CHƯƠNG 8

HỆ MẬT MÃ KHÓA CÔNG KHAI
PUBLIC-KEY ENCRYPTION

Nội dung

- Hệ mật mã khóa công khai RSA

Nội dung

- Hệ mật mã khóa công khai RSA
- Hệ mật mã khóa công khai Rabin

Nội dung

- Hệ mật mã khóa công khai RSA
- Hệ mật mã khóa công khai Rabin
- Hệ mật mã khóa công khai ElGamal

Nhắc lại một số khái niệm về hệ mật mã khóa công khai

- Hệ mật mã khóa công khai hay còn gọi là hệ mật mã phi đối xứng

Nhắc lại một số khái niệm về hệ mật mã khóa công khai

- Hệ mật mã khóa công khai hay còn gọi là hệ mật mã phi đối xứng

- Trong một hệ mật mã khóa công khai, mỗi thực thể A sẽ có khóa công khai là e và khóa bí mật là d, ở đó không khả thi để tìm d từ e. Khóa công khai xác định biến đổi mã hóa E_e, khóa riêng sẽ liên quan đến biến đổi giải mã D_d.

$$c = E_e(m), \quad m = D_d(c)$$

Hệ mật mã khóa công khai RSA

- Hệ mật mã khóa công khai RSA được phát minh bởi R. Rivest, A. Shamir và L. Adleman

Hệ mật mã khóa công khai RSA

- Hệ mật mã khóa công khai RSA được phát minh bởi R. Rivest, A. Shamir và L. Adleman

- RSA được sử dụng cho cả bảo mật và chữ ký số

Hệ mật mã khóa công khai RSA

- Hệ mật mã khóa công khai RSA được phát minh bởi R. Rivest, A. Shamir và L. Adleman
- RSA được sử dụng cho cả bảo mật và chữ ký số
- Độ an toàn của RSA dựa vào sự phức tạp của bài toán phân tích một số thành nhân tử

Hệ mật mã khóa công khai RSA

- Hệ mật mã khóa công khai RSA được phát minh bởi R. Rivest, A. Shamir và L. Adleman
- RSA được sử dụng cho cả bảo mật và chữ ký số
- Độ an toàn của RSA dựa vào sự phức tạp của bài toán phân tích một số thành nhân tử
- Cơ sở của phương pháp này là bài toán RSA

Thuật toán sinh khóa cho RSA

Mỗi thực thể A cần tạo một khóa công khai e và tương ứng là khóa bí mật d như sau:

Thuật toán sinh khóa cho RSA

Mỗi thực thể A cần tạo một khóa công khai e và tương ứng là khóa bí mật d như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau

Thuật toán sinh khóa cho RSA

Mỗi thực thể A cần tạo một khóa công khai e và tương ứng là khóa bí mật d như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau

2. Tính $n = pq$ và $\phi = (p-1)(q-1)$

Thuật toán sinh khóa cho RSA

Mỗi thực thể A cần tạo một khóa công khai e và tương ứng là khóa bí mật d như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau

2. Tính $n = pq$ và $\phi = (p-1)(q-1)$

3. Chọn ngẫu nhiên số tự nhiên e, $1 < e < \phi$ và $gcd(e, \phi) = 1$

Thuật toán sinh khóa cho RSA

Mỗi thực thể A cần tạo một khóa công khai e và tương ứng là khóa bí mật d như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau

2. Tính $n = pq$ và $\phi = (p-1)(q-1)$

3. Chọn ngẫu nhiên số tự nhiên e, $1 < e < \phi$ và $gcd(e, \phi) = 1$

4. Tìm số d, $1 < d < \phi$, sao cho $ed \equiv 1 (mod \phi)$

Thuật toán sinh khóa cho RSA

Mỗi thực thể A cần tạo một khóa công khai e và tương ứng là khóa bí mật d như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau
2. Tính $n = pq$ và $\phi = (p-1)(q-1)$
3. Chọn ngẫu nhiên số tự nhiên e, $1 < e < \phi$ và $gcd(e, \phi) = 1$
4. Tìm số d, $1 < d < \phi$, sao cho $ed \equiv 1 (mod \phi)$
5. Khóa công khai của A là (n, e) và khóa bí mật là d.

Mã hóa và giải mã của RSA

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

Mã hóa và giải mã của RSA

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau

Mã hóa và giải mã của RSA

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (n, e) từ A

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (n, e) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$

Mã hóa và giải mã của RSA

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (n, e) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^e \mod n$

Mã hóa và giải mã của RSA

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (n, e) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^e \mod n$
   (d) Gửi c cho A

Mã hóa và giải mã của RSA

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (n, e) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^e \mod n$
   (d) Gửi c cho A
2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau

Mã hóa và giải mã của RSA

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (n, e) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^e \mod n$
   (d) Gửi c cho A
2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau
   (a) Sử dụng khóa riêng d để khôi phục $m = c^d \mod n$

Mật mã hóa công khai Rabin

- Hệ mật mã khóa công khai Rabin được chứng tỏ là có độ khó tính toán tương đương với bài toán phân tích thành nhân tử hoặc bài toán Logarit rời rạc, trong khi hệ mật mã RSA được xem là có độ khó tính toán tương tự nhưng chưa có chứng minh

Mật mã hóa công khai Rabin

- Hệ mật mã khóa công khai Rabin được chứng tỏ là có độ khó tính toán tương đương với bài toán phân tích thành nhân tử hoặc bài toán Logarit rời rạc, trong khi hệ mật mã RSA được xem là có độ khó tính toán tương tự nhưng chưa có chứng minh

- Cơ sở của hệ mật mã Rabin là bài toán căn bậc hai modulo

Mật mã hóa công khai Rabin

- Hệ mật mã khóa công khai Rabin được chứng tỏ là có độ khó tính toán tương đương với bài toán phân tích thành nhân tử hoặc bài toán Logarit rời rạc, trong khi hệ mật mã RSA được xem là có độ khó tính toán tương tự nhưng chưa có chứng minh

- Cơ sở của hệ mật mã Rabin là bài toán căn bậc hai modulo

Thuật toán sinh khóa của Rabin

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

Thuật toán sinh khóa của Rabin

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau

Thuật toán sinh khóa của Rabin

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau

2. Tính $n = pq$

Thuật toán sinh khóa của Rabin

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

1. Sinh ra 2 số nguyên tố ngẫu nhiên lớn p, q khác nhau và có kích thước bit gần bằng nhau

2. Tính $n = pq$

3. Khóa công khai của A là n và khóa bí mật là cặp (p, q).

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai n từ A

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai n từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai n từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^2 \mod n$

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai n từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^2 \mod n$
   (d) Gửi c cho A

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai n từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^2 \mod n$
   (d) Gửi c cho A
2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai n từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^2 \mod n$
   (d) Gửi c cho A
2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau
   (a) Tìm 4 căn bậc hai m_1, m_2, m_3, m_4 của c modulo n

Mã hóa và giải mã của Rabin

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai n từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, n-1]$
   (c) Tính $c = m^2 \mod n$
   (d) Gửi c cho A
2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau
   (a) Tìm 4 căn bậc hai m_1, m_2, m_3, m_4 của c modulo n
   (b) Kết quả mã hóa là một trong 4 giá trị trên

Kỹ thuật thêm phần dư của Rabin

- Hạn chế của Rabin là khi giải mã cần tìm giá trị nào của m_i trong số 4 căn bậc hai của c modulo n?

Kỹ thuật thêm phần dư của Rabin

- Hạn chế của Rabin là khi giải mã cần tìm giá trị nào của m_i trong số 4 căn bậc hai của c modulo n?

- Giải pháp là thêm vào tin gốc (chẳng hạn như lặp một số bit cuối) và sau đó kiểm tra m_i nào có dư như vậy

Mật mã hóa công khai ElGamal

- Mật mã hóa ElGamal còn được gọi như thỏa thuận trao đổi khóa Diffie-Hellman

Mật mã hóa công khai ElGamal

- Mật mã hóa ElGamal còn được gọi như thỏa thuận trao đổi khóa Diffie-Hellman
- Cơ sở của hệ mật mã ElGamal là bài toán Diffie-Hellman

Mật mã hóa công khai ElGamal

- Mật mã hóa ElGamal còn được gọi như thỏa thuận trao đổi khóa Diffie-Hellman
- Cơ sở của hệ mật mã ElGamal là bài toán Diffie-Hellman

Thuật toán sinh khóa của ElGamal

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

Thuật toán sinh khóa của ElGamal

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

1. Sinh ra số nguyên tố ngẫu nhiên lớn p và phần tử sinh α của nhóm $\mathbb{Z}_p^*$

Thuật toán sinh khóa của ElGamal

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

1. Sinh ra số nguyên tố ngẫu nhiên lớn p và phần tử sinh α của nhóm $\mathbb{Z}_p^*$

2. Chọn số ngẫu nhiên $1 \leq a \leq p-2$, và tính $\alpha^a \mod p$

Thuật toán sinh khóa của ElGamal

Mỗi thực thể A cần tạo một khóa công khai e và khóa bí mật d tương ứng như sau:

1. Sinh ra số nguyên tố ngẫu nhiên lớn p và phần tử sinh α của nhóm $\mathbb{Z}_p^*$
2. Chọn số ngẫu nhiên $1 \leq a \leq p-2$, và tính $\alpha^a \mod p$
3. Khóa công khai của A là p, α, α^a, khóa bí mật là cặp a.

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, p-1]$

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, p-1]$
   (c) Chọn số ngẫu nhiên $1 \leq k \leq p-2$

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, p-1]$
   (c) Chọn số ngẫu nhiên $1 \leq k \leq p-2$
   (d) tính $\gamma = \alpha^k \mod p$ và $\delta = m * (\alpha^a)^k \mod p$

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, p-1]$
   (c) Chọn số ngẫu nhiên $1 \leq k \leq p-2$
   (d) tính $\gamma = \alpha^k \mod p$ và $\delta = m * (\alpha^a)^k \mod p$
   (e) Gửi $c = (\gamma, \delta)$ cho A

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, p-1]$
   (c) Chọn số ngẫu nhiên $1 \leq k \leq p-2$
   (d) tính $\gamma = \alpha^k \mod p$ và $\delta = m * (\alpha^a)^k \mod p$
   (e) Gửi $c = (\gamma, \delta)$ cho A

2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, p-1]$
   (c) Chọn số ngẫu nhiên $1 \leq k \leq p-2$
   (d) tính $\gamma = \alpha^k \mod p$ và $\delta = m * (\alpha^a)^k \mod p$
   (e) Gửi $c = (\gamma, \delta)$ cho A

2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau
   (a) Sử dụng khóa riêng a để tính $\gamma^{p-1-a} \mod p$

$$(\gamma^{p-1-a} = \gamma^{-a} = \alpha^{-ak})$$

Mã hóa và giải mã của ElGamal

Mỗi thực thể B mã hóa tin m và gửi cho A, A giải mã:

1. **Mã hóa**. Thực thể B thực hiện các bước sau
   (a) Nhận khóa công khai (p, α, α^a) từ A
   (b) Biểu diễn tin ở dạng số tự nhiên m trong khoảng $[0, p-1]$
   (c) Chọn số ngẫu nhiên $1 \leq k \leq p-2$
   (d) tính $\gamma = \alpha^k \mod p$ và $\delta = m * (\alpha^a)^k \mod p$
   (e) Gửi $c = (\gamma, \delta)$ cho A

2. **Giải mã**. Để khôi phục tin gốc m từ c, thực thể A thực hiện như sau
   (a) Sử dụng khóa riêng a để tính $\gamma^{p-1-a} \mod p$

$$(\gamma^{p-1-a} = \gamma^{-a} = \alpha^{-ak})$$

   (b) Khôi phục m bởi tính $\gamma^{-a}.\delta \mod p$

Tài liệu tham khảo

Handbook of Applied Crytography, chapter 8

http://cacr.uwaterloo.ca/hac/