NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

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

Lecture 06: Basic Cryptographic Primitives - IV

CONCEPTS COVERED

- Basic Concepts of Cryptography
- Public Key Cryptography
- Encryption and Decryption using Public Key Cryptography
- Digital Signature

KEYWORDS

- **Public Key Cryptography**
- **RSA**

What we have learnt so far

- **Cryptographically Secure Hash Function**
  - Collision Free
  - Information Hiding
  - Puzzle Friendly

- **Hash Pointers and Data Structures**
  - Hashchain
  - Hash Tree – Merkle Tree

Basic Concepts of Cryptography

- **Symmetric Key Cryptography**
  - Same key used for encryption and decryption
  - How to share the key securely
  - Cannot address certain requirements

- **Public Key Cryptography**
  - One key for encryption, one for decryption
  - Handles several requirements like those in blockchain

Digital Signature

- A **digital code**, which can be included with an electronically transmitted document to verify
  - The content of the document is authenticated
  - The identity of the sender
  - Prevent *non-repudiation* – sender will not be able to deny about the origin of the document

Purpose of Digital Signature

- Only the **signing authority** can sign a document, but everyone can verify the signature

- Signature is **associated with** the particular document
  - Signature of one document cannot be transferred to another document

Public Key Cryptography

- Also known as **asymmetrical cryptography** or **asymmetric key cryptography**

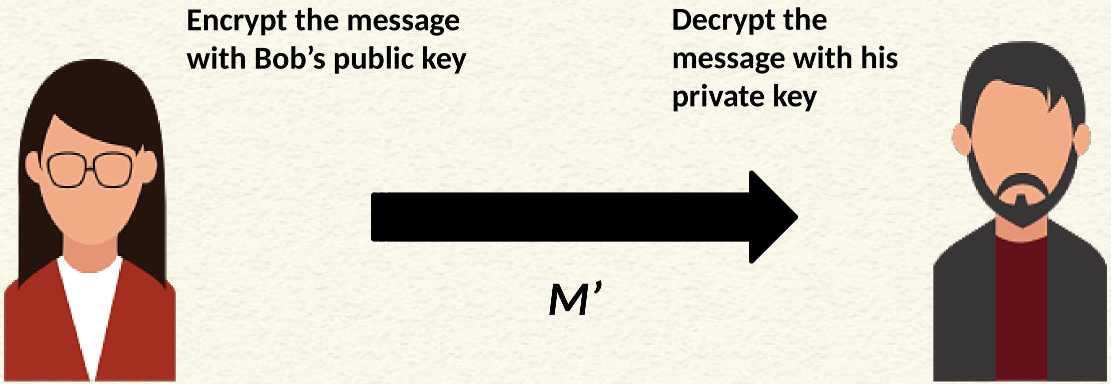
- **Key:** A parameter that determines the functional output of a cryptography algorithm
  - **Encryption:** The key is used to convert a plain-text to a cypher-text;
  - **Decryption:** The key is used to convert the cypher-text to the original plain text;

Public Key Cryptography

- Properties of a cryptographic key (you need to prevent it from being guessed)
  - Generate the key truly randomly so that the attacker cannot guess it
  - The key should be of sufficient length – increasing the length makes the key difficult to guess
  - The key should contain sufficient entropy, all the bits in the key should be equally random

Public Key Cryptography

- Two keys are used
  - **Private key**: Only Alice has her private key
  - **Public key:** “Public” to everyone – everyone knows Alice’s public key



Encrypt the message with Bob’s public key

Decrypt the message with his private key

M’

Public Key Encryption - RSA

- Named over (Ron) Rivest – (Adi) Shamir – (Leonard) Adleman – inventors of the public key cryptosystem

- The encryption key is public and decryption key is kept secret (private key)
  - Anyone can encrypt the data
  - Only the intended receiver can decrypt the data

RSA Algorithm

- Four phases
  - Key generation
  - Key distribution
  - Encryption
  - Decryption

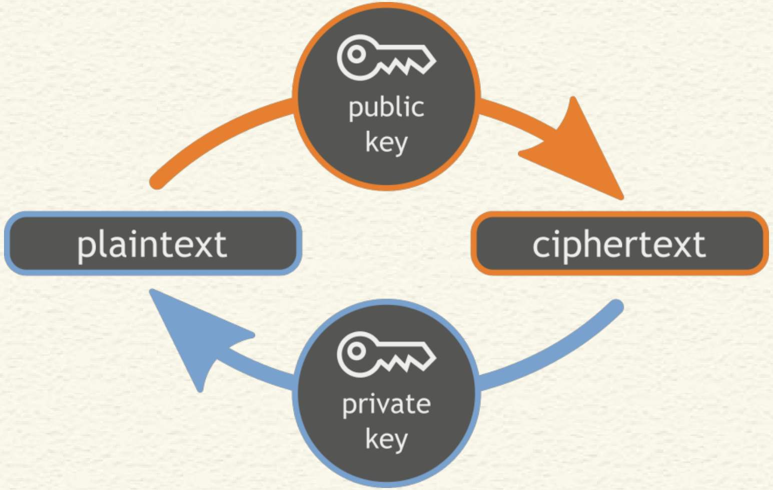


Image source: https://commons.wikimedia.org/

Public and Private Keys in RSA

- It is feasible to find **three very large positive integers** , and ; such that *modular exponentiation* for integers :

- Even if you know , and ; it is extremely difficult to find
- Note that

- is used as the public key and is used as the private key. is the message that needs to be encrypted.

RSA Key Generation and Distribution

- Chose two distinct prime integers and
  - and should be chosen at random to ensure tight security
- Compute ; is used as the modulus, the length of is called the key length
- Compute   (*Euler totient function*)
- Choose an integer such that and ; and are co-prime
- Determine : is the *modular multiplicative inverse* of

  [Note]

CONCLUSIONS

- We have discussed the basic concepts of public key cryptography
- How to generate keys in RSA

REFERENCES

- **Cryptography and Network Security – Principles and Practice by William Stallings, Pearson (2017)**

Thank you