UBND TỈNH THANH HÓA
TRƯỜNG CAO ĐẲNG NGHỀ CÔNG NGHIỆP THANH HÓA

GIÁO TRÌNH

XÂY DỰNG AN TOÀN BẢO MẬT THÔNG TIN

NGHỀ: CÔNG NGHỆ THÔNG TIN(ƯDPM)

TRÌNH ĐỘ: CAO ĐẲNG

Chương 3. MÃ CÔNG KHAI VÀ QUẢN LÝ KHOÁ
Mã chương: MH2/03

Giới thiệu:

Khoá công khai ra đời vào đầu nh ững n ăm 1970. Đây là bước tiến quan tr ọng nhất trong lịch sử 3000 n m mã hoá. Ở đây người ta sử dụng 2 khoá: một khoá riêng để giải mã và một khoá công khai để mã hóa. Hai khoá này khác nhau, mã khoá công khai còn được gọi là mã không đối xứng. Khoá công khai ra đời hỗ trợ thêm để giải quyết m ột số bài toán an toàn, chứ không phải thay thế khoá riêng. Cả hai khoá cùng tồn tại, phát triển và bổ sung cho nhau.

Mục tiêu bài học:

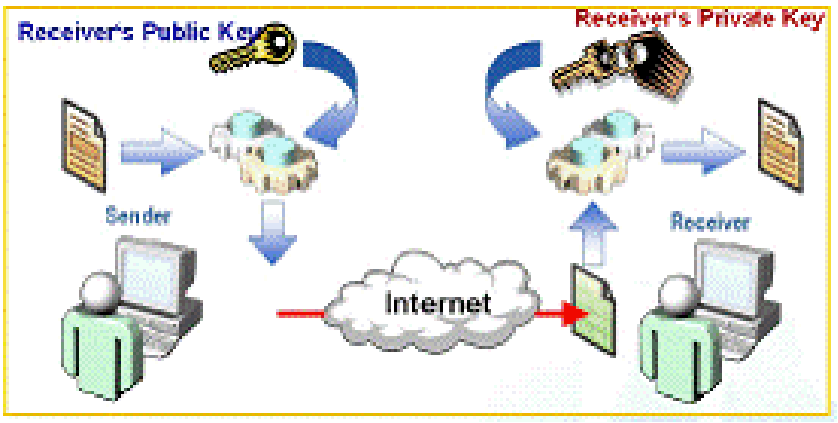
Sau khi học xong chương này người học có khả năng:

- Hiểu khái niệm về khóa công khai và chữ ký điện tử;
- Hiểu mô hình khóa công khai trong hệ thống;
- Thiết kế được cơ sở hạ tầng khóa công khai;
- Biết các giải thuật về chữ ký điện tử;
- Biết cách sử dụng hàm băm
- Chính xác, cẩn thận, tỉ mỉ, khoa học.

3.1 Mã khoá công khai

Mã khoá riêng: Mã khoá riêng còn được gọi là mã khoá đơn hay mật. Ở đây chỉ dùng một khoá, dùng chung cả người nhận và người gửi. Khi khoá này được dùng, việc trao đổi thông tin về khoá sẽ được thỏa thuận trước.

Người ta còn gọi đây là mã đối xứng, vì hai đối tác có vai trò như nhau. Do đó không bảo vệ người gửi khỏi việc người nhận giả mạo mẩu tin và tuyên bố là nó được gửi bằng người gửi. Nghĩa là khi hai người dùng mã đối xứng, thì họ giữ được bí mật nội dung trao đổi, nhưng bản thân mẩu tin không mang thông tin xác thực được người gửi.



3.1.1 Mã khoá công khai

Khoá công khai ra đời vào đầu những năm 1970. Có thể nói đây là bước tiến quan trọng nhất trong lịch sử 3000 năm mã hoá. Ở đây người ta sử dụng 2 khoá: một khoá riêng và một khoá công khai. Hai khoá này khác nhau, không đối xứng với nhau, do đó mã khoá công khai, còn được gọi là mã không đối xứng. Người ta đã ứng dụng một cách thông minh các kết quả của lý thuyết số về hàm số.

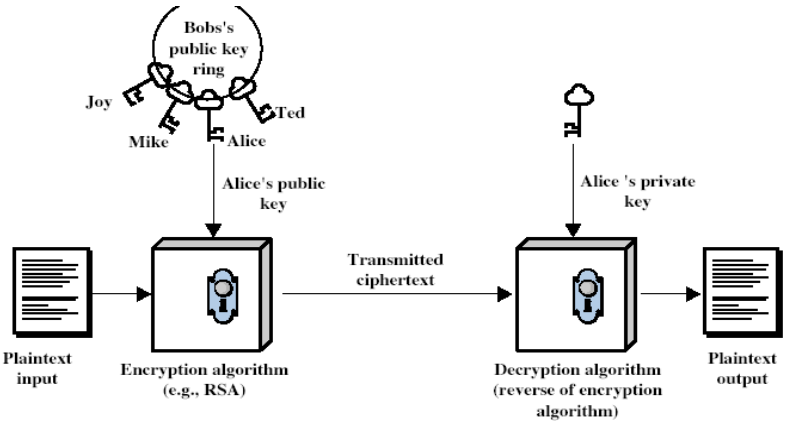
Khoá công khai ra đời hỗ trợ thêm để giải quyết một số bài toán an toàn, chứ không phải thay thế khoá riêng. Cả hai khoá cùng tồn tại, phát triển và bổ sung cho nhau.

Khoá công khai/hai khoá/không đối xừng bao gồm việc sử dụng 2 khoá:

Khoá công khai, mà mọi người đều biết, được dùng để mã hoá mẩu tin và kiểm chứng chữ ký.

Khoá riêng, chỉ người nhận biết, đề giải mã bản tin hoặc để tạo chữ ký.

Là không đối xứng vì những người mã hoá và kiểm chứng chữ ký không thể giải mã hoặc tạo chữ ký.



3.1.2 Tại sao lại phải dùng mã khoá công khai

Người ta muốn giải quyết hai vấn đề sau về khoá nảy sinh trong thực tế:

o Phân phối khoá - làm sao có thể phân phối khóa an toàn mà không cần trung tâm phân phối khoá tin cậy

o Chữ ký điện tử - làm sao có thể kiểm chứng được rằng mẩu tin gửi đến nguyên vẹn từ đúng người đứng tên gửi.

Nếu chỉ dùng khoá đối xứng, thì không có giải pháp cho hai bài toán trên. Mã khoá công khai được phát minh trước công chúng bởi hai nhà bác học Whitfield Diffie & Martin Hellman ở trường Đại học Stanford vào năm 1976.

Tuy nhiên khái niệm ban đầu về nó đã được biết đến sớm hơn bởi cộng đồng các nhà khoa học.

3.1. 3 Các đặc trưng của khoá công khai

Các thuật toán khoá công khai dùng 2 khoá với các đặc trưng sau:

o Không có khả năng tính toán để tìm khoá giải mã nếu chỉ biết thuật toán mã và khoá dùng để mã.

o Có thể dễ dàng mã hoá hoặc giải mã mẩu tin nếu biết khoá tương ứng

o Trong một số sơ đồ: một khoá bất kỳ trong hai khoá có thể dùng để mã, còn khoá kia dùng để giải mã. Chúng có vai trò đối ngược nhau.

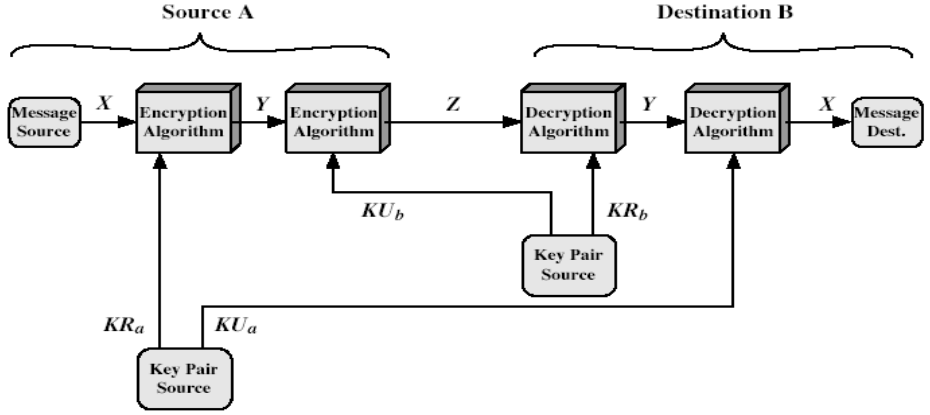


Figure 9.4 Public-Key Cryptosystem: Secrecy and Authentication

3.1.4 Ứng dụng khoá công khai

Có thể phân loại các ứng dụng của khoá công khai thành 3 loại khác nhau:

o Mã/giải mã – cung cấp bảo mật. Đây là ứng dụng bảo mật truyền thống giống như ta vẫn thường dùng với khoá đối xứng.

o Chữ ký điện tử - cung cấp xác thực. Một trong các ứng dụng mới của khoá công khai mà khoá đối xứng không thể thực hiện được, đó là khoá công

khai có đủ cơ sở để xác nhận người gửi và có thể là một lựa chọn để tạo chữ ký điện tử của người gửi.

Một số thuật toán mã công khai phù hợp với mọi ứng dụng, còn một số khác chuyên dùng cho ứng dụng cụ thể.

3.1.5 Tính an toàn của các sơ đồ khoá công khai

Cũng giống như khoá riêng việc tìm kiếm vét cạn luôn luôn có thể, tức là khi biết một trong hai khoá và thuật toán mã hoá về nguyên tắc ta có thể dò tìm khoá thứ hai bằng cách tính toán các giá trị liên quan. Nói chung khối lượng cần tính toán là rất lớn do độ phức tạp của bài toán xác định khoá. Nếu khoá sử dụng là rất lớn cỡ hơn 512 bit, thì hầu như bài toán tìm khoá thứ hai là không khả thi, không thể thực hiện được trong thời gian có nghĩa, cho dù nguồn lực có thể rất lớn.

Tính an toàn dựa trên sự khác biệt đủ lớn giữa các bài toán dễ là mã/giải mã khi biết khoá và bài toán khó là thám mã khi không biết khoá tương ứng. Vì bài toán thám mã nằm trong lớp các bài toán khó tổng quát hơn đã được biết đến và về mặt lý thuyết đã được chứng minh là nó rất khó có thể thực hiện trên thực tế. Bởi vì nó đòi hỏi sử dụng số rất lớn, nên số phép toán cần thực hiện là rất nhiều. Đây là ý tưởng chính để tạo nên một mã công khai. Ta tìm kiếm các bài toán mà nếu biết thông tin mật nào đó được che dấu thì nó rất dễ thực hiện, còn nếu không thì nó thuộc lớp bài toán rất khó giải, hầu như không thể giải trên thực tế.

Mã công khai thường chậm hơn khá nhiều so với mã đối xứng, nên nó thường được dùng mã những thông tin nhỏ quan trọng.

3.2. Hệ mật mã RSA

RSA là mã công khai được sáng tạo bởi Rivest, Shamir & Adleman ở MIT (Trường Đại học Công nghệ Massachusetts) vào năm 1977. RSA là mã công khai được biết đến nhiều nhất và sử dụng rộng rãi nhất hiện nay. Nó dựa trên các phép toán lũy thừa trong trường hữu hạn các số nguyên theo modulo nguyên tố. Cụ thể, mã hoá hay giải mã là các phép toán luỹ thừa theo modulo số rất lớn. Việc thám mã, tức là tìm khoá riêng khi biết khoá công khai, dựa trên bài toán khó là phân tích một số rất lớn đó ra thừa số nguyên tố. Nếu

không có thông tin gì, thì ta phải lần lượt kiểm tra tính chia hết của số đó cho tất cả các số nguyên tố nhỏ hơn căn của nó. Đây là việc làm không khả thi.

Người ta chứng minh được rằng, phép lũy thừa cần $O((\log n)^3)$ phép toán, nên có thể coi lũy thừa là bài toán dễ. Cần chú ý rằng ở đây ta sử dụng các số rất lớn khoảng 1024 bit, tức là cỡ 10^{350}. Tính an toàn dựa vào độ khó của bài toán phân tích ra thừa số các số lớn.

3.2.1 Khởi tạo khoá RSA

Mỗi người sử dụng tạo một cặp khoá công khai – riêng như sau:

Chọn ngẫu nhiên 2 số nguyên tố lớn p và q

Tính số làm modulo của hệ thống:

$N = p.q$

Ta đã biết $\Phi N)=(p-1)(q-1)$

Và có thể dùng Định lý Trung Hoa để giảm bớt tính toán

Chọn ngẫu nhiên khoá mã e

Trong đó $1<e<\Phi N)$, $\gcd(e,\Phi(N))=1$

Giải phương trình sau để tìm khoá giải mã d sao cho

$e.d=1 \bmod \Phi(N)$ với $0\le d\le \Phi(N)$

In khoá mã công khai $KU=\{e,N\}$

Giữ khoá riêng bí mật $KR=\{d,p,q\}$

3.2.2 Sử dụng RSA

Để mã hoá mẩu tin, người gửi:

Lấy khoá công khai của người nhận $KU=\{e,N\}$

Tính $C=M^e \bmod N$, trong đó $0\le M<N$

Để giải mã hoá bản mã, người sở hữu nhận:

Sử dụng khóa riêng $KR=\{d,p,q\}$

Tính $M=C^d \bmod N$

Lưu ý rằng bản tin $M < N$, do đó khi cần chia khối bản rõ.

Cơ sở của RSA

Theo Định lý Ole

$a^{\Phi(n)} \bmod N = 1$ trong đó $\gcd(a,N)=1$

Ta có $N=p.q$

$\Phi(N)=(p-1)(q-1)$

e.d=1 mod Φ(N)

e.d=1+k.Φ(N) đối với một giá trị k nào đó.

Suy ra

$C^d = (M^e)^d = M^{1+k.\Phi(N)} = M^1.(M^{\Phi(N)})^k$

suy ra C^dMod N = $M^1.(1)^k$ modN = M^1 modN = M modN

Ví dụ

Chọn các số nguyên tố: p=17 & q=11.

Tính $n = pq$, n = 17×11=187

Tính $\Phi(n)=(p-1)(q-1)$=16×10=160

Chọn e *:* gcd(e,160)=1; Lấy e=7

Xác định d*:* de=1 mod 160 và $d < 160$

Giá trị cần tìm là d=23, vì 23×7=161= 10×160+1

In khoá công khai KU={7,187}

Giữ khoá riêng bí mật KR={23,17,11}

Ví dụ áp dụng mã RSA trên như sau:

Cho mẩu tin M = 88 (vậy 88<187)

Mã C = 88^7 mod 187 = 11

Giải mã M = 11^{23} mod 187 = 88

Có thể dùng định lý phần dư Trung Hoa để giải mã cho nhanh như sau:

Tính 11^{23} mod 11 = 0

Tính 11^{23}mod 17 = $(-6)^{23}$ mod 17 = $(-6)^{16}$

$(-6)^4$ $(-6)^2$ (-6) mod 17 = 3

Vì $(-6)^2$ mod 17 = 2, nên $(-6)^4$ mod 17 = 4, $(-6)^8$ mod 17 = -1

$(-6)^{16}$ mod 17 = 1

11-1 mod 17 = (-6)-1 mod 17 = 14 nên c2 = 11(11-1 mod 17) = 11 (14 mod 17) = 154

Vậy M = (3.154) mod 187 = 462 mod 187 = 88

3.2.3 Lũy thừa

Trong các bài toán mã hoá công khai, chúng ta sử dụng nhiều phép toán lũy thừa với số mũ lớn. Như vậy cần có thuật toán nhanh hiệu quả đối với phép toán này. Trước hết ta phân tích số mũ theo cơ số 2, xét biểu diễn nhị phân của số mũ, sau đó sử dụng thuật toán bình phương và nhân. Khái niệm được dựa

trên phép lặp cơ sở bình phương và nhân để nhận được kết quả mong muốn. Độ phức tạp của thuật toán là O($\log_2$ n) phép nhân đối với số mũ n.

Ví dụ:

$7^5 = 7^4.7^1 = 3.7 = 10 \bmod 11$

vì $7^2 = 7.7 = 49 = 5 \bmod 11$

$7^4 = 7^2.7^2 = 5.5 = 3 \bmod 11$

$3^{129} = 3^{128}.3^1 = 5.3 = 4 \bmod 11$

Phân tích số mũ theo cơ số 2

Trước hết ta chuyển số mũ từ cơ số 10 sang cơ số 2: $(11)_{10} = (1011)_2$. Sau đó tính toán như sau:

$$M^{11} = M^{1.2\hat{}3 + 0.2\hat{}2 + 1.2\hat{}1 + 1.2\hat{}0}$$
$$= (M^{1.2\hat{}2 + 0.2\hat{}1 + 1.2\hat{}0})^2 M$$
$$= (M^{1.2\hat{}1 + 0.2\hat{}0})^2 M)^2 M$$
$$= ((M^2)^2 M)^2 M$$

3.2.4 Mã hiệu quả:

Mã sử dụng lũy thừa của khoá công khai e, nếu giá trị của e nhỏ thì tính toán sẽ nhanh, nhưng dễ bị tấn công. Thường chọn e nhỏ hơn hoặc bằng 65537 (2^{16}-1), tức là độ dài khoá công khai là 16 bit. Chẳng hạn trong ví dụ trên ta có thể lựa chọn e = 23 hoặc e = 7. Ta có thể tính mã hoá nhanh, nếu biết n=pq và sử dụng Định lý phần dư Trung Hoa với mẩu tin M theo các Modulo p và q khác nhau. Nếu khoá công khai e cố định thì cần tin tưởng rằng khi chọn n ta luôn có gcd(e,Φ(n)) = 1. Loại bỏ mọi p, q mà làm cho Φ(n) không nguyên tố cùng nhau với e.

3.2.5 Giải mã hiệu quả:

Có thể sử dụng Định lý phần dư Trung Hoa để tính theo mod p và q, sau đó kết hợp lại để tìm ra bản rõ. Vì ở đây người sử dụng khoá riêng biết được p và q, do đó có thể sử dụng kỹ thuật này. Nếu sử dụng định lý phần dư Trung Hoa để giải mã thì hiệu quả là nhanh gấp 4 lần so với giải mã tính trực tiếp.

3.2.6 Sinh khoá RSA

Người sử dụng RSA cần phải xác định ngẫu nhiên 2 số nguyên tố rất lớn, thông thường khoảng 512 bit. Do đó việc sinh ra ngẫu nhiên p, q và kiểm tra xác suất tính nguyên tố của chúng có nhiều giải pháp khác nhau với độ tin

cậy cao. Sau khi chọn được một khoá e hoặc d nguyên tố cùng nhau với Φ(n), dễ dàng tính được khoá kia chính là số nghịch đảo của nó qua thuật toán Euclide mở rộng.

3.2.7 An toàn của RSA

Trên thực té có nhiều cách tấn công khác nhau đối với mã công khai RSA như sau:

Tìm kiếm khoá bằng phương pháp vét cạn, phương pháp này không khả thi với kích thước đủ lớn của các số hoặc tấn công bằng toán học dựa vào độ khó việc tính Φ(n) bằng cách phân tích n thành hai số nguyên tố p và q hoặc tìm cách tính trực tiếp Φ(n). Trong quá trình nghiên cứu việc thám mã người ta đề xuất kiểu tấn công thời gian trong khi giải mã, tức là căn cứ vào tốc độ mã hoá và giải mã các mẩu tin cho trước mà phán đoán các thông tin về khoá.

Cuối cùng có những nghiên cứu tấn công RSA với điều kiện biết trước bản mã cho trước. Cu thể như sau:

Bài toán phân tích

Tấn công toán học có 3 dạng

Phân tích N = p.q, sau đó tính Φ(N) và d

Tìm n trực tiếp Φ(N) và tính d

Tìm d trực tiếp

Hiện tại tin rằng tất cả đều tương đương với bài toán phân tích

Có các bước tiến chậm theo thời gian

Hiện tại cho rằng RSA 1024 hoặc 2048 là an toàn

Tấn công thời gian

Phát triển vào giữa năm 1990

Paul Kocher chỉ ra rằng kẻ thám mã có thể xác định được khoá riêng nếu theo dõi thời gian máy tính cần để giải mã các bản tin.

Tấn công thời gian không chỉ áp dụng cho RSA, mà cả với các hệ mã công khai khác.

Tấn công thời gian giống như kẻ cướp đoán số điện thọai bằng cách quan sát một người nào đó trong bao lâu chuyển quay điện thoại từ số này sang số khác.

Tấn công bản mã chọn trước

RSA có điểm yếu với tấn công bản mã chọn trước

Kẻ tấn công chọn bản mã và đoán bản rõ được giải mã

Chọn bản mã để khám phá RSA cung cấp thông tin để thám mã

Có thể tính với bộ đệm ngẫu nhiên của bản rõ

Hoặc sử dụng bộ đệm mã hoá phản xứng.

3.3 Quản lý khoá

3.3.1 Phân phối khoá

Mã khoá công khai giúp giải bài toán phân phối khoá, đây là nhu cầu cấp bách cần phải tạo ra một cơ chế chia sẻ khoá trong môi trường thường xuyên trao đổi thông tin và thường xuyên thay đổi khoá. Nó bao gồm hai khía cạnh sau:

Phân phối khoá một cách công khai nhưng đảm bảo được bí mật.

Sử dụng mã khoá công khai để phân phối khoá mật (còn khoá mật dùng để mã hoá thông tin).

3.3.2 Phân phối khoá công khai

Có thể xem xét để được sử dụng vào một trong những việc sau:

Thông báo công khai khoá của người sử dụng.

Thư mục truy cập công cộng cho mọi người.

Chủ quyền khoá công khai, người nắm giữ khoá công khai.

Chứng nhận khoá công khai, khoá công khai của người sử dụng được nơi có thẩm quyền chứng nhận.

Thông báo công khai

- Người dùng phân phối khoá công khai cho người nhận hoặc thông báo rộng rãi cho cộng đồng. Chẳng hạn như người sử dụng có thể tự bổ sung khoá PGP vào thư điện tử hoặc gửi cho nhóm chia sẻ tin hoặc một danh sách thư điện tử.

- Điểm yếu chính của thông báo công khai là mạo danh: một người nào đó có thể tạo khoá và tuyên bố mình là một người khác và gửi thông báo cho mọi người khác. Cho đến khi giả mạo bị phát hiện thì kẻ mạo danh đã có thể lừa trong vai trò người khác

Thư mục truy cập công cộng