Bài 7: Một số ứng dụng bảo mật trên mạng

Thời lượng: 3 tiết

Lương Thái Lê

Nội dung

1. Trao đổi khóa
2. Xác thực người dùng - Kerberos
3. Một số giao thức an ninh
4. An toàn thư điện tử
5. Thanh toán điện tử an toàn

Một số loại khoá

- Khóa mật (secret key): chỉ 2 bên biết
- Khóa công khai (public key): mọi người có thể biết
- Khóa riêng (private key): chỉ người tạo ra biết
- Khoá phiên (section key):
  - Khoá tạm thời
  - Dùng để mã hoá dữ liệu giữa nhóm người sử dụng
  - Cho một phiên logic và sau đó bỏ đi (chống trì hoãn)
- Khoá chính (master key):
  - Dùng để mã các khoá phiên
  - Chia sẻ giữa người sử dụng và trung tâm phân phối khoá (dùng càng ít càng tốt)

Các phương án trao đổi khóa

1. A có thể chọn khóa và giao trực tiếp cho B
2. Bên thứ ba có thể lựa chọn khóa và giao khóa cho A & B
3. Nếu A & B đã từng liên lạc trước đó thì có thể sử dụng khoá cũ để mã hóa một khóa mới để gửi khóa cho nhau
4. Nếu A & B có thể liên lạc an toàn với một bên thứ ba C, C có thể chuyển tiếp khóa giữa A & B

Mô hình phân phối khóa qua KDC (Key distribution center)

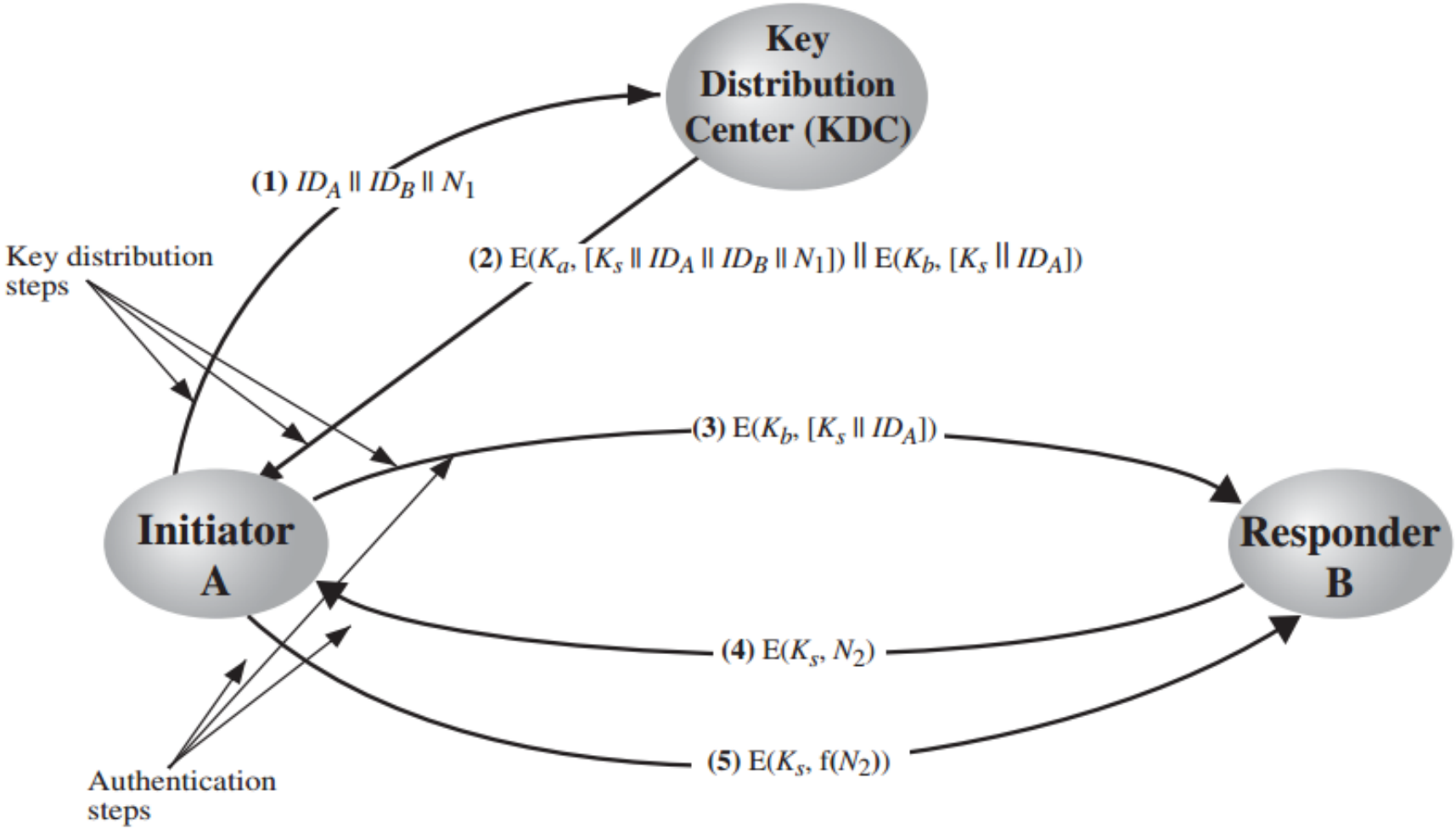


Figure 14.3 Key Distribution Scenario

Phân tích mô hình KDC

1. A yêu cầu từ KDC một khóa phiên (Section key) để bảo vệ một kết nối tới B.

   N_1 : thời gian, số đếm hoặc 1 số ngẫu nhiêu
2. KDC trả lại A một tin nhắn được mã hóa sử dụng K_a nó gồm:
   - khóa phiên (session key) sử dụng một lần K_s được sử dụng cho phiên giao dịch,
   - tin nhắn do A gửi đến KDC: $(ID_A \| ID_B \| N_1)$
   - thông tin gửi cho B: $E(K_b, [K_s \| ID_A])$ => xác thực A
3. A lưu K_s để giao dịch với B và forward cho B thông tin. Tại thời điểm này, một khóa phiên đã được chuyển an toàn tới A và B, và họ có thể bắt đầu các trao đổi được bảo vệ.

Phân tích mô hình KDC (tiếp)

4. B sử dụng khóa phiên K_s mới nhận được để mã hóa giá trị N_2 rồi gửi cho A
5. A sử dụng K_s mã hóa $f(N_2)$ gửi lại cho B
   - trong đó f là một hàm thực hiện một số biến đổi trên N_2.

   $\Rightarrow$ 2 bước này đảm bảo với B rằng tin nhắn B nhận được ở bước 3 là đúng

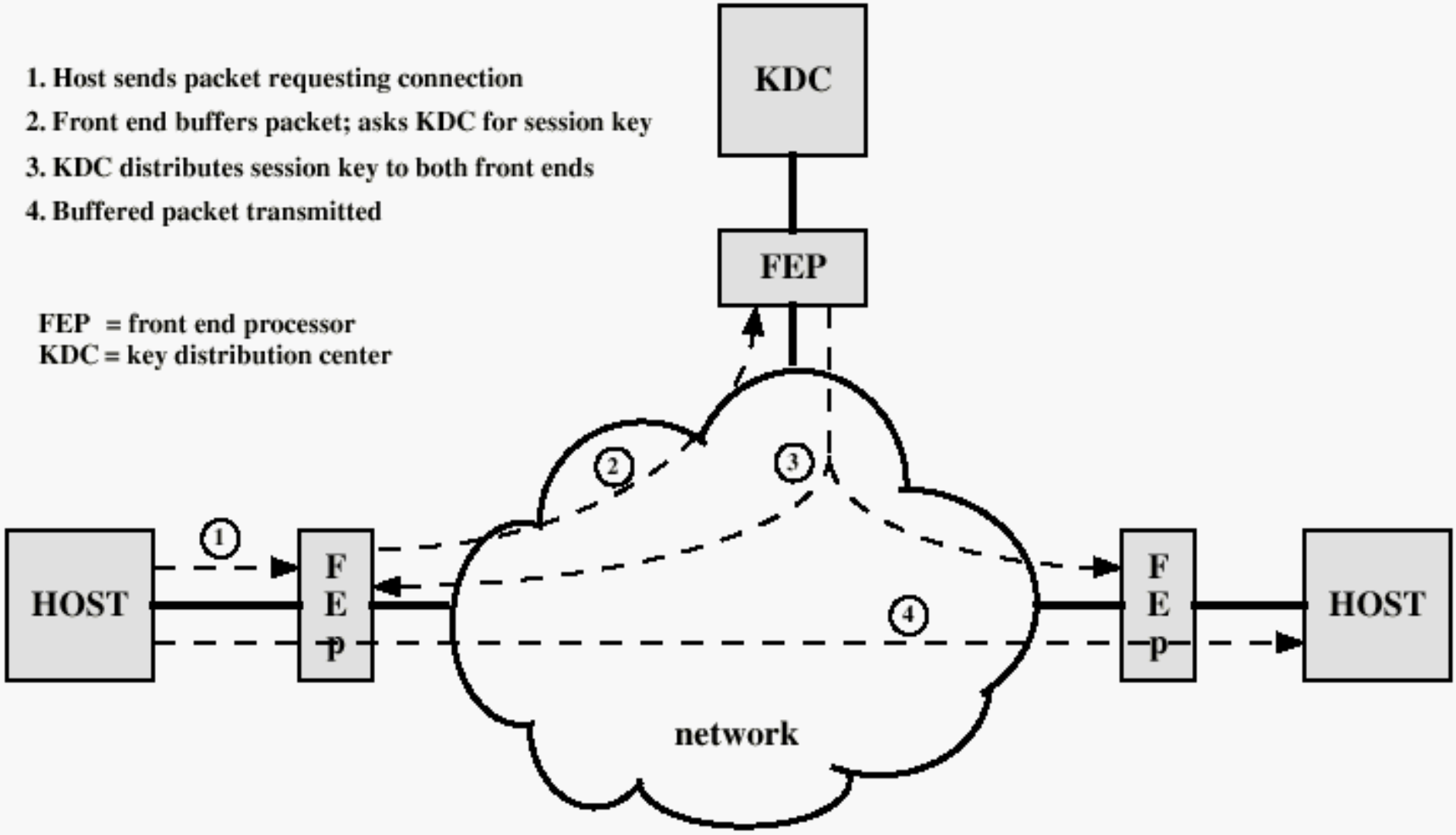
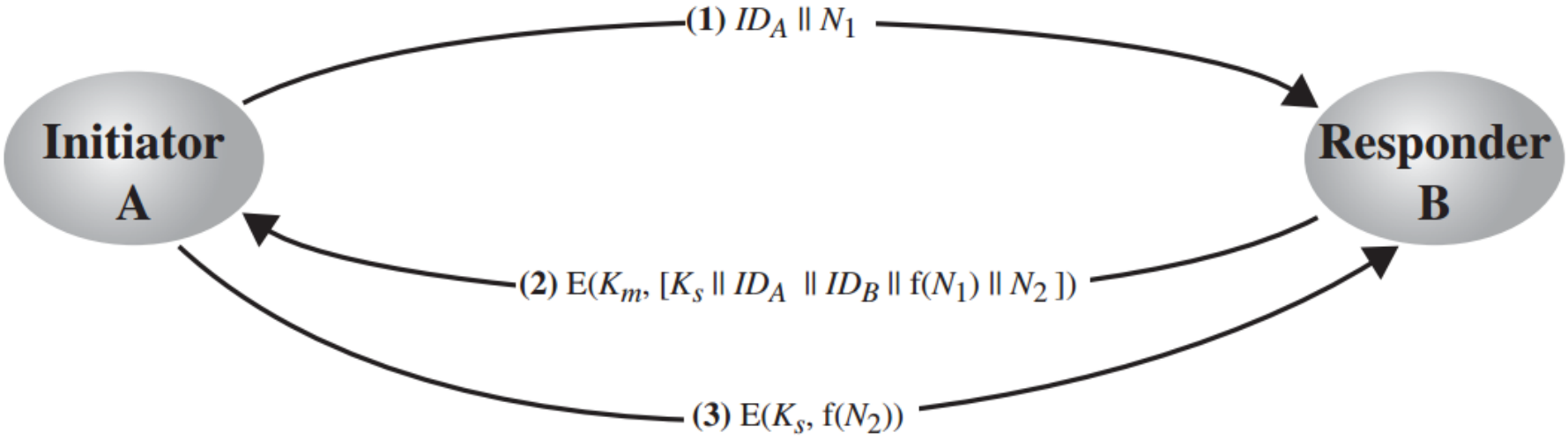


Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol

Mô hình phân phối khóa phân tán



Dùng cho mạng local

Mô hình phân phối khóa mật đơn giản (Merkel)

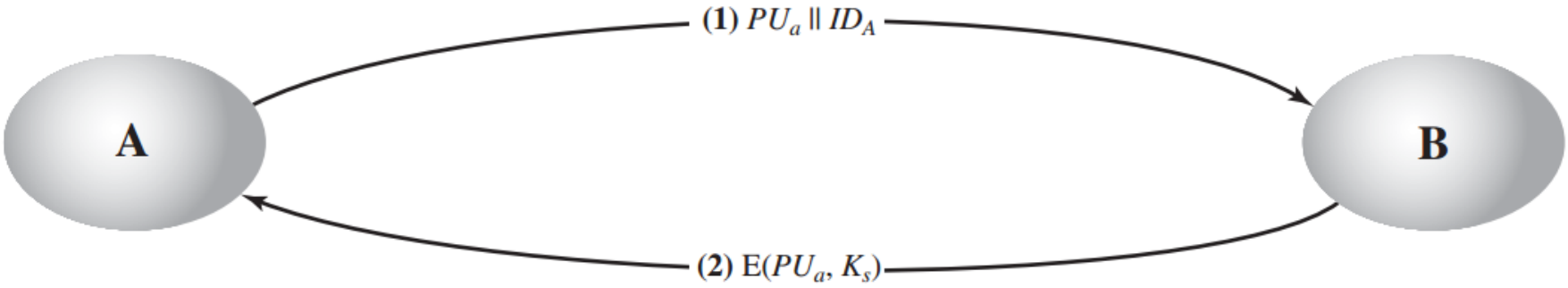


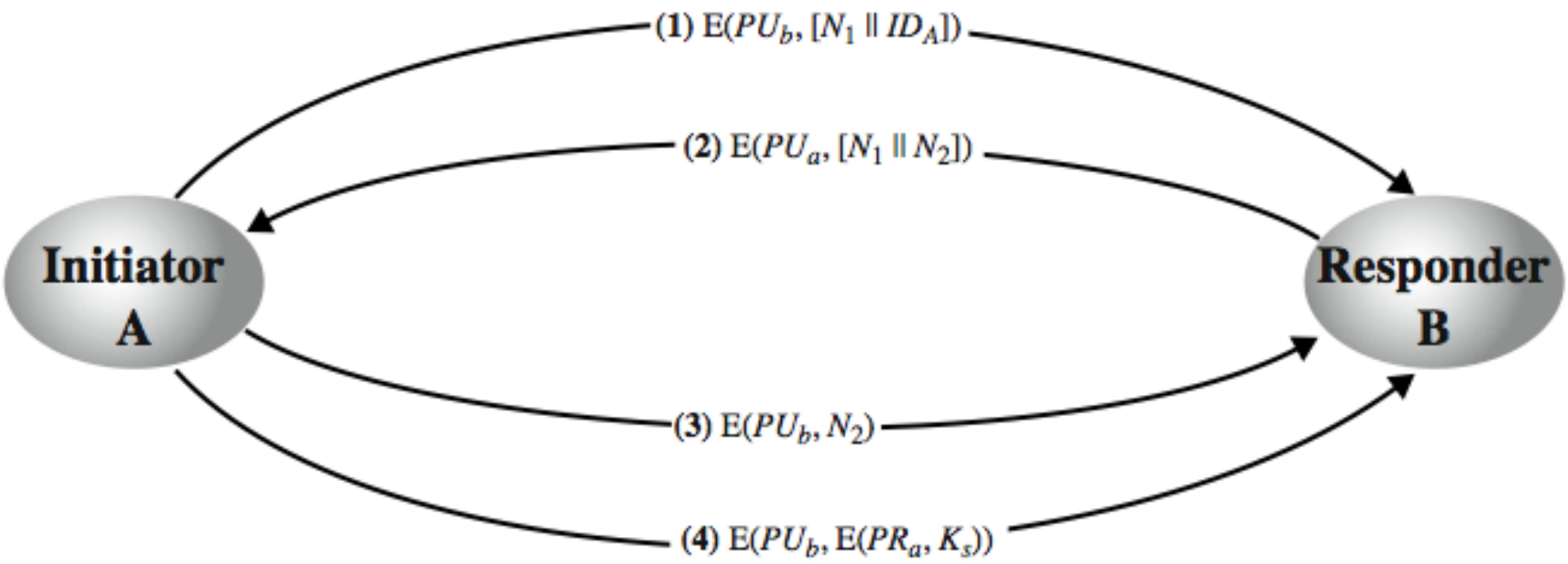
Figure 14.7 Simple Use of Public-Key Encryption to Establish a Session Key

- Merkel đề xuất (1979)
- Merkle đề xuất lược đồ rất đơn giản này
  - cho phép liên lạc an toàn
  - không có khóa trước/sau khi tồn tại
  - lược đồ này là dễ bị tổn thương bởi kiểu tấn công chủ động man-in-the-middle-attack

Mô hình Merkel (tiếp)

1. A tạo cặp khóa {PUa, PRa} và gửi một tin nhắn cho B gồm PUa và một mã định danh của A, IDA.
2. B tạo một khóa bí mật, Ks, và gửi nó cho A, được mã hóa bằng khóa PUa.
3. A tính D(PRa, E(PUa, Ks)) khôi phục được khóa bí mật. Bởi chỉ có A mới có thể giải mã tin nhắn của B, do đó chỉ có A và B biết khóa bí mật Ks.

Mô hình phân phối khóa mật có bảo mật & xác thực



Mô hình phân phối khóa mật có bảo mật & xác thực (tiếp)

1. A dùng khóa PUb của B để mã hóa một tin nhắn tới B chứa một định danh của A (ID_A) và một giá trị N_1 để xác định duy nhất giao dịch này.
2. B gửi một tin nhắn tới A được mã hóa bằng PUa và chứa giá trị N_1 của A cùng với một giá trị mới N_2 của B. Bởi chỉ B mới có thể giải mã tin nhắn (1), sự có mặt của N_1 trong tin nhắn (2) khẳng định với A rằng người gửi là B.
3. A trả lại N_2, được mã hóa bằng PUb, để khẳng định với B rằng người gửi là A.
4. A chọn một khóa bí mật Ks và gửi M = E(PUb, E(PRa, Ks)) cho B. Việc mã hóa bằng khóa công khai của B khẳng định rằng chỉ có B có thể đọc được nó, việc mã hóa bằng khóa riêng của A để khẳng định rằng chỉ A mới có thể gửi nó.
5. B tính D(PUa, D(PRb, M)) để khôi phục khóa bí mật.

Phân phối khóa công khai

- Có thể dùng 1 trong các cách:
  1. Thông báo công khai (public announcement)
  2. Thư mục công bố công khai (public available directory)
  3. Chủ quyền khóa công khai (public-key authority)
  4. Giấy chứng nhận khóa công khai (public-key certificates)

Thông báo công khai
Public Announcement

- Người dùng phân phối khoá công khai cho người nhận hoặc thông báo rộng rãi cho cộng đồng.
  - Bổ sung khoá công khai vào thư điện tử hoặc gửi cho nhóm diễn đàn hoặc danh sách email
- Điểm yếu chính là mạo danh
  - Một người nào đó có thể tạo khoá và tuyên bố mình là một người khác và gửi thông báo
  - Cho đến khi giả mạo bị phát hiện nó có thể lừa trong vai trò người khác

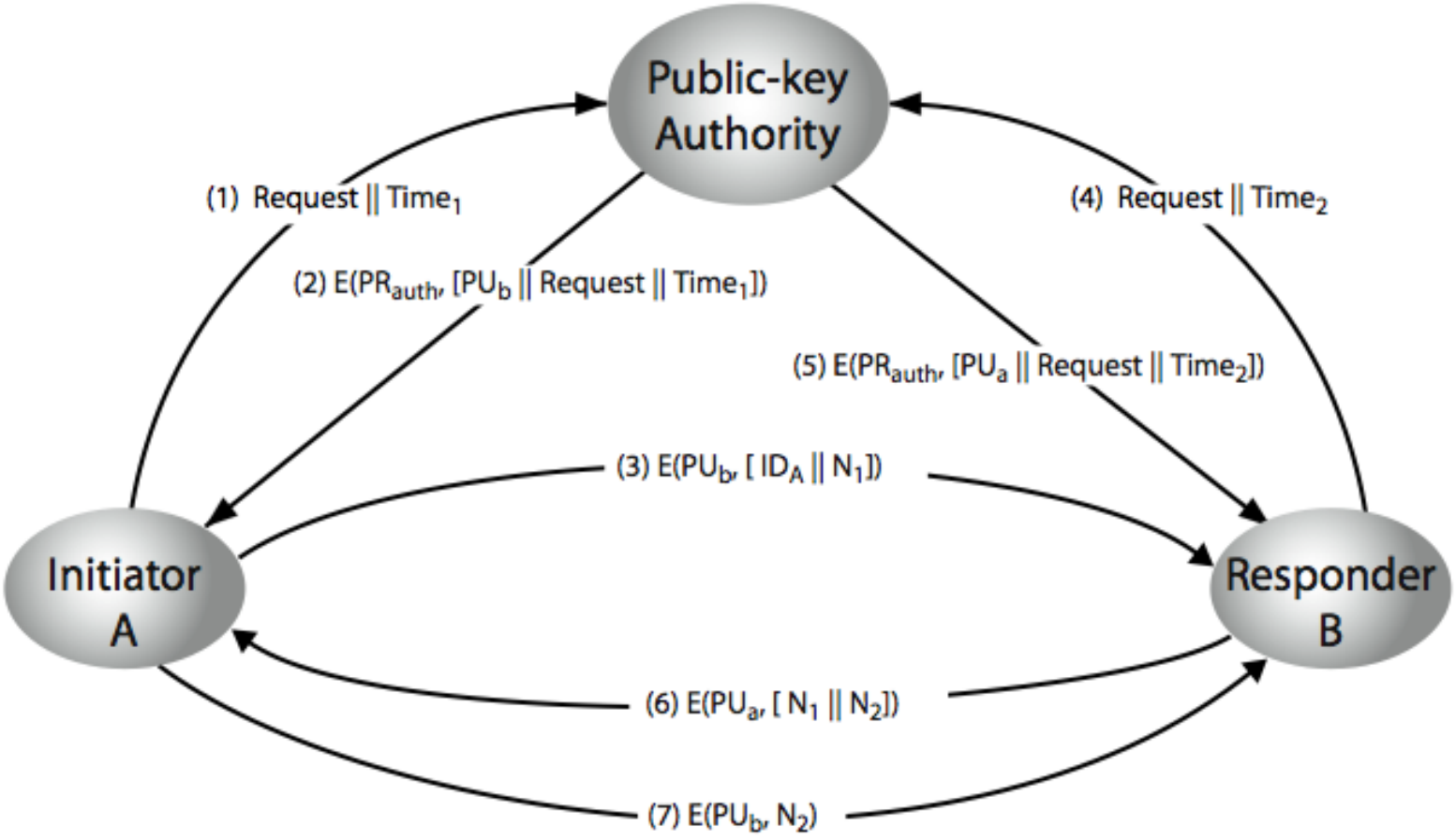
Thư mục truy cập công cộng

- Có thể đạt được tính an toàn cao hơn bằng cách đăng ký khoá với thư mục công cộng
- Thư mục cần được đảm bảo tin cậy với các tính chất sau:
  - Duy trì việc nhập tên và khoá công khai của người dùng
  - Người dùng đăng ký mật (có xác thực) với Thư mục
  - Người dùng có thể thay khoá bất cứ lúc nào
  - Thư mục được in định kỳ
  - Thư mục có thể truy cập qua mạng
- Vẫn còn lỗ hổng để sửa hoặc giả mạo

Chủ quyền khoá công khai

- Cải thiện tính an toàn bằng việc kiểm soát chặt chẽ việc phân phối khoá từ quản trị Thư mục
- Có các tính chất của một Thư mục như đã nêu trên
- Đòi hỏi người dùng biết khoá công khai của quản trị Thư mục đó
- Sau đó người dùng nhận được bất kỳ khoá công khai mong muốn nào một cách an toàn
  - Đòi hỏi truy cập thời gian thực đến Thư mục khi cần đến khoá

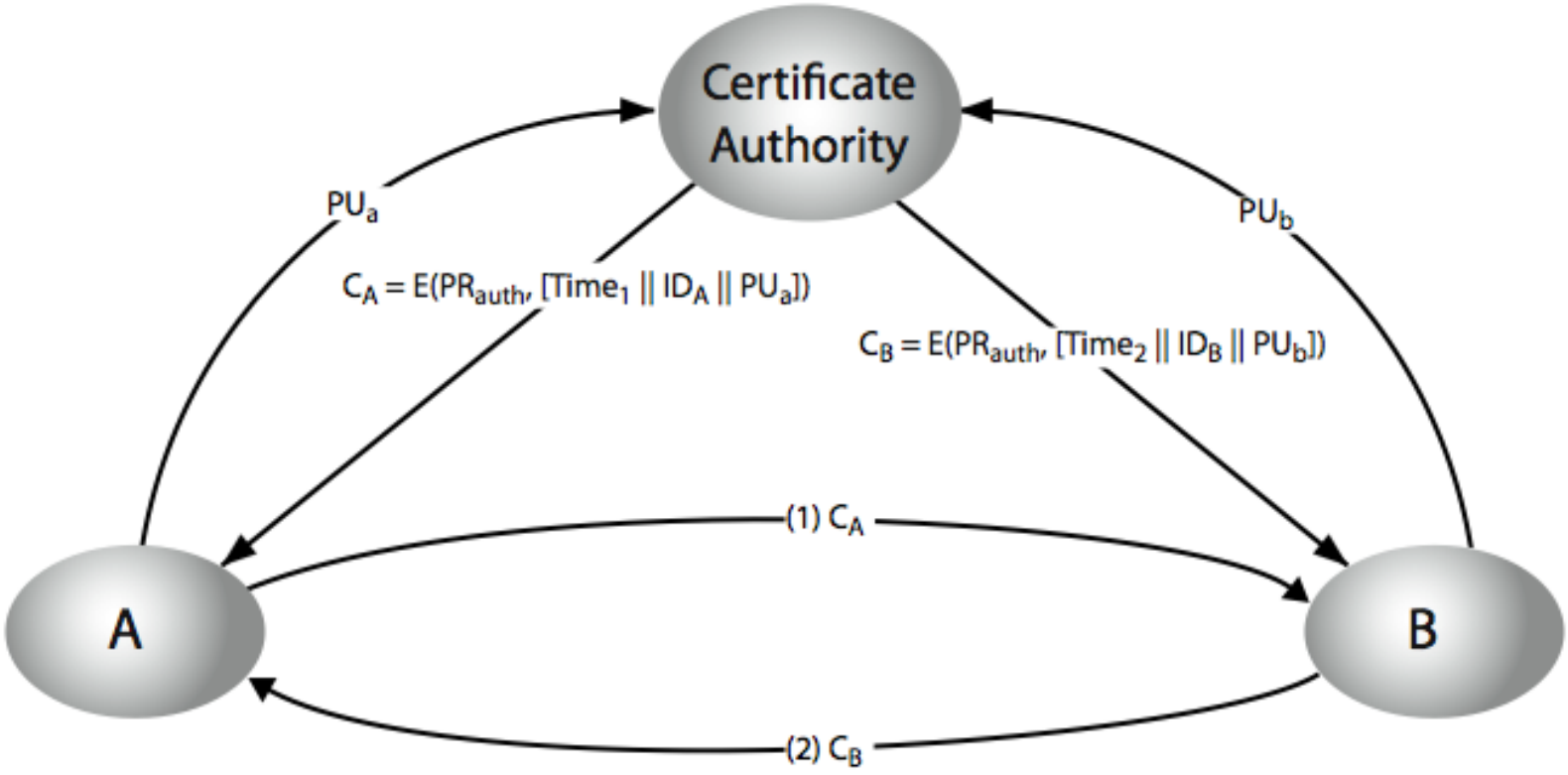
Chủ quyền khoá công khai



Giấy chứng nhận khoá công khai

- Giấy chứng nhận cho phép trao đổi khoá không cần truy cập thời gian thực đến chủ quyền thư mục khoá công khai
- Giấy chứng nhận trói danh tính với khoá công khai
  - thường với các thông tin khác như chu kỳ kiểm định, quyền sử dụng, …
- Với mọi nội dung được ký bởi khoá công khai tin cậy hoặc Bản quyền chứng nhận (**CA**, Certificate Authority)
- Có thể được kiểm chứng bởi một người nào đó biết khoá công khai của Chủ quyền khoá công khai

Trao đổi Giấy chứng nhận Khóa công khai



Các vấn đề liên quan đến phân phối khoá

- Đối với mạng lớn đòi hỏi phân cấp Trung tâm phân phối khoá KDC, nhưng cần phải tạo tin cậy cho nhau
- Thời gian sống của khoá bộ phận cần được hạn chế để cho an toàn hơn
- Sử dụng phân phối khoá tự động thay mặt người dùng, nhưng phải có hệ thống tin cậy
- Sử dụng phân phối khoá phân tán

Xác thực người dùng – Kerberos

- Keberos là dịch vụ xác thực dùng trong môi trường phân tán
- Keberos cung cấp bên thứ 3 đảm bảo xác thực cho mọi kết nối giữa clients và severs
- Vấn đề mà Kerberos đưa ra là:
  - môi trường phân tán mở trong đó người dùng tại các máy trạm muốn truy cập các dịch vụ trên các máy chủ được phân phối trên toàn mạng.
  - các máy chủ có thể giới hạn quyền truy cập với người dùng (đã được xác thực) và có thể xác thực yêu cầu dịch vụ.
  - máy trạm không đủ tin cậy để xác định người dùng của nó một cách chính xác với các dịch vụ mạng.
- Kerberos dựa hoàn toàn vào mã hóa đối xứng, không sử dụng khóa công khai.
- Có hai phiên bản đang sử dụng: 4 và 5

Tổng quan Kerberos 4

- Cung cấp dịch vụ xác thực dùng DES
- Dùng 1 máy chủ xác thực (AS-authentication service)
  - Người dùng thỏa thuận với AS về danh tính của mình
  - AS cung cấp sự tin cậy xác thực (thẻ cấp thẻ TGT – Ticket Granting Ticket)
- Dùng 1 máy chủ cấp thẻ (TGS – Ticket Granting Server)
  - Người sử dụng thường xuyên yêu cầu TGS cho truy cập đến các dịch vụ khác dựa trên thẻ cấp thẻ TGT của người sử dụng

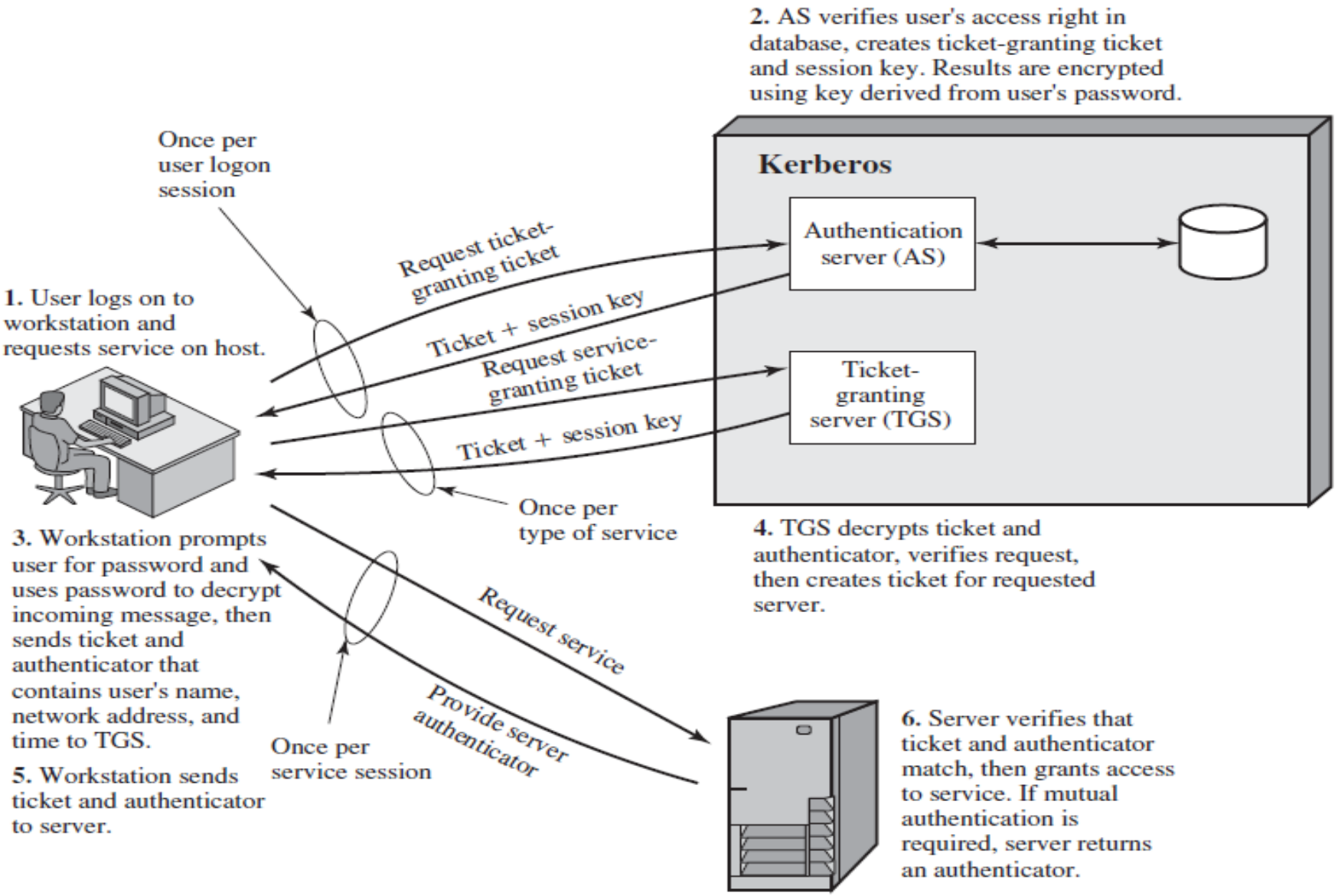


Figure 15.1 Overview of Kerberos

Kerberos 4

(1) $\mathbf{C \rightarrow AS}$ $ID_c \| ID_{tgs} \| TS_1$

(2) $\mathbf{AS \rightarrow C}$ $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) $\mathbf{C \rightarrow TGS}$ $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) $\mathbf{TGS \rightarrow C}$ $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$$

$$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$$

$$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) $\mathbf{C \rightarrow V}$ $Ticket_v \| Authenticator_c$

(6) $\mathbf{V \rightarrow C}$ $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$$

$$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$$

(c) Client/Server Authentication Exchange to obtain service

Yêu cầu dịch vụ ở lãnh địa khác

Figure 15.2 Request for Service in Another Realm

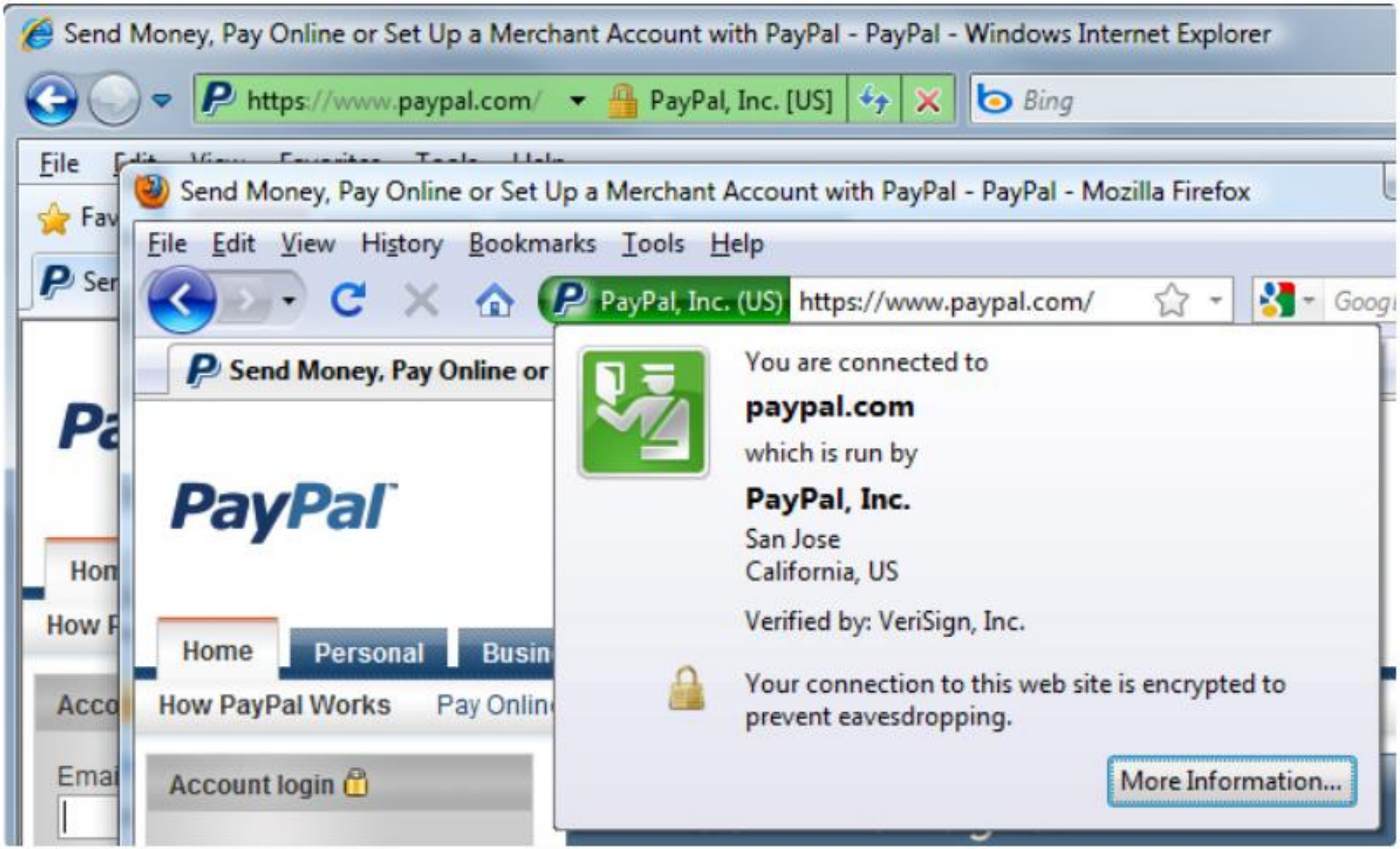
Kerberos phiên bản 5

- Phát triển vào giữa những năm 1990
- Được thiết kế theo chuẩn RFC 1510
- Cung cấp những cải tiến so với phiên bản 4
  - Hướng tới các thiếu xót về môi trường
    - Thuật toán mã, thủ tục mạng thứ tự byte, thời gian sử dụng thẻ, truyền tiếp xác thực, xác thực lãnh địa con
  - Và các sự khác biệt về kỹ thuật
    - Mã kép, các dạng sử dụng không chuẩn, khoá kỳ, chống tấn công mật khẩu
  - Đặc biệt có thuật toán sinh khóa mật từ mật khẩu

Ứng dụng mã hóa trong một số giao thức an ninh

1. Secure socket layer (SSL)
2. Transport layer security (TLS)
3. HyperText transfer protocol secure (HTTPS)
4. Secure shell (SSH)

Ví dụ trang web có dùng SSL



An toàn thư điện tử

- An toàn thư điện tử nói đến một tập các biện pháp được sử dụng để bảo mật truy cập và nội dung của một tài khoản hoặc dịch vụ email.
- Một nhà cung cấp dịch vụ đảm bảo an toàn email bằng việc sử dụng strong password và cơ chế kiểm soát truy cập vào email server; mã hóa và chữ ký số cho email khi ở trong inbox hoặc trên đường truyền hoặc đăng ký địa chỉ email. Đồng thời triển khai firewall và bộ lọc spam.
- Có 2 cách tiếp cận chính:
  - Pretty good privacy (PGP)
  - Secure/Multipurpose Internet Mail Extension (S/MIME)

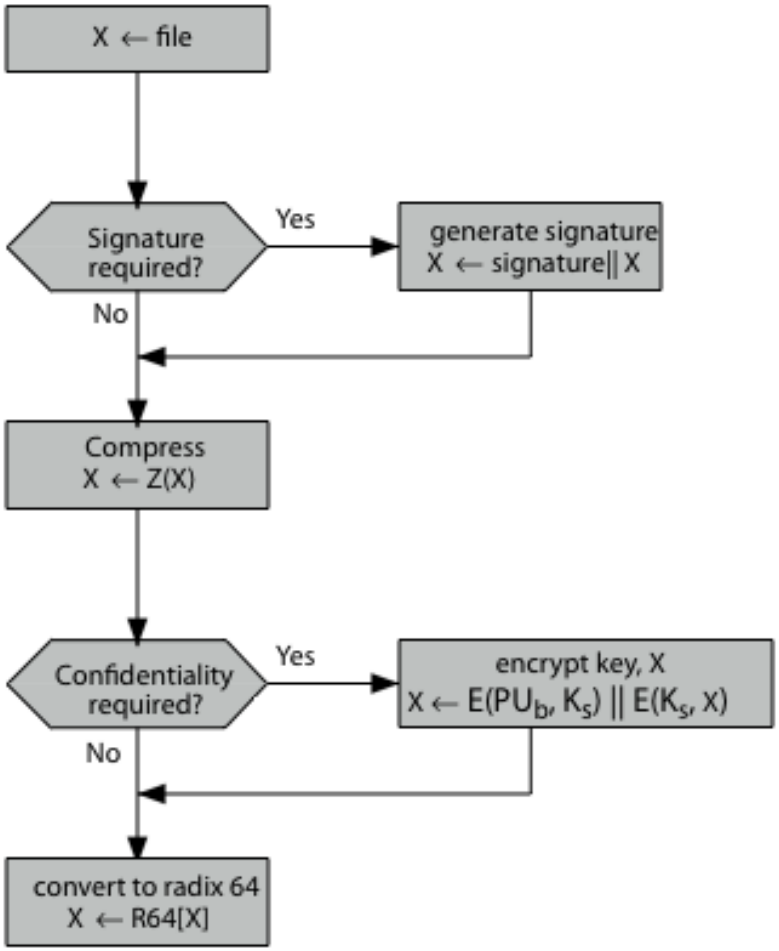
Pretty Good Privacy (PGP)

- Được sử dụng rộng rãi cho chuẩn an toàn thư điện tử
- Được phát triển bởi Phil Zimmermann
- Lựa chọn các thuật toán mã hoá tốt nhất để dùng
- Tích hợp thành một chương trình thống nhất
- Chạy trên Unix, PC, Macintosh và các hệ thống khác
- Ban đầu là mã nguồn mở, bây giờ có các phiên bản thương mại

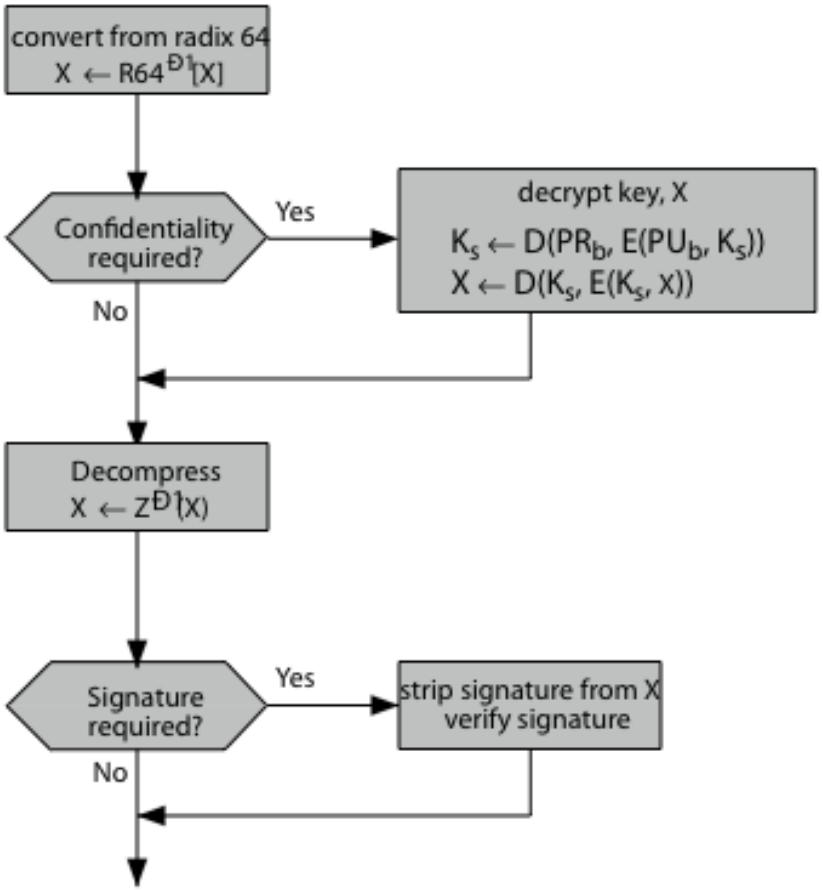
Các chức năng chính của PGP

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Tổng hợp Thao tác PGP



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

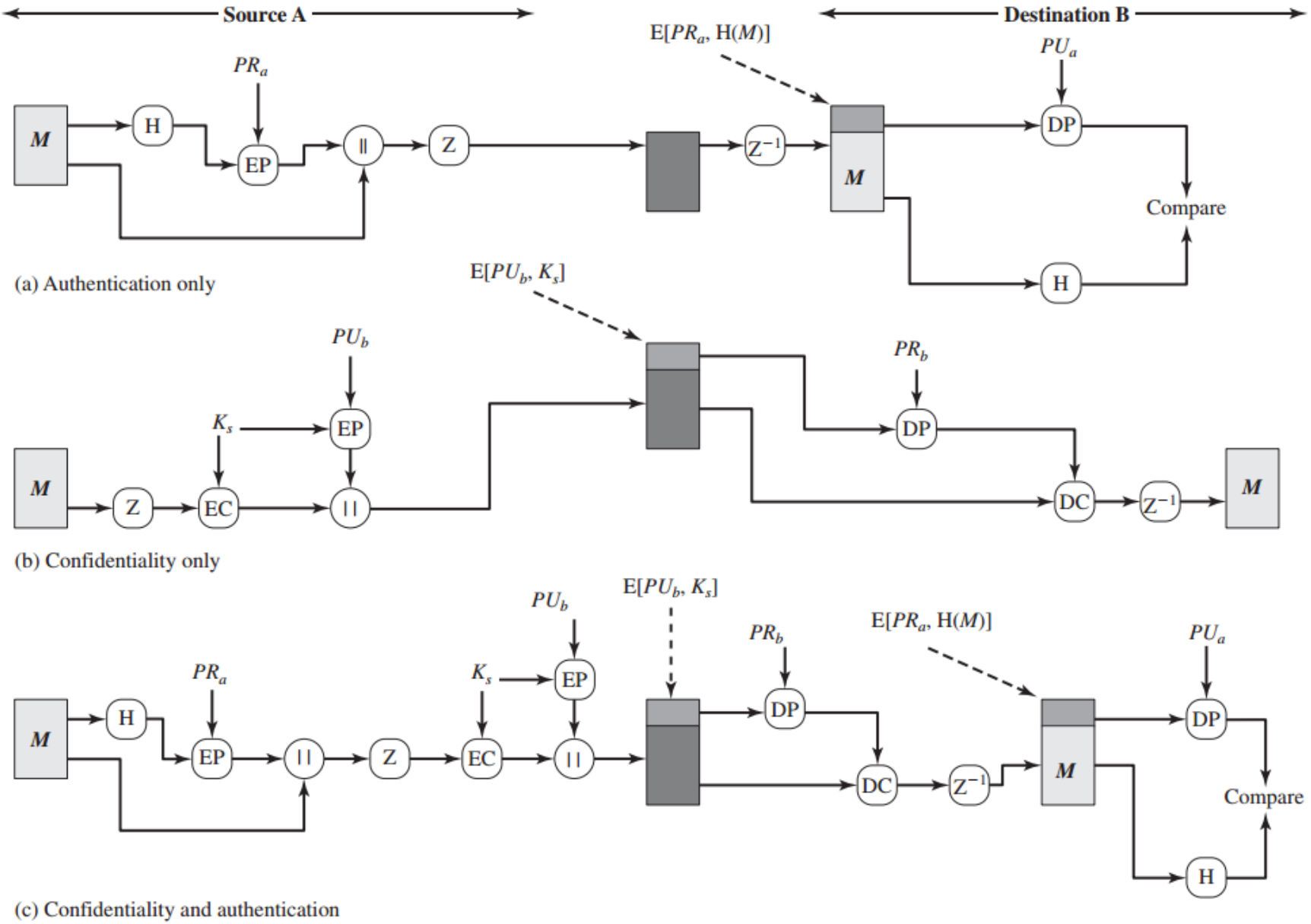
Ví dụ về chuyển đổi R64

M								a								n							
77 (0x4d)								97 (0x61)								110 (0x6e)							
0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
19								22								5							
T								W								F							
u																							

Thanh toán điện tử an toàn

Secure Electronic Transactions (SET)

- Là dịch vụ an ninh hướng ứng dụng được nhúng trong ứng dụng cụ thể
- Mã mở và đặc tả an toàn
- Bảo vệ thanh toán thẻ tín dụng trên Internet
- Phát triển năm 1996 bởi Master, Visa Card
- Không phải hệ thống trả tiền
- Là tập các giao thức và định dạng an toàn
  - Trao đổi an toàn giữa các đối tác
  - Tin tưởng vì sử dụng X509v3
  - Riêng biệt vì hạn chế thông tin cho người cần khi trao đổi thông tin


Source A
Destination B
M
H
EP
||
Z
PR_a
$E[PR_a, H(M)]$
Z^{-1}
DP
PU_a
Compare
(a) Authentication only
$E[PU_b, K_s]$
PU_b
K_s
EC
PR_b
DC
(b) Confidentiality only
(c) Confidentiality and authentication

Thao tác PGP – xác thực

1. Người gửi tạo mẩu tin
2. Sử dụng tạo bản băm của mẩu tin
3. Ký Hash với RSA sử dụng khoá riêng của người gửi và đính kèm vào mẩu tin
4. Người nhận sử dụng RSA với khoá công khai của người gửi để giải mã và khôi phục bản hash
5. Người nhận kiểm tra mẩu tin nhận sử dụng bản hash của nó và so sánh với bản hash đã được giải mã

Thao tác PGP – bảo mật

1. Người gửi tạo mẩu tin và sing số ngẫu nhiên làm khoá phiên cho nó
2. Mã hoá mẩu tin sử dụng khóa phiên
3. Khoá kỳ được mã sử dụng RSA với khoá công khai người nhận và đính kèm với mẩu tin
4. Người nhận sử dụng RSA với khoá riêng để giải mã và khôi phục khoá kỳ
5. Khoá kỳ được sử dụng để giải mã mẩu tin

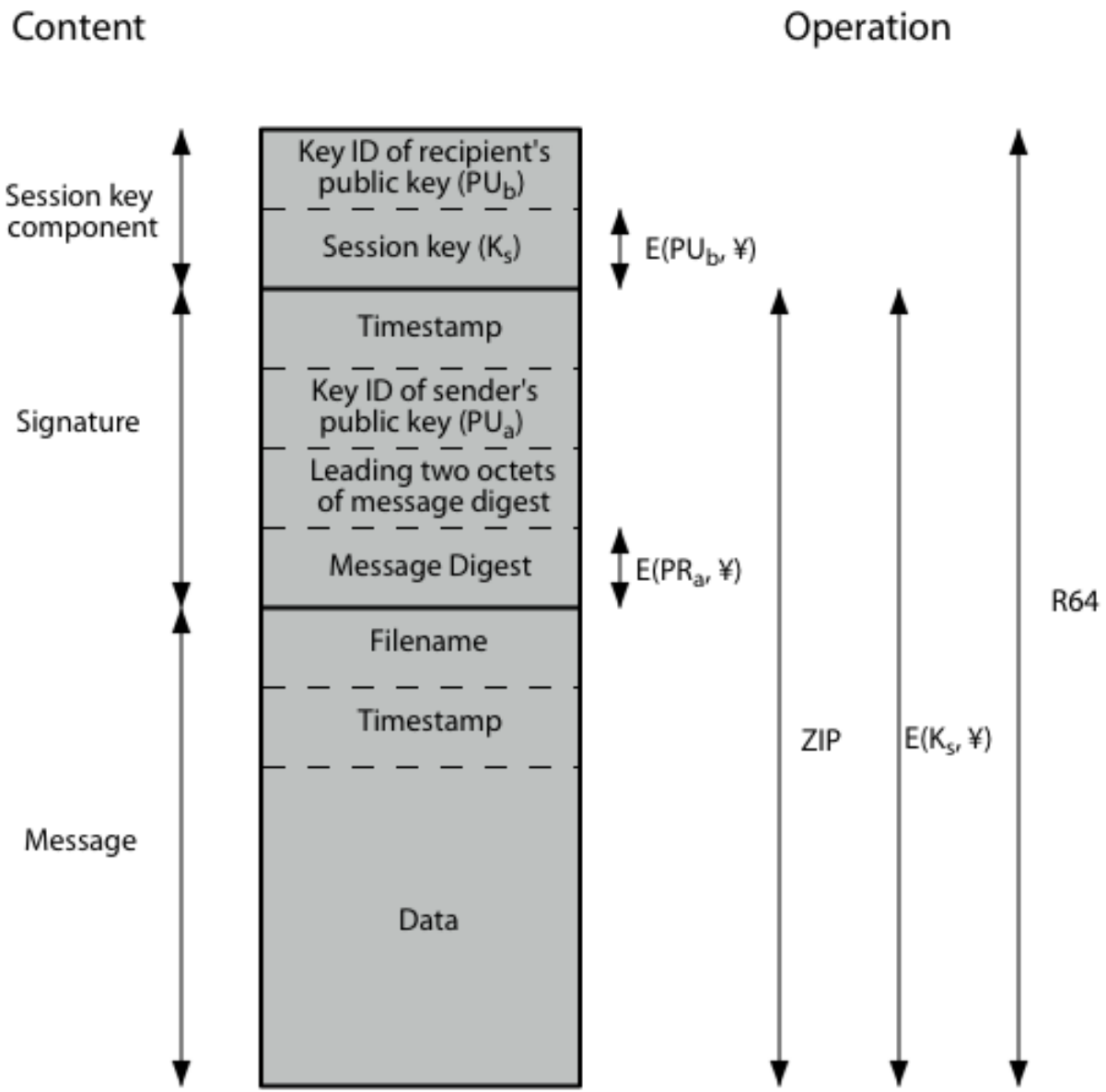
Thao tác PGP – Nén và tương thích thư điện tử

- Theo mặc định PGP nén mẩu tin sau khi ký nhưng trước khi mã
  - Như vậy cần lưu mẩu tin chưa nén và chữ ký để kiểm chứng về sau
  - Vì rằng nén là không duy nhất
- Sử dụng thuật toán nén ZIP
- Khi sử dụng PGP sẽ có dữ liệu nhị phân để gửi (mẩu tin được mã)
- Tuy nhiên thư điện tử có thể thiết kế chỉ cho văn bản
- Suy ra PGP cần mã dữ liệu nhị phân thô vào các ký tự ASCII in được (A->Z, a->z, +,/)
- Sử dụng thuật toán Radix 64 – R64
  - Ánh xạ 3 byte vào 4 ký tự in được
- PGP sẽ chia đoạn mẩu tin nếu nó quá lớn

Khoá kỳ PGP

- Cần có khoá kỳ cho mỗi mẩu tin
  - Có kích thước khác nhau: 56 bit – DES, 128 bit CAST hoặc IDEA, 168 bit Triple - DES
- Được sinh ra sử dụng chế độ ANSI X12.17
  - Sử dụng dữ liệu đầu vào ngẫu nhiên lấy từ sử dụng trước và thời gian gõ bàn phím của người sử dụng

Định dạng mẩu tin PGP



Các chùm khoá PGP

- Mỗi người sử dụng PGP có một cặp chum khoá:
  - Chùm khoá công khai chứa mọi khoá công khai của các người sử dụng PGP khác được người đó biết và được đánh số bằng định danh khoá (ID key)
  - Chùm khoá riêng chứa các cặp khoá công khai/riêng của người đó được đánh số bởi định danh khoá và mã của khoá lấy từ giai đoạn duyệt được hash
- An toàn của khoá công khai như vậy phụ thuộc vào độ an toàn của giai đoạn duyệt

Câu hỏi

- Câu hỏi: Bạn giải thích quá trình nhận thư điện tử PGP?
- Trả lời: Người nhận tiến hành các bước sau:
  - Nhập mật khẩu tạo khóa giải mã khóa riêng trong chùm khóa riêng
  - Dùng khóa riêng giải mã khóa phiên trong thư
  - Dùng khóa phiên giải mã thư
  - Dùng khóa công khai người gửi trong chùm khóa công khai giải mã bản băm đính kèm so sánh với bản băm thư để xác thực gốc.

Tóm tắt

- Đã xem xét:
  - Phân phối và quản lý khóa công khai, khóa chính, khóa phiên
  - Hệ thống xác thực tin cậy Kerberos
  - Hạ tầng khóa công khai PKI
  - Hệ thống thư điện tử PGP

Câu hỏi trắc nghiệm

1. Giải pháp nào là kém an toàn nhất để phân phối khóa công khai:

A. @Thông báo công khai

B. Thư mục công cộng

C. Chủ quyền khóa công khai

D. Chủ quyền cấp giấy chứng nhận

2. Đâu là ưu điểm chính của Chủ quyền cấp giấy chứng nhận so với chủ quyền khóa công khai

A. Chủ quyền khóa công khai cung cấp trực tuyến khóa công khai

B. Chủ quyền chứng nhận cấp các giấy chứng nhận về khóa công khai

C. Cả hai đều cho phép người sử dụng dễ dàng thay đổi khóa công khai của mình

D. @Chủ quyền khóa công khai dùng online, chủ quyền chứng nhận có thể offline

3. Giải pháp nào không dùng để phân phối công khai khóa mật giữa hai người sử dụng

A. Dùng Trung tâm phân phối khóa KDC hỗ trợ phân phối khóa

B. Trao đổi trực tiếp khóa mật dùng thủ tục trao đổi khóa Diffie-Helman

C. @Trao đổi khoá mật mới bằng khoá mật cũ

D. Trao đổi trực tiếp khóa mật dùng khóa công khai

Câu hỏi trắc nghiệm 2

4. Trong phương pháp kết hợp phân phối khóa, điều nào không đúng

A. Mỗi người sử dụng và Trung tâm phân phối khóa KDC có cặp khóa riêng và khóa công khai

B. Trung tâm dùng khóa công khai để tạo khóa chính giữa KDC và mỗi NSD

C. @NSD dùng khóa công khai để trao đổi khóa phiên với NSD khác

D. NSD dùng khóa chính để xin KDC tạo khóa phiên với NSD khác

5. Tự động phân phối khóa cho giao thức hướng đối tượng không sử dụng

A. Máy chủ gửi gói tin kèm với yêu cầu kết nối với máy chủ khác

B. @Cả bên nhận và bên gửi cần thỏa thuận trước khoá phiên trước khi gửi gói tin

C. Bộ xử lý đầu cuối lưu gói tin và yêu cầu KDC cấp khóa phiên

D. KDC cấp khóa phiên cho cả hai bộ xử lý đầu cuối và sau đó mã hóa, rồi truyền gói tin lưu

6. Đối với Kerberos điều khẳng định nào sau đây không đúng:

A. Hệ thống máy chủ xác thực tin cậy

B. Xác thực một lần cho một phiên làm việc

C. Cung cấp nhiều loại dịch vụ phân tán và kiểm soát quyền truy cập

D. @Mỗi lần sử dụng một dịch vụ trong hệ thống cần phải xác thực để kiểm soát quyền truy cập

Câu hỏi trắc nghiệm 3

7. Mục nào không phải là yêu cầu ban đầu của Kerberos:

A. An toàn

B. Tin cậy

C. @Xác thực tập trung

D. Có thể mở rộng

8. Vấn đề nào không thuộc cải tiến của Kerberos 5

A. Tạo khóa mã từ mật khẩu

B. Gửi khóa phiên và thẻ được mã bởi khóa sinh từ mật khẩu

C. @Cấp thẻ và khóa truy cập vào các máy chủ ứng dụng

D. Thêm yếu tố thời gian vào các khóa cho dịch vụ để chống dùng lặp lại

9. Mục nào không nằm trong qui trình xác thực của Kerberos

A. Người dùng nhập vào tên truy cập và mật khẩu ở phía máy trạm

B. @Tên và mật khẩu sẽ được truyền đến máy chủ xác thực để kiểm tra

C. Máy trạm gởi một thông điệp dưới dạng bản rõ đến AS để yêu cầu dịch vụ.

D. AS kiểm tra xem có tồn tại người dùng trong cở sở dữ liệu của nó hay không. Nếu có, nó gởi ngược lại cho máy trạm thông điệp được mã bằng khóa sinh từ mật khẩu người dùng.

Câu hỏi trắc nghiệm 4

10. Điều nào không đúng với hạ tầng khóa công khai PKI

A. @Đây là thuật toán mã hóa công khai
B. Đây là cơ chế quản lý và phân phối khóa công khai
C. Giấy chứng nhận được ký bởi mã công khai của chủ quyền chứng nhận
D. Có danh sách thu hồi các giấy chứng nhận

11. Đâu không phải là thành phần của hạ tầng khóa công khai

A. Chủ quyền đăng ký CR
B. Chủ quyền chứng nhận CA
C. @Chủ quyền khóa công khai
D. Xuất bản danh sách thu hồi CRL

12. Đâu không phải là thao tác PGP

A. Bảo mật
B. Xác thực
C. @Mã xác thực thông điệp
D. Nén và chuyển dữ liệu thành các ký tự in được

Câu hỏi trắc nghiệm 5

13. Sơ đồ tổng quát người gửi không bao gồm

A. Nếu có ký, thì ký rồi nén

B. @Nén, rồi xét đến việc ký hay không

C. Sau nén, xét đến việc có bản mật hay không

D. Sau bảo mật sẽ dùng hàm chuyển R64

14. Trong chùm khóa riêng không có trường nào

A. Nhãn thời gian và khóa công khai

B. Mã khóa riêng

C. @Khóa riêng

D. Mã người sử dụng

15. Trong chùm khóa công khai không có trường nào

A. Nhãn thời gian và khóa công khai

B. @Mã khóa riêng

C. Mã người sử dụng

D. Chữ ký chứng nhận

Câu hỏi trắc nghiệm 6

16. Trong định dạng mẩu tin PGP không có trường nào.

A. Thành phần khóa phiên gồm mã khóa của khóa công khai người nhận

B. Thành phần chữ ký gồm nhãn thời gian, khóa công khai người gửi, ký bản băm

C. Thành phần mẩu tin

D. @Thành phần số ngẫu nhiên

17. Trong quá trình sinh mẫu tin để gửi điều gì sau đây không đúng

A. Người gửi nhập mật khẩu, băm thành khóa giải mã khóa riêng

B. Người gửi ký bằng cách mã bản băm bằng khóa riêng

C. @Người gửi dùng khóa phiên đã thỏa thuận để mã mẩu tin

D. Người gửi mã bằng khóa phiên sinh ngẫu nhiên và mã khóa phiên bằng khóa công khai của người nhận

18. Trong quá trình nhận mẫu tin điều gì sau đây không đúng

A. Người nhận nhập mật khẩu, băm thành khóa giải mã khóa riêng

B. @Người nhận dùng khóa phiên đã thỏa thuận

C. Người nhận dùng khóa riêng giải mã lấy khóa phiên

D. Người nhận dùng khóa phiên giải mã mẩu tin hoặc dùng khóa công khai và băm bản tin để kiểm tra chữ ký

Đáp án câu hỏi trắc nghiệm

- Câu 1
  - A, Thông báo công khai, cần phải chống mạo danh
- Câu 2
  - D, Chủ quyền khóa công khai dùng online, chủ quyền chứng nhận có thể offline, nên không phụ thuộc
- Câu 3
  - C, Không thể trao đổi khoá mật mới bằng khoá mật cũ, vì nếu khóa mật cũ đã lộ, thì không an toàn
- Câu 4 Trong phương pháp kết hợp, có bên thứ 3
  - C, @NSD dùng khóa chính chứ không phải khóa công khai để trao đổi khóa phiên với NSD khác thông qua KDC

Đáp án câu hỏi trắc nghiệm

- Câu 5
  - B, Hai bên không cần thỏa thuận khóa phiên trước khi trao đổi
- Câu 6
  - D, Mỗi lần sử dụng dịch vụ, không cần xác thực lại, vì đã được xác thực và cấp thẻ
- Câu 7
  - C, Xác thực tập trung không phải yêu cầu ban đầu
- Câu 8
  - C, Sử dụng thẻ và khóa đã có trong phiên bản trước

Đáp án câu hỏi trắc nghiệm

- Câu 9
  - B, Mật khẩu không được truyền đến máy chủ để kiểm tra
- Câu 10
  - A, Đây không phải là thuật toán, mà là hạ tầng gồm nhiều chức năng
- Câu 11
  - C, Không có chủ quyền khóa công khai mà có chủ quyền chứng nhận CA
- Câu 12
  - C, Không dùng mã xác thực mà dùng bản băm và ký bằng khóa riêng

Đáp án câu hỏi trắc nghiệm

- Câu 13
  - B, Ký nếu có thì xảy ra trước nén
- Câu 14
  - C, Không chứa khóa riêng dạng tường minh
- Câu 15
  - C, Không chứa mã khóa riêng
- Câu 16
  - C, Không chứa số ngẫu nhiên
- Câu 17
  - C, Dùng khóa phiên sinh ngẫu nhiên rồi mã bằng khóa công khai người nhận
- Câu 18
  - B, Không dùng khóa phiên thỏa thuận

Glossary - Từ điển thuật ngữ

- Phân phối khóa công khai: cung cấp khóa công khai của người sử dụng một cách an toàn
- Thư mục công cộng: Thư mục có người quản trị để mọi người sử dụng đăng ký và chia sẻ khóa công khai
- Chủ quyền khóa công khai: Người có thẩm quyền quản trị và cung cấp khóa công khai trực tuyến, dùng mã khóa riêng ký nhận khóa công khai của người sử dụng
- Chủ quyền Giấy chứng nhận: Người có thẩm quyền quản trị khóa công khai và cung cấp Giấy chứng nhận khóa công khai của người sử dụng được ký bằng mã khóa riêng
- Khóa phiên (section key): Khóa tạm thời, dùng để mã hoá dữ liệu giữa nhóm người sử dụng cho một phiên logic và sau đó bỏ đi.

Glossary - Từ điển thuật ngữ

- Khóa chính (master key): khóa dùng để mã các khóa phiên, chia sẻ giữa người sử dụng và trung tâm phân phối khóa.
- Kerberos: Hệ thống máy chủ xác thực và cung cấp các dịch vụ phân tán được phát triển ở MIT.
- Hạ tầng khóa công khai PKI: Hệ thống cung cấp và quản lý Giấy chứng nhận về khóa công khai của người sử dụng
- An toàn thư điện tử nhằm đảm bảo các yêu cầu sau: tính bảo mật nội dung tin gửi, xác thực người gửi mẩu tin, tính toàn vẹn của mẩu tin, hơn nữa bảo vệ khỏi bị sửa, tính chống từ chối gốc, chống từ chối của người nhận.

FAQ – Câu hỏi thường gặp

- **Câu 1.** Ưu nhược điểm của việc quản lý khóa công khai bằng thư mục công cộng?
- **Câu 2.** Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền khóa công khai?
- **Câu 3.** Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền chứng nhận khóa công khai?
- **Câu 4.** Giải thích sơ đồ trao đổi trực tiếp khóa mật dùng chung bằng khóa công khai?
- **Câu 5.** Giải thích sơ đồ trao đổi khóa mật dùng chung bằng phương pháp kết hợp dùng khóa công khai với sự hỗ trợ của bên thứ ba?
- **Câu 6.** Mục đích dùng khóa chính và khóa phiên là gì? Thời gian sử dụng chúng khác nhau nhiư thế nào?

Câu hỏi tự luận 2

- **Câu 7**. Nêu các vấn đề gặp phải khi giải quyết bài toán phân phối khóa?
- **Câu 8.** Nêu mục đích và yêu cầu của hệ thống Kerberos?
- **Câu 9.** Nêu cấu tạo mô hình Kerberos? Và việc yêu cầu dịch vụ trong lãnh địa khác được thực hiện như thế nào?
- **Câu 10.** Mô tả giao thực xác thực sử dụng dịch vụ trong hệ thống Kerberos?
- **Câu 11.** Kerberos phiên bản 5 có những cải tiến gì? Giải thích quá trình sinh khóa từ mật khẩu?

Câu hỏi tự luận 3

- **Câu 12**. Mô tả hoạt động của cơ sở hạ tầng khóa công khai PKI?
- **Câu 13.** Nêu các nhiệm vụ an ninh chính của Hệ thống thư điện tử?
- **Câu 14**. Giải thích sơ đồ bảo mật và xác thực thư điện tử?
- **Câu 15.** Mô tả các bước gửi một bức thư điện tử?
- **Câu 16**. Mô tả các bước nhận một bức thư điện tử?

Hướng dẫn trả lời câu hỏi tự luận

1. Thư mục có người quản trị kiểm soát quyền đăng ký và thay đổi, tuy vẫn còn lỗ hổng để giả mạo và sử đổi và phải hỗ trợ trực tuyến.
2. Chủ quyền Khóa công khai cung cấp khóa công khai có chử ký của Chủ quyền chống giả mạo và sửa đổi, nhưng vẫn hỗ trợ trực tuyến
3. Chủ quyền chứng nhận cấp Giấy chứng nhận có chữ ký chủ quyền, không cần trực tuyến
4. Trao đổi trực tiếp dùng khóa công khai: Lỗ hổng là thông điệp 4 dễ bị sử dụng lại của các lần trước đó, do không có nhãn thời gian
5. Trao đổi kết hợp với KDC: Thông điệp 3 vẫn có lỗ hổng, có thể bị dùng lặp, cần thêm nhãn thời gian, kéo theo vấn đề đồng hồ đồng bộ
6. Khóa chính trao đổi với KDC, ít thay đổi, Khóa phiên dùng cho phiên làm việc thay đổi thường xuyên, không có cơ hội phân tích cho kẻ thám mã.

Hướng dẫn trả lời câu hỏi tự luận

7. Đối với mạng lớn đòi hỏi phân cấp Trung tâm phân phối khóa KDC, nhưng cần phải tạo tin cậy cho nhau, giữa người sử dụng với Trung tâm và các Trung tâm với nhau. Thời gian sống của khóa bộ phận cần được hạn chế để cho an toàn hơn. Sử dụng phân phối khóa tự động thay mặt người dùng, nhưng phải có hệ thống tin cậy, các khóa cấp phát được sinh ra càng ngẫu nhiên càng tốt.
8. Xác thực trung tâm, login một lần, an toàn, tin vậy, trong suốt, có thể mở rộng
9. Có máy chủ xác thực cấp thẻ cho phiên làm việc, máy chủ cấp thẻ cho các dịch vụ, có thể có nhiều lãnh địa
10. Xem bài giảng. Vấn đề là mật khẩu không truyền trên mạng và các thẻ phải được mã hóa, có yếu tố thời gian tránh dùng lại
11. Keberos 5 đã khắc phục các yếu điểm của Keberos 4 như dùng khóa sinh từ mật khẩu, mã kép, thêm nhãn thời gian
12. Nhiệm vụ của PKI:

Hướng dẫn trả lời câu hỏi tự luận

- Quản lý danh tính người sử dụng (NSD) với khóa công khai
- Cấp chứng nhận của Chủ quyền Giấy chứng nhận CA cho NSD
- Huỷ và Thu hồi các giấy chứng nhận không còn hiệu lực
- Tạo ra Thư mục để lưu trữ các chứng nhận và danh sách thu hồi
- Cung cấp dịch vụ sẵn sàng cung cấp cho NSD như: đăng ký, truy cập, xin giấy chứng nhận, đưa ra danh sách thu hồi CRL

13. An toàn thư điện tử. Đảm bảo các yêu cầu sau: tính bảo mật nội dung tin gửi, xác thực người gửi mẩu tin, tính toàn vẹn của mẩu tin, hơn nữa bảo vệ khỏi bị sửa, tính chống từ chối gốc, chống từ chối của người nhận.
14. Xem bài giảng
15. Xem bài giảng
16. Xem bài giảng