

ICT Course: Information Security

Nguyen Minh Huong

ICT Department, USTH

October 2, 2020

Session 5: Asymmetric Cryptography - Introductions

1 Introduction to Public Key Cryptography

- Symmetric cryptography issues
- Principle of asymmetric cryptography
- Security mechanisms of Public Key Cryptography

Symmetric cryptography issues

- Key Distribution: The key must be established between Alice and Bob in secured channel
- Number of keys: a key for each pairs of users
- No protection against cheating of either Alice or Bob

Principle of asymmetric cryptography

- Trap door one-way function
- A key pair:
 - public key k_1 : is broadcast to anyone
 - private key k_2 :is kept secret
- Algorithm: plaintext M, Ciphertext C

$$C = e_{k_1}(M)$$

$$M = e_{k_2}(C)$$

Security mechanisms of Public Key Cryptography

- Key Distribution without a pre-shared secret key, e.g, Diffie-Hellman key exchange, RSA
- Digital Signatures
 - providing integrity
 - preventing 'reputation'
 - identification: using challenge-response protocols
- Encryption, e.g, RSA

Practical protocols

Most protocol are hybrid protocol, incorporate both symmetric and public-key algorithms:

- Key exchange and digital signature: use asymmetric algorithms (slow)
- Encryption: uses symmetric ciphers (fast)

How to build Public-Key algorithm

Asymmetric schemes are based on **one-way function** $f()$

- Computing $y = f(x)$: easy
- Computing $x = f^{-1}(y)$: infeasible

One-way function are based on mathematically hard problems:

- Factoring integers: given a composite integer n , find its prime factors
- Discrete Logarithm: given a , y , and m , find x such that $a^x \equiv y \pmod{m}$
- Elliptic Curves: Generalization of discrete logarithm