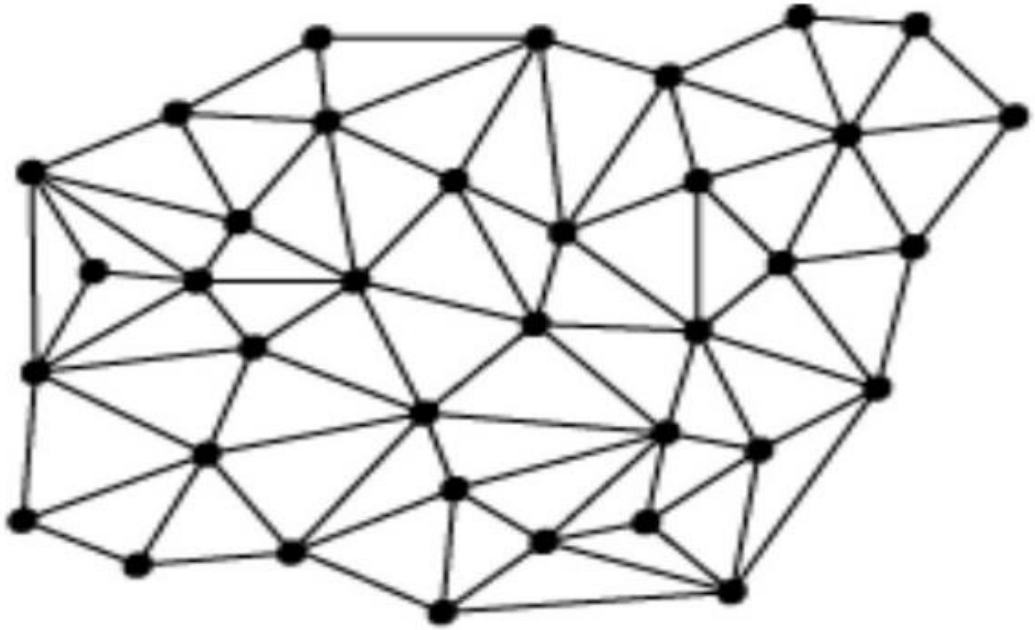
Distributed System Course

2021-22-GICI41SSD-Distributed System



Academic Year: 2021-2022 Lecturer: SOK Kimheng

Information

Course	Distributed System	48h, 12 Weeks, 4h/week (3 Groups = 96h)
	Week 1	Information, Self-Study Skill, Introduction
General Distributed System	Week 2	Distributed Communication (TCP/IP, Socket, RPC, REST, gRPC, OMQ)
	Week 3	Clock, Timestamp
	Week 4	Fault Tolerance (Two general problem, Byzantine General Problem)
	Week 5	Consensus Algorithm (Paxos, ZooKeeper, Raft)
	Week 6	**Quiz**
Blockchain	Week 7	Basic Cryptography
	Week 8	Blockchain and Bitcoin (Proof of Work)
	Week 9	Ethereum and Smart Contract (Proof of Stake)
	Week 10	Hyperledger and Self-Sovereign Identity
	Week 11	Security
	Week 12	**Final Exam**

Distributed System Course

2021-22-GICI41SSD-Distributed System

Week7:

Basic Cryptography

Academic Year: 2021-2022 Lecturer: SOK Kimheng

Agenda

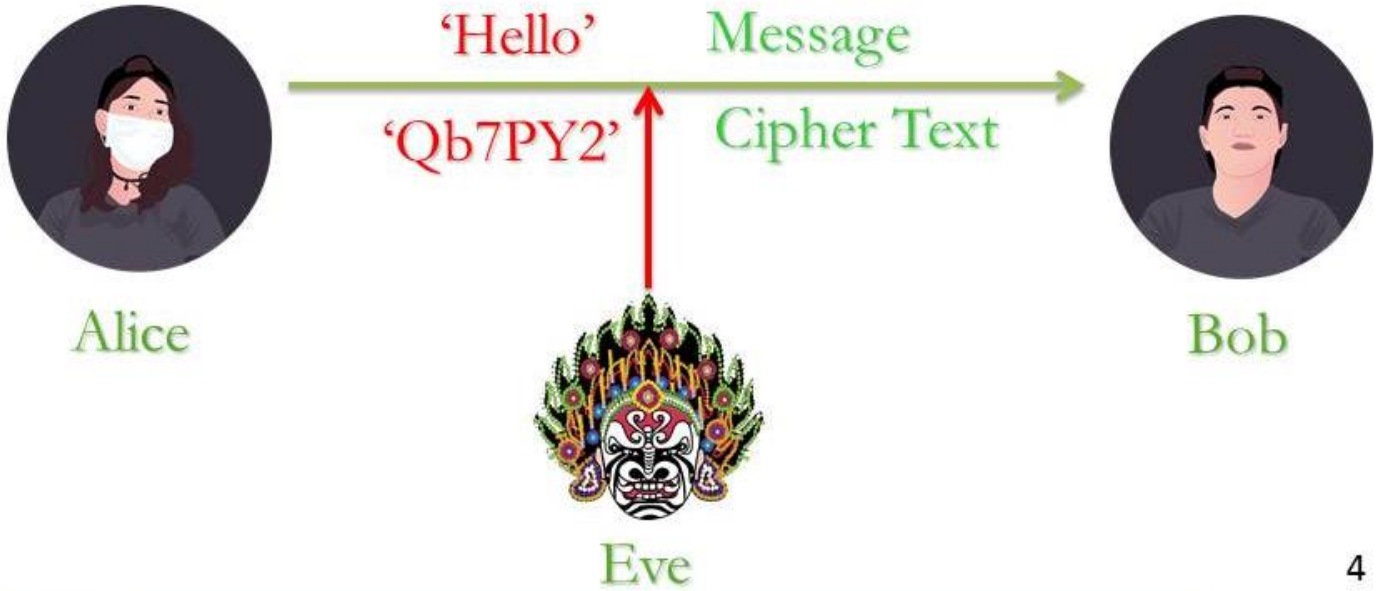
1. Definition
2. Terminology & Prior Knowledge
3. Symmetry Cryptography
4. Asymmetry Cryptography
5. Others

Basic Cryptography

Definition

Cryptography = Crypto (Secret) + Graphy (Write,Study)

Cryptography is the science of writing or creating secret.



Basic Cryptography

Why do we need to keep our message secret?

- ✓ We have some secret that don't want somebody to know
- ✓ We only want to share the secret with only the people we want to share
- ✓ Some sensitive transaction online such as payment, health information, business, government need to keep secret
- ✓ Even a simple chat messaging, we need private chat

"Our message need to be encrypted"

Basic Cryptography

Terminology

Notation	Description
P, M	Plaintext, Message
CT	Cipher Text
K, PK, SK, MSK	Key, Public Key, Secret Key, Master Secret Key
ENC	Encryption
DEC	Decryption

Encryption: The process of encoding a message into a cipher text.

Decryption: The process of decoding a cipher text into a message.

Basic Cryptography

Prior Knowledge

Discret Log $g, g^x \longrightarrow x$

CDH $g, g^x, g^y \longrightarrow g^{xy}$

DDH $g, g^x, g^y, g^z \longrightarrow \begin{cases} 0 \text{ if } z=xy \\ 1 \text{ otherwise} \end{cases}$

CDH: Computational Diffie Hellman
DDH: Decisional Diffie Hellman

"RANDOMNESS IS THE KEY"

Basic Cryptography

Prior Knowledge

Discret Log $g, g^x \longrightarrow x$

Ex:

$g= 5 \quad p=7$

$g^x \bmod p \quad => \quad 5^x \bmod 7 = 6 \quad$ find x=?

There are many possible answers, if p is big the answers are many more.

X is chosen to be a secret key.

Basic Cryptography

Symmetry Cryptography

Aka Secret Key Cryptography or Private Key Cryptography

Encryption: CT = Enc (M , K)
Ex: Qb7PY2 = Enc('Hello',123456)

Decryption: M = Dec (CT , K)
Ex: Hello= Dec('Qb7PY2',123456)

"Encryption and Decryption Key is the same"

Basic Cryptography

Symmetry Cryptography

Key Size (bits): 128, 256, 512, 1024, 2048,4096,…
Strength: randomness

Algorithm: Caesar Cipher, Vigenère Cipher, Enigma, DES, AES, RC4, …
Mode of operation: ECB, CBC, CFB, CTR, GCM, …
Help: $ openssl help

Basic Cryptography

Symmetry Cryptography

Advantage and Disadvantage of symmetric cryptography?

- ✓ Secure and Fast computation

- ❖ Secret key need to be transferred all the time that create high risk of key compromising

=> **Diffie Hellman Key Exchange** [1]

- ❖ Secret key is leaving the owner of the message to other receiver or at the attacker hand, which means the same key is on the hand of many people

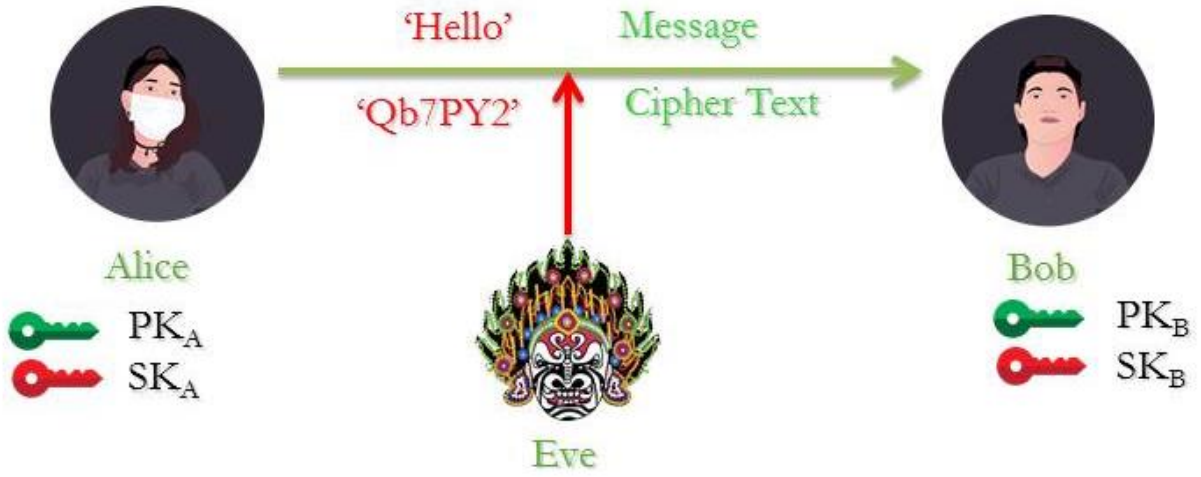
Basic Cryptography

Asymmetry Cryptography

Aka Public Key Cryptography

Public Key (PK)

Secret Key (SK) Aka. Private Key



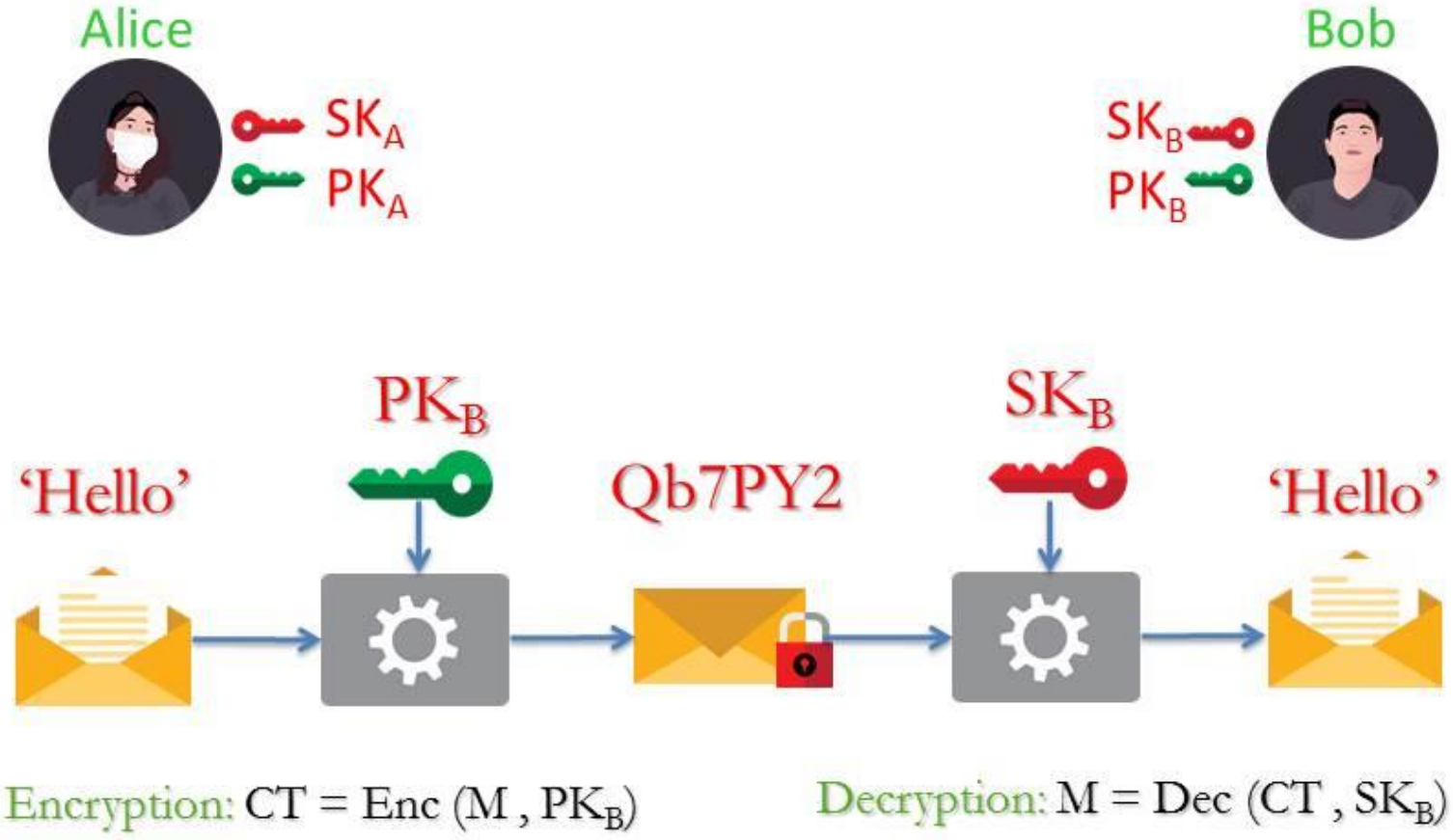
Basic Cryptography

Asymmetry Cryptography

- ✓ The algorithm that use the two different keys, one for encryption and another for decryption.
- ✓ Public Key (PK) is used for encryption and can be share to public, everyone can see it.
- ✓ Secret Key (SK) *aka. Private Key* is used for decryption and this key need to keep secret only on the owner hand.

Basic Cryptography

Asymmetry Cryptography



Basic Cryptography

Asymmetry Cryptography

Key Size (bits): 128, 256, 512, 1024, 2048,4096,…
Strength: randomness

Algorithm: RSA, El Gamal, ECC, Pairing…

2^{λ} Best known attack time

Algorithm	Signature Size	λ = 128
RSA	$O(\lambda^3)$	2048 bits
EC-DSA	4λ	512 bits
Schnorr	3λ	384 bits
BLS (Ecc,Pairing)	2λ	256 bits

Basic Cryptography

Example 1

M = 656667 **,** **K=**171717

CT = Enc (M,K) = Enc (656667,171717**)**

CT = 656667 XOR 171717 = 564190

M = Dec (CT, K) = Dec (564190**,** 171717**)**

M = 564190 XOR 171717 = 656667

Basic Cryptography

Example 2: RSA

Security Parameter: p=11, q=5, φ(n) = (p-1)(q-1)=40
Public Parameter: n = p * q = 55 (p, q are prime numbers)
Keypair: SK = 23, PK=7 (Satisfy RSA formula gcd(PK,φ(n))=1 , $SK=PK^{-1} \bmod \varphi(n)$)
M = 12

CT = Enc (M,PK) = Enc (12,7**)**
CT = 12^7 mod 55 = 23

M = Dec (CT, SK) = Dec (23, 23**)**
M = 23^23 mod 55 = 12

Basic Cryptography

Others

- Hash Function (MD5, SHA1, SHA256)
- Diffie Hellman Key Exchange
- Joux Protocol
- Digital Signature
- Certification (X.509)
- Encryption
  - Identity-Based Encryption
  - Attributed-Based Encryption
  - Homomorphic Encryption
  - Multi-Authority Attribute-Based Encryption
- Schnorr Protocol
- Pedersen Commitment
- Fiat-Shamir Heuristic
- Camenisch Lysyanskaya (CL) Signature Scheme
- Zero Knowledge Proof (zkSNARK, Bullet Proof, ….)