BÀI 4.
GIAO THỨC MẬT MÃ

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

Nội dung

- Tổng quan về giao thức mật mã
- Các giao thức trao đổi khóa
- Các giao thức chữ ký điện tử

2

1. TỔNG QUAN VỀ GIAO THỨC MẬT MÃ

3

3

Giao thức mật mã là gì?

- Chúng ta đã biết về "mật mã" và các ứng dụng của nó:
  - Bảo mật
  - Xác thực
- Nhưng chúng ta cần biết "Sử dụng mật mã như thế nào?"
  - Hệ mật mã an toàn chưa đủ để làm cho quá trình trao đổi thông tin an toàn
  - Cần phải tính đến các yếu tố, cá nhân tham gia không trung thực
- *Giao thức là một chuỗi các bước thực hiện mà các bên phải thực hiện để hoàn thành một tác vụ nào đó.*
  - Bao gồm cả quy cách biểu diễn thông tin trao đổi
- *Giao thức mật mã: giao thức sử dụng các hệ mật mã để đạt được các mục tiêu an toàn bảo mật*

4

4

Các thuộc tính của giao thức mật mã

- Các bên tham gia phải hiểu về các bước thực hiện giao thức
- Các bên phải đồng ý tuân thủ chặt chẽ các bước thực hiện
- Giao thức phải rõ ràng, không nhập nhằng
- Giao thức phải đầy đủ, xem xét mọi tình huống có thể
- ***Với giao thức mật mã: Giao thức phải được thiết kế để khi thực hiện không bên nào thu được nhiều lợi ích hơn so với thiết kế ban đầu.***

5

5

Yêu cầu Perfect Forward Secrecy

- Một giao thức cần đảm bảo an toàn cho khóa ngắn hạn(short-term key) trong các phiên làm việc trước là an toàn khi khóa dài hạn (long-term key) không còn an toàn.

6

6

Tấn công khóa đã biết (known-key)

- Sử dụng khóa phiên đã biết trong các phiên làm việc trước để tấn công các phiên làm việc tới.
  - Dùng khóa phiên cũ đã biết để tính toán khóa phiên trong các phiên truyền thông mới
  - Dùng khóa phiên cũ đã biết để đánh lừa nạn nhân sử dụng lại → Tấn công phát lại (Replay Attack)

7

7

Giao thức có trọng tài(Trusted arbitrator)

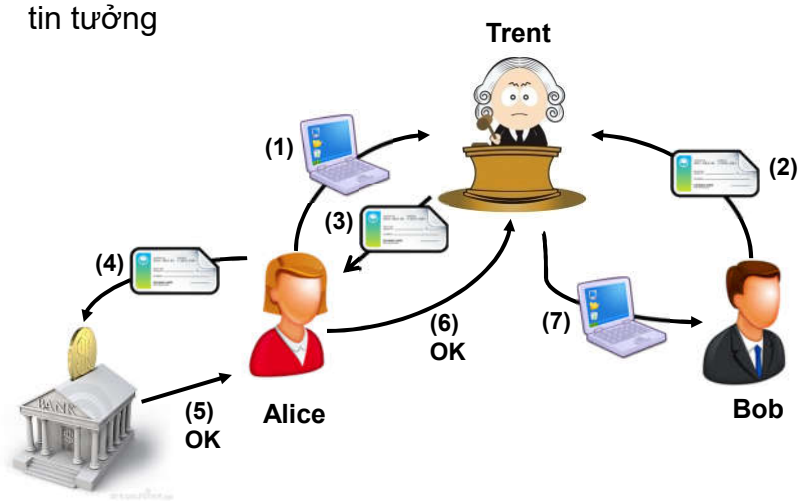
- Trọng tài là bên thứ 3 thỏa mãn:
  - Không có quyền lợi riêng trong giao thức
  - Không thiên vị
- Các bên cần tin tưởng vào trọng tài
  - Mọi thông tin từ trọng tài là đúng và tin cậy
  - Trọng tài luôn hoàn thành đầy đủ nhiệm vụ trong giao thức
- Ví dụ: Alice cần bán một chiếc máy tính cho Bob, người sẽ trả bằng séc
  - Alice muốn nhận tờ séc trước để kiểm tra
  - Bob muốn nhận máy tính trước khi giao séc

8

8

Giao thức có trọng tài – Ví dụ

- Alice và Bob tin tưởng vào Trent-Bên thứ 3 mà cả 2 cùng tin tưởng

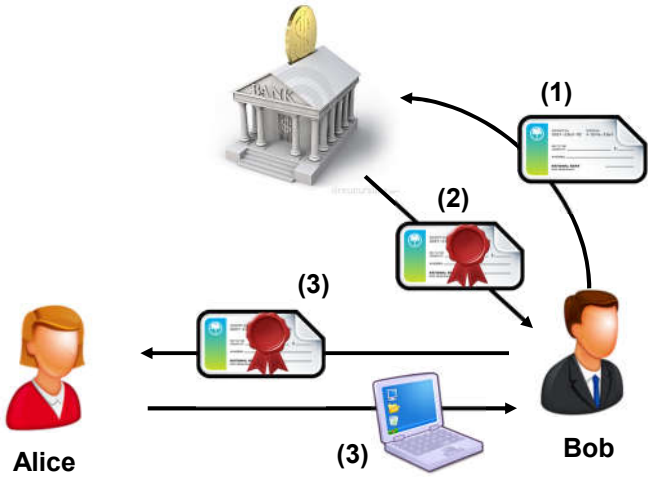


9

9

Giao thức có trọng tài – Ví dụ

- Alice tin tưởng vào ngân hàng mà Bob ủy nhiệm



10

10

Giao thức sử dụng trọng tài

- Khi 2 bên đã không tin tưởng nhau, có thể đặt niềm tin vào bên thứ 3 không?
- Tăng chi phí
- Tăng trễ
- Trọng tài trở thành "cổ chai" trong hệ thống
- Trọng tài bị tấn công

11

11

Giao thức có người phân xử(*Adjudicated Protocols)*

- Chia giao thức có trọng tài thành 2 giao thức:
  - Giao thức không cần đến trọng tài, có thể thực hiện bất kỳ khi nào 2 bên muốn
  - Giao thức cần người phân xử: chỉ sử dụng khi có tranh chấp
- Hãy xem xét lại giao dịch trong ví dụ trên với giải pháp mới này!

(1) Alice và Bob thỏa thuận hợp đồng

(2) Hai bên cùng ký xác thực vào hợp đồng

(3) Thực hiện giao dịch

Nếu có tranh chấp:

(4) Alice trình bằng chứng cho người phán xử

(5) Bob trình bằng chứng cho người phán xử

12

12

Giao thức tự phân xử(*Self-Enforcing Protocols*)

- Không cần đến bên thứ 3
- Giao thức có cơ chế để một bên có thể phát hiện sự gian lận của bên còn lại
- Không phải tình huống nào cũng có thể tìm ra giao thức như vậy

13

13

Các dạng tấn công vào giao thức mật mã

- Có thể lợi dụng các điểm yếu trong:
  - Hệ mật mã
  - Các bước thực hiện
- Tấn công thụ động: nghe trộm
- Tấn công chủ động: can thiệp vào giao thức
  - Chèn thông điệp
  - Thay thế thông điệp
  - Sử dụng lại thông điệp
  - Giả mạo một trong các bên

14

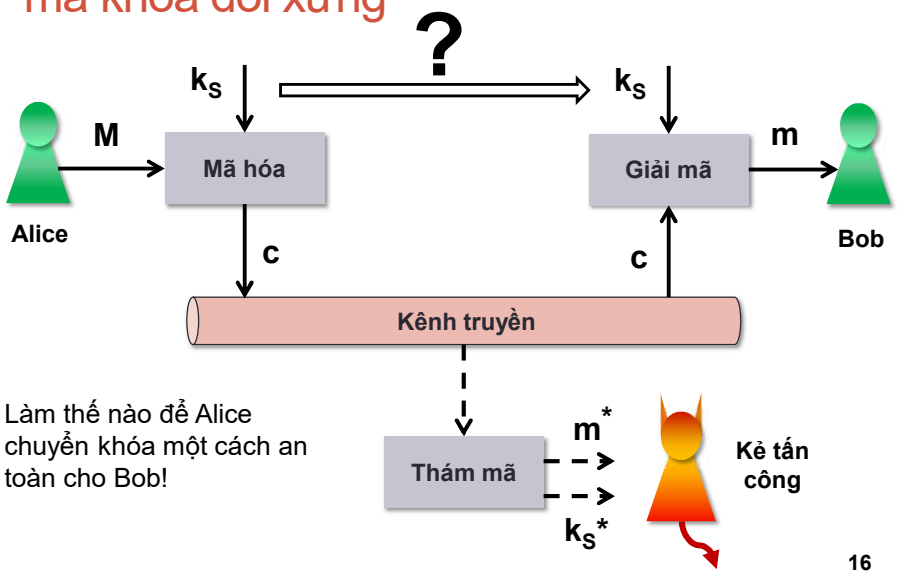
14

2. CÁC GIAO THỨC PHÂN PHỐI KHÓA BÍ MẬT

15

15

Hãy xem lại sơ đồ bảo mật sử dụng mật mã khóa đối xứng



16

16

Giao thức phân phối khóa không tập trung

- Khóa chính: k_M đã được A và B chia sẻ an toàn
  - Làm thế nào vì đây chính là bài toán đang cần giải quyết ☺
  - Khóa chính được sử dụng để trao đổi khóa phiên K_S
- Khóa phiên k_S: sử dụng để mã hóa dữ liệu trao đổi
- Giao thức 1.1

  (1) A → B: ID_A

  (2) B → A: $E(k_M, ID_B||k_S)$
- Giao thức này đã đủ an toàn chưa?
  - Tấn công nghe lén
  - Tấn công thay thế
  - Tấn công giả mạo
  - Tấn công phát lại

17

17

Giao thức phân phối khóa không tập trung – Giao thức 1.2

- Sử dụng các yếu tố chống tấn công phát lại (replay attack)

  (1) A → B: $ID_A || N_1$

  (2) B → A: $E(k_M, ID_B || k_S || N_1 || N_2)$

  (3) A → B: A kiểm tra N_1 và gửi $E(k_S, N_2)$

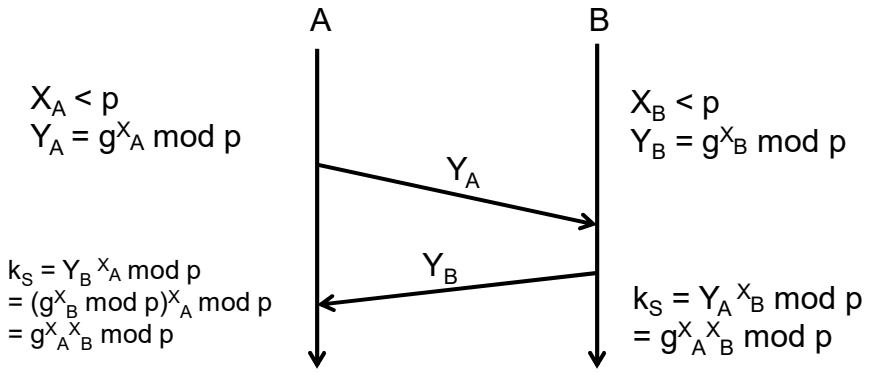
  (4) B kiểm tra N_2
- E: Hàm mã hóa có xác thực
- N_1, N_2: Giá trị nonce (dùng 1 lần)
- Hạn chế của phân phối khóa không tập trung?

18

18

Sơ đồ trao đổi khóa Diffie-Hellman

- Alice và Bob cùng chia sẻ một khóa nhóm (p, g). Trong đó
  - p là một số nguyên tố
  - 1< g < p thỏa mãn: $(g^i \bmod p) \neq g^j \bmod p \ \forall\ 1 \leq i \neq j < p$

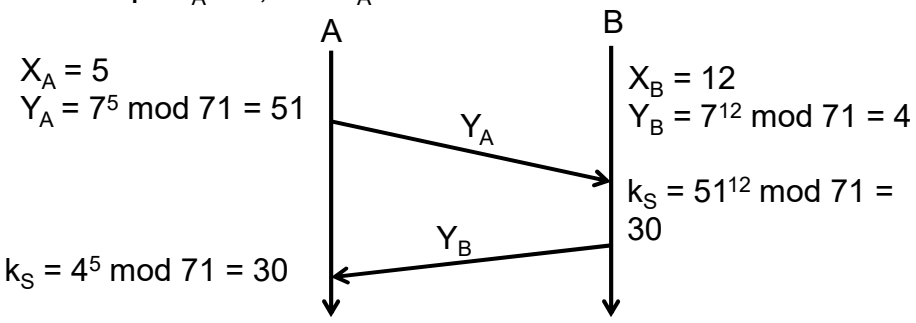


19

19

Ví dụ

- Khóa chung của nhóm p = 71, g= 7
  - Hãy tự kiểm tra điều kiện thỏa mãn của g
- A chọn $X_A = 5$, tính $Y_A = 7^5 \bmod 71 = 51$



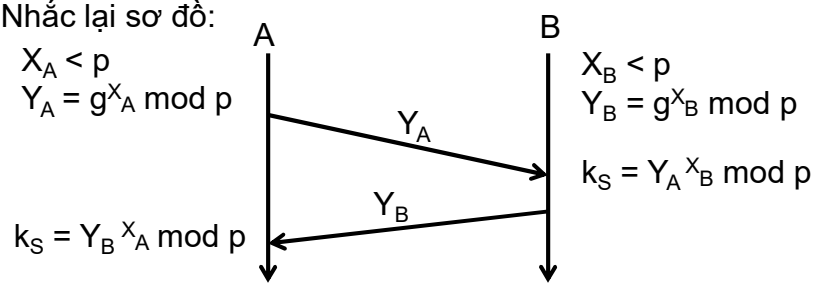
Rút ra được điều gì từ sơ đồ này?

20

20

Tấn công sơ đồ trao đổi khóa Diffie-Hellman

- Nhắc lại sơ đồ:



- Kịch bản tấn công man-in-the-middle
  - C sinh 2 cặp khóa (X'_A, Y'_A) và (X'_B, Y'_B)
  - Tráo khóa Y_A bằng Y'_A, Y_B bằng Y'_B
  - Hãy suy luận xem tại sao C có thể biết được mọi thông tin A và B trao đổi với nhau

21

21

Giao thức phân phối khóa tập trung

- Sử dụng bên thứ 3 được tin cậy – KDC (Key Distribution Centre):
  - Sinh khóa bí mật k_S
  - Phân phối k_S tới A và B
- A và KDC đã chia sẻ một khóa bí mật k_A, B và KDC đã chia sẻ một khóa bí mật k_B
  - Làm thế nào?

22

22

Giao thức phân phối khóa tập trung- Giao thức 2.1

(1) A → KDC: ID_A || ID_B

(2) KDC → A: E(k_A, k_S || ID_A || ID_B || E(k_B, ID_A || k_S))

(3) A giải mã (2), thu được k_S

(4) A → B: E(k_B, ID_A || k_S). B giải mã, thu được k_S

(5) A ↔ B: E(k_S, Data)

- E: Mã hóa có xác thực
- Hãy xem xét tính an toàn của giao thức này?
  - Tấn công nghe lén
  - Tấn công thay thế
  - Tấn công giả mạo
  - Tấn công phát lại

23

23

Giao thức phân phối khóa tập trung- Giao thức 2.2 (Needham-Schroeder)

(1) A → KDC: ID_A || ID_B || **N_1**

(2) KDC → A: E(k_A, k_S || ID_A || ID_B || **N_1** || E(k_B, ID_A || k_S))

(3) A giải mã, kiểm tra N_1 thu được k_S

(4) A → B: E(k_B, ID_A || k_S) ← B giải mã, thu được k_S

(5) B → A: E(k_S, N_2) ← A giải mã, có được N_2, tính f(N_2)

(6) A → B: E(k_S, f(N_2)) ← B giải mã kiểm tra f(N_2)

(7) A ↔ B: E(k_S, Data)

E: mã hóa có xác thực

N_1, N_2: giá trị dùng 1 lần (nonce)

f(x): hàm biến đổi sao cho f(x) ≠ x với mọi x(Tại sao cần?)

- Hãy xem xét lại tính an toàn của giao thức này!

24

24

Tính đúng đắn của giao thức

- Xem xét việc tấn công phát lại vào bản tin số 4:

(4) Attacker →B: $E(k_B, ID_A \| k^{old}_S)$

(5) B → A: $E(k^{old}_S, N_2)$

A giải mã $D(k^{new}_S, E(k^{old}_S, N_2)) = N_2' \neq N_2$

(6) A → B: $E(k^{new}_S, f(N_2'))$

B giải mã: $D(k^{old}_S, E(k^{new}_S, f(N_2'))) \neq f(N_2)$ → B từ chối sử dụng khóa $k^{old}S$

25

Giao thức phân phối khóa tập trung- Giao thức 2.3 (Denning)

(1) A → KDC: $ID_A \| ID_B$

(2) KDC → A: $E(k_A, k_S \| ID_A \| ID_B \| \mathbf{T} \| E(k_B, ID_A \| k_S \| \mathbf{T}))$

(3) A giải mã, kiểm tra T, thu được k_S

(4) A → B: $E(k_B, ID_A \| k_S \| \mathbf{T})$ ← B giải mã, kiểm tra T

(5) B → A: $E(k_S, N_1)$

(6) A → B: $E(k_S, f(N_1))$ ← B giải mã, kiểm tra N_1

(7) A ↔ B: $E(k_S, Data)$

E: mã hóa có xác thực

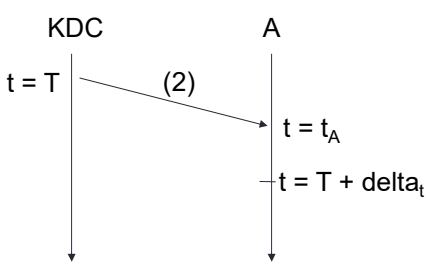
T: nhãn thời gian (time stamp) là thời điểm KDC phát bản tin

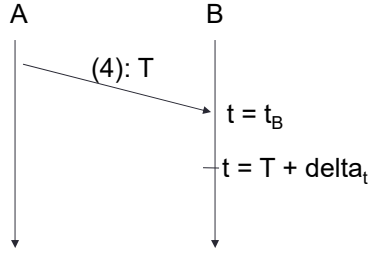
- Kiểm tra tính an toàn của sơ đồ này:
  - Mất đồng bộ đồng hồ của các bên

26

Giao thức 2.3 (Denning)

Kiểm tra nhãn thời gian





A kiểm tra: t_A – (T + *X*) < $delta_{tA}$
→ bản tin hợp lệ

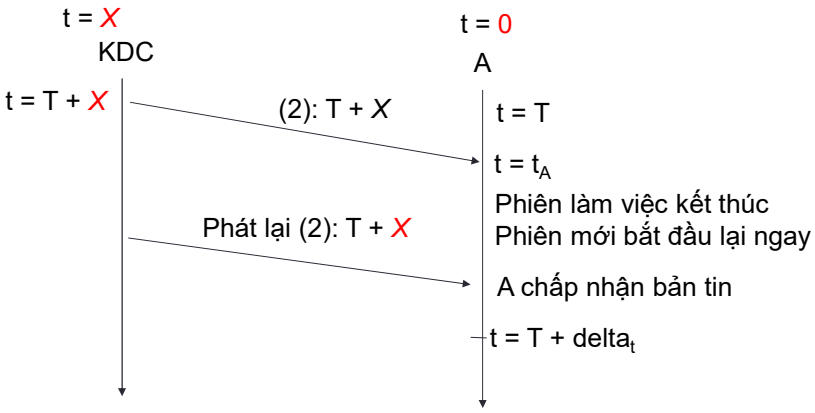
B kiểm tra: t_B – T < $delta_{tB}$
→ bản tin hợp lệ

27

27

Giao thức 2.3 (Denning)

- Tấn công khi mất đồng bộ đồng hồ



28

28

Giao thức phân phối khóa tập trung- Giao thức 2.4 (Kehne)

(1) A → B: $ID_A \| N_A$

(2) B → KDC: $ID_B \| N_B \| E(k_B, ID_A \| N_A \| T_B)$

(3) KDC → A: $E(k_A, ID_B \| N_A \| k_S) \| E(k_B, ID_A \| k_S \| T_B) \| N_B$

A giải mã, kiểm tra N_A → chấp nhận k_S nếu N_A hợp lệ

(4) A →B: $E(k_B, ID_A \| k_S \| T_B) \| E(k_S, N_B)$

B giải mã, kiểm tra T_B → chấp nhận k_S nếu T_B hợp lệ

→ giải mã với k_S, biết $N_B^{(4)}$ và so sánh với $N_B^{(2)}$ → xác nhận được khóa k_S mà A dùng giống B đang có

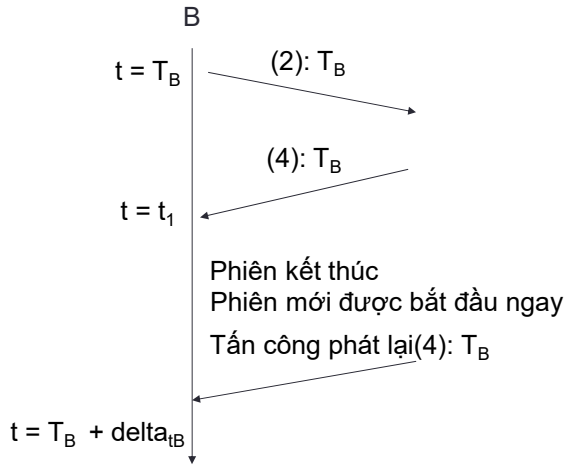
T_B: Thời điểm B gửi bản tin số (2)

- Vì sao việc sử dụng nhãn thời gian T_B của B tốt hơn nhãn thời gian T của KDC trong giao thức 2.3

29

29

Giao thức 2.4 (Kehne)



B kiểm tra: $t_1 - T_B < delta_{tB}$

→ bản tin hợp lệ

30

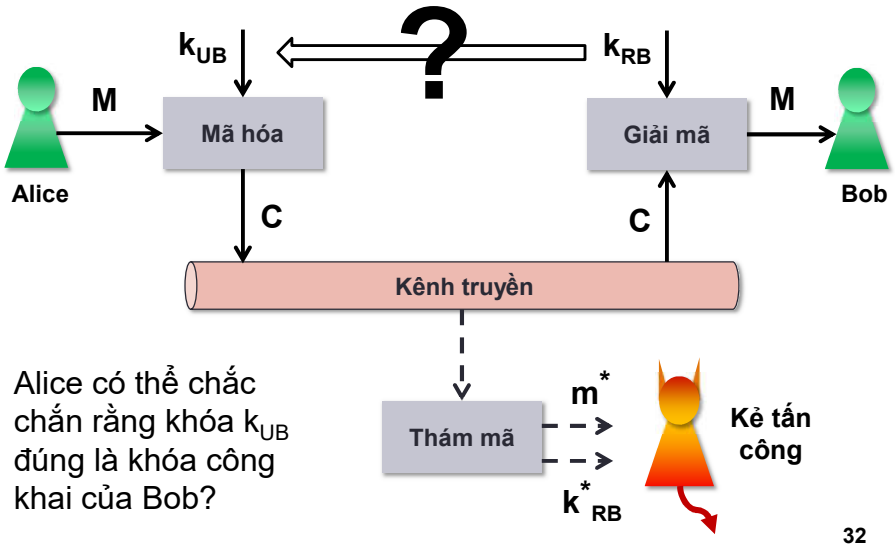
30

3. CÁC GIAO THỨC PHÂN PHỐI KHÓA CÔNG KHAI

31

31

Hãy xem lại sơ đồ bảo mật sử dụng mật mã khóa công khai



Alice có thể chắc chắn rằng khóa k_{UB} đúng là khóa công khai của Bob?

32

32

Giao thức phân phối khóa không tập trung

- Hãy xem xét giao thức sau(Giao thức 3.1):

(1) A → B: ID_A || k_{UA} || N_1

(2) B → A: ID_B || k_{UB} || N_2 || $E(k_{UA}, f(N_1))$

(3) A kiểm tra $f(N_1)$

A → B: $E(k_{UB}, g(N_2))$

(4) B kiểm tra $g(N_2)$

(5) B → A: $E(k_{UA}, Data_A)$

(6) A → B: $E(k_{UB}, Data_B)$

- f(x) và g(x) là các hàm xác thực như MAC, HMAC

33

- Tấn công 1: Kẻ tấn công thay thế k_{UA} thành k'_{UA} trong (1)

(2) B → A: $E(k'_{UA}, f(N1))$

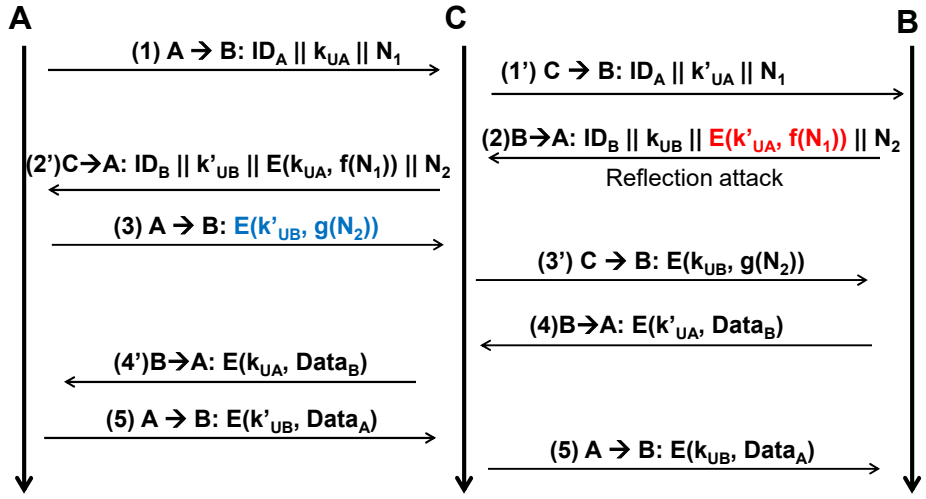
(3) A giải mã: $D(k_{RA}, (E(k'_{UA}, f(N1))) \neq f(N1)$ → A từ chối.

- Tấn công 2: Tấn công 1: Kẻ tấn công thay thế k_{UB} thành k'_{UB} trong (1)
  - Giải thích tương tự

34

Giao thức 3.1 – Tấn công man-in-the-middle

- C tự sinh cặp khóa (k'_{UA}, k'_{RA}) và (k'_{UB}, k'_{RB})



35

35

Giao thức 3.2

- Hãy xem xét giao thức sau(Giao thức 3.2):

(1) A → B: ID_A || k_{UA} || N_1

(2) B → A: ID_B || k_{UB} || N_2 || $E(k_{UA}, f(N_1))$ — B chỉ gửi một phần của mẫu tin này cho A

(3) A → B: $E(k_{UB}, g(N_2))$ — A chỉ gửi một phần mẫu tin này cho B

(4) B gửi phần còn lại bản tin $E(k_{UA}, f(N_1))$

(4') A giải mã với k_{RA} nhận được $f(N_1)$ và kiểm tra
A gửi phần còn lại của bản tin $E(k_{UB}, g(N_2))$ cho B

(4'') B giải mã với k_{RB} nhận được $g(N_2)$ và kiểm tra.

(5) B → A: $E(k_{UA}, Data_A)$

(6) A → B: $E(k_{UB}, Data_B)$

36

36

Giao thức phân phối khóa tập trung- Giao thức 4.1

- Sử dụng bên thứ 3 tin cậy – PKA (Public Key Authority)
  - Có cặp khóa (k_{UPKA}, k_{RPKA})
  - Nhận các khóa công khai k_{UA} của A và k_{UB} của B một cách an toàn. Làm thế nào vì đây chính là bài toán đang cần giải quyết ☺
- A và B đều có khóa công khai k_{UPKA} của PKA
- Giao thức 4.1

(1) A → PKA: $ID_A \| ID_B$
(2) PKA → A: $E(k_{RPKA}, ID_B \| k_{UB})$
(3) A → B: $E(k_{UB}, N_1)$
(4) B → PKA: $ID_B \| ID_A$
(5) PKA → B: $E(k_{RPKA}, ID_A \| k_{UA})$
(6) B → A: $E(k_{UA}, N_1)$

- Kiểm tra tính an toàn của giao thức này?
- Có thể tấn công vào giao thức này như thế nào?

37

37

Giao thức 4.1

38

38

Giao thức phân phối khóa tập trung- Giao thức 4.2

(1) A → PKA: $ID_A \,||\, ID_B \,||\, T_1$

(2) PKA → A: $E(k_{RPKA}, ID_B \,||\, k_{UB} \,||\, T_1)$

(3) A → B: $E(k_{UB}, N_1)$

(4) B → PKA: $ID_B \,||\, ID_A \,||\, T_2$

(5) PKA → B: $E(k_{RPKA}, ID_A \,||\, k_{UA} \,||\, T_2)$

(6) B → A: $E(k_{UA}, N_1)$

T_1, T_2: nhãn thời gian chống tấn công phát lại

- Giao thức này có hạn chế gì?

39

39

Giao thức 4.2

40

40

Giao thức phân phối khóa tập trung- Giao thức 4.3

- Bên thứ 3 được tin cậy – CA(Certificate Authority)
  - Có cặp khóa (k_{UCA}, k_{RCA})
  - Phát hành chứng thư số cho khóa công khai của các bên có dạng

  Cert = E(k_{RCA}, ID || k_U || Time)

  ID: định danh của thực thể

  k_U: khóa công khai của thực thể đã được đăng ký tại CA

  Time: Thời hạn sử dụng khóa công khai. Thông thường có thời điểm bắt đầu có hiệu lực và thời điểm hết hiệu lực.

41

41

Giao thức phân phối khóa tập trung- Giao thức 4.3 (tiếp)

(1) A → CA: ID_A || k_{UA} || $Time_A$

(2) CA → A: $Cert_A$= E(k_{RCA}, ID_A || k_{UA} || $Time_A$)

(3) B → CA: ID_B || k_{UB} || $Time_B$

(4) CA → B: $Cert_B$= E(k_{RCA}, ID_B || k_{UB} || $Time_B$)

(5) A → B: $Cert_A$

(6) B → A: $Cert_B$

- Làm thế nào để A và B có thể yên tâm sử dụng khóa công khai của nhau?
- Hãy cải tiến lại các giao thức trong các khâu cần đến xác thực thông điệp (sử dụng MAC hoặc hàm băm)
- Đọc thêm về PKI và chứng thư số theo chuẩn X.509

42

42

Giao thức 4.3 (tiếp)

43

43

Phân phối khóa bí mật của hệ mật mã khóa đối xứng

- Hạn chế chung của các giao thức phân phối khóa bí mật trong hệ mật mã khóa đối xứng
  - Giao thức không tập trung: Số lượng khóa sử dụng lớn
  - Giao thức tập trung: PKA phải đáp ứng yêu cầu với tần suất rất lớn
  - Không có cơ chế xác thực rõ ràng

  → Sử dụng mật mã khóa công khai trong các giao thức phân phối khóa bí mật

  (1) A → B: $E(k_{UB}, E(k_{RA}, k_S))$

  (2) B giải mã với k_{RB}, sau đó kiểm tra để chắc chắn thông điệp xuất phát từ A. Khóa k_S thu được là khóa phiên.

  (3) A ↔ B: $E(k_S, Data)$
- Tất nhiên giao thức trên không chống được tấn công phát lại. Việc cải tiến giao thức trên như là một bài tập.

44

44

Kết luận

- Hệ thống có nguy cơ mất an toàn ngay cả khi chúng ta sử dụng hệ mật mã tốt nếu không có một giao thức quản lý và phân phối khóa an toàn
- Hãy sử dụng các giao thức tiêu chuẩn: IPSec, TLS, IEEE802.11x, Keberos,…
- Mật mã phải gắn liền với xác thực
- Thực tế các giao thức phân phối khóa đã trình bày đều xác thực dựa trên các sơ đồ mã hóa của hệ mật mã. Chúng ta biết rằng, giải pháp này chưa thực sự an toàn (hãy xem lại những phân tích trong bài §3. Xác thực thông điệp).
  - Bài tập: Hãy sử dụng MAC, hàm băm, chữ ký điện tử để tăng cường an toàn cho các sơ đồ trên.

45

45

Một số lưu ý khác

- Đảm bảo tính bí mật:
  - Khóa bí mật
  - Khóa cá nhân
  - Các giá trị chia sẻ bí mật khác
- Đảm bảo tính toàn vẹn, xác thực:
  - Khóa bí mật
  - Khóa công khai
  - Thông tin sinh khóa
- Kiểm tra tính hợp lệ của các tham số nhóm
- Kiểm tra tính hợp lệ của khóa công khai
- Kiểm tra quyền sở hữu khóa cá nhân

46

46

Một số lưu ý khác

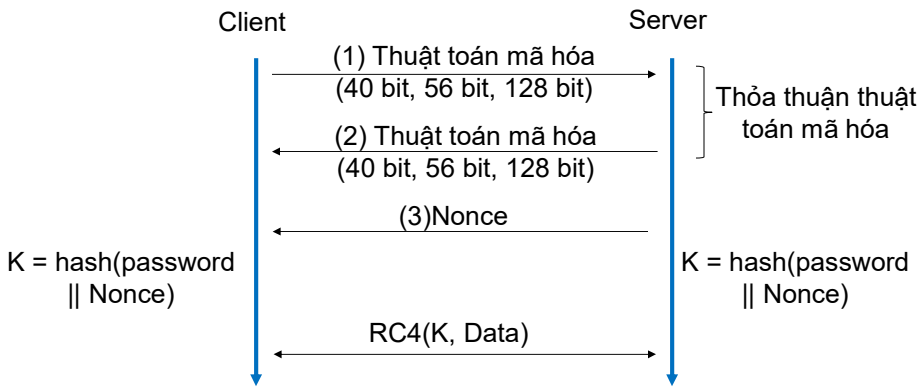
- Không kết thúc ngay giao thức khi có 1 lỗi xảy ra
  - Làm chậm thông báo lỗi
- Chỉ sử dụng các giao thức tiêu chuẩn
- Thông báo lỗi không nêu cụ thể nguyên nhân lỗi
- Không sử dụng khóa giống nhau cho cả 2 chiều truyền tin
- Không sử dụng khóa giống nhau cho 2 mục đích mã mật và xác thực
- Tấn công vào quá trình thỏa thuận của giao thức

47

47

MS Point-to-Point Encryption

- Sử dụng mật mã RC4
- Hoạt động của giao thức



48

48