Chương II

2

MÃ HÓA
(Cryptography)

Mã hóa bất đối xứng
ASYMMETRIC CIPHERS

NỘI DUNG

1. Mở đầu
2. Mã hóa khóa công khai (Public-Key Cryptosystems)
3. Thuật toán RSA
4. Một số mã hóa khóa công khai khác

(Cryptography and Network Security: Principles and Practices (3rd Ed.) – Chapter 9, 10)

Đặt vấn đề

Khuyết điểm của mã hóa đối xứng:

- Vấn đề trao đổi khóa giữa người gửi và người nhận: Cần phải có một kênh an toàn để trao đổi khóa sao cho khóa phải được giữ bí mật chỉ có người gửi và người nhận biết. Điều này tỏ ra không hợp lý khi mà ngày nay, khối lượng thông tin luân chuyển trên khắp thế giới là rất lớn. Việc thiết lập một kênh an toàn như vậy sẽ tốn kém về mặt chi phí và chậm trễ về mặt thời gian.
- Tính bí mật của khóa: không có cơ sở quy trách nhiệm nếu khóa bị tiết lộ.

Ý tưởng

- Vào năm 1976 Whitfield Diffie và Martin Hellman đã tìm ra một phương pháp mã hóa khác mà có thể giải quyết được hai vấn đề trên, đó là mã hóa khóa công khai (public key cryptography) hay còn gọi là mã hóa bất đối xứng (asymetric cryptography).
- Whitfield Diffie và Martin Hellman đưa ra 2 phương án sau:

Ý tưởng

- Phương án 1: người nhận (Bob) giữ bí mật khóa *K*2, còn khóa *K*1 thì công khai cho tất cả mọi người biết.
- Alice muốn gởi dữ liệu cho Bob thì dùng khóa *K*1 để mã hóa. Bob dùng *K*2 để giải mã.
- Ở đây Trudy cũng biết khóa *K*1, tuy nhiên không thể dùng chính *K*1 để giải mã mà phải dùng *K*2. Do đó chỉ có duy nhất Bob mới có thể giải mã được.
- Điều này bảo đảm *tính bảo mật* của quá trình truyền dữ liệu.
- Ưu điểm của phương án này là không cần phải truyền khóa *K*1 trên kênh an toàn.

Ý tưởng

- *Phương án 2*: người gửi (Alice) giữ bí mật khóa *K*1, còn khóa *K*2 thì công khai cho tất cả mọi người biết. Alice muốn gởi dữ liệu cho Bob thì dùng khóa *K*1 để mã hóa. Bob dùng *K*2 để giải mã.
- Ở đây Trudy cũng biết khóa *K*2 nên Trudy cũng có thể giải mã được. Do đó phương án này *không đảm bảo tính bảo mật*.
- Tuy nhiên lại có tính chất quan trọng là *đảm bảo tính chứng thực và tính không từ chối*. Vì chỉ có duy nhất Alice biết được khóa *K*1, nên nếu Bob dùng *K*2 để giải mã ra bản tin, thì điều đó có nghĩa là Alice là người gửi bản mã. Nếu Trudy cũng có khóa *K*1 để gửi bản mã thì Alice sẽ bị quy trách nhiệm làm lộ khóa *K*1.
- Trong phương án này cũng không cần phải truyền *K*2 trên kênh an toàn→Mã bất đối xứng kết hợp 2 phương án trên

Mã hóa công khai (Public-Key Cryptosystems)

- Mã bất đối xứng là một dạng của hệ thống mật mã mà trong đó mã hóa (encryption) và giải mã (decryption) được thực hiện bằng cách dùng hai khóa (Key) khác nhau
- Một là khóa công khai (Public key) và một là khóa bí mật (Private key).
- Nó cũng được gọi tên là

MÃ HÓA KHÓA CÔNG KHAI

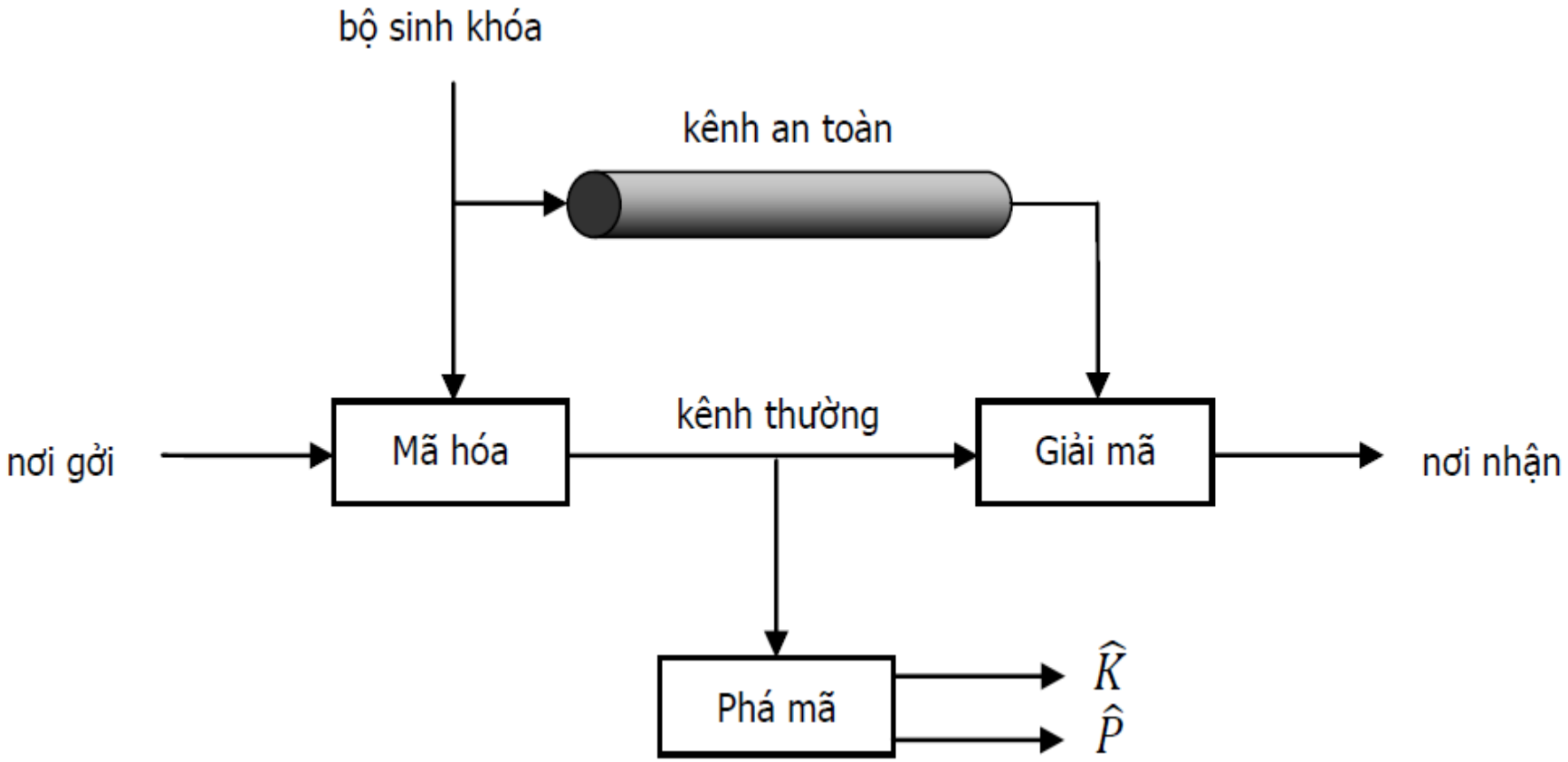
(Public-key Encryption)

Có hai mode làm việc :

- Bảo mật : Mã bằng public key → giải mật bằng private key
- Xác thực : Mã bằng private key →giải mật bằng public key

Mã hóa công khai (Public-Key Cryptosystems)

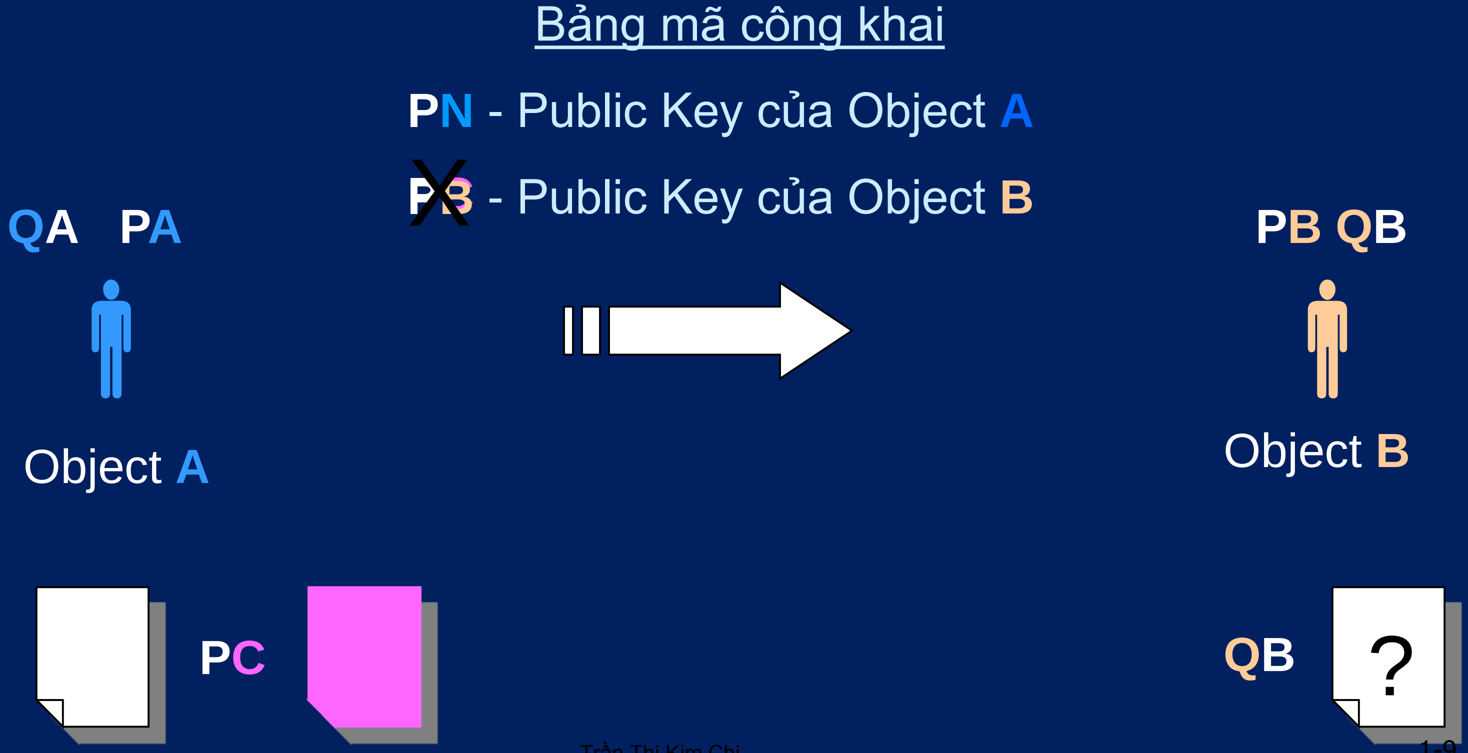
- Mô hình mã hóa đối xứng



Mã hóa công khai
(Public-Key Cryptosystems)

Nếu mã Public (**P**) của Object bị thay thế, giả mạo thì Object sẽ không thể giải mã nội dung dữ liệu bằng mã Private (**Q**) của mình

Với phương pháp PKI, một trong những vấn đề quan trọng của PKI là bảo vệ và xác nhận giá trị của mã Public (**P**) trong Bảng mã Công khai



Mã hóa công khai (Public-Key Cryptosystems)

- Mã bất đối xứng biến đổi bản rõ (plaintext) thành bản mã (Ciphertext) bằng cách dùng một trong hai khóa và một thuật toán mã hóa (Encryption Algorithm). Sử dụng khóa còn là và một thuật toán giải mã (Decryption), bản rõ sẽ được phục hồi từ bản mã.
- Mã đối xứng có thể dùng để bảo mật (Confidentiality), chứng thực (Authentication), hoặc cả hai.