Trường Đại học Đà Lạt

Đề tài:

HỆ THỐNG MẬT MÃ ELGAMAL

NHÓM 7-VTK37:

Nguyễn Thị Kim Nga 1310471

To Tiang Sampo 1310477

Ngô Hữu Nguyện 1310466

1
- Hệ thống mật mã

2
- Mã hóa và giải mã hệ Elgamal

3
- Thám mã hệ Elgamal

4
- Đánh giá hệ Elgamal

HỆ THỐNG MẬT MÃ

I) GIỚI THIỆU VỀ HỆ MẬT MÃ.

Hệ mật mã gồm **5** thành phần sau:

P (Plaintext)

C (Ciphertext)

K (Key)

E (Encrytion)

D (Decrytion)

HỆ THỐNG MẬT MÃ

1. Hệ mật mã đối xứng (cổ điển)
2. Hệ mật mã bất đối xứng (công khai)

HỆ THỐNG MẬT MÃ ELGAMAl

II) HỆ MẬT MÃ ELGAMAL.

Do ông Teher Elgalmal người Ai cập đề xuất vào năm 1984

HỆ THỐNG MẬT MÃ ELGAMAL

II) HỆ MẬT MÃ ELGAMAL.

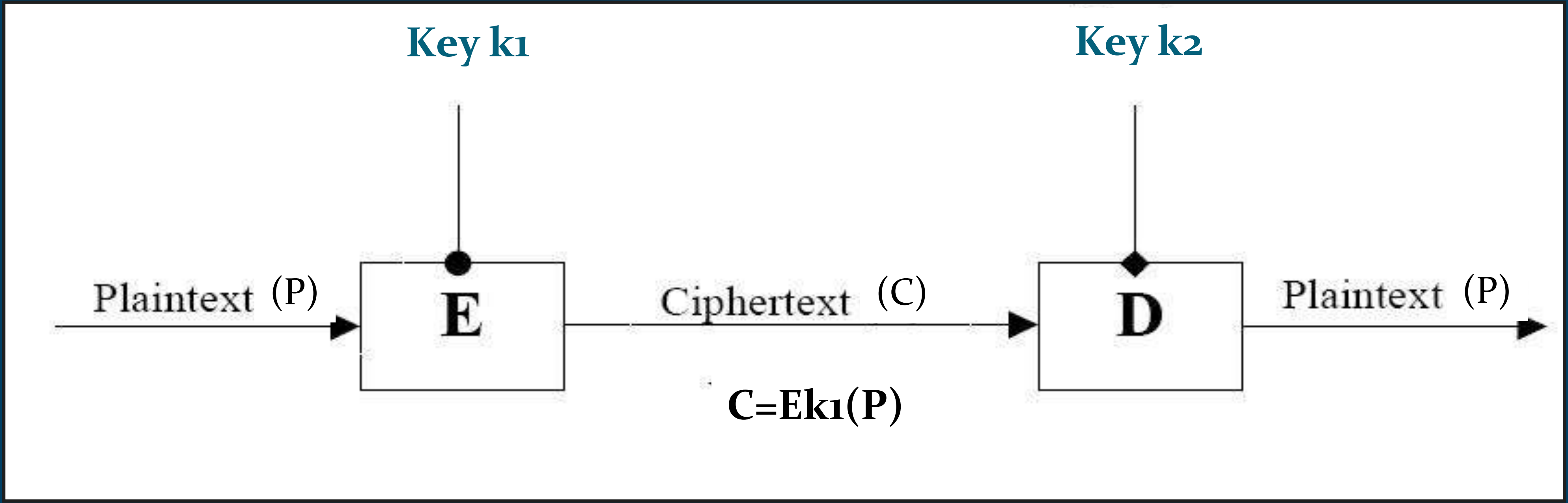
-Hệ mật mã công khai.

-Tính an toàn phụ thuộc vào độ phức tạp của bài toán logarith.

-Biến thể sơ đồ phân phối Diffie-Hellmal.

HỆ THỐNG MẬT MÃ

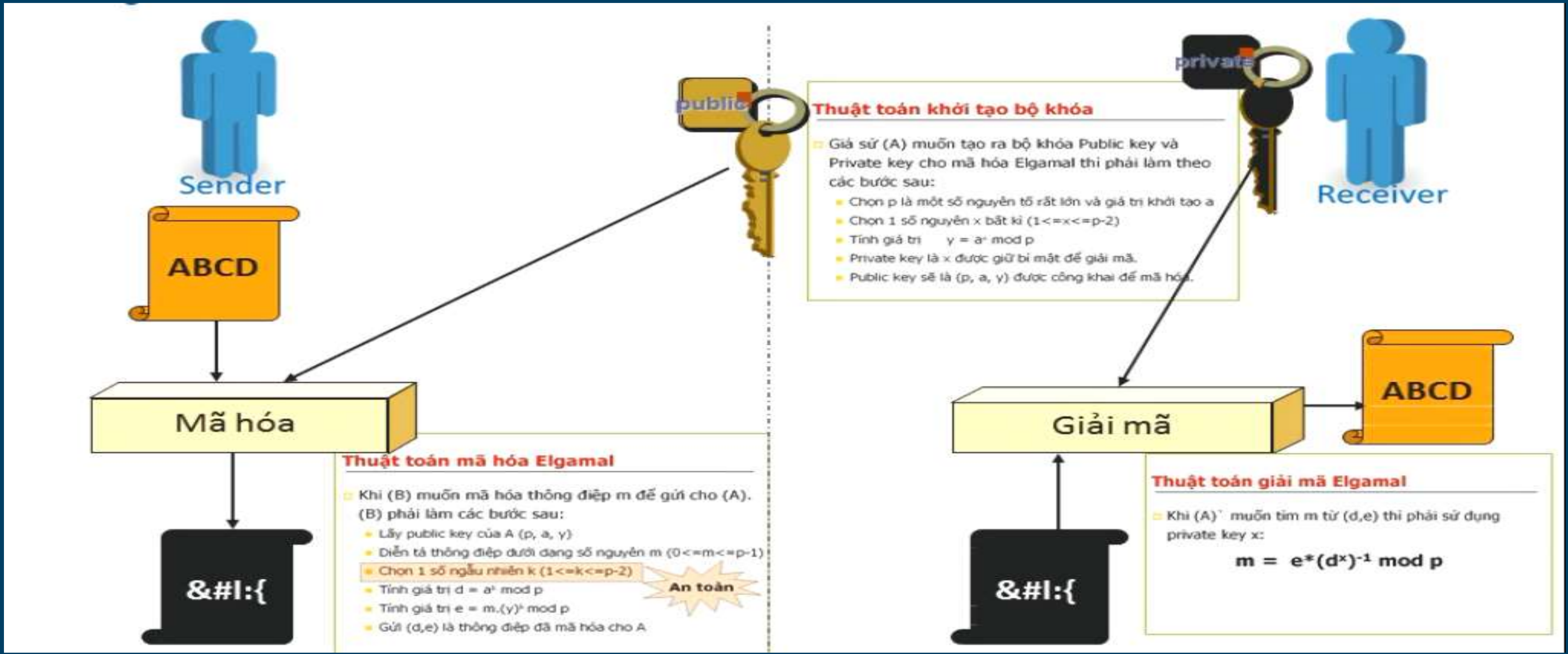
III) MÃ HOÁ VÀ GIẢI MÃ HỆ ELGAMAL.



Quá trình mã hoá và giải mã

HỆ THỐNG MẬT MÃ

III) MÃ HOÁ VÀ GIẢI MÃ HỆ ELGAMAL.



HỆ THỐNG MẬT MÃ ELGAMAL

III) MÃ HOÁ VÀ GIẢI MÃ HỆ ELGAMAL.

1) Mã hóa

- Ban đầu người ta sẽ lựa chọn một số nguyên tố lớn **p** và 2 số nguyên tố nhỏ hơn p là **alpha** và **a** (khóa bí mật của người nhận) sau đó tính khóa công khai:

$$\textbf{beta} = \textbf{alpha}^{\textbf{a}} \textbf{ mod p}$$

HỆ THỐNG MẬT MÃ ELGAMAL

III) MÃ HOÁ VÀ GIẢI MÃ HỆ ELGAMAL.

1) Mã hóa

- Để mã hóa một thông điệp **M** (một số nguyên tố trên Zp) thành bản mã **C** người gửi chọn một số ngẫu nhiên k nhỏ hơn p và tính cặp bản mã:

$$\mathbf{C_1 = alpha^k \bmod p}$$

$$\mathbf{C_2 = (M*beta^k)\bmod p}$$

HỆ THỐNG MẬT MÃ ELGAMAl

III) MÃ HOÁ VÀ GIẢI MÃ HỆ ELGAMAL.

1) Mã hóa

- Bản mã **E(C_1 , C_2)** được gửi đi với:

$$\mathbf{C_1 = alpha^k \bmod p}$$

$$\mathbf{C_2 = (M*beta^k)\bmod p}$$

Sau đó k sẽ bị hủy đi.

HỆ THỐNG MẬT MÃ ELGAMAL

III) MÃ HOÁ VÀ GIẢI MÃ HỆ ELGAMAL.

2) Giải mã

- Để giải mã thông điệp **M** đầu tiên ta dùng khóa bí mật **a** và tính theo công thức:

$$\mathbf{M = (C2 * (C1^{a})^{-1}) \bmod p}$$

Với: $\mathbf{(C1^{a})^{-1}) \bmod p = (C1^{(p-1-a)}) \bmod p}$

HỆ THỐNG MẬT MÃ ELGAMAL

III) MÃ HOÁ VÀ GIẢI MÃ HỆ ELGAMAL.

3) Kết luận

K=(p, alpha, a, beta) với:

- Thành phần khóa công khai:

Ku= (alphal, beta, p)

- Thành phần khóa bí mật:

Kr= (a, p)

HỆ THỐNG MẬT MÃ ELGAMAl

VÍ DỤ:

Cho Hệ **Elgama**l có **p = 2579**; **alpha = 2**; **a = 765**; chọn **k** ngẫu nhiêu là **853**. Bản rõ **M = 1299**.

Tìm khóa của hệ mã trên?

HỆ THỐNG MẬT MÃ ELGAMAL

Giải:

Mã hóa :

Trước hết ta tính: beta = alpha^{a} mod p

$= 2^{765} \bmod 2579 = 949$

Để mã hóa thông điệp M = 1299 ta tính theo k =853:

C1 = alpha^{k} mod p = $2^{853} \bmod 2579 = 435$

C2 = (M*beta^{k})mod p = $(1299 * 949^{853}) \bmod 2579 = 2396$

Vậy bản mã được gửi đi sẽ là **C = (435, 2396).**

HỆ THỐNG MẬT MÃ ELGAMAl

Giải mã :

Với khóa bí mật a= 765:

$(C1^{a})^{-1}) \bmod p = (C1^{(p-1-a)}) \bmod p$

$= (435^{(2579-1-765)}) \bmod 2579$

$= (435^{1813}) \bmod 2579 = 1980$

$M = (C2 * (C1^{a})^{-1}) \bmod p = (2396*1980) \bmod 2579 = 1299$

HỆ THỐNG MẬT MÃ ELGAMAL

Kết luận:

Xây dựng được hệ mã Elgamal bộ khóa:

K=(p, alpha, a, beta) = (2579, 2, 765, 949) với:

- Thành phần khóa công khai:

Ku= (alphal, beta, p) = (2, 949, 2579)

- Thành phần khóa bí mật:

Kr= (a, p) = (765, 2579)

- Mã hóa **M=1299** với **E(C1, C2) = (435,2396)**

HỆ THỐNG MẬT MÃ ELGAMAl

IV) THÁM MÃ HỆ ELGAMAL.

-Thuật toán Shank

-Thuật toán Pohlig_Hellman (Link: http://123doc.org/document/2556734-tim-hieu-he-mat-ma-elgamal.htm)

HỆ THỐNG MẬT MÃ ELGAMAI

Bài toán logarith rời rạc:

- Logarith rời rạc là sự kết nối của phép tính logarith trên trường số thực vào các nhóm hữu hạn. Ta nhắc lại rằng với hai số thực x,y và cơ số a>0, a#0, nếu a^x – y=0 thì x được gọi là logarith cơ số a của y, ký hiệu x = $\log_a y$.
- Logarith rời rạc là bài toán khó. Trong khi bài toán ngược lũy thừa rời rạc lại không khó.

HỆ THỐNG MẬT MÃ ELGAMAl

- Cho p là một số nguyên tố , xét nhóm nhân các số nguyên modulo p:

$$Z_p^* = \{ 1,2\ldots.,p \}$$ với phép nhân modulo p.

- Nếu ta tính lũy thừa bậc k của một số trong nhóm rồi rút gọn theo modulo p thì ta được một số trong nhóm đó. Quá trình này được gọi là lũy thừa rời rạc modulo p.

HỆ THỐNG MẬT MÃ ELGAMAl

Ví dụ: Với p = 17 , lấy a = 3, k = 4 ta có :

$$3^4 = 81 = 13 \bmod 17$$

Logarith rời rạc là phép tính ngược lại :

- **Biết : $3^k = 13 \pmod{17}$ hãy tìm k.?**

=>Thực hiện thuật toán Shank => k=4. Tuy nhiên đây là một bài toán tương đối khó. Trong trường hợp p lớn (có ít nhất 150 chữ số) thì bài toán trở thành bất khả thi => an toàn

HỆ THỐNG MẬT MÃ ELGAMAL

Thuật toán shank:

Input : Số nguyên tố **p**, phần tử nguyên thủy **alphal** của Z^*p, số nguyên **y**.

Output : Cần tìm a sao cho **beta =alpha**^{a} **mod p**.

HỆ THỐNG MẬT MÃ ELGAMAL

Thuật toán shank:

Thuật toán :

Gọi **m = [(p-1)$^{1/2}$]** (lấy phần nguyên).

Bước 1: Tính **alpha^{mj} mod p** với 0<=j<=m-1.

Bước 2: **Sắp xếp** các cặp **(j, alpha^{mj} mod p)** theo alphal^{mj} mod p và lưu vào danh sách **L1**.

Bước 3: Tính **beta*alpha^{-i} mod p** với 0<=i<=m-1.

HỆ THỐNG MẬT MÃ ELGAMAL

Thuật toán shank:

Bước 4: **Sắp xếp** các cặp **(i, beta*alpha^{-i} mod p)** theo beta*alpha^{-i} mod p và lưu vào danh sách **L2**.

Bước 5: Tìm trong hai danh sách **L1** và **L2** xem có tồn tại cặp:

(j, alpha^{mj} mod p) và (i, beta*alpha^{-i} mod p) sao cho **alpha^{mj} mod p = beta*alpha^{-i} mod p** (tọa độ thứ hai của hai cặp bằng nhau).

HỆ THỐNG MẬT MÃ ELGAMAl

Thuật toán shank:

Bước 6: Tính **a=log$_{alpha}$ beta=(mj + i) mod (p - 1)**

Kết quả này có thể kiểm chứng từ công thức:

$alpha^{mj}$ mod p = beta*$alpha^{-i}$ mod p

=>$alpha^{mj+i}$ mod p = beta mod p

=> log_{alpha} beta =(mj + i) mod (p – 1) = **a.**

HỆ THỐNG MẬT MÃ ELGAMAl

Thuật toán shank:

Ví dụ: Với bài toán trên người ta thám mã chỉ có khóa công khai

$$K_p = (\, p, alpha, beta \,) = (\, 97, 5, 44 \,)$$

Ta có:

$$m = [(p-1)^{1/2}] = [(\, 97-1)^{1/2}] = 10$$

HỆ THỐNG MẬT MÃ ELGAMAl

Thuật toán shank:

Bước 1: Tính **$alpha^{mj}$ mod p** với 0<=j<=m-1.

Bước 2: Sắp xếp các cặp (j, $alpha^{mj}$ mod p) theo $alpha^{mj}$ mod p và lưu vào danh sách **L1**

HỆ THỐNG MẬT MÃ ELGAMAL

Thuật toán shank:

J(0<=j<=m-1)	5^{10j} mod 97(alpha^{mj} mod p)
0	1
1	53
2	93
3	79
4	16
5	72
6	33
7	3
8	62
9	85

HỆ THỐNG MẬT MÃ ELGAMAL

Thuật toán shank:

Bước 3: Tính beta*alpha^{-i} mod p với 0<=i<=m-1.

Bước 4: Sắp xếp các cặp (i, beta*alpha^{-i} mod p) theo beta*alpha^{-i} mod p và lưu vào danh sách L2.

HỆ THỐNG MẬT MÃ ELGAMAL

Thuật toán shank:

J(0<=j<=m-1)	$44*5^i$ mod 97(beta*alpha^{-i} mod p)
0	44
1	26
2	33
3	68
4	49
5	51
6	61
7	14
8	70
9	59

HỆ THỐNG MẬT MÃ ELGAMAI

Thuật toán shank:

Bước 5: Tìm trong hai danh sách L1 và L2 xem có tồn tại cặp (j, $alpha^{mj}$ mod p) và (i, beta*$alpha^{-i}$ mod p) nào mà $alpha^{mj}$ mod p = beta*$alpha^{-i}$ mod p (tọa độ thứ hai của hai cặp bằng nhau).

Dựa vào bảng 2 bảng danh sách L1 và L2 khi j = 6 và i = 2 thì:

$$alpha^{mj} \bmod p = beta*alpha^{-i} \bmod p = 33$$

HỆ THỐNG MẬT MÃ ELGAMAI

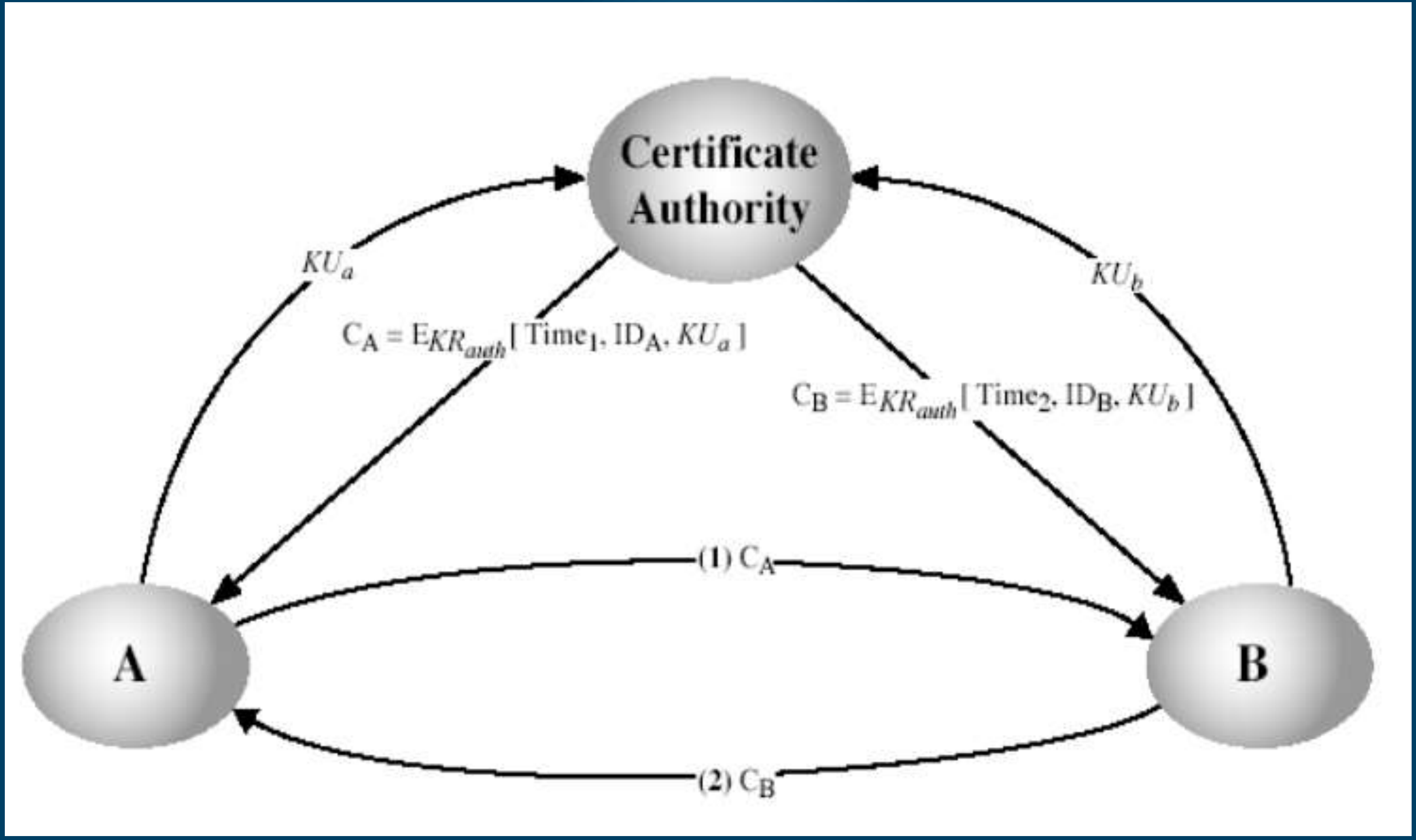
Thuật toán shank:

Bước 6: Tính a= (mj + i) mod (p - 1). Kết quả này có thể kiểm chứng từ công thức

Vậy ta có a = (10 * 6 +2) mod (97 – 1) = 62.

HỆ THỐNG MẬT MÃ ELGAMAl

Quản lý khóa



HỆ THỐNG MẬT MÃ ELGAMAL

- **Độ an toàn**

Hệ thống elgamal

- Hệ thống elgamal dựa trên bài toàn logarith rời rạc. Tính an toàn của nó tùy thuộc vào độ phức tạp của bài toán logarith.

- Trong bài toán về hệ Elgamal:

+ p là số nguyên tố, a là phần tử nguyên thủy của Z*p. (p và a là cố định)

+ Bài toán logorith rời rạc có thể được phát biểu như sau: Tìm 1 số mũ x duy nhất, 0<=x<=p-2 sao cho a^x=y mod p, với y thuộc Z*p cho trước.

HỆ THỐNG MẬT MÃ ELGAMAL

- **Độ an toàn**

- Bài toán có thể giải được bởi phương pháp vét cạn (tức là duyệt tất cả phần tử x) để tìm x thỏa mãn.

- Bài toán có độ phức tạp là: O(p) (bỏ qua thừa số logarit). Vấn đề đặt ra là nếu p lớn, rất lớn thì để thực hiện phương pháp này cần thời gian rất lớn. Suy ra không khả thi.

HỆ THỐNG MẬT MÃ ELGAMAL

- **Độ an toàn**

Xét thuật toán Shank để thám mã hệ mã hóa Elgamal

+ Người thám mã chỉ có khóa công khai (p,a,y).

+ Bài toán logarit rời rạc cũng được phát biểu như sau: Tìm 1 số mũ x duy nhất, 0<=x<=p-2 sao cho a^x=y mod p, với y thuộc Z*p cho trước.

HỆ THỐNG MẬT MÃ ELGAMAI

- **Độ an toàn**

+ Độ phức tạp của bài toán là O([p-1]^1\2) và bộ nhớ O([p-1]^1\2)(bỏ qua thừa số logarit), giảm rất nhiều so với phương pháp vét cạn.

+ Chúng ta cần tính các phần tử thuộc 2 danh sách L1, L2 đều là phép toán lũy thừa phụ thuộc và i, j; i và j lại phụ thuộc vào m nên ta nhận thấy bài toán chỉ áp dụng với những trường hợp p nhỏ.

HỆ THỐNG MẬT MÃ ELGAMAL

- Đánh giá độ an toàn của hệ mã hóa Elgamal:

- Hệ mã hóa Elgamal áp dụng bài toán logarit rời rạc chính vì vậy độ an toàn của hệ mã hóa là rất lớn vì bài toán logarit rời rạc chưa có phương pháp hiệu quả để tính.

- Với 1 số p đủ lớn, thuật toán mã hóa Elgamal không có phương pháp thám mã hiệu quả.

HỆ THỐNG MẬT MÃ ELGAMAl

- **Ưu điểm, nhược điểm của hệ mã Elgamal**

- Ưu điểm:

Độ phức tạp của bài toán logarith lớn nên đọ an toàn cao.

Bản mã phụ thuộc vào bản rõ x và giá trị ngẫu nhiên nên từ một bản rõ ta có thể có nhiều bản ma khác nhau.

HỆ THỐNG MẬT MÃ ELGAMAL

- **Ưu điểm, nhược điểm của hệ mã Elgamal**

- Nhược điểm:

Tốc độ chậm (do phải xử lý số nguyên lớn)

Dung lượng bộ nhớ dành cho việc lưu trữ khoa yêu cầu phải lớn.

HỆ THỐNG MẬT MÃ ELGAMAl

Tài liệu tham khảo:

- Bài giảng an toàn và bảo mật thông tin - Trần Minh Văn – Đại học Nha Trang
- Elgamal encryption - Wikipedia
- Bài giảng hệ mật mã Elgamal. Link: http://doc.edu.vn/tai-lieu/bai-giang-he-mat-elgamal-57863/
- Tìm hiểu hệ mật mã Elgamal. Link: http://123doc.org/document/2556734-tim-hieu-he-mat-ma-elgamal.htm

Thank you for listening!

why
when
who
where
what
why
QUESTIONS
who
how
where
who
what
how
when