88^4 \bmod 187)\times(88^2 \bmod 187)\times(88^1 \bmod 187)] \bmod 187 = (88\times77\times132) \bmod 187 =$ 11

Decryption of Ciphertext C = 11

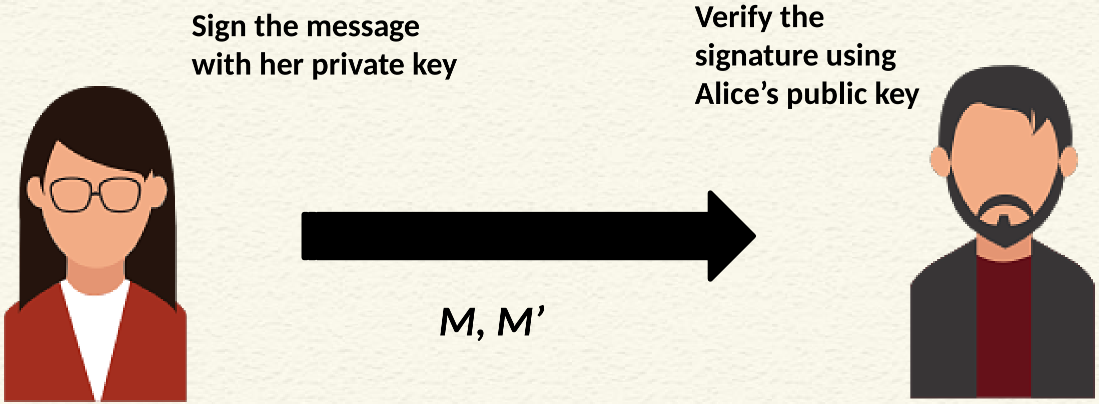
- $M=11^{23} \bmod 187$
- $=[(11^1 \bmod 187)\times(11^2 \bmod 187) \times(11^4 \bmod 187) \times(11^8 \bmod 187) \times(11^8 \bmod 187)] \bmod 187$
- $=(11\times121\times55\times33\times33) \bmod 187 = (79720245) \bmod 187 =$ 88

RSA Encryption and Decryption - Illustration

https://www.devglan.com/online-tools/rsa-encryption-decryption

Digital Signature using Public Key Cryptography

- **Sign the message using the Private key**
  - Only Alice can know her private key
- **Verify the signature using the Public key**
  - Everyone has Alice’s public key and they can verify the signature



Sign the message with her private key

Verify the signature using Alice’s public key

M, M’

Reduce the Signature Size

- Use the message digest to sign, instead of the original message

Sign the message with her private key

Verify the signature using Alice's public key

Digital Signature - Illustration

https://www.devglan.com/online-tools/rsa-encryption-decryption

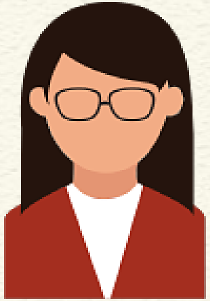
http://www.blockchain-basics.com/HashFunctions.html

Digital Signature in Blockchain

- Used to validate the origin of a transaction
  - Prevent non-repudiation
    - **Alice cannot deny her own transactions**
    - **No one else can claim Alice's transaction as his/her own transaction**

- Bitcoin uses *Elliptic Curve Digital Signature Algorithm* ***(ECDSA)***
  - Based on elliptic curve cryptography
  - Supports good randomness in key generation

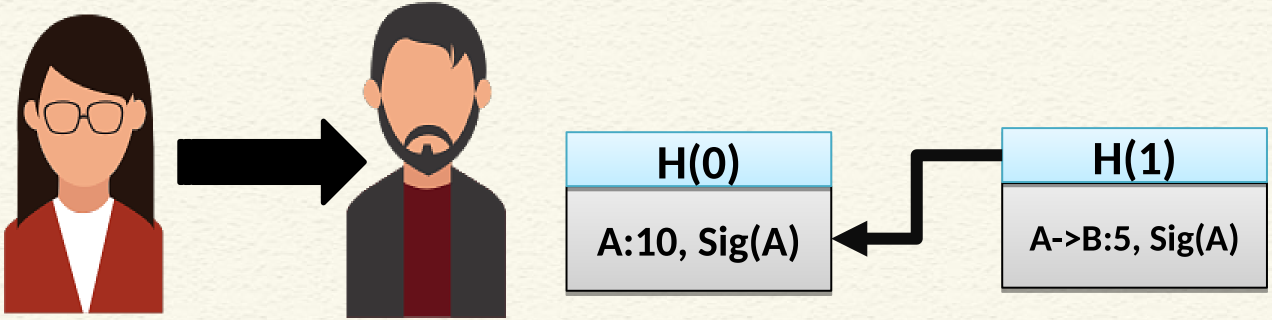
A Cryptocurrency using Hashchain and Digital Signatures



A:10, Sig(A)

- Alice generates 10 coins
- Sign the transaction A:10 using Alice’s private key and put that in the blockchain

A Cryptocurrency using Hashchain and Digital Signatures



- Alice transfers 5 coins to Bob
- Sign the transaction A-B:5 using Alice’s private key and put that in the blockchain

CONCLUSIONS

- We have shown how to encrypt and decrypt using public key cryptography
- Application in digital signature
- Use of digital signature in blockchain

REFERENCES

- Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)
- Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher, Apress (2017)

Thank you