Trường Đại Học Công Nghệ Thông Tin
Khoa Mạng Máy Tính và Truyền Thông

AN TOÀN MẠNG MÁY TÍNH

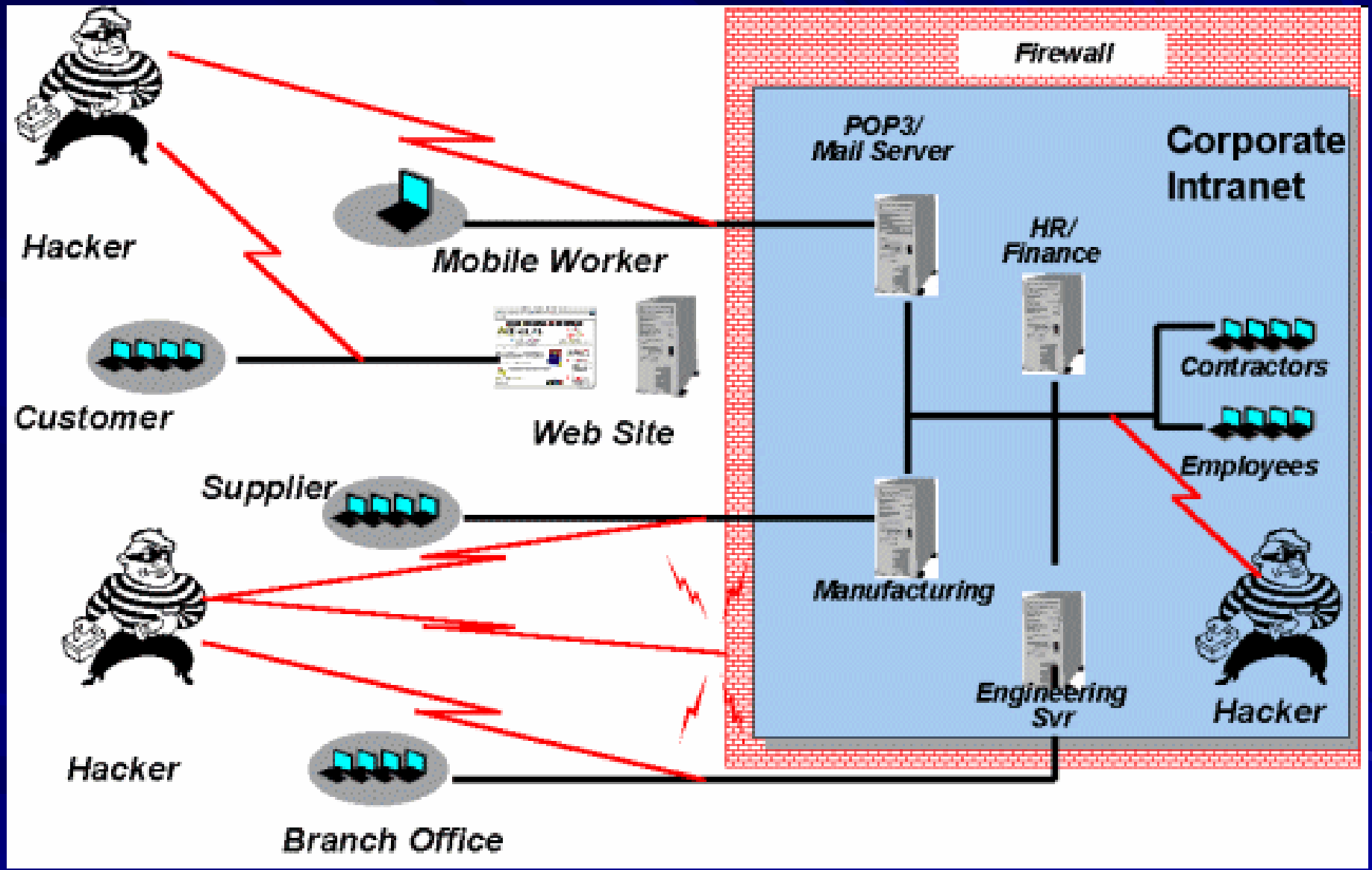
ThS. Tô Nguyễn Nhật Quang

NỘI DUNG MÔN HỌC

1. Tổng quan về an ninh mạng
2. Các phần mềm gây hại
3. Các giải thuật mã hoá dữ liệu
4. Mã hoá khoá công khai và quản lý khoá
5. Chứng thực dữ liệu
6. Một số giao thức bảo mật mạng
7. Bảo mật mạng không dây
8. Bảo mật mạng vành đai
9. Tìm kiếm phát hiện xâm nhập

BÀI 6

MỘT SỐ GIAO THỨC BẢO MẬT MẠNG


Firewall
POP3/
Mail Server
Corporate
Intranet
HR/
Finance
Contractors
Employees
Hacker
Mobile Worker
Customer
Web Site
Supplier
Manufacturing
Engineering
Svr
Hacker
Hacker
Branch Office

NỘI DUNG BÀI HỌC

1. Vị trí của mật mã trong mạng máy tính
2. Cơ sở hạ tầng khoá công khai
3. IPsec
4. SSL/TLS
5. PGP và S/MIME
6. Kerberos
7. SSH
8. Bài tập

1. Vị trí của mật mã trong mạng máy tính

Tổng quan

- Việc sử dụng mật mã trên mạng máy tính nhằm xây dựng các giao thức bảo mật mạng:
  - Giải thuật mã hoá khoá đối xứng
  - Giải thuật mã hoá khoá công khai
  - Giải thuật sinh khoá và trao đổi khoá
  - Hàm băm
  - Giải thuật chứng thực
  - Chữ ký số
  - Cơ sở hạ tầng khoá công khai

1. Vị trí của mật mã trong mạng máy tính

Tổng quan

- Để bảo vệ truyền thông trên mạng, có thể triển khai các giải thuật mã hóa tại lớp bất kỳ trong kiến trúc mạng. Sử dụng các giải thuật mã hóa ở các lớp khác nhau sẽ cung cấp các mức độ bảo vệ khác nhau.
- Các giao thức bảo mật mạng ứng dụng trong thực tế:
  - Tầng mạng: Cơ sở hạ tầng khoá công khai (PKI) X.509, giao thức IP security (IPsec).
  - Tầng vận chuyển: giao thức Secure Sockets Layer/Transport Layer Security (SSL/TLS).
  - Tầng ứng dụng: Pretty Good Privacy (PGP), Secure/ Multipurpose Internet Mail Extension (S/MIME), Kerberos, Secure Shell (SSH).

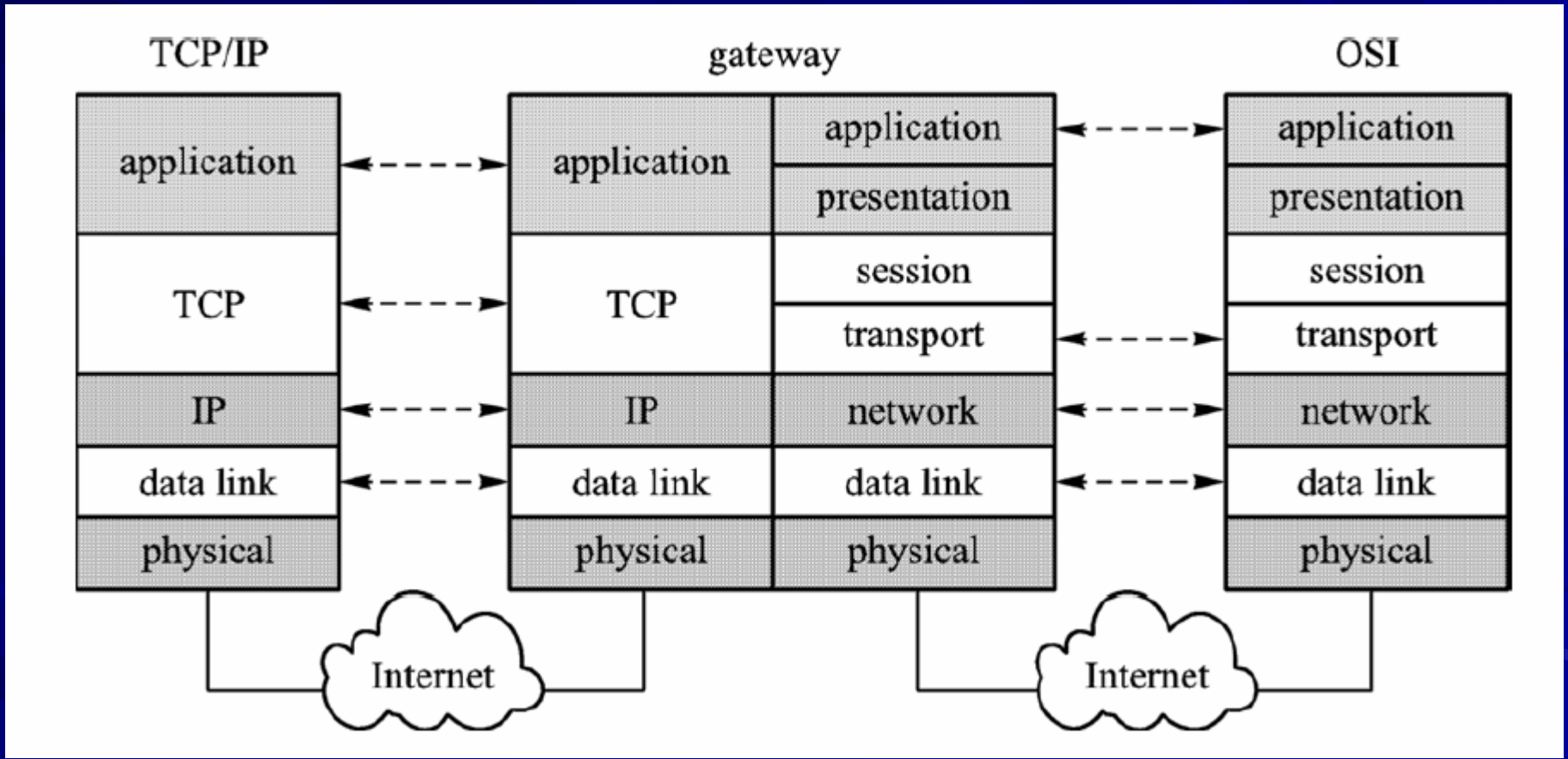
1. Vị trí của mật mã trong mạng máy tính

Tổng quan

	Riêng tư/Mã hoá	Chứng thực	Ký/ Toàn vẹn dữ liệu
Nhân viên nội bộ hoặc từ xa truy cập đến server	SSL 2.0 hoặc 3.0 (cung cấp bởi Secure Server ID)	-Server chứng thực bởi Server ID - Client chứng thực bởi mật khẩu hoặc bởi SSL 3.0 với Client ID	Ký vào văn bản, S/MIME sử dụng Client ID
Khách hàng truy cập đến server	SSL 2.0 hoặc 3.0 (cung cấp bởi Secure Server ID)	Như trên	Không cần thiết
Nhân viên từ xa sử dụng e-mail	- SSL trên POP3 hoặc IMAP mail server - S/MIME Client ID hoặc VPN sử dụng IPsec	Server chứng thực bởi mật khẩu của Server ID	S/MIME sử dụng Client ID
Truyền thông với chi nhánh	- SSL - VPN sử dụng IPsec	- Server chứng thực bởi Server ID - Router/ tường lửa chứng thực bởi IPsec ID - Client chứng thực bởi mật khẩu hoặc SSL 3.0 với Client ID	Ký vào văn bản, S/MIME

1. Vị trí của mật mã trong mạng máy tính

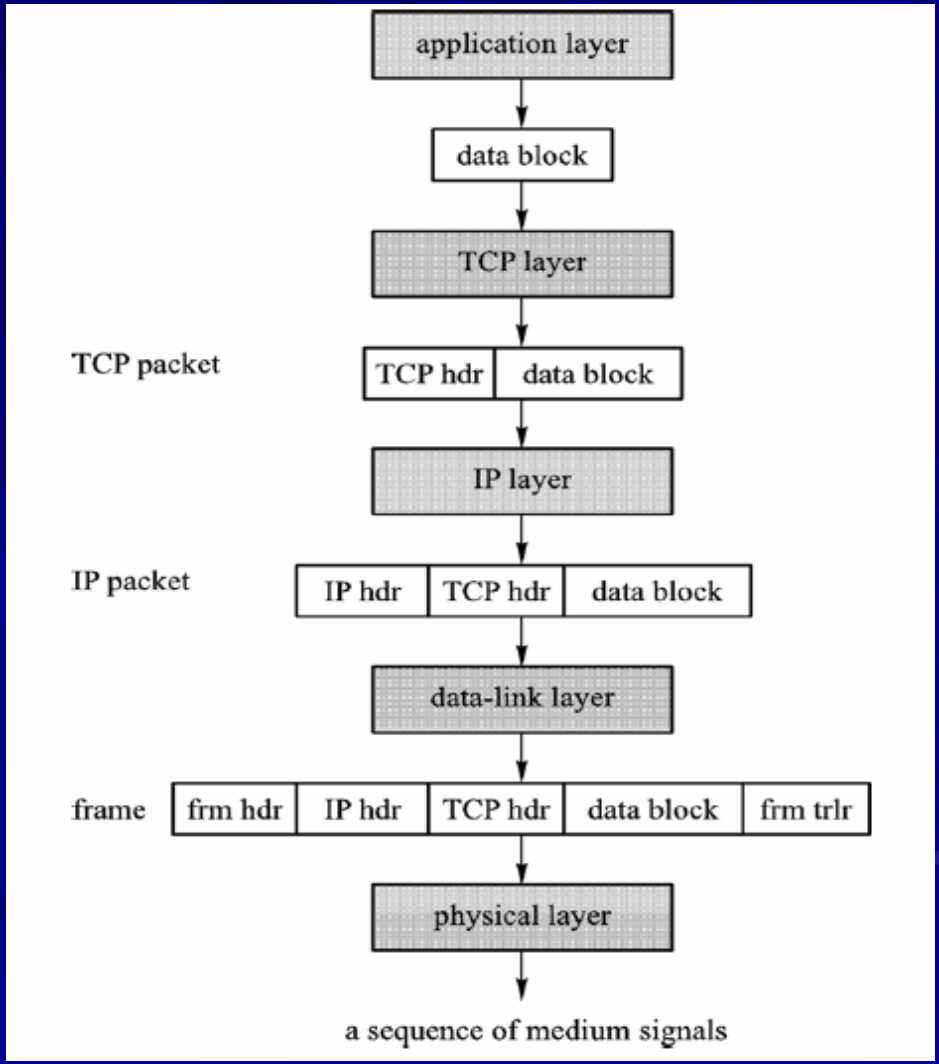
Sự tương ứng giữa kiến trúc TCP/IP và mô hình OSI



1. Vị trí của mật mã trong mạng máy tính

Sự đóng gói và mã hoá dữ liệu tại các lớp mạng

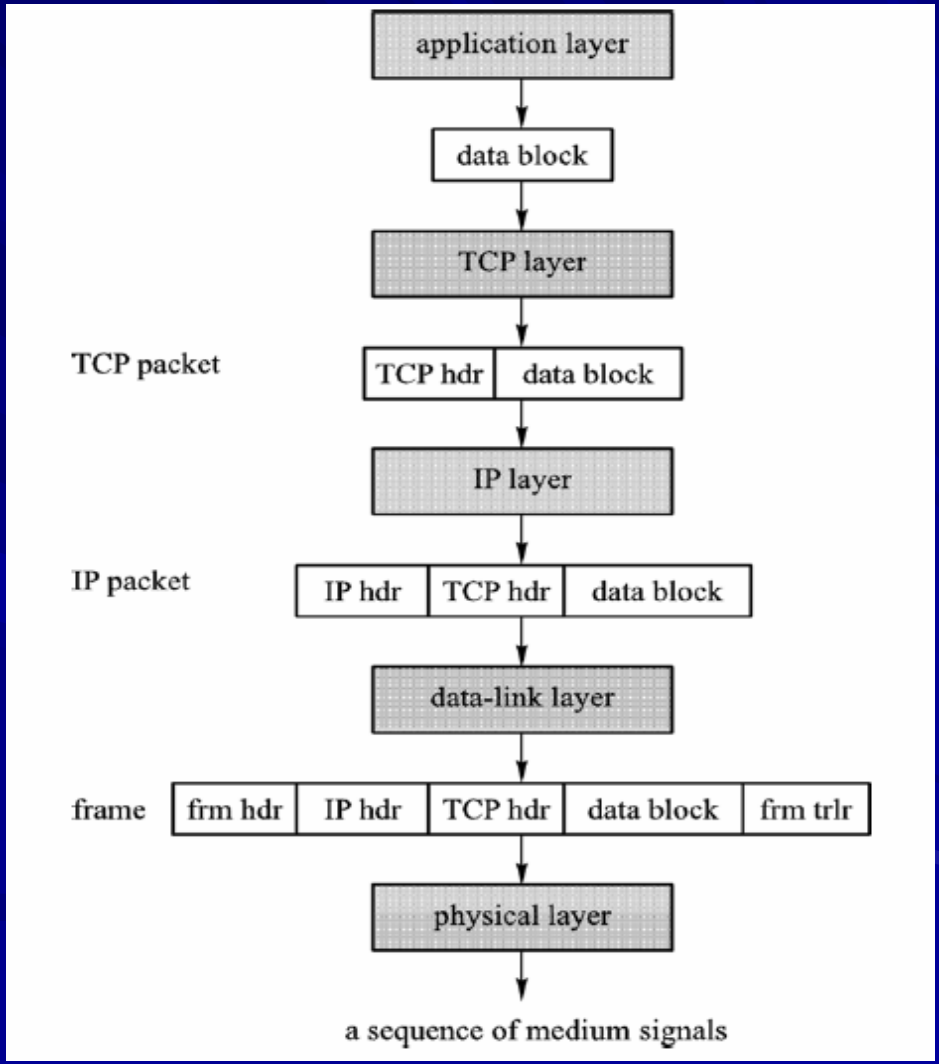
- Mã hoá tại lớp ứng dụng (Application Layer):
  - Bảo mật end-to-end.
  - Dữ liệu được mã hoá hoặc chứng thực tại lớp này sẽ tiếp tục đi qua các lớp khác như dữ liệu bình thường (không cần giải mã hoặc kiểm tra).
  - TCP header và IP header sẽ không được mã hoá (do nằm ở các lớp dưới) → attacker có thể phân tích và sửa đổi nội dung.
  - VD: Malice có thể thay đổi địa chỉ IP đích trong IP header để phân phối gói tin cho người khác.



1. Vị trí của mật mã trong mạng máy tính

Sự đóng gói và mã hoá dữ liệu tại các lớp mạng

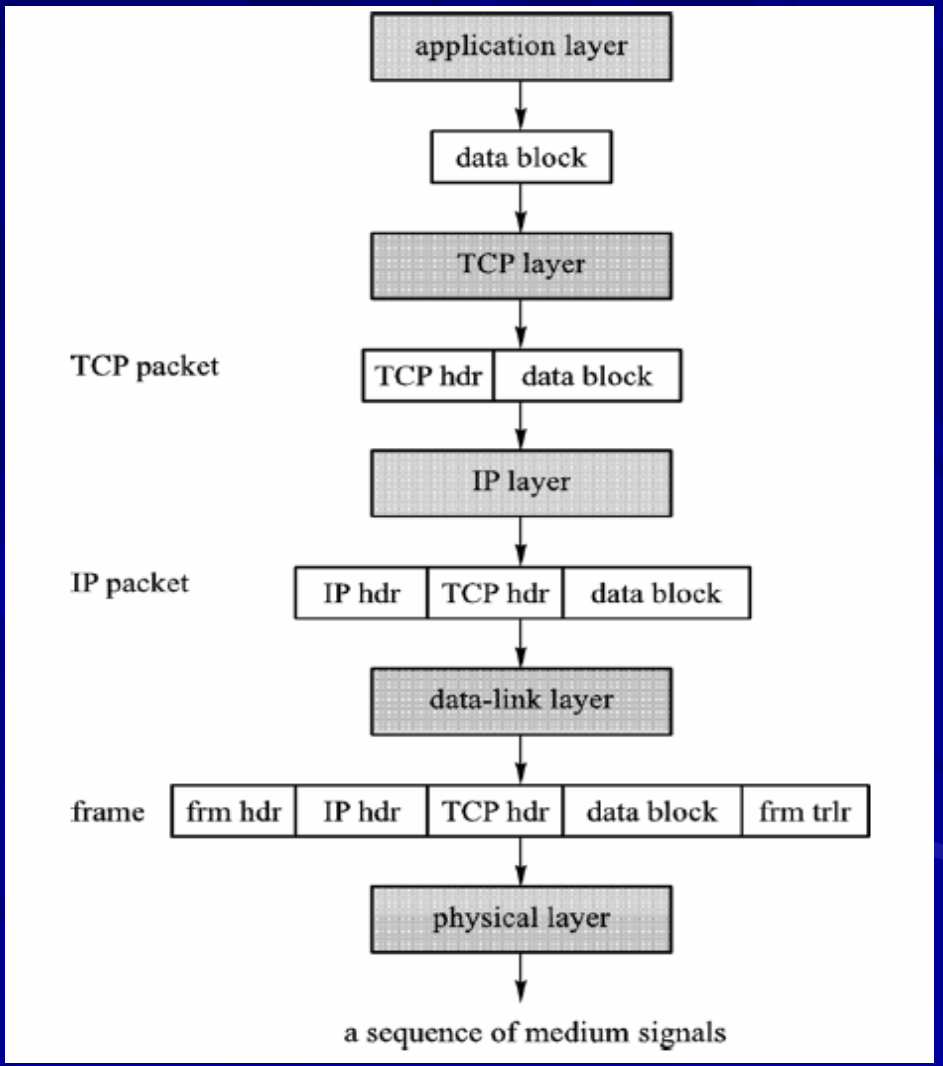
- Mã hoá tại lớp vận chuyển (Transport Layer):
  - Nhằm cung cấp sự an toàn cho các gói TCP.
  - Có thể mã hoá hoặc chứng thực cho phần payload hoặc cả gói tin TCP (mã hoá cả header và payload).
  - Việc mã hoá này không ảnh hưởng đến dữ liệu nhận được từ lớp ứng dụng.
  - → IP header không được mã hoá → các attacker có thể thu được giá trị sequence number và sử dụng chúng để tấn công.



1. Vị trí của mật mã trong mạng máy tính

Sự đóng gói và mã hoá dữ liệu tại các lớp mạng

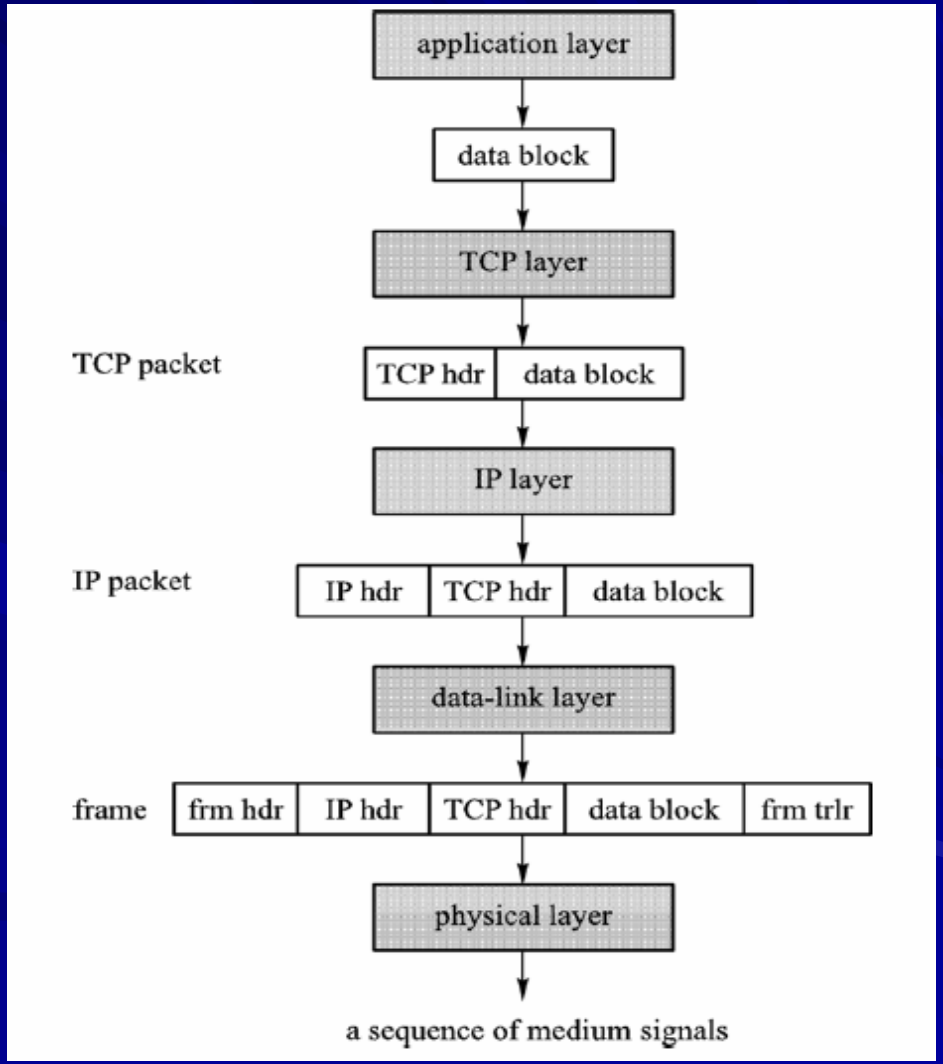
- Mã hoá tại lớp mạng (Network Layer):
  - Bảo mật link-to-link.
  - Mã hoá hoặc chứng thực phần payload hoặc cả gói IP.
  - Không ảnh hưởng đến chức năng định tuyến.
  - Được xem như một ứng dụng ở tunnel-mode.



1. Vị trí của mật mã trong mạng máy tính

Sự đóng gói và mã hoá dữ liệu tại các lớp mạng

- Mã hoá tại lớp liên kết dữ liệu (Data-Link Layer):
  - Cung cấp bảo mật cho các frames.
  - Thực hiện mã hoá hoặc chứng thực cho Payload của frame.
  - Việc phân tích traffic trên các frame đã được mã hoá sẽ không thu được nhiều thông tin đối với các attacker.
  - Việc mã hoá tại lớp liên kết dữ liệu sẽ được giới thiệu trong bài 7 (Bảo mật mạng không dây).



1. Vị trí của mật mã trong mạng máy tính

Các giải thuật mã hoá đối với phần cứng và phần mềm

- Các giải thuật mã hoá có thể được thực hiện trên phần mềm hoặc trên phần cứng sử dụng công nghệ vi mạch tích hợp ứng dụng (Application Specific Integrated Circuit – ASIC).
  - Tại lớp ứng dụng: được thực hiện bởi phần mềm.
  - Tại lớp liên kết dữ liệu: được thực hiện bởi phần cứng.
  - Tại các lớp khác: được thực hiện bởi phần mềm hoặc phần cứng hoặc cả hai.
  - Việc triển khai mã hoá được thực hiện bởi phần cứng có hiệu suất cao nhất nhưng chi phí cao và kém linh hoạt khi cần thay đổi.

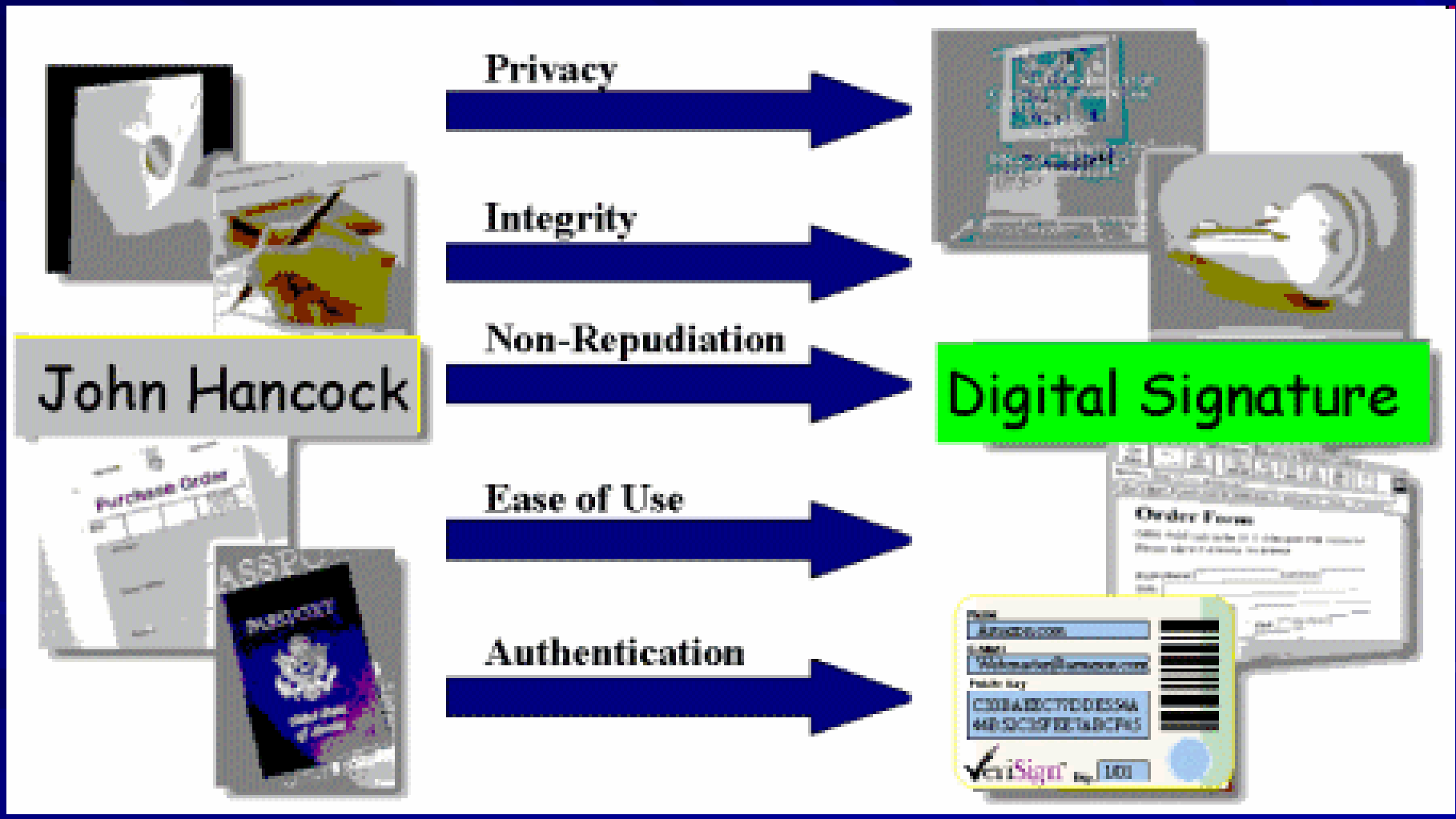
2. Cơ sở hạ tầng khoá công khai

Tổng quan

- Để triển khai các giải thuật mã hóa trong các ứng dụng mạng, cần một cách để phân phối các khóa bí mật sử dụng các mạng mở. Mật mã khoá công khai là cách tốt nhất để phân phối các khóa bí mật này.
- Để sử dụng mật mã khoá công khai, cần phải xây dựng một cơ sở hạ tầng khoá công khai (Public-key infrastructure - PKI) để hỗ trợ và quản lý các chứng chỉ khoá công khai.
- PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng thông tin từ các chứng chỉ khóa công khai để mã hóa và giải mã thông tin trong quá trình trao đổi.

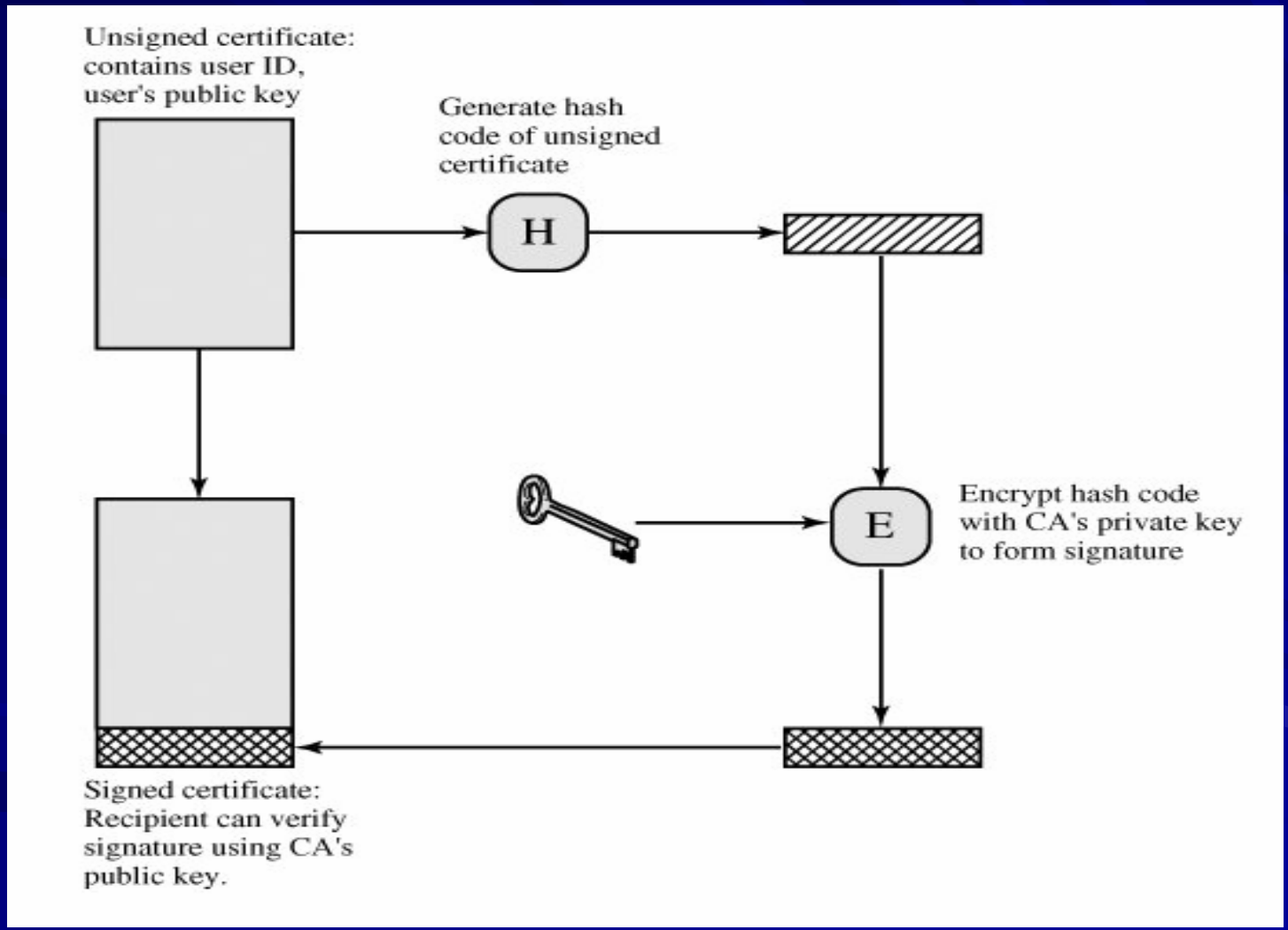
2. Cơ sở hạ tầng khoá công khai

Tổng quan



2. Cơ sở hạ tầng khoá công khai

Tổng quan



2. Cơ sở hạ tầng khoá công khai

Tổng quan

- Thông thường, PKI bao gồm phần mềm máy khách (client), phần mềm máy chủ (server), phần cứng (như thẻ thông minh) và các quy trình hoạt động liên quan.
- Người sử dụng cũng có thể ký các văn bản điện tử với khóa bí mật của mình và mọi người đều có thể kiểm tra với khóa công khai của người đó.
- PKI cho phép các giao dịch điện tử được diễn ra đảm bảo tính bí mật, toàn vẹn và xác thực lẫn nhau mà không cần phải trao đổi các thông tin mật từ trước.
- Hệ điều hành Windows XP và Windows Server đều hỗ trợ cho PKI.

2. Cơ sở hạ tầng khoá công khai

Tổng quan

Các PKI thực hiện các chức năng sau:

- Xác định tính hợp pháp của người sử dụng trước khi cấp chứng chỉ khoá công khai (public-key certificate) cho họ.
- Phát hành chứng chỉ khoá công khai theo yêu cầu của người dùng.
- Gia hạn thời gian hợp lệ của chứng chỉ khi có yêu cầu.
- Thu hồi chứng chỉ khoá công khai theo yêu cầu của người sử dụng hoặc khi các khóa riêng không còn an toàn.
- Lưu trữ và quản lý các chứng chỉ khoá công khai.
- Ngăn chặn người ký chữ ký số phủ nhận chữ ký của họ.
- Hỗ trợ việc cho phép các CA khác chứng thực chứng chỉ khoá công khai phát hành bởi các CA này.

2. Cơ sở hạ tầng khoá công khai

Tổng quan

- Hầu hết các hệ thống PKI quy mô doanh nghiệp đều dựa trên các chuỗi chứng thực để xác thực các thực thể. Chứng thực của người dùng sẽ được một nhà cung cấp chứng thực số cấp, đến lượt nhà cung cấp này lại có chứng thực được một nhà cung cấp khác ở cấp cao hơn tạo ra... Hệ thống sẽ bao gồm nhiều máy tính thuộc nhiều tổ chức khác nhau với các gói phần mềm tương thích từ nhiều nguồn khác nhau.
- Các hệ thống PKI doanh nghiệp thường được tổ chức theo mô hình danh bạ trong đó khóa công khai của mỗi người dùng được lưu trữ (bên trong các chứng chỉ số) kèm với các thông tin cá nhân (số điện thoại, email, địa chỉ, nơi làm việc...). Hiện nay, công nghệ danh bạ tiên tiến nhất là LDAP và định dạng chứng thực phổ biến nhất (X.509) cũng được phát triển từ mô hình tiền nhiệm của LDAP (X.500).

2. Cơ sở hạ tầng khoá công khai
Tổng quan

- Danh sách một số hệ thống PKI:
  - Computer Associates eTrust PKI
  - Entrust
  - Microsoft
  - VeriSign
  - Nexus
  - OpenCA
  - RSA Security
  - …

2. Cơ sở hạ tầng khoá công khai

VeriSign

- **VeriSign®** là thương hiệu uy tín nhất trên toàn thế giới hiện nay trong lĩnh vực cung cấp chứng chỉ số.
- VeriSign hiện đang bảo mật cho hơn 1,000,000 máy chủ Web trên toàn thế giới.
- Hơn 40 ngân hàng lớn nhất thế giới và hơn 95% trong số các công ty hàng đầu thế giới theo danh sách của Fortune 500 lựa chọn chứng chỉ số SSL cung cấp bởi Verisign.
- Hơn 90,000 tên miền tại 145 quốc gia hiển thị logo **VeriSign Secured® Seal**, dấu hiệu được tin cậy nhất trên Internet.

2. Cơ sở hạ tầng khoá công khai

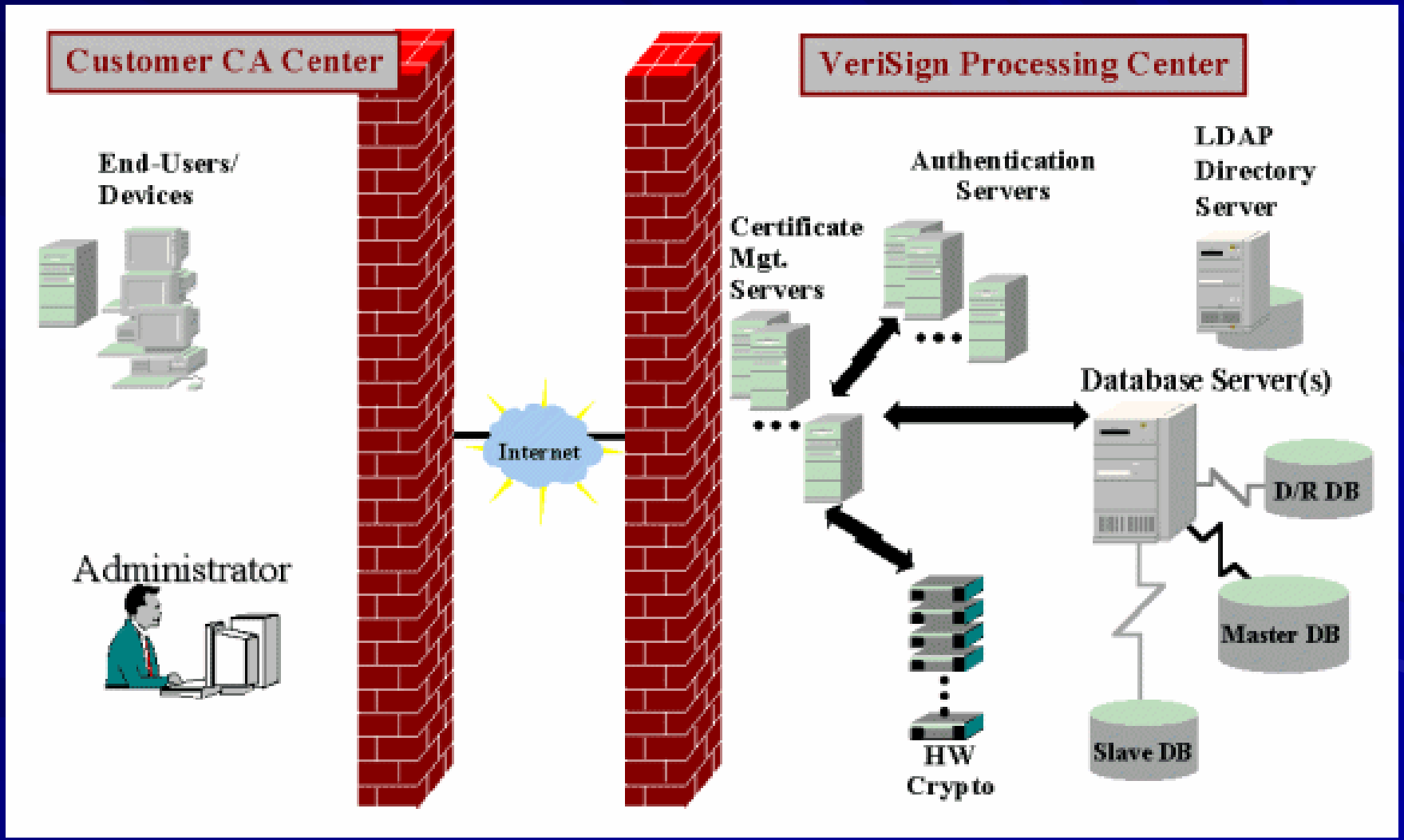
VeriSign

VeriSign sử dụng giải thuật mã hóa SSL mạnh mẽ nhất:

- Giải thuật mã hóa cao cấp từ 128 bits, an toàn gấp 288 lần so với giải thuật mã hóa 40 bits.
- Chứng chỉ số VeriSign cho phép dữ liệu trao đổi giữa người dùng và website được mã hóa từ 40-256 bits.

2. Cơ sở hạ tầng khoá công khai

VeriSign



2. Cơ sở hạ tầng khoá công khai

VeriSign

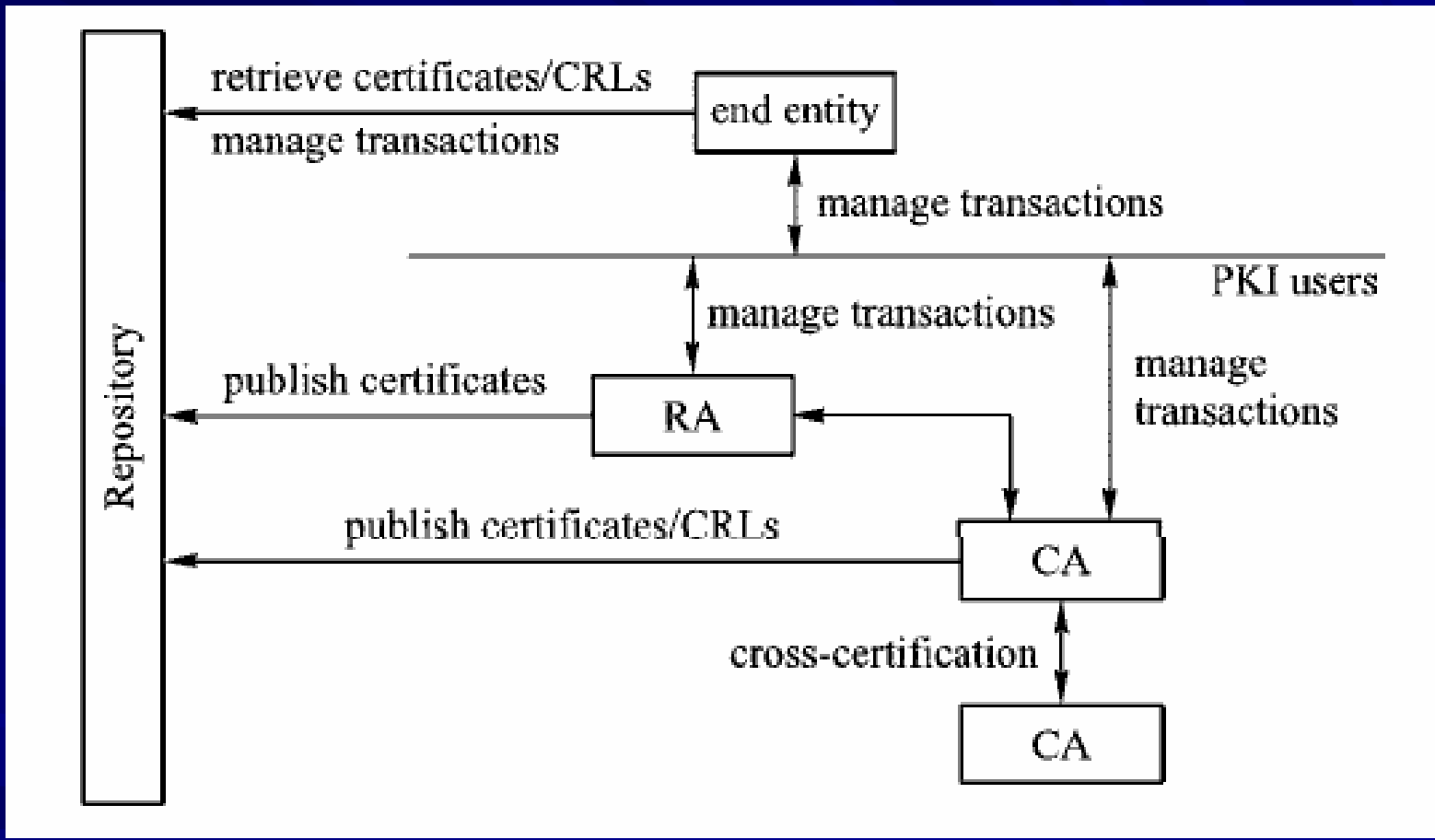
	Secure Site Pro with EV >>	Secure Site with EV >>	Secure Site Pro >>	Secure Site >>
Thích hợp	Ngân hàng điện tử, sàn chứng khoán, sàn vàng	Đặt phòng, đặt bàn, đặt vé trực tuyến	Trao đổi dữ liệu giữa các chi nhánh thông qua website	Trang web bán hàng có giao dịch nhỏ
Độ bảo mật dữ liệu	★★★	★★☆	★★★	★★☆
Độ tin cậy	★★★	★★★	★★☆	★★☆
Thanh địa chỉ của trình duyệt có màu xanh lá cây	✓	✓		
Hiển thị logo **VeriSign Secured® Seal** trên website	VeriSign Secured	VeriSign Secured	VeriSign Secured	VeriSign Secured
Thời gian cấp	Trong vòng 25 ngày làm việc	Trong vòng 25 ngày làm việc	Trong vòng 20 ngày làm việc	Trong vòng 20 ngày làm việc
Thời hạn 1 năm	**$1,499**	**$995**	**$995**	**$399**
Thời hạn 2 năm	**$2,695** *Tiết kiệm $300*	**$1,790** *Tiết kiệm $200*	**$1,790** *Tiết kiệm $200*	**$695** Tiết kiệm *$100*
Thời hạn 3 năm			**$2,480** Tiết kiệm *$500*	**$995** *Tiết kiệm $200*

2. Cơ sở hạ tầng khoá công khai
X.509

- Được thành lập theo các tiêu chuẩn ngành viễn thông của Liên minh Viễn thông Quốc tế (ITU) năm 1988.
- Thường được gọi tắt là PKIX, gồm 4 phần cơ bản:
  - End entity: là người dùng chứng chỉ hoặc thiết bị (server, router) có hỗ trợ PKIX.
  - Certificate Authority (CA): tổ chức có trách nhiệm phát hành và thu hồi chứng chỉ.
  - Registration Authority (RA): có trách nhiệm xác minh danh tính của người chủ sở hữu chứng chỉ.
  - Repository: có trách nhiệm lưu trữ, quản lý chứng chỉ và danh sách các chứng chỉ bị thu hồi bởi CA.

2. Cơ sở hạ tầng khoá công khai

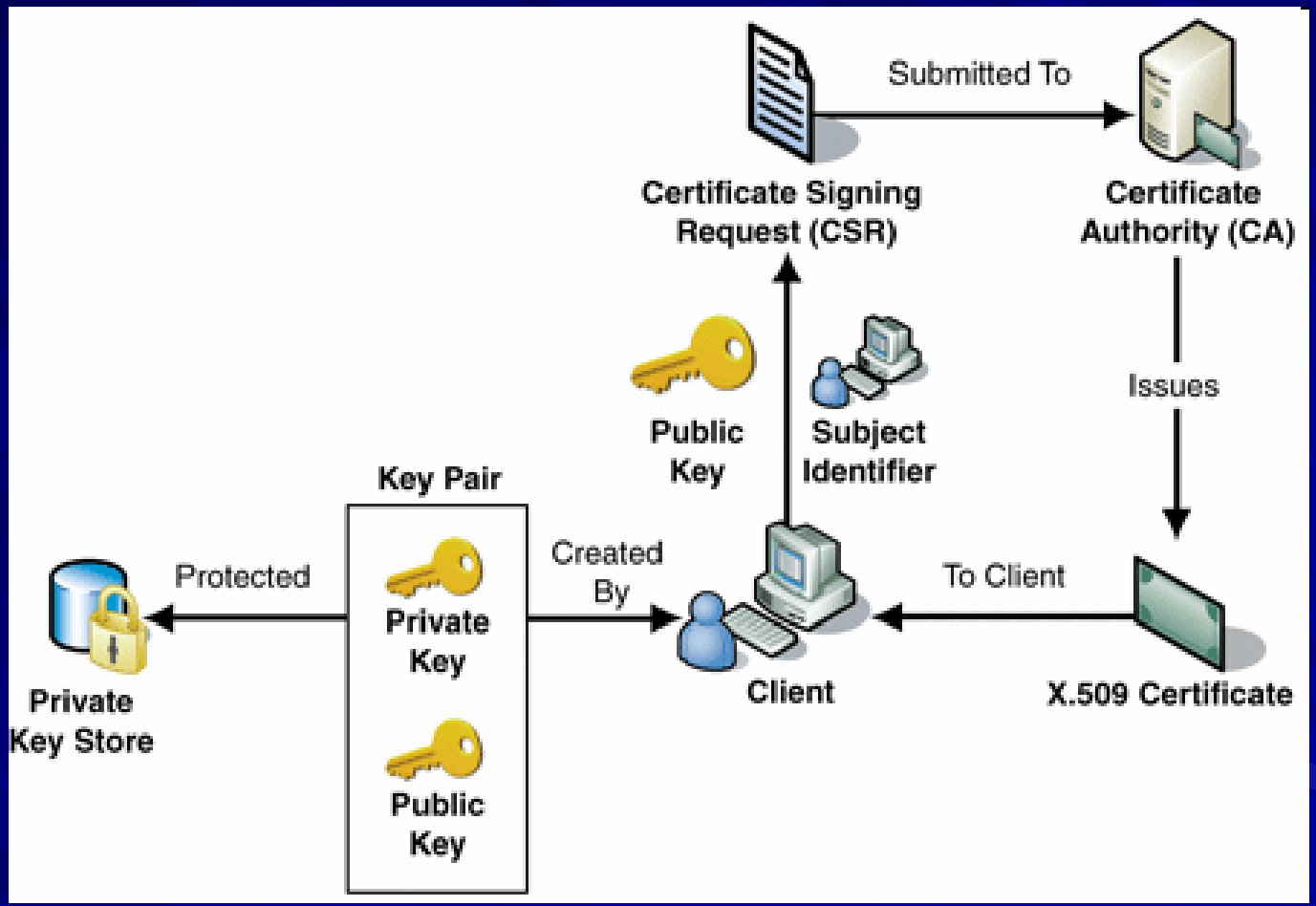
X.509



Kiến trúc PKIX

2. Cơ sở hạ tầng khoá công khai

X.509



Kiến trúc PKIX

2. Cơ sở hạ tầng khoá công khai
X.509

Các giao dịch giữa người dùng, RA, CA và kho:

1. Đăng ký: Người dùng đăng ký với CA hoặc RA (trực tiếp hoặc gián tiếp) trước khi chứng chỉ được cấp cho họ.
2. Khởi tạo: Người sử dụng có được thông tin ban đầu, bao gồm khóa công khai của CA và RA, các giải thuật chữ ký...
3. Chứng chỉ được phát hành: CA hoặc RA phát hành chứng chỉ trong kho lưu trữ cho người dùng.
4. Phục hồi khoá: CA hoặc RA cung cấp cơ chế cần thiết cho người dùng để khôi phục lại khóa riêng bị mất hoặc bị hỏng.
5. Tạo khoá: CA hoặc RA tạo ra cặp khóa mới cho người dùng.
6. Thu hồi chứng chỉ: Người dùng thông báo cho CA hoặc RA thu hồi chứng chỉ nếu họ bị mất khóa riêng, thay đổi tên/địa chỉ...
7. Chứng chỉ chéo: Các CA có thể chứng thực cho các chứng chỉ được phát hành bởi CA khác.

2. Cơ sở hạ tầng khoá công khai

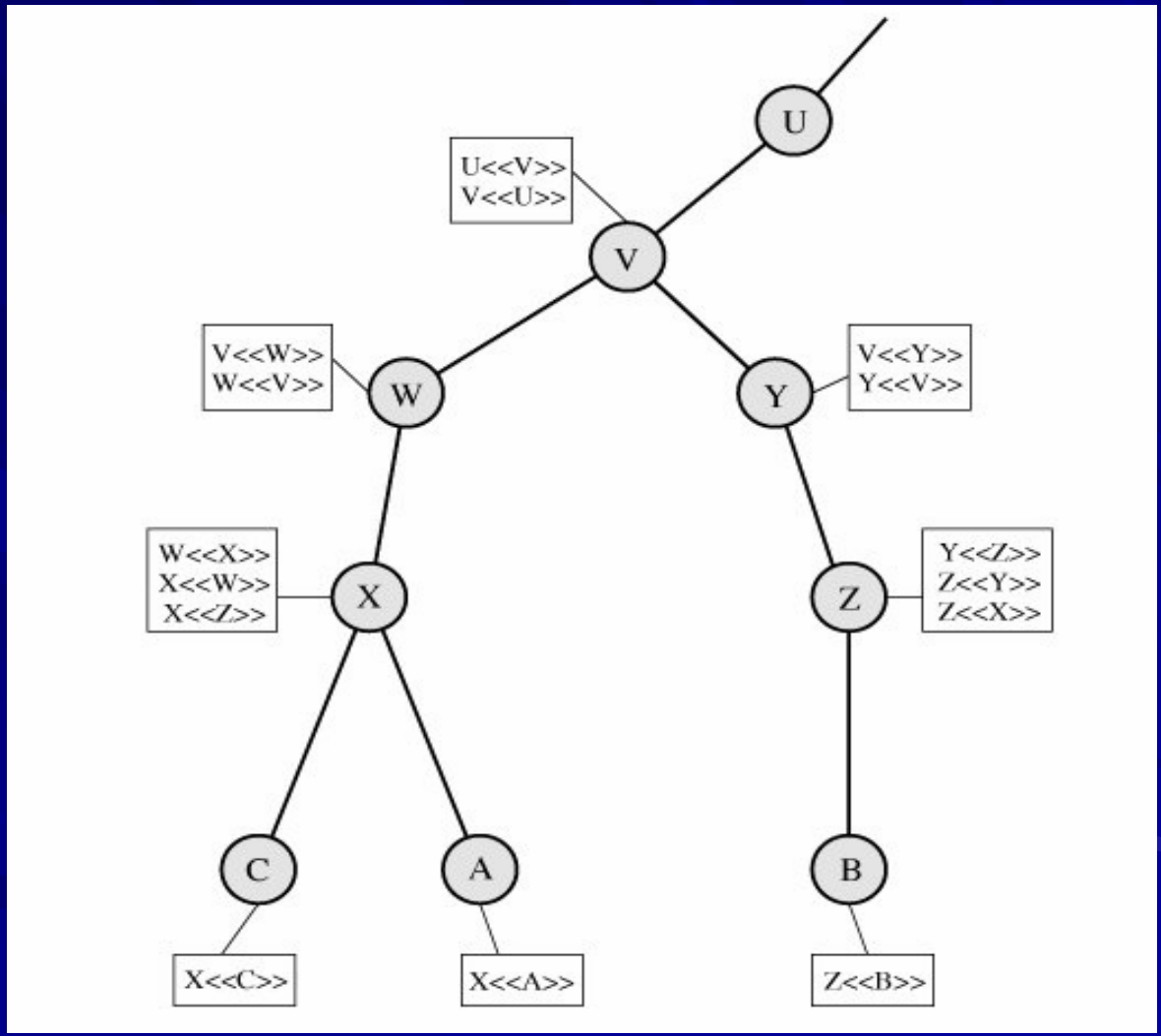
X.509

- User A:

X<<W>> W
<<V>> V <<Y>>
<<Z>> Z <<B>>

- User B:

Z<<Y>> Y <<V>>
V <<W>> W
<<X>>X <<A>>



2. Cơ sở hạ tầng khoá công khai

X.509

- Các định dạng của chứng chỉ X.509:
  - X.509 version 1 được phát hành năm 1988.
  - X.509 version 2 không được sử dụng rộng rãi.
  - X.509 version 3 được phát hành vào năm 1996, phổ biến nhất và được sử dụng đến ngày nay.
- Chứng chỉ X.509 bao gồm các thành phần sau:

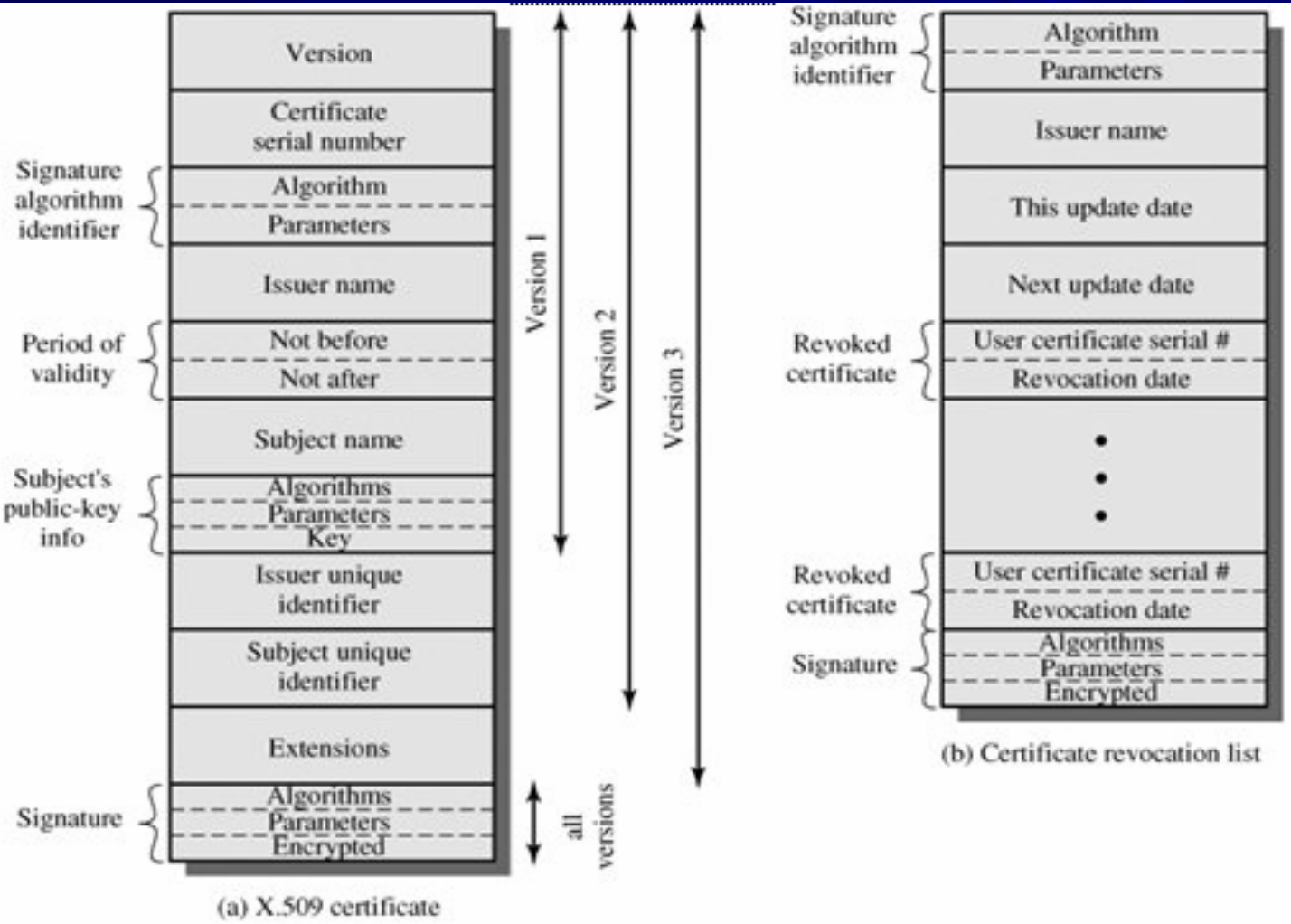
1. Version: chỉ ra phiên bản được sử dụng.
2. Serial number: số duy nhất được gán cho chứng chỉ.
3. Algorithm: liệt kê tên của hàm băm và giải thuật mã hoá khoá công khai dùng để sinh ra chữ ký cho chứng chỉ. Ví dụ: sha1RSA.

2. Cơ sở hạ tầng khoá công khai
X.509

4. Issuer: tổ chức phát hành (CA ký và cấp chứng chỉ).
5. Validity period: thời hạn hiệu lực của chứng chỉ.
6. Subject: tên chủ sở hữu của chứng chỉ.
7. Public key: chứa khoá công khai và những tham số liên quan; xác định thuật toán sử dụng cùng với khoá.
8. Extension: cung cấp thêm một số thông tin.
9. Properties: cho giá trị của hàm băm của chứng chỉ.

2. Cơ sở hạ tầng khoá công khai

X.509



2. Cơ sở hạ tầng khoá công khai

X.509

Version 1 field:

Version: v3

Serial number: 19 b4 11 44 fc 84 79 d2 36 f1 91 f9 11 05

Signature algorithm: sha1RSA

Issuer:

C = US, OU = Department of Computer Science

O = UMass Lowell, E = wang@cs.uml.edu, CN = Jed Wang

Valid from: Friday, March 10, 2006 12:15:05 PM

Valid to: Thursday, March 10, 2011 12:15:05 PM

Subject:

C = US, OU = Department of Computer Science

O = UMass Lowell, E = wang@cs.uml.edu, CN = Jed Wang

Public key: RSA (1024 Bits)

```
30 81 89 02 81 81 00 a6 98 0c 78 98 e4 34
00 e5 e7 7e 5e c2 c3 6a af 0d 22 4b 97 4d
f4 61 1c 34 a4 4e f8 77 cd 97 33 54 35 0c
ec 21 ba ca 36 d0 e2 4b b9 10 dc 28 0a 7f
32 57 00 f8 ba 99 14 98 da bd 20 b6 36 fb
1b 24 ff 9c b1 a9 f7 49 22 e4 79 7f 3f 06
c1 85 41 61 63 a1 84 b7 e7 57 c8 c3 cd f7
3d e4 26 bd 10 bb fb ab 24 b2 b5 6b cc c1
94 b7 06 b7 58 cd 55 46 5a 31 71 3e 33 f4
bc bc e4 3a f6 cf f2 1e cd 02 03 01 00 01
```

Extension:

Key Usage: Digital Signature, Data Encipherment (90)

Properties:

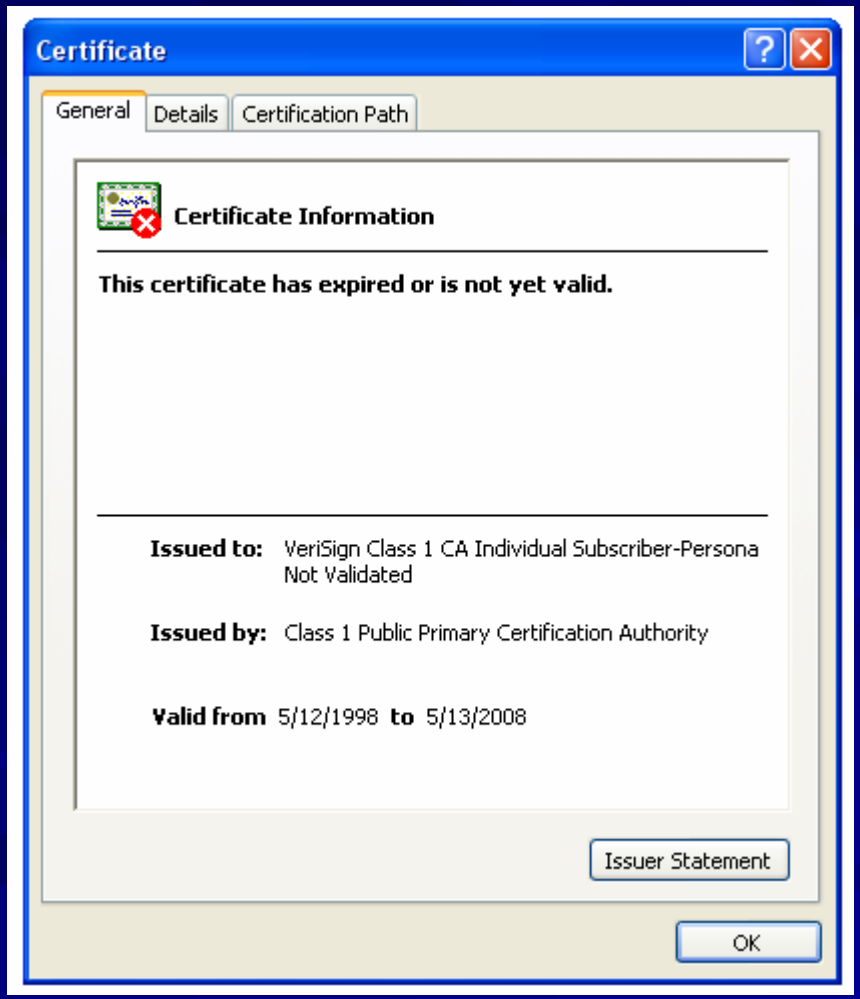
Thumbprint algorithm: sha1

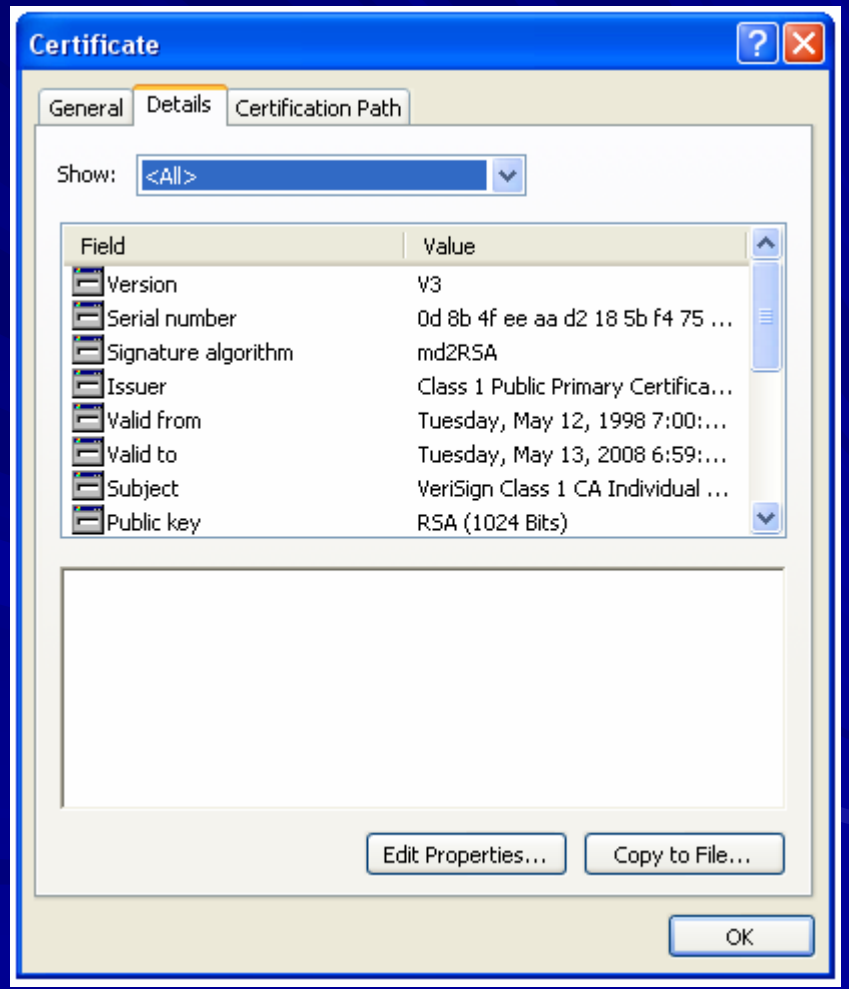
Thumbprint:

```
bd 04 62 16 aa a4 31 1f a0 9a 53 88 2f 3d b4 69 c4 3a 44 c2
```

2. Cơ sở hạ tầng khoá công khai

X.509





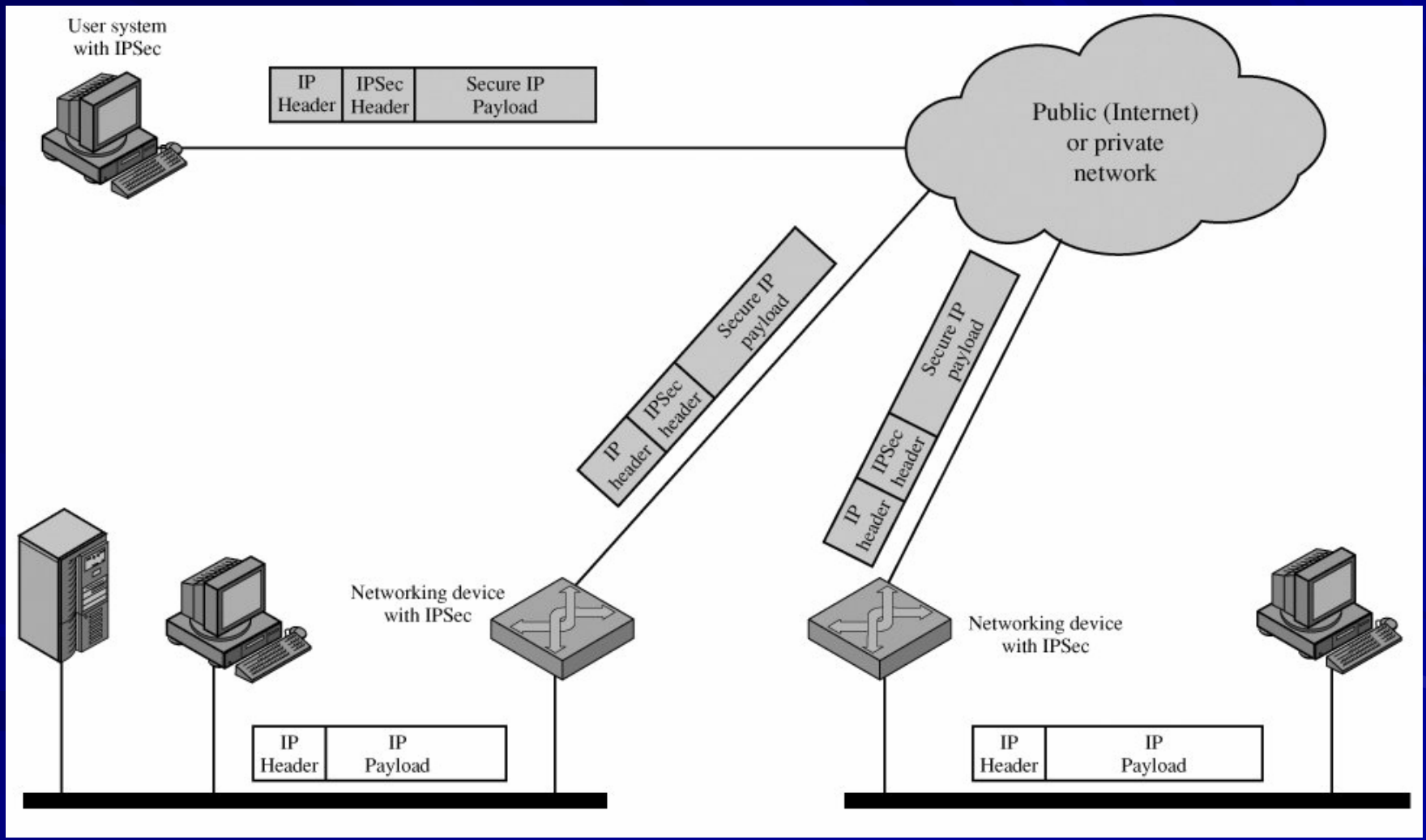
3. IPsec
Tổng quan

- Là một giao thức bảo mật chính tại lớp Mạng (Network Layer – OSI) hoặc lớp Internet (Internet Layer – TCP/IP).
- IPsec là yếu tố quan trọng để xây dựng mạng riêng ảo (VPN – Virtual Private Networks).
- Bao gồm các giao thức chứng thực, các giao thức mã hoá, các giao thức trao đổi khoá:
  - AH (Authentication header): được sử dụng để xác định nguồn gốc gói tin IP và đảm bảo tính toàn vẹn của nó.
  - ESP (Encapsulating Security Payload): được sử dụng để chứng thực và mã hoá gói tin IP (phần payload hoặc cả gói tin).
  - IKE (Internet key exchange): được sử dụng để thiết lập khoá bí mật cho người gởi và người nhận.

3. IPsec
Tổng quan

- Ứng dụng của IPsec:
  - Bảo mật kết nối giữa các chi nhánh văn phòng qua Internet.
  - Bảo mật truy cập từ xa qua Internet.
  - Thực hiện những kết nối Intranet và Extranet với các đối tác (Partners).
  - Nâng cao tính bảo mật trong thương mại điện tử.

3. IPsec
Tổng quan



3. IPsec
Tổng quan

- Ví dụ minh hoạ:
  - Khi Alice muốn giao tiếp với Bob sử dụng IPsec, Alice trước tiên phải chọn một tập hợp các giải thuật mã hóa và các thông số, sau đó thông báo cho Bob về lựa chọn của mình.
  - Bob có thể chấp nhận lựa chọn của Alice hoặc thương lượng với Alice cho một tập hợp khác nhau của các giải thuật và các thông số.
  - Một khi các giải thuật và các thông số được lựa chọn, IPsec thiết lập sự kết hợp bảo mật (Security Association - SA) giữa Alice và Bob cho phần còn lại của phiên làm việc.

3. IPsec

Security Association (SA)

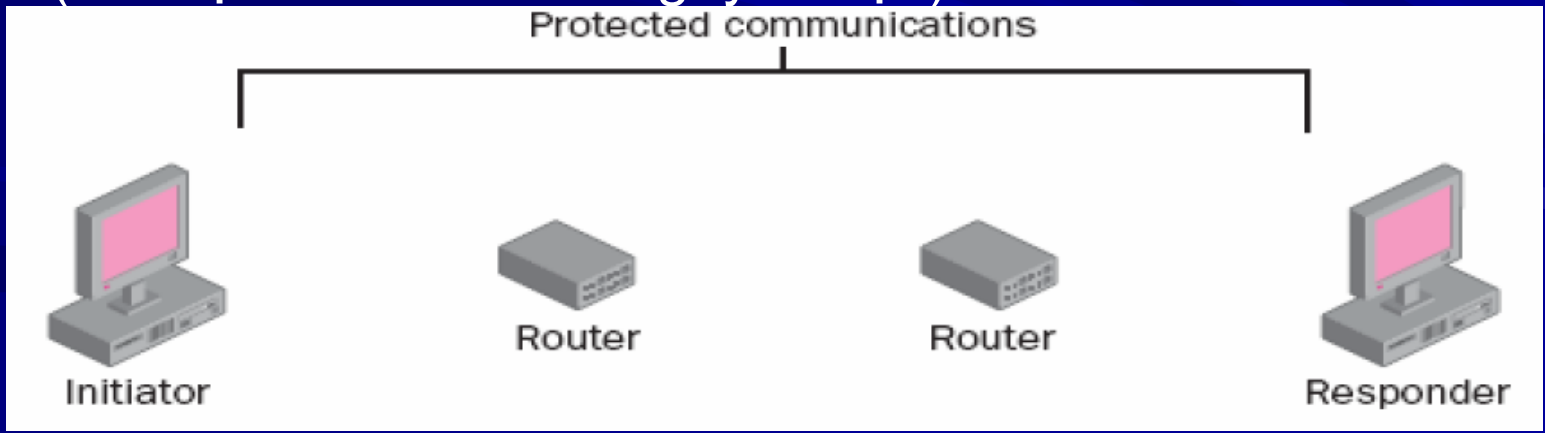
- Một SA cung cấp các thông tin sau:
  - Chỉ mục các thông số bảo mật (SPI - Security parameters index): là một chuỗi nhị phân 32 bit được sử dụng để xác định một tập cụ thể của các giải thuật và thông số dùng trong phiên truyền thông. SPI được bao gồm trong cả AH và ESP để chắc chắn rằng cả hai đều sử dụng cùng các giải thuật và thông số.
  - Địa chỉ IP đích.
  - Giao thức bảo mật: AH hay ESP. IPsec không cho phép AH hay ESP sử dụng đồng thời trong cùng một SA.

3. IPsec

Các phương thức của IPsec

IPsec bao gồm 2 phương thức:

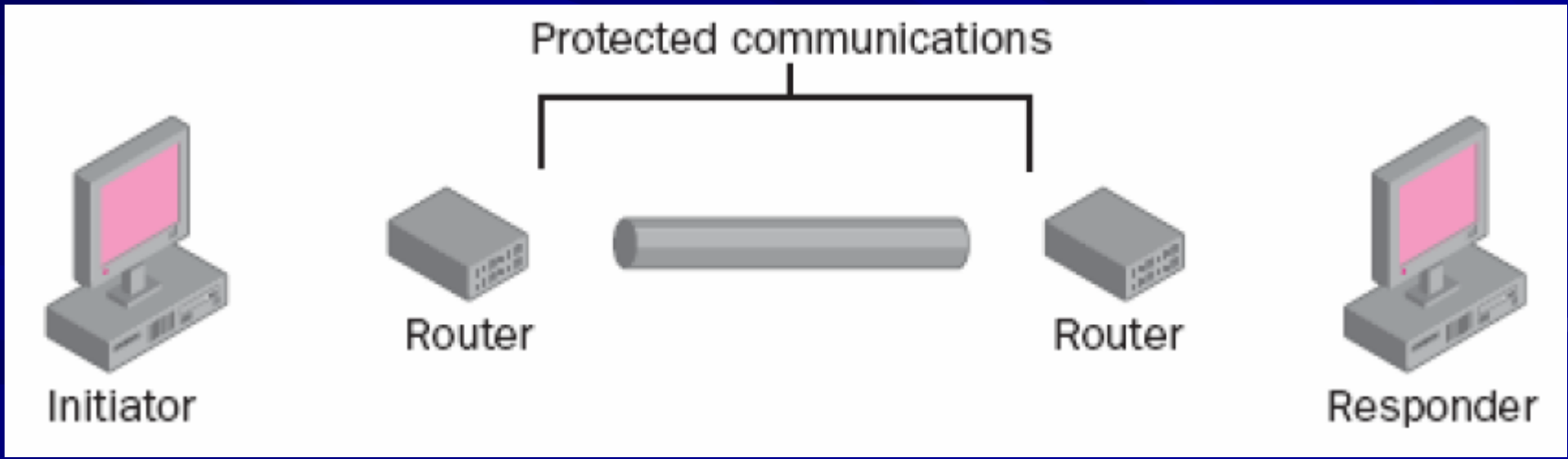
- Phương thức Vận chuyển (Transport Mode): sử dụng Transport Mode khi có yêu cầu lọc gói tin và bảo mật điểm-tới-điểm. Cả hai trạm cần hỗ trợ IPSec sử dụng cùng giao thức xác thực và không được đi qua một giao tiếp NAT nào. Nếu dữ liệu đi qua giao tiếp NAT sẽ bị đổi địa chỉ IP trong phần header và làm mất hiệu lực của ICV (Giá trị kiểm soát tính nguyên vẹn)



3. IPsec

Các phương thức của IPsec

- Phương thức đường hầm (Tunel mode): sử dụng mode này khi cần kết nối Site-to-Site thông qua Internet (hay các mạng công cộng khác). Tunel Mode cung cấp sự bảo vệ Gateway-to-Gateway (cửa-đến-cửa).

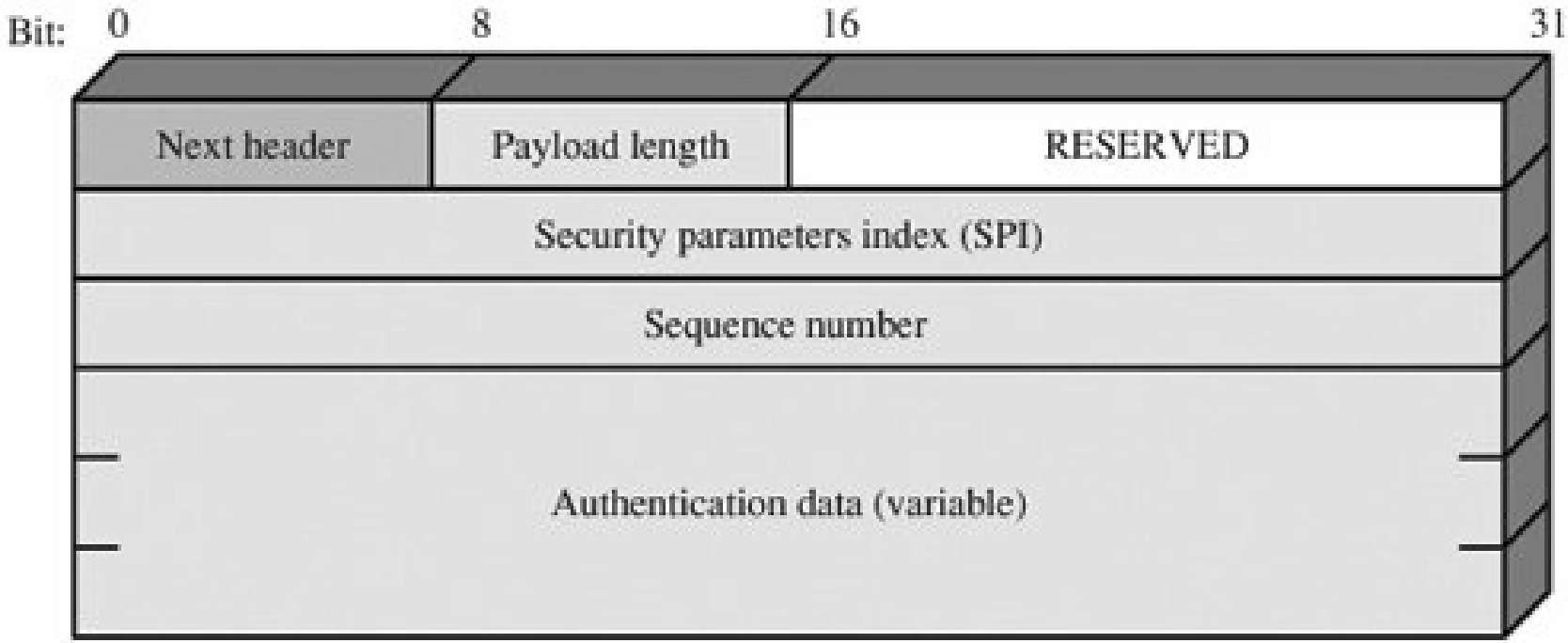


3. IPsec
Định dạng AH

- Authentication Header (AH) bao gồm các vùng:
  - Next Header (8 bits): xác định header kế tiếp.
  - Payload Length (8 bits): chiều dài của Authentication Header theo từ 32-bit, trừ 2.
  - Reserved (16 bits): sử dụng cho tương lai.
  - Security Parameters Index (32 bits): xác định một SA.
  - Sequence Number (32 bits): một giá trị tăng đơn điệu.
  - Authentication Data (variable): Một vùng có chiều dài biến đổi (phải là một số nguyên của từ 32 bits) chứa giá trị kiểm tra tính toàn vẹn (Integrity Check Value - ICV) đối với gói tin này.

3. IPsec

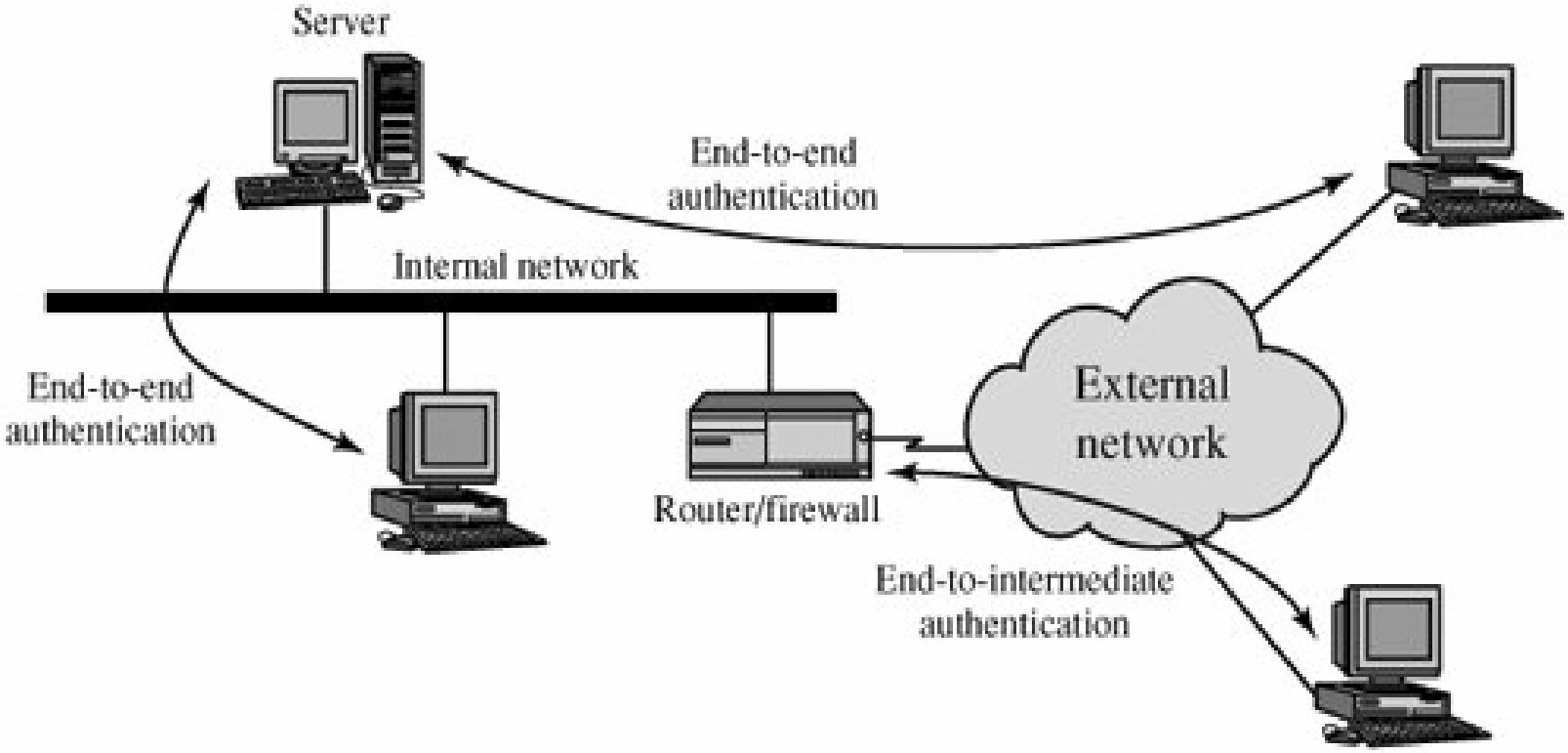
Định dạng AH



IPSec Authentication Header

3. IPsec

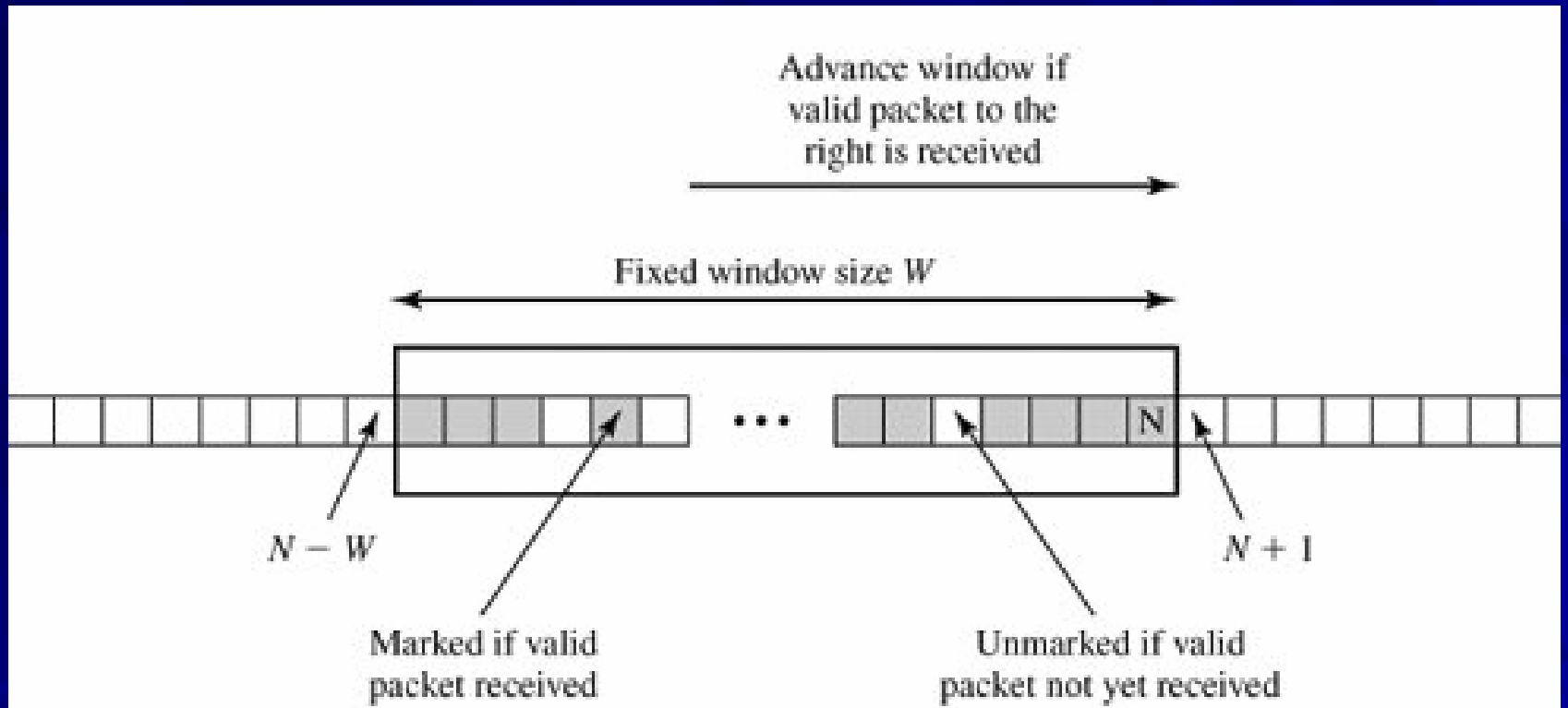
Các phương thức chứng thực



End-to-End versus End-to-Intermediate Authentication

3. IPsec

Cơ chế chống Replay attack



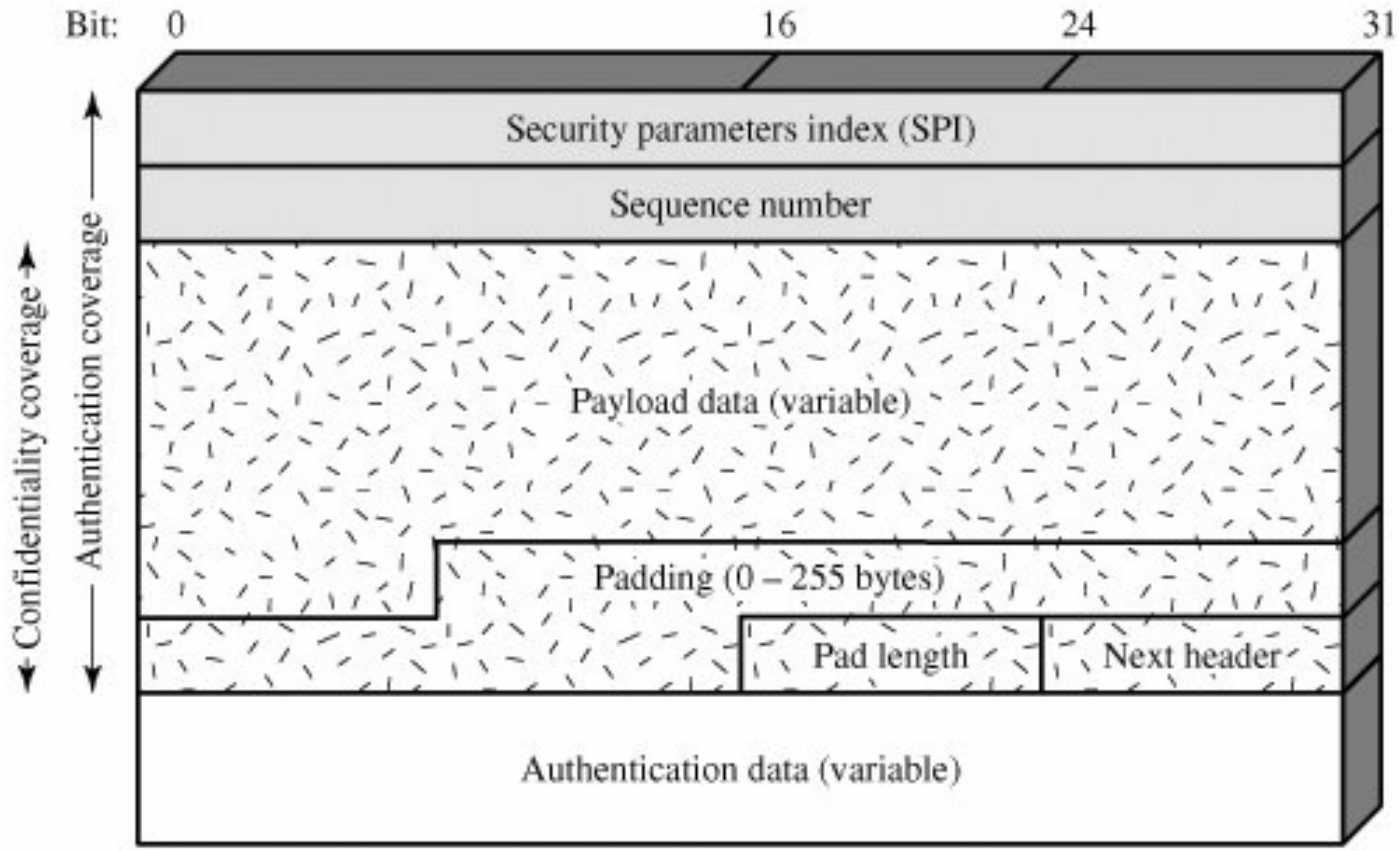
Antireplay Mechanism

3. IPsec
Định dạng ESP

- Một gói ESP chứa các vùng sau:
  - Security Parameters Index (32 bits): xác định một SA.
  - Sequence Number (32 bits): một giá trị đếm tăng đơn điệu, cung cấp chức năng anti-replay (giống AH).
  - Payload Data (variable): đây là một segment ở transport-level (transport mode) hoặc gói IP (tunnel mode) được bảo vệ bởi việc mã hoá.
  - Padding (0255 bytes):.
  - Pad Length (8 bits): chỉ ra số byte vùng đứng ngay trước vùng này.
  - Next Header (8 bits): chỉ ra kiểu dữ liệu chứa trong vùng payload data bằng cách chỉ ra header đầu tiên của vùng payload này.
  - Authentication Data (variable): một vùng có chiều dài biến đổi (phải là một số nguyên của từ 32-bit) chứa ICV được tính bằng cách gói ESP trừ vùng Authentication Data.

3. IPsec

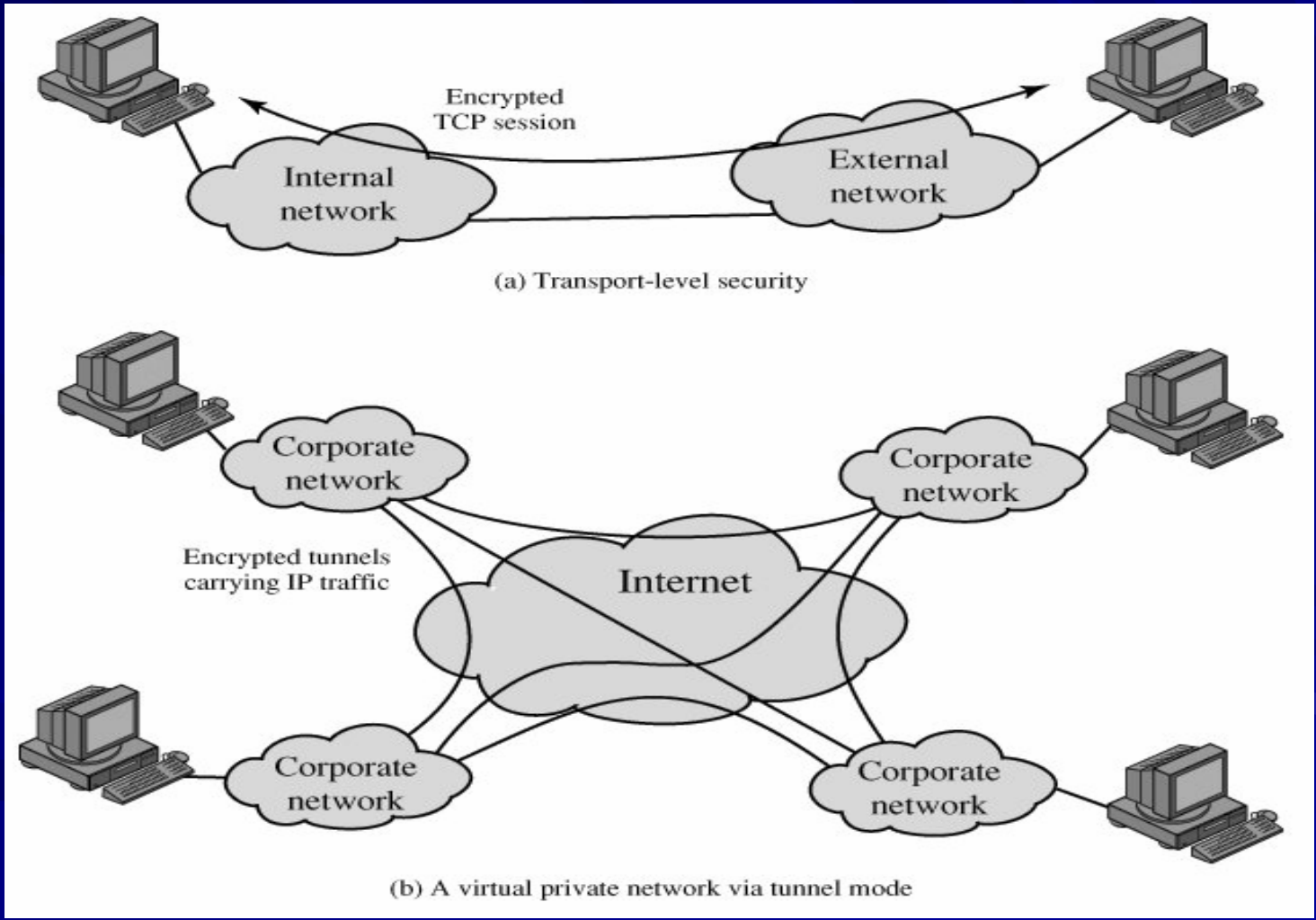
Định dạng ESP



IPSec ESP format

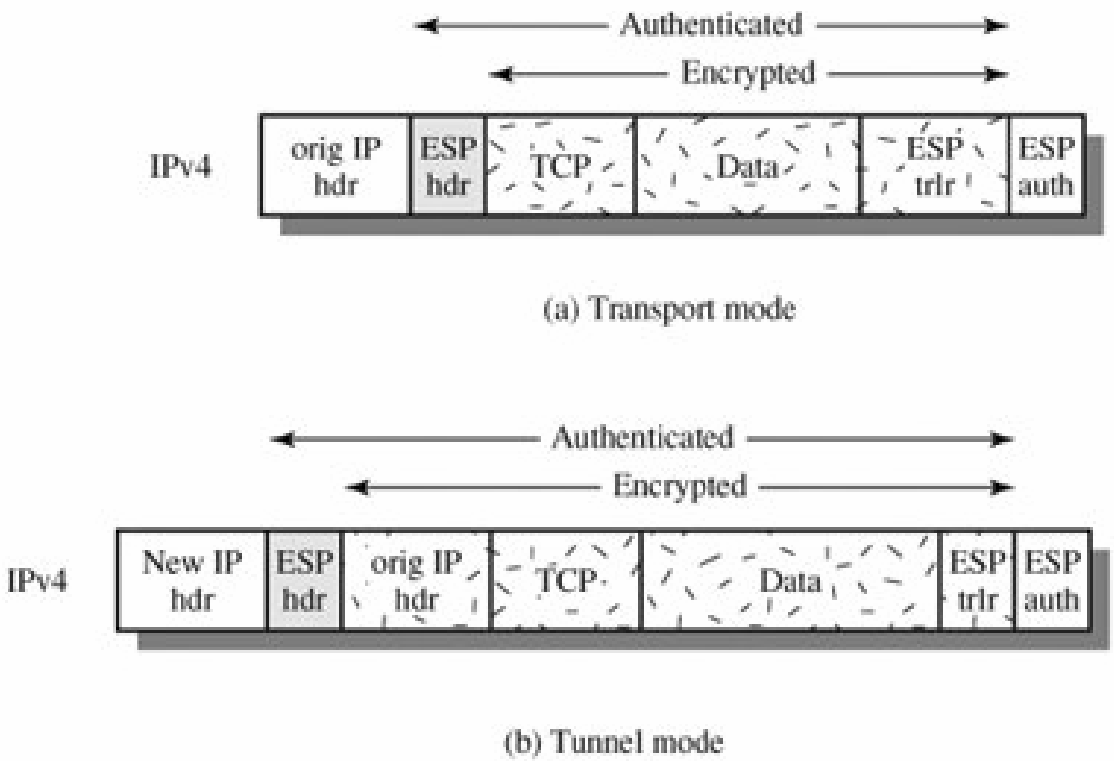
3. IPsec

Các phương thức mã hoá



3. IPsec

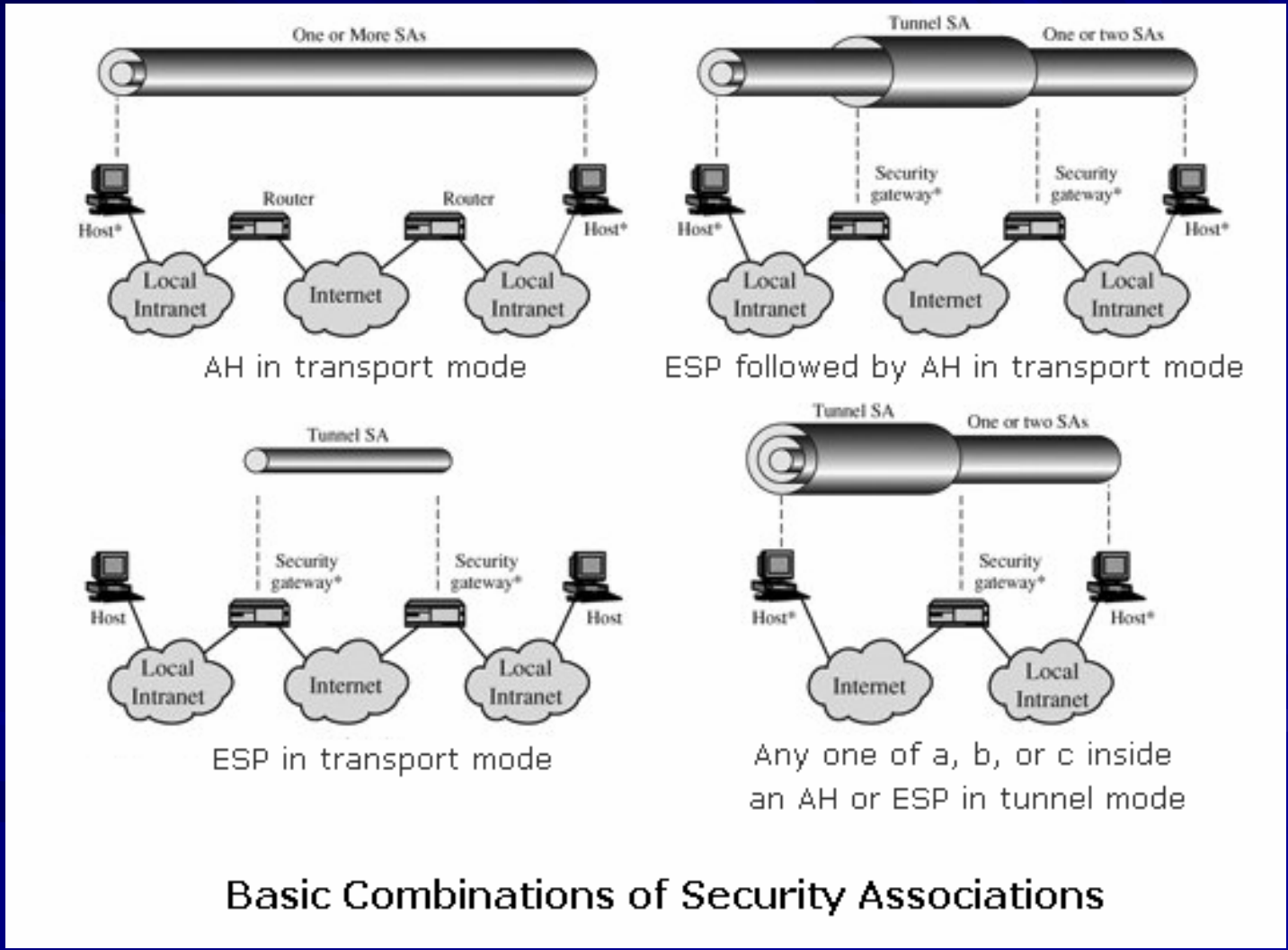
Các phương thức mã hoá



Scope of ESP Encryption and Authentication

3. IPsec

Sự kết hợp của các SA



3. IPsec

Các giải thuật mã hoá và chứng thực

- Các giải thuật sử dụng để mã hoá và chứng thực bao gồm:
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish

4. SSL/TLS

Tổng quan

- Giao thức SSL (Secure Socket Layer Protocol) và giao thức TLS (Transport Layer Security Protocol) là những giao thức bảo mật tại lớp vận chuyển được dùng chủ yếu trong thực tế.
- Được thiết kế và phát triển bởi Netscape từ năm 1994, SSL được sử dụng để bảo vệ những ứng dụng World-Wide-Web và các giao dịch điện tử.
- TLS là một phiên bản sửa đổi của SSL v3, được xuất bản năm 1999 như là tiêu chuẩn bảo mật lớp vận chuyển bởi tổ chức Internet Engineering Task Force (IETF). Chỉ có khác biệt nhỏ giữa TLS và SSL v3.

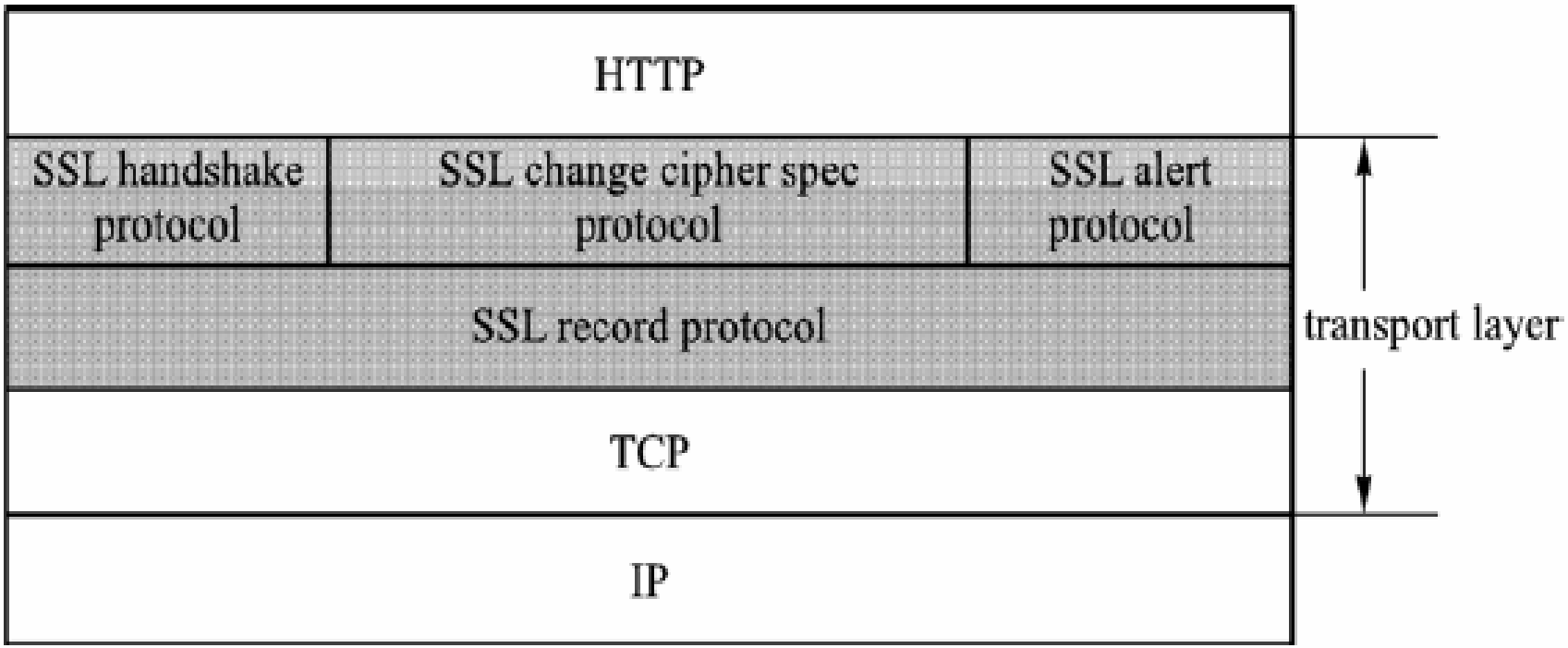
4. SSL/TLS

Các thành phần của SSL

- Giao thức SSL bao gồm 2 thành phần:
  - Thành phần thứ nhất được gọi là record protocol, được đặt trên đỉnh của các giao thức lớp vận chuyển.
  - Thành phần thứ hai được đặt giữa các giao thức tầng ứng dụng (như HTTP) và record protocol , bao gồm các giao thức:
    - Handshake protocol
    - Change-cipher-spec protocol
    - Alert protocol

4. SSL/TLS

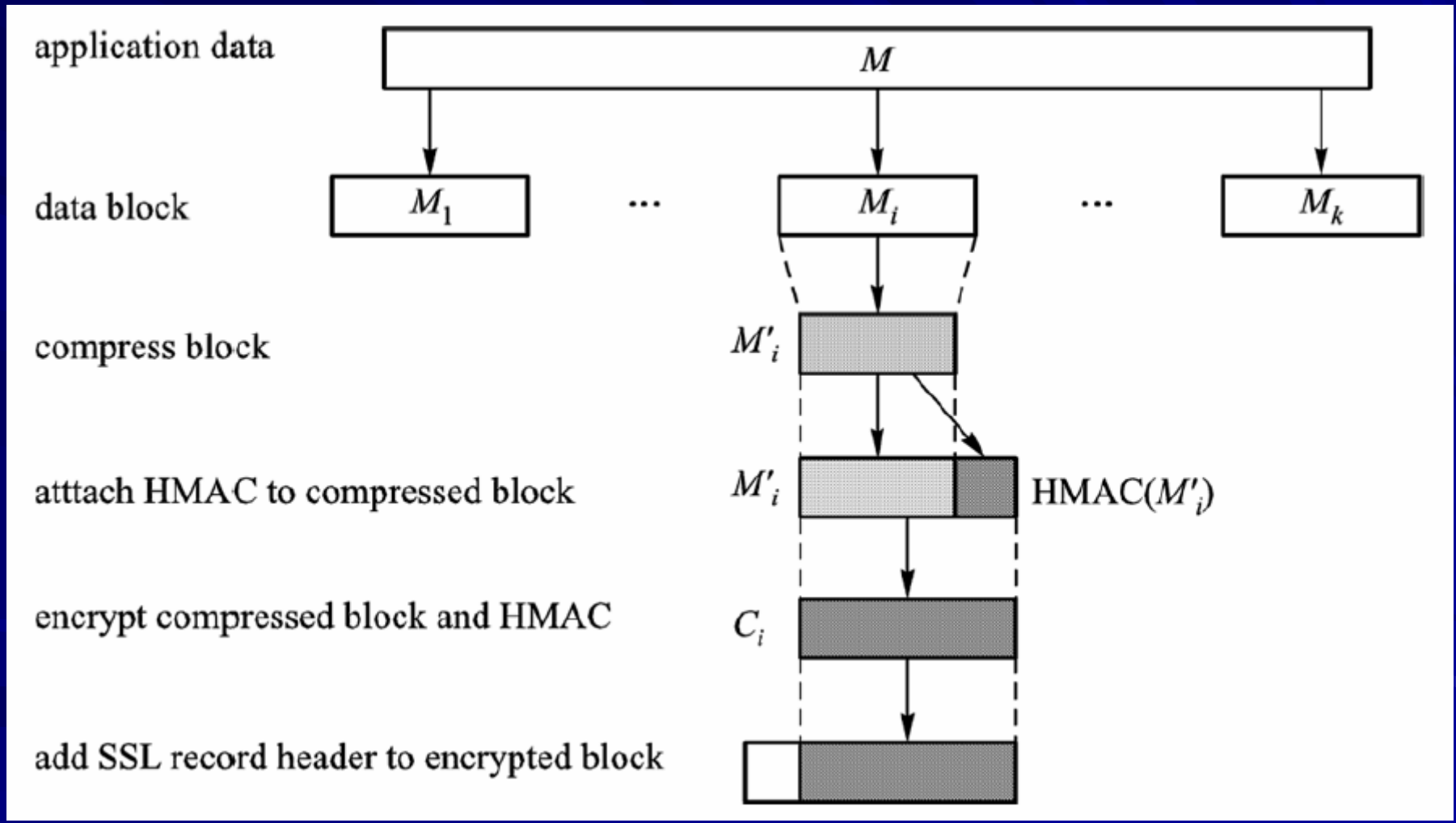
Cấu trúc SSL



SSL structure

4. SSL/TLS

Giao thức bản ghi (record protocol) của SSL



4. SSL/TLS

Các giao thức của SSL

- Giao thức bắt tay (handshake protocol) thành lập các giải thuật mã hóa, giải thuật nén, và các thông số sẽ được sử dụng bởi cả hai bên trong việc trao đổi dữ liệu được mã hóa. Sau đó, các giao thức bản ghi (record protocol) chịu trách nhiệm phân chia thông điệp vào các khối, nén mỗi khối, chứng thực chúng, mã hóa chúng, thêm header vào mỗi khối, và sau đó truyền đi các khối kết quả.
- Các giao thức đổi mật mã (change-cipher-spec protocol) cho phép các bên giao tiếp có thể thay đổi các giải thuật hoặc các thông số trong một phiên truyền thông.
- Các giao thức cảnh báo (alert protocol) là một giao thức quản lý, nó thông báo cho các bên tham gia truyền thông khi có vấn đề xảy ra.

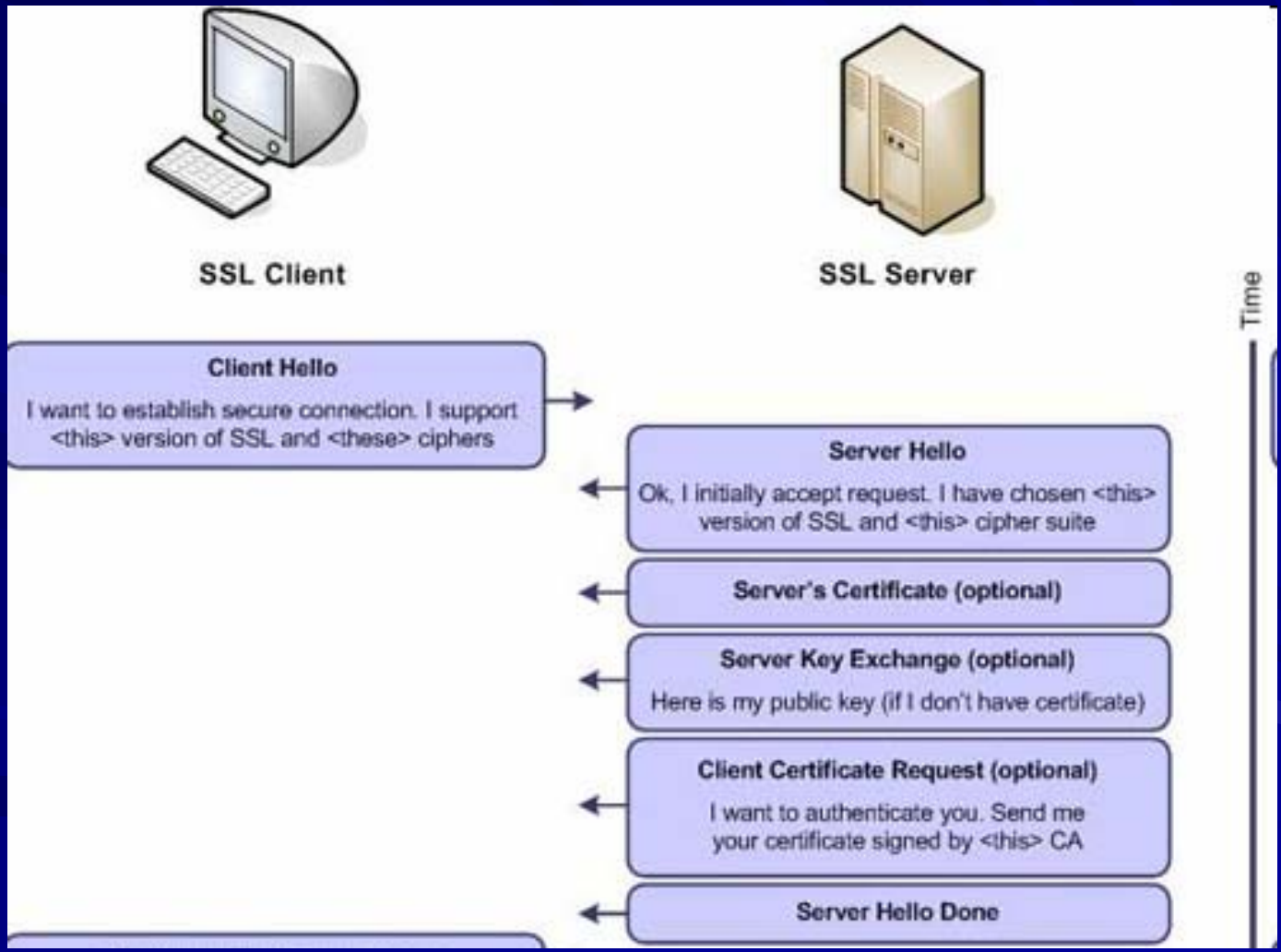
4. SSL/TLS

Giao thức bắt tay của SSL

- Phase 1: chọn giải thuật mã hoá. Các giải thuật được chọn có thể là RSA, AES-128, 3DES, RC6, SHA-1… Client sẽ khởi tạo với một thông điệp client-hello.
- Phase 2: server xác thực và trao đổi khoá. Server sẽ gởi cho client:
  - Chứng chỉ khoá công khai của server
  - Thông tin trao đổi khoá của server
  - Yêu cầu chứng chỉ khoá công khai của client
- Phase 3: client xác thực và trao đổi khoá. Client trả lời cho server các thông tin:
  - Chứng chỉ khoá công khai của client
  - Thông tin trao đổi khoá của client
- Phase 4: hoàn thành việc bắt tay. Server và client sẽ gởi cho nhau thông điệp finish.

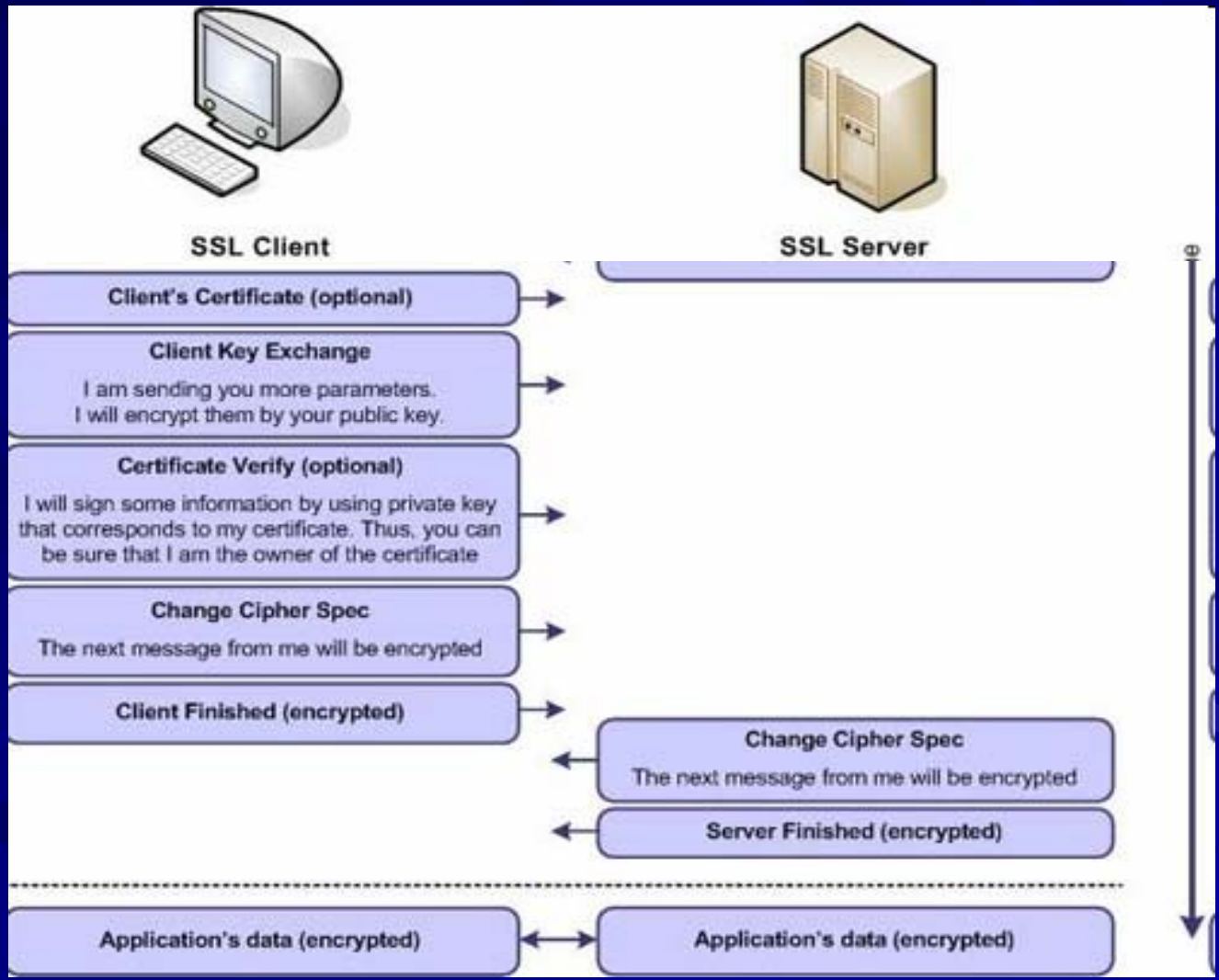
4. SSL/TLS

Quá trình thiết lập kết nối SSL



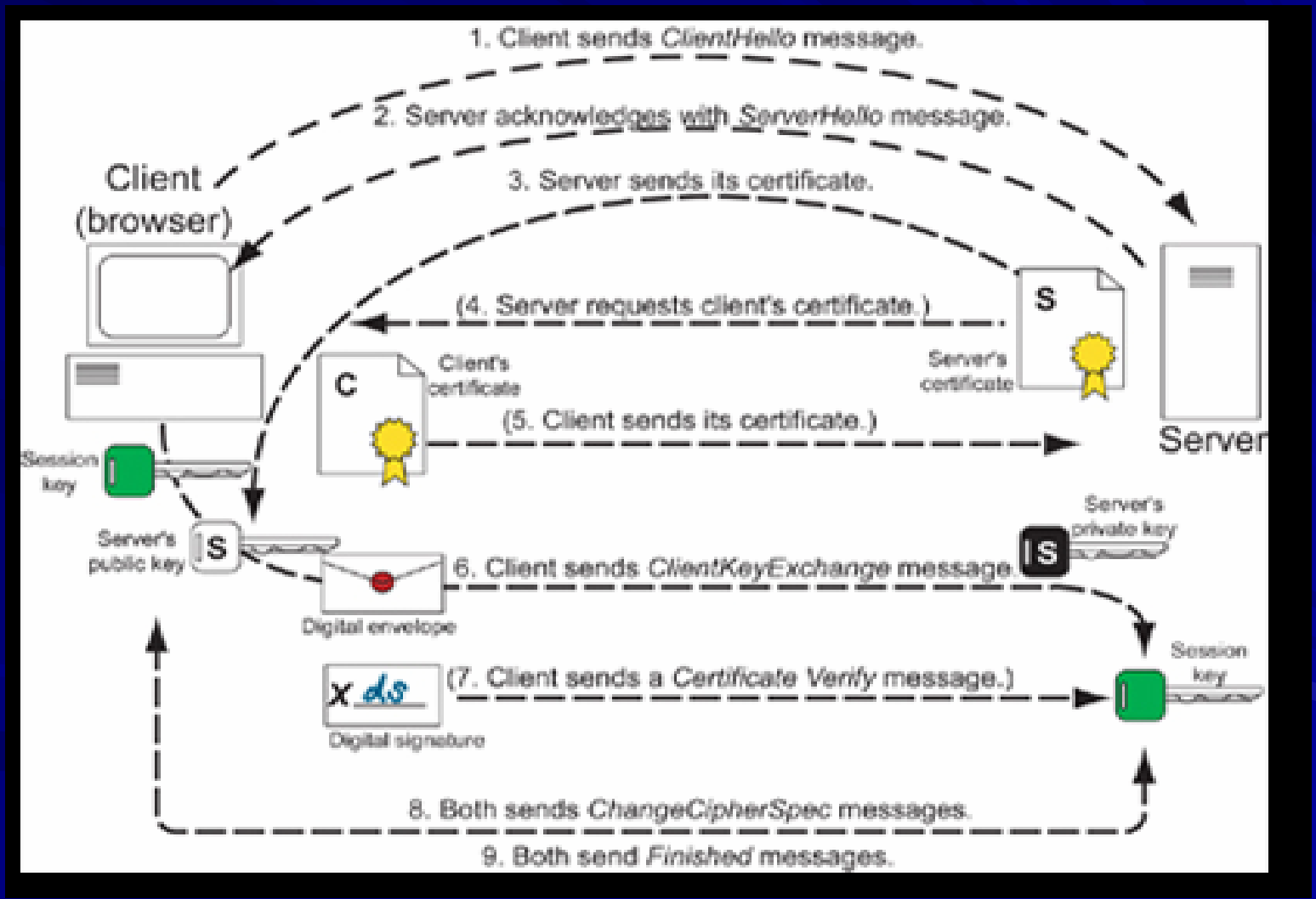
4. SSL/TLS

Quá trình thiết lập kết nối SSL



4. SSL/TLS

Quá trình thiết lập kết nối SSL

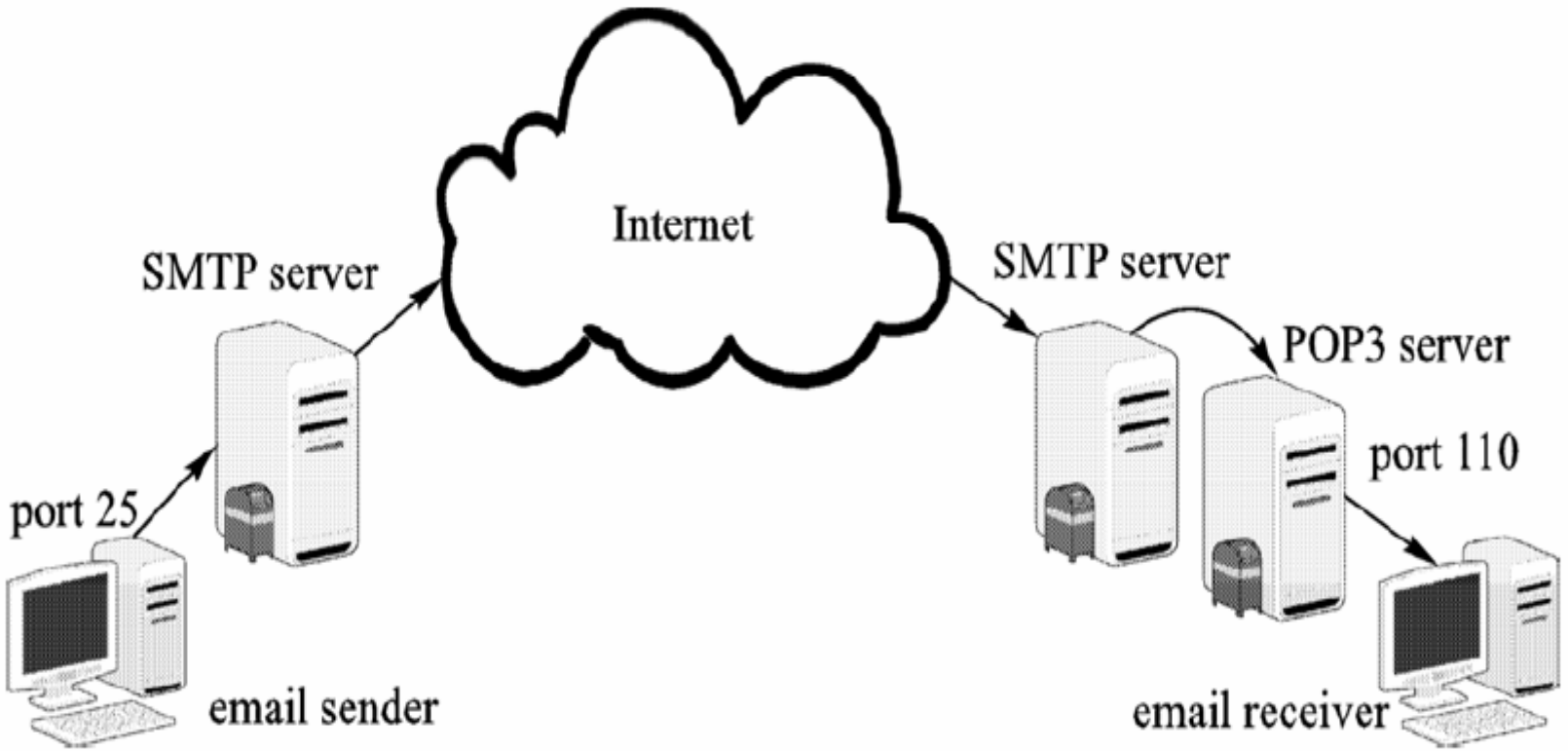


5. PGP và S/MIME
Tổng quan

- Có nhiều giao thức bảo mật cho tầng ứng dụng. Hầu hết đều tập trung vào bảo mật cho E-mail và bảo mật cho việc đăng nhập từ xa. Được sử dụng nhiều nhất là:
  - PGP (Pretty Good Privacy)
  - S/MIME (Secure/Multipurpose Internet Mail Extension).
  - SSH (Secure Shell).
  - Kerberos (dùng chứng thực cho mạng cục bộ).

5. PGP và S/MIME

Tổng quan



SMTP and POP3 flow diagram

5. PGP và S/MIME
Cơ chế bảo mật E-mail

- Bảo mật email là một ứng dụng cổ điển của các giải thuật mã hoá.
- Cho E và D biểu thị một giải thuật mã hoá và giải mã khoá đối xứng. Cho E^ và D^ biểu thị một giải thuật mã hoá và giải mã khoá công khai.
- Giả sử Alice muốn chứng minh với Bob là email M mà Bob nhận được là từ Alice gởi, Alice có thể gởi chuỗi sau cho Bob:

$$M \| \hat{E}_{K_A^r}(H(M)) \| \mathrm{CA}\langle K_A^u \rangle,$$

5. PGP và S/MIME
Cơ chế bảo mật E-mail

- Với K^u_A và K^r_A lần lượt là khoá công khai và khoá riêng của Alice.
- Sau khi nhận được $M \| S_M \| \mathrm{CA}\langle K^u_A \rangle$ từ Alice, với S_M là chữ ký vào M sử dụng khoá riêng của Alice. Trước tiên Bob so sánh chữ ký của CA trên chứng chỉ khoá công khai $CA(K^u_A)$ và rút trích K_A từ đó. Sau đó Bob rút trích M và so sánh

$$S_M = \tilde{E}_{K^r_A}(H(M))$$

Nếu đúng, Bob có thể tin rằng M đến từ Alice.

5. PGP và S/MIME
Cơ chế bảo mật E-mail

- Giả sử Alice muốn đảm bảo rằng M giữ được tính bí mật trong suốt quá trình truyền và cô ấy biết khoá công khai của Bob (K^u_B), cô ấy sẽ gởi chuỗi sau cho Bob:

$$E_{K_A}(M) \,\|\, \hat{E}_{K_B^u}(K_A),$$

  với K_A là khoá bí mật của Alice.

- Sau khi nhận được chuỗi này từ Alice, trước tiên Bob sẽ sử dụng khoá riêng của mình để giải mã:

$$\hat{D}_{K_B^r}(\hat{E}_{K_B^u}(K_A)) = K_A.$$

- Kế đó, Bob sử dụng K_A giải mã để thu được M:

$$D_{K_A}(E_{K_A}(M)) = M.$$

5. PGP và S/MIME

Tổng quan về PGP

- PGP có thể được sử dụng để chứng thực một thông điệp, mã hoá thông điệp, hoặc cả chứng thực lẫn mã hoá.
- PGP cho phép những định dạng tổng quát như chứng thực, nén ZIP, mã hoá...
- Phiên bản đầu tiên của PGP do Phil Zimmermann công bố vào năm 1991. Đến nay đã có nhiều cải tiến, trở thành một giải pháp mã hoá cho các công ty lớn, chính phủ, cá nhân, trên máy tính xách tay, máy để bàn, máy chủ...
- Kể từ năm 2002, PGP đã được đa dạng hoá thành một tập hợp ứng dụng mật mã và có thể đặt dưới sự quản trị của một máy chủ. Các ứng dụng PGP bao gồm thư điện tử, chữ ký số, mật mã hoá ổ đĩa cứng, bảo mật tập tin thư mục, tập tin nén tự giải mã, xoá tập tin an toàn...

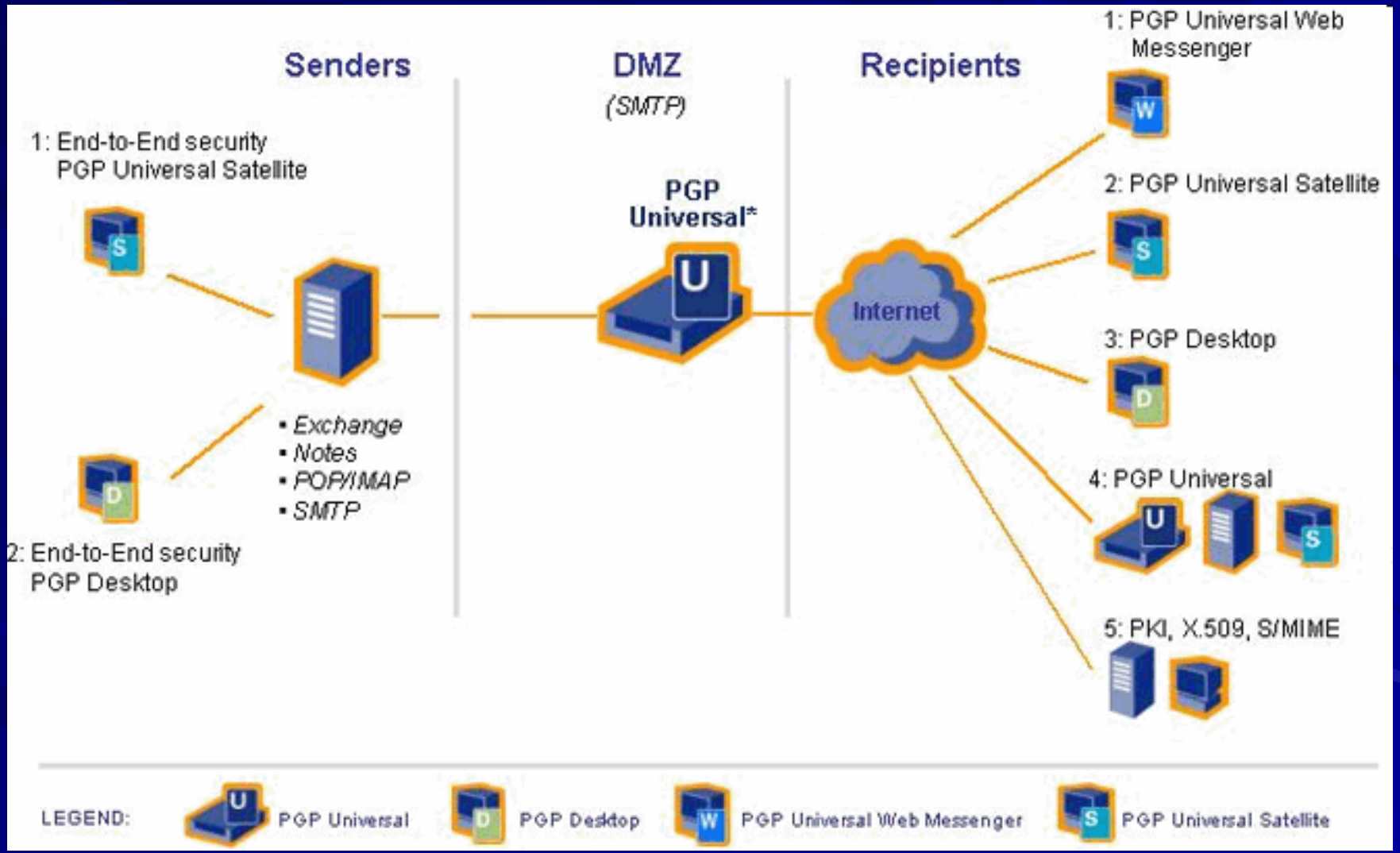
5. PGP và S/MIME

Tổng quan về PGP

- Phiên bản PGP Universal 2.x dành cho máy chủ cho phép triển khai ứng dụng tập trung, thiết lập chính sách an ninh và lập báo cáo. Phần mềm này được dùng để mật mã hóa thư điện tử một cách tự động tại cổng ra vào (gateway) và quản lý các phần mềm máy khách PGP Desktop 9.x. Nó làm việc với máy chủ khóa công khai PGP (gọi là PGP Global Directory) để tìm kiếm khóa của người nhận và có khả năng gửi thư điện tử an toàn ngay cả khi không tìm thấy khóa của người nhận bằng cách sử dụng phiên làm việc HTTPS.
- Các phiên bản mới của PGP cho phép sử dụng cả 2 tiêu chuẩn: OpenPGP và S/MIME.

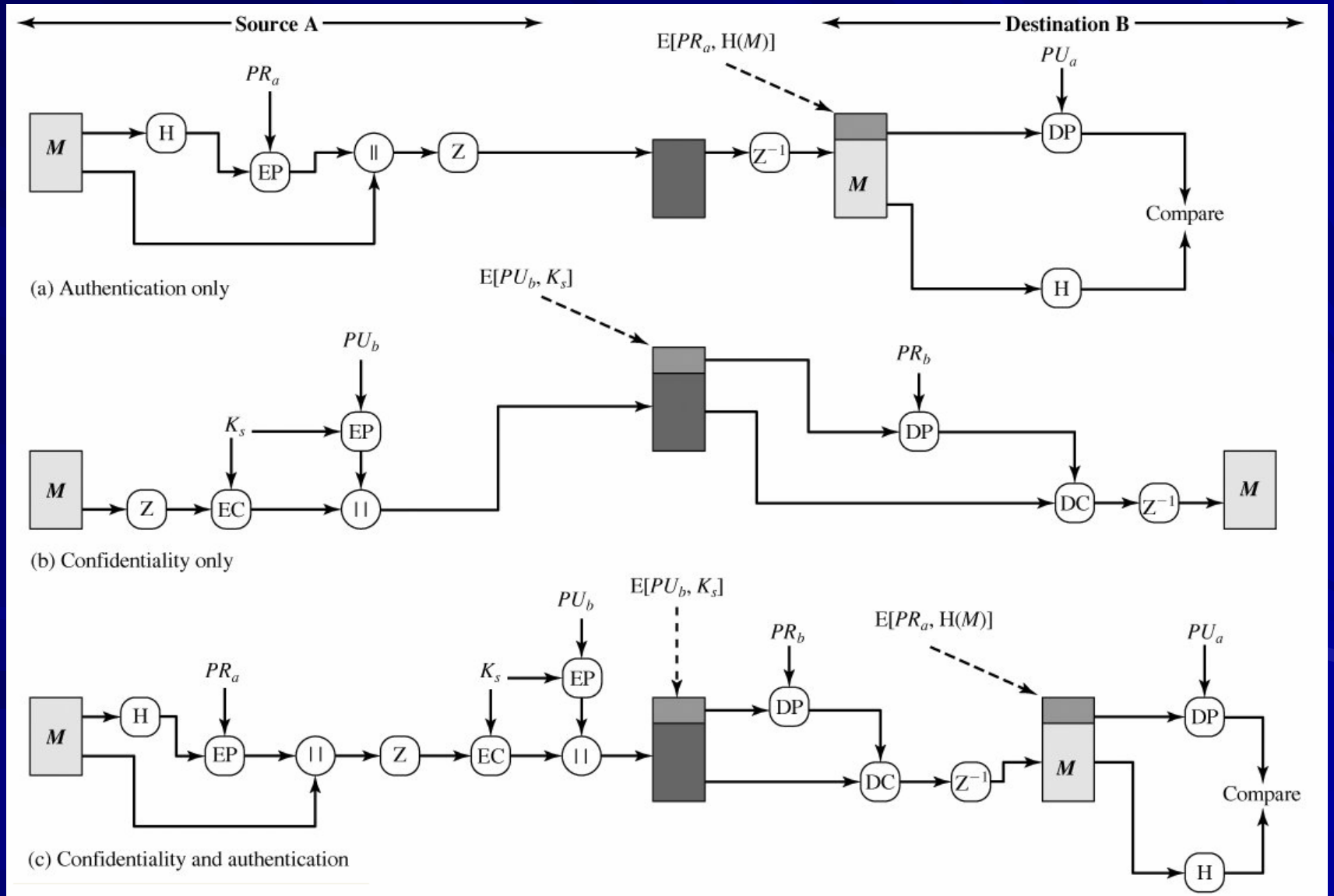
5. PGP và S/MIME

Tổng quan về PGP



5. PGP và S/MIME

Các chức năng của PGP



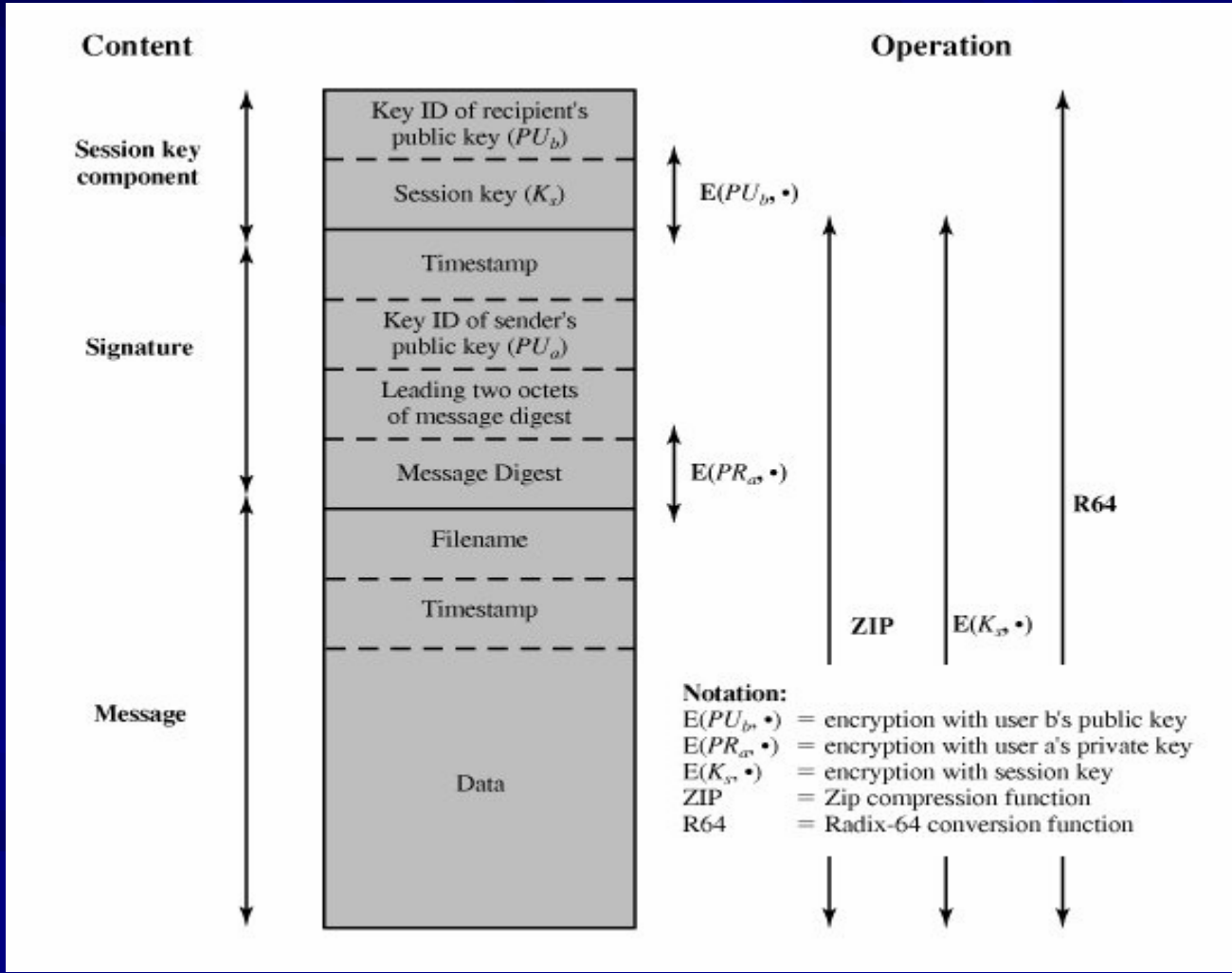
5. PGP và S/MIME

Các chức năng của PGP

- Chú thích:
  - K_s: session key dùng trong mã hoá symmetric
  - Pr_a: private key của user A
  - PU_a: public key of user A
  - EP: mã hoá public-key (asymmetric)
  - DP: giải mã public-key (asymmetric)
  - EC: mã hoá symmetric
  - DC: giải mã symmetric
  - H: hàm băm
  - ||: kết nối, ghép chuỗi
  - Z: nén sử dụng giải thuật ZIP
  - R64: convert sang định dạng ASCII 64 bit

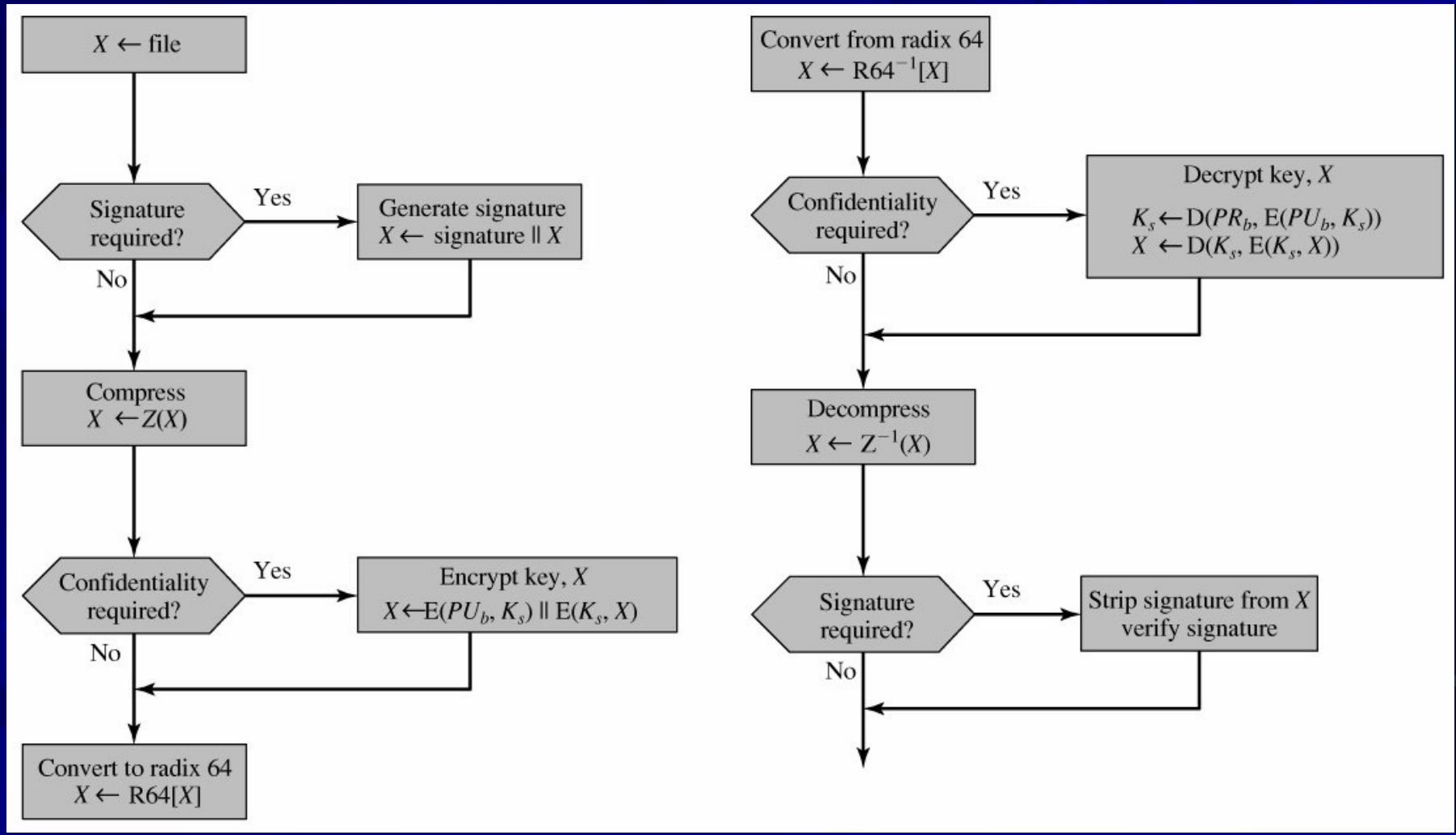
5. PGP và S/MIME

Định dạng tổng quát của một thông điệp PGP



5. PGP và S/MIME

Truyền và nhận thông điệp PGP



5. PGP và S/MIME

Một số đặc tính của PGP

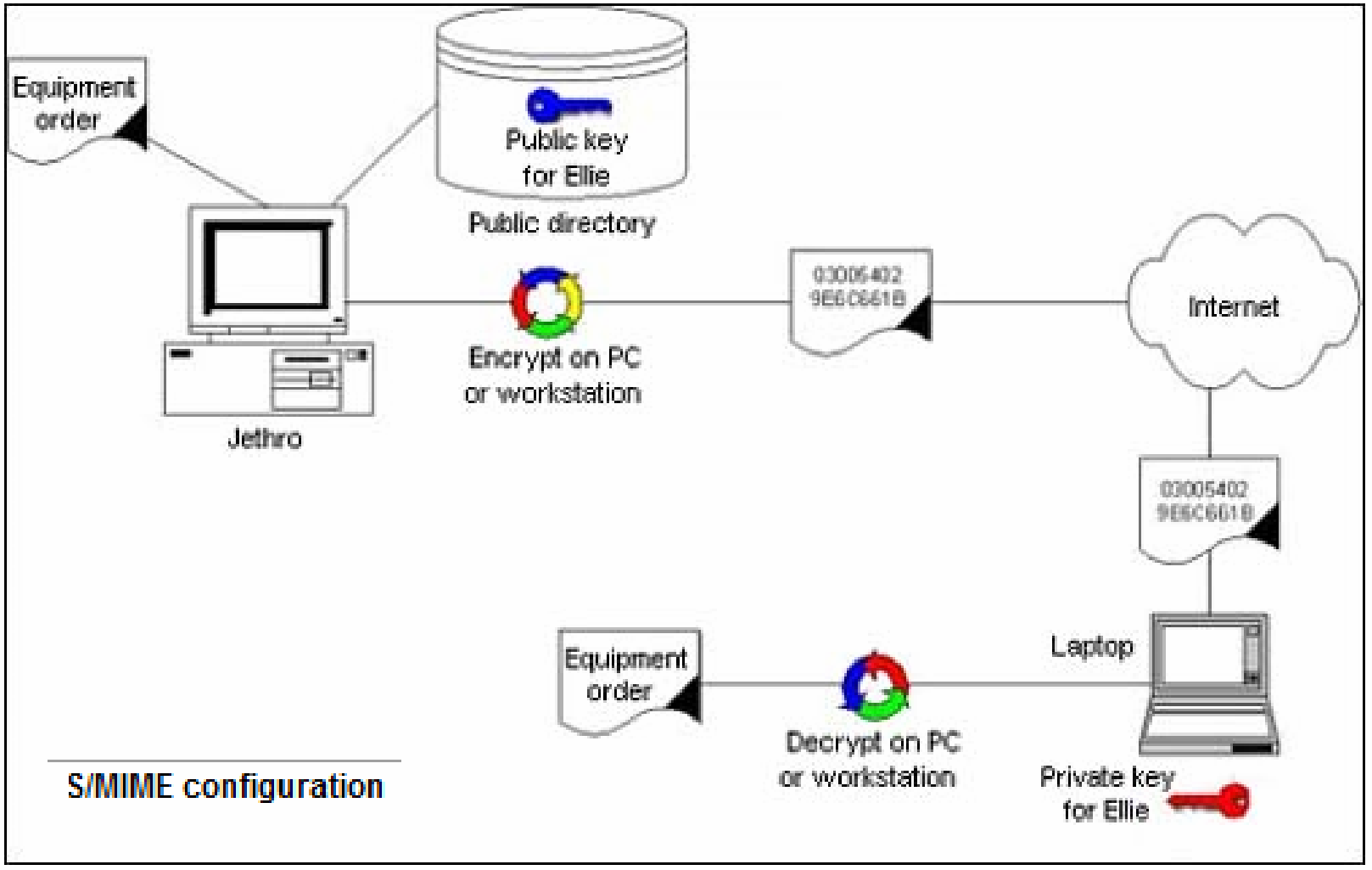
Đặc tính	PGP 2.x (RFC 1991)	OpenPGP (RFC 2440)
Định dạng khóa	Khóa V3	Khóa V4
Thuật toán khóa bất đối xứng	*RSA (mã hóa & chữ ký)	RSA (mã hóa & chữ ký) *DSA (chữ ký) *Elgamal (mã hóa)
Thuật toán khóa đối xứng	*IDEA	IDEA *Triple-DES CAST5 Blowfish AES 128, 192, 256 Twofish
Hàm băm mật mã	*MD5	MD5 *SHA-1 RIPEMD-160 SHA-256 SHA-384 SHA-512
Thuật toán nén	ZIP	ZIP gzip bzip2

5. PGP và S/MIME
S/MIME

- S/MIME (Secure/Multipurpose Internet Mail Extensions)
- Là một chuẩn Internet về định dạng cho email. Hầu như mọi email trên Internet được truyền qua giao thức SMTP theo định dạng MIME.
- S/MIME đưa vào hai phương pháp an ninh cho email: mã hóa email và chứng thực. Cả hai cách đều dựa trên mã hóa bất đối xứng và PKI.

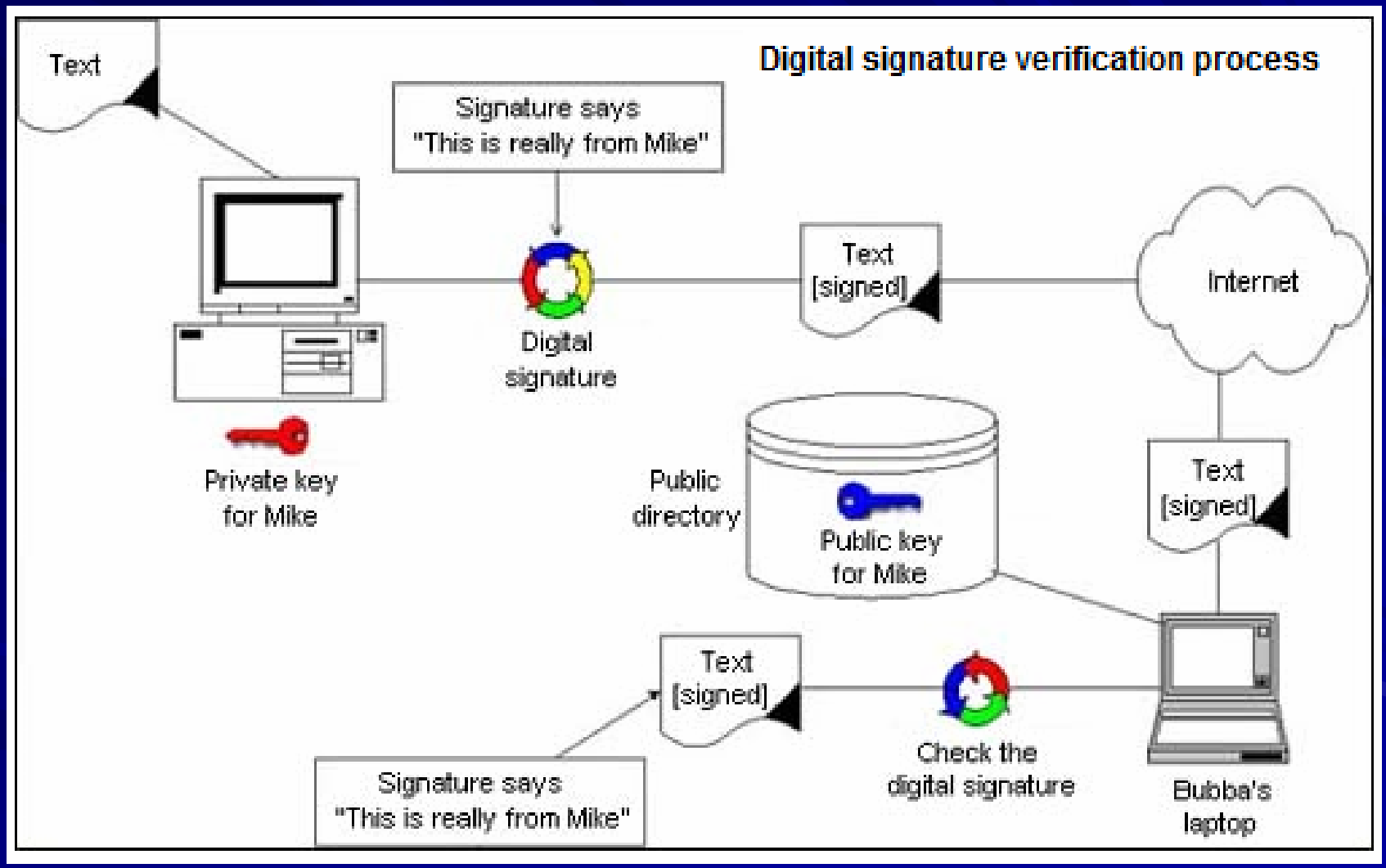
5. PGP và S/MIME

S/MIME



5. PGP và S/MIME

S/MIME



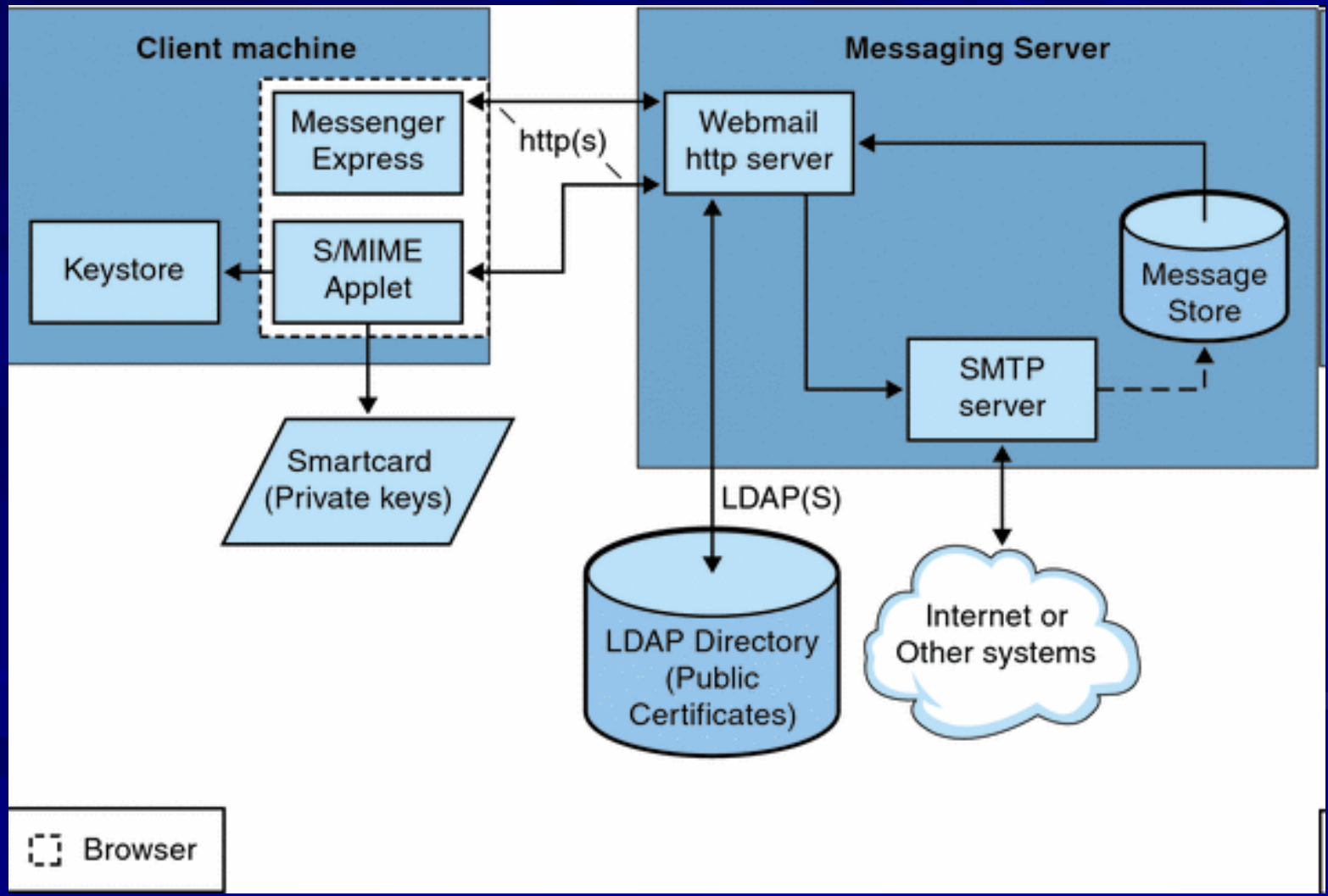
5. PGP và S/MIME
S/MIME

Các tính năng của một Webmail client hỗ trợ S/MIME:

- Tạo ra một chữ ký số cho một email gửi đi để đảm bảo người nhận email tin rằng không có sự can thiệp và được đến từ người gửi.
- Mã hóa một email gửi đi để ngăn chặn bất cứ ai xem, thay đổi... Nội dung của email trước khi đến với người nhận.
- Xác minh chữ ký số của một email đã ký đến với một quá trình liên quan đến một danh sách thu hồi chứng chỉ (CRL).
- Tự động giải mã một email gửi đến để người nhận có thể đọc được nội dung của email.
- Trao đổi chữ ký hoặc email đã được mã hóa với những người dùng khác của S/MIME.

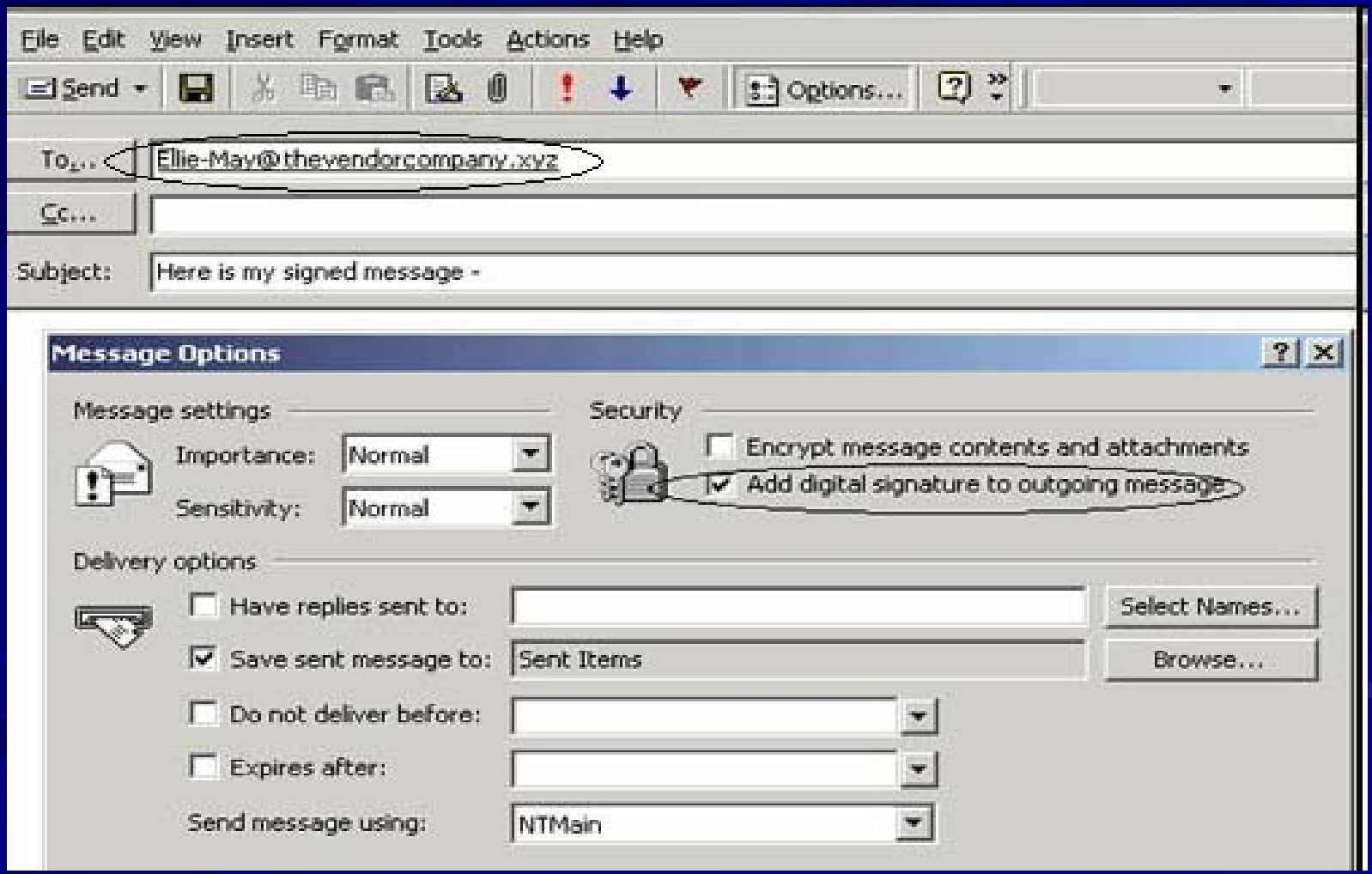
5. PGP và S/MIME

S/MIME



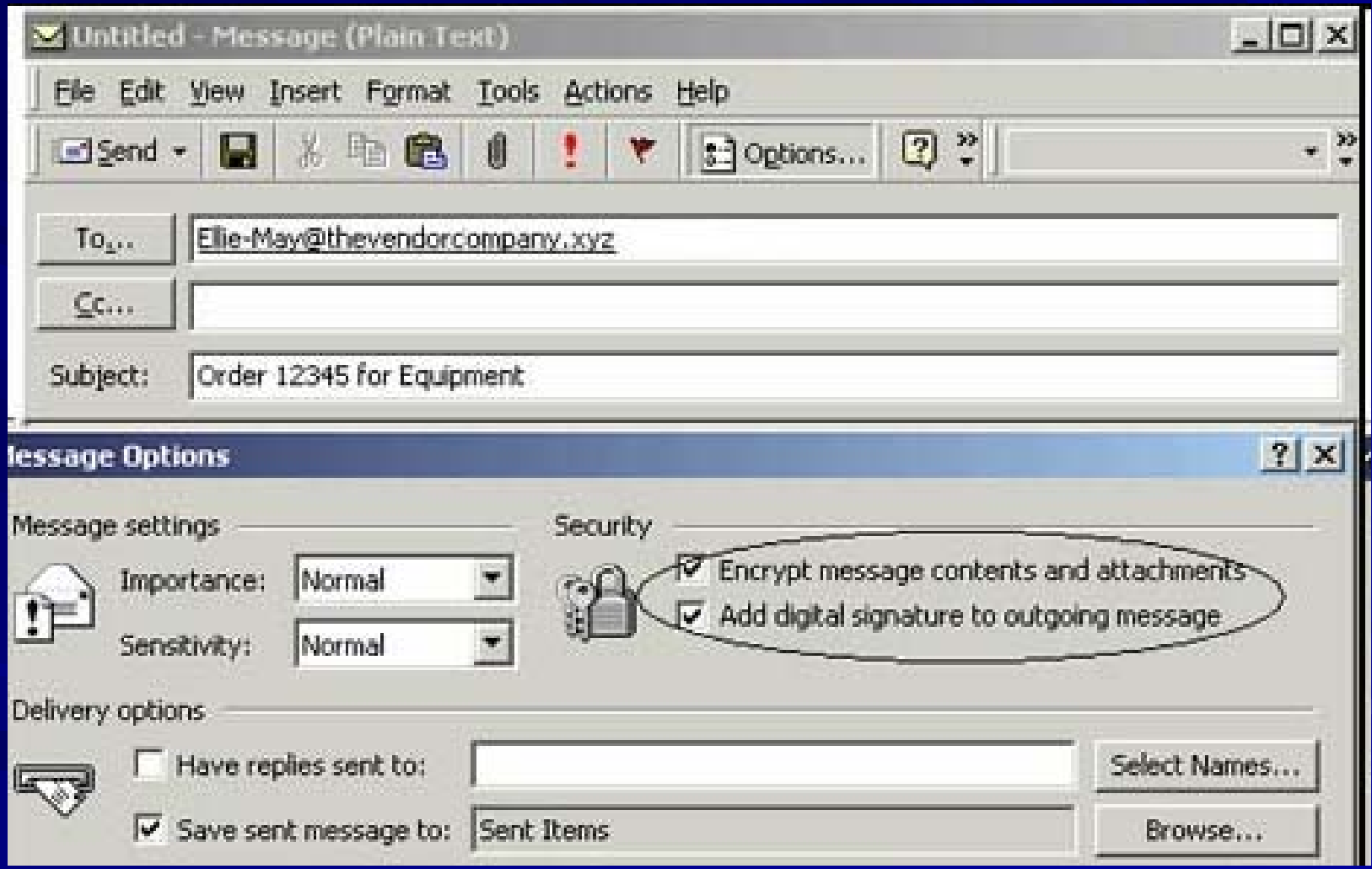
5. PGP và S/MIME

S/MIME



5. PGP và S/MIME

S/MIME



5. PGP và S/MIME

S/MIME

6. Kerberos

6. Kerberos

Tổng quan

- Kerberos là một giao thức mã hoá dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn.
- Giao thức Kerberos có khả năng chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu.
- Mục tiêu khi thiết kế giao thức này là nhằm vào *client-server* và đảm bảo chứng thực cho cả hai chiều.
- Giao thức được xây dựng dựa trên mật mã hóa khóa đối xứng và cần đến một bên thứ ba mà cả hai phía tham gia giao dịch tin tưởng.

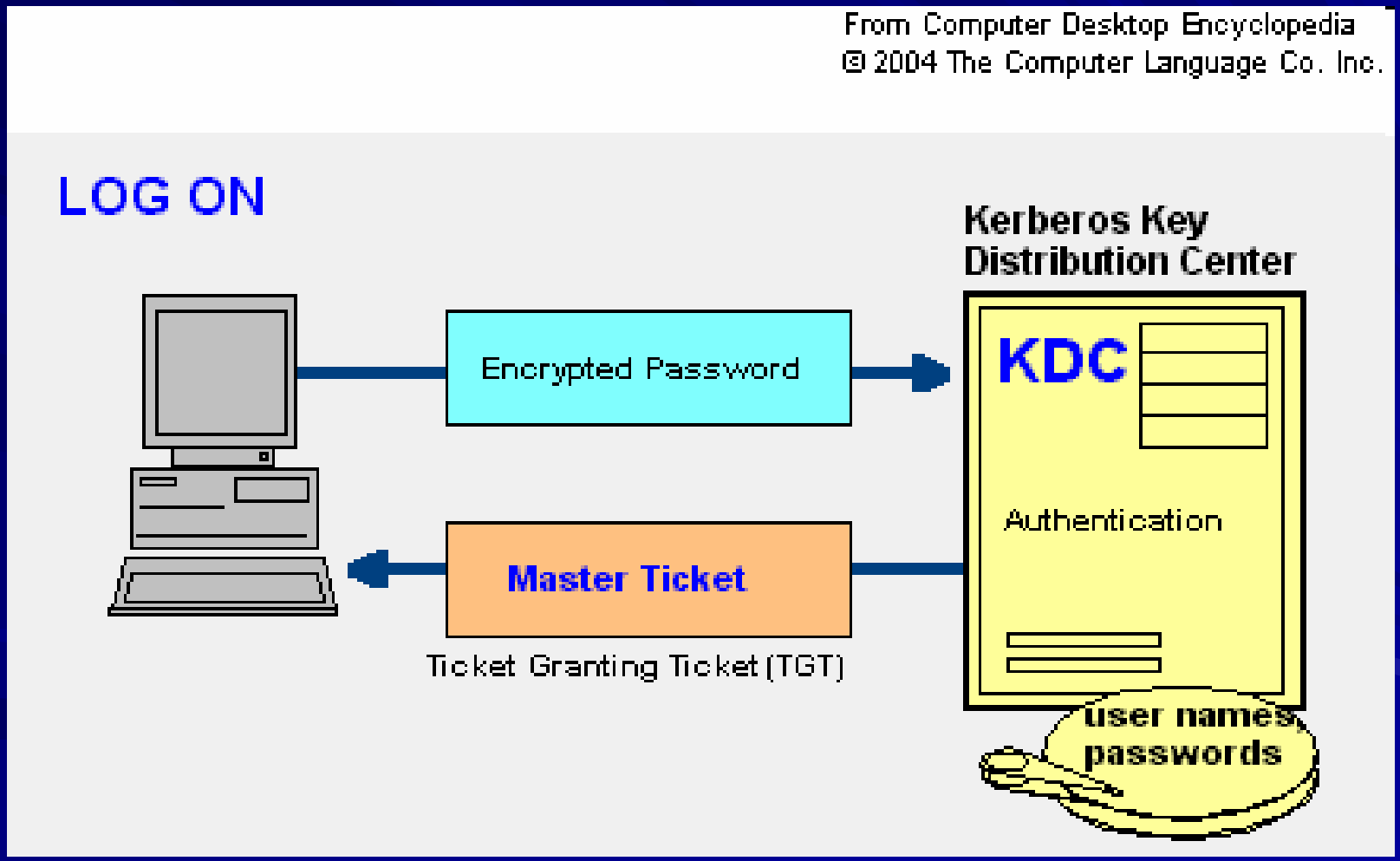
6. Kerberos

Tổng quan

- Học viện kỹ thuật Massachusetts (MIT) phát triển Kerberos để bảo vệ các dịch vụ mạng cung cấp bởi dự án Athena. Tên của giao thức được đặt theo tên của con chó ba đầu Cerberus canh gác cổng địa ngục trong thần thoại Hy Lạp. Giao thức đã được phát triển dưới nhiều phiên bản, trong đó các phiên bản từ 1 đến 3 chỉ dùng trong nội bộ MIT.
- Các hệ điều hành Windows XP và Windows Server 2003 sử dụng một phiên bản thực hiện Kerberos làm phương pháp mặc định để chứng thực. Hệ điều hành Mac OS cũng sử dụng Kerberos trong các phiên bản máy khách và máy chủ của mình.

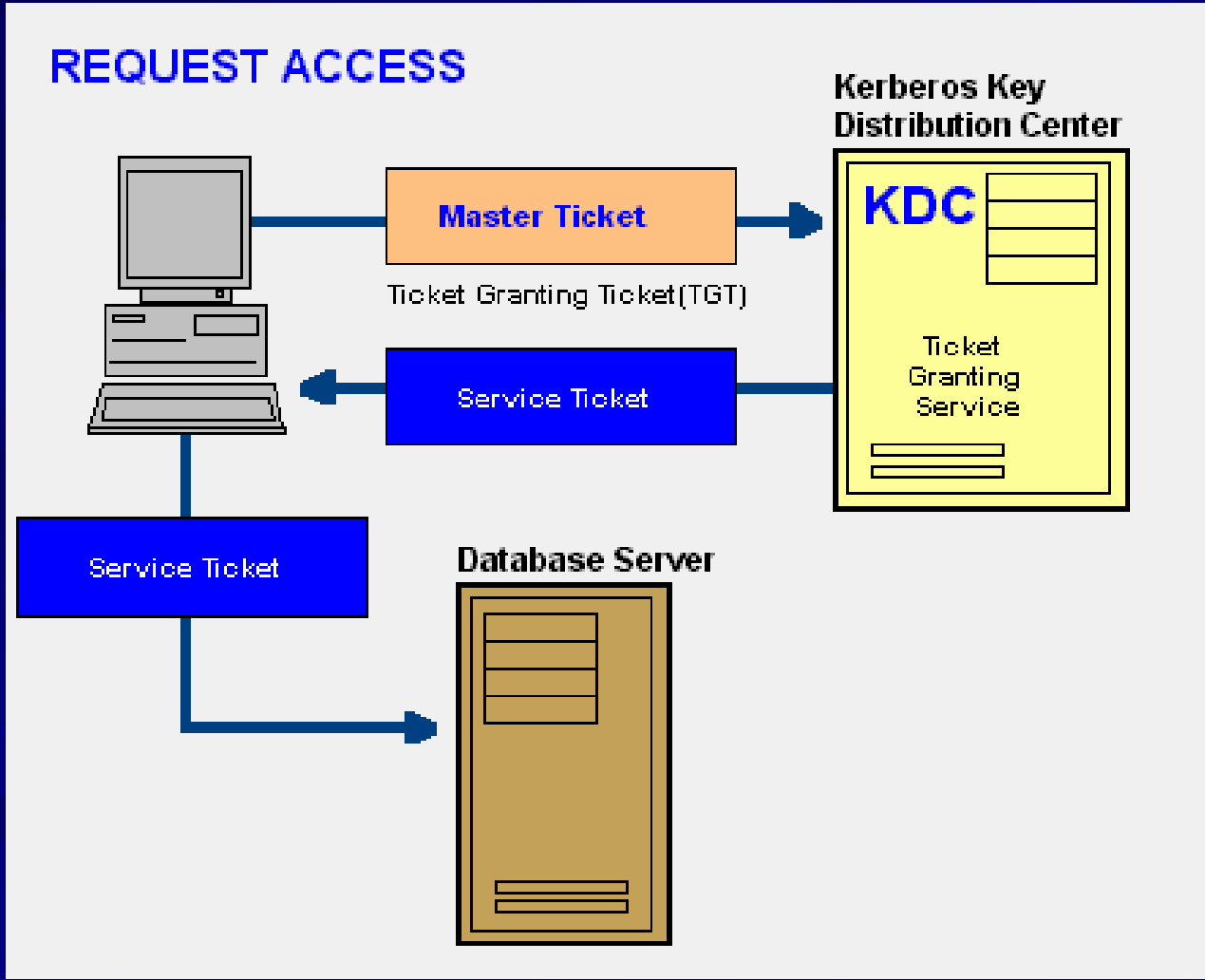
6. Kerberos

Tổng quan



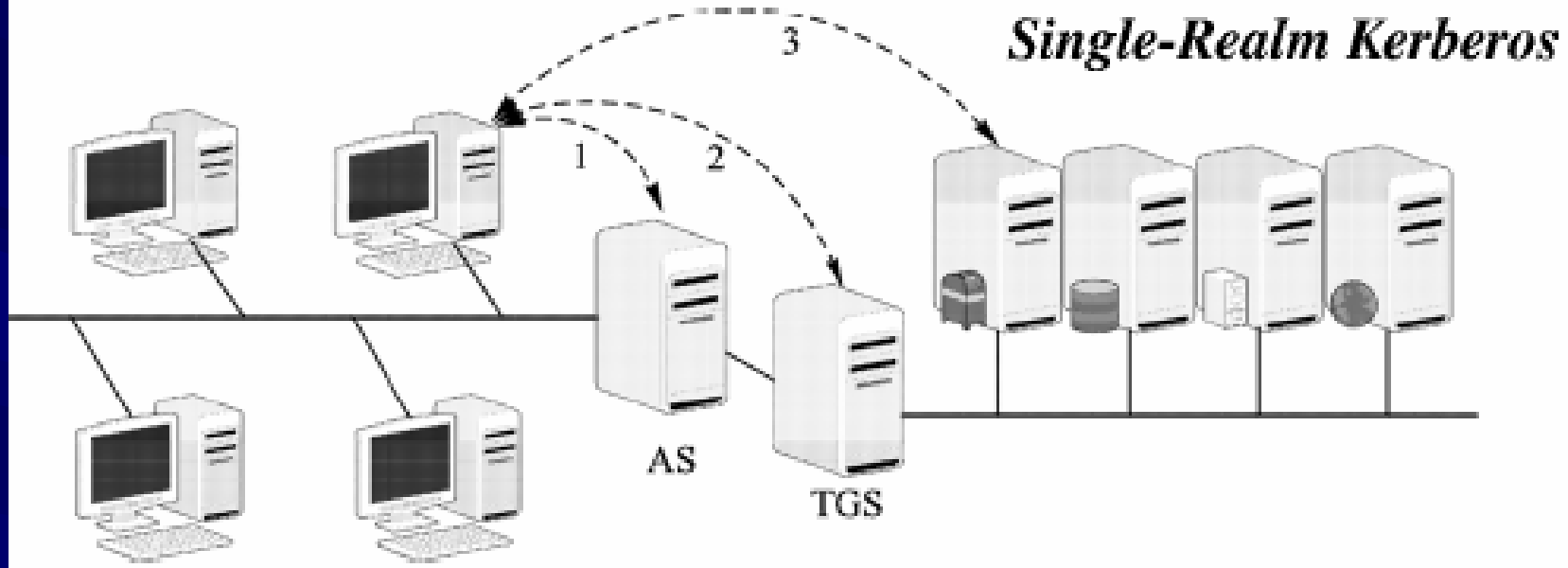
6. Kerberos

Tổng quan



6. Kerberos

Tổng quan



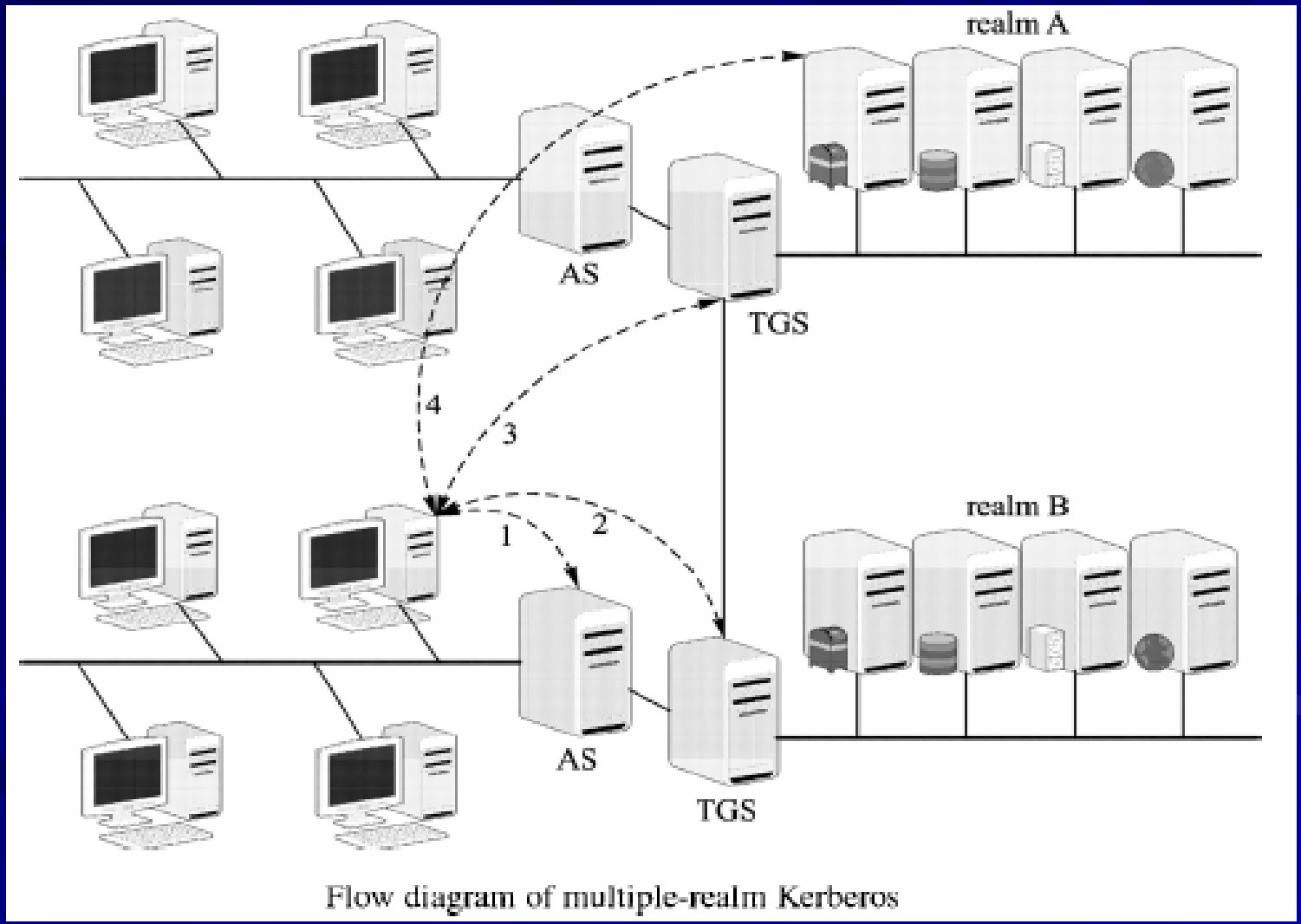
In the first phase, the user requests a TGS-ticket.

In the second phase, the user requests a server ticket.

In the third phase, the user presents his server ticket to the server to obtain service.

6. Kerberos

Tổng quan



Flow diagram of multiple-realm Kerberos

6. Kerberos

Mô tả phiên giao dịch

Với: AS = Máy chủ chứng thực (*authentication server*), TGS = Máy chủ cấp vé (*ticket granting server*), SS = Máy chủ dịch vụ (*service server*).

Nội dung chính: người sử dụng chứng thực mình với máy chủ chứng thực AS, sau đó chứng minh với máy chủ cấp vé TGS rằng mình đã được chứng thực để nhận vé, cuối cùng chứng minh với máy chủ dịch vụ SS rằng mình đã được chấp thuận để sử dụng dịch vụ.

1. Người sử dụng nhập tên và mật khẩu tại máy tính của mình (máy khách).
2. Phần mềm máy khách thực hiện hàm băm một chiều trên mật khẩu nhận được. Kết quả sẽ được dùng làm khóa bí mật của người sử dụng.

6. Kerberos

Mô tả phiên giao dịch

3. Phần mềm máy khách gửi một gói tin (không mật mã hóa) tới máy chủ dịch vụ AS để yêu cầu dịch vụ. Nội dung của gói tin đại ý: "người dùng XYZ muốn sử dụng dịch vụ". (Cả khóa bí mật lẫn mật khẩu đều không được gửi tới AS).
4. AS kiểm tra nhân dạng của người yêu cầu có nằm trong cơ sở dữ liệu của mình không. Nếu có thì AS gửi 2 gói tin sau tới người sử dụng:

- Gói tin A: "Khóa phiên TGS/máy khách" được mật mã hóa với khóa công khai của người sử dụng.
- Gói tin B: "Vé chấp thuận" (bao gồm định danh người sử dụng (ID), địa chỉ mạng của người sử dụng, thời hạn của vé và "Khóa phiên TGS/máy khách") được mật mã hóa với khóa bí mật của TGS.

6. Kerberos

Mô tả phiên giao dịch

5. Khi nhận được 2 gói tin trên, phần mềm máy khách giải mã gói tin A để có khóa phiên với TGS. (Người sử dụng không thể giải mã được gói tin B vì nó được mã hóa với khóa bí mật của TGS). Tại thời điểm này, người dùng có thể nhận thực mình với TGS.
6. Khi yêu cầu dịch vụ, người sử dụng gửi 2 gói tin sau tới TGS:

- Gói tin C: Bao gồm "Vé chấp thuận" từ gói tin B và chỉ danh (ID) của yêu cầu dịch vụ.
- Gói tin D: Phần nhận thực (bao gồm chỉ danh người sử dụng và thời điểm yêu cầu), mật mã hóa với "Khóa phiên TGS/máy khách".

6. Kerberos

Mô tả phiên giao dịch

7. Khi nhận được 2 gói tin C và D, TGS giải mã D rồi gửi 2 gói tin sau tới người sử dụng:

- Gói tin E: "Vé" (bao gồm chỉ danh người sử dụng, địa chỉ mạng người sử dụng, thời hạn sử dụng và "Khóa phiên máy chủ/máy khách") mật mã hóa với khóa bí mật của máy chủ cung cấp dịch vụ.
- Gói tin F: "Khóa phiên máy chủ/máy khách" mật mã hóa với "Khóa phiên TGS/máy khách".

6. Kerberos

Mô tả phiên giao dịch

8. Khi nhận được 2 gói tin E và F, người sử dụng đã có đủ thông tin để nhận thực với máy chủ cung cấp dịch vụ SS. Máy khách gửi tới SS 2 gói tin:

- Gói tin E thu được từ bước trước (trong đó có "Khóa phiên máy chủ/máy khách" mật mã hóa với khóa bí mật của SS).
- Gói tin G: phần nhận thực mới, bao gồm chỉ danh người sử dụng, thời điểm yêu cầu và được mật mã hóa với "Khóa phiên máy chủ/máy khách".

6. Kerberos

Mô tả phiên giao dịch

9. SS giải mã "Vé" bằng khóa bí mật của mình và gửi gói tin sau tới người sử dụng để xác nhận định danh của mình và khẳng định sự đồng ý cung cấp dịch vụ:

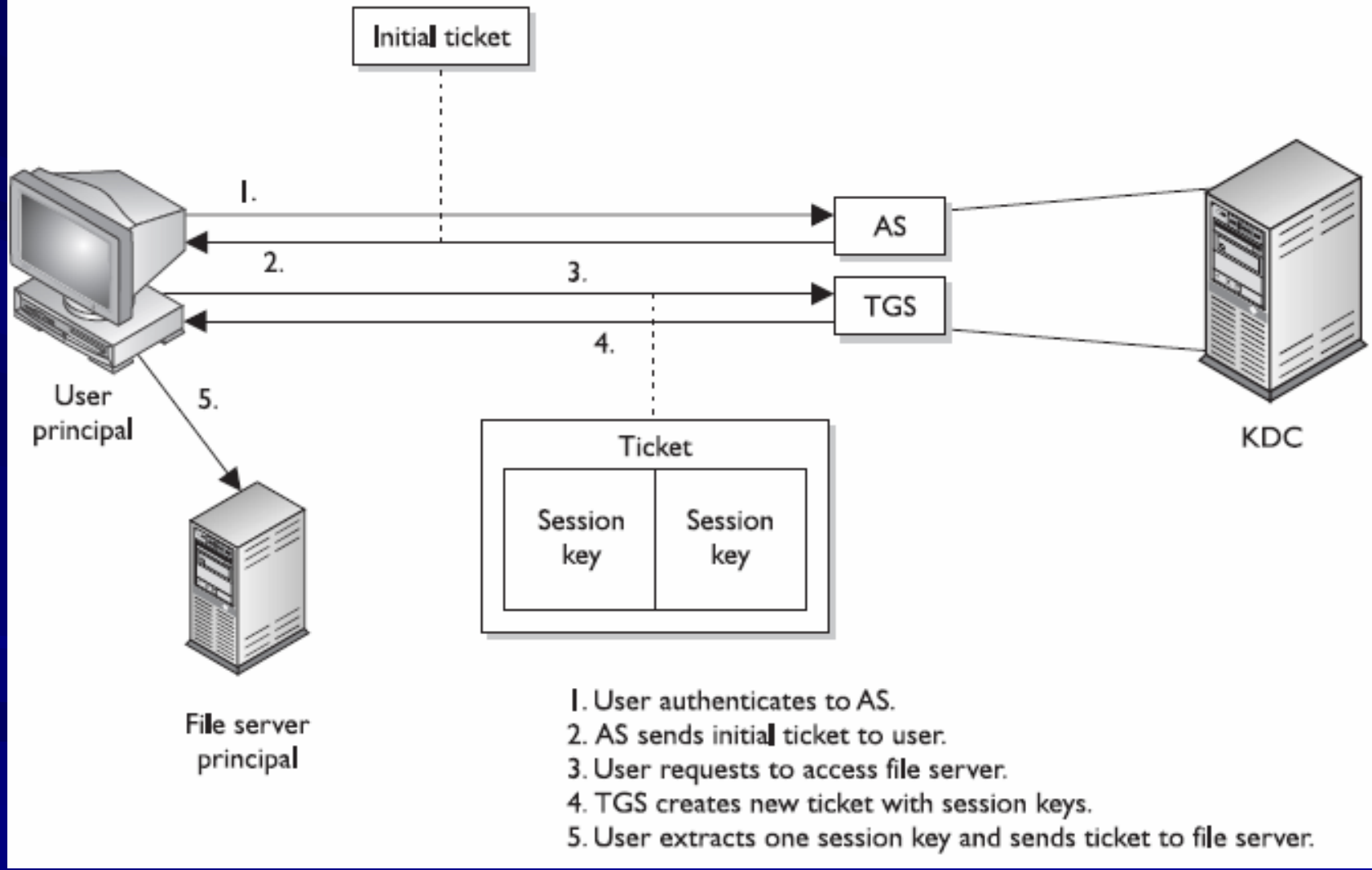
- Gói tin H: Thời điểm trong gói tin yêu cầu dịch vụ cộng thêm 1, mật mã hóa với "Khóa phiên máy chủ/máy khách".

10. Máy khách giải mã gói tin xác nhận và kiểm tra thời gian có được cập nhật chính xác. Nếu đúng thì người sử dụng có thể tin tưởng vào máy chủ SS và bắt đầu gửi yêu cầu sử dụng dịch vụ.

11. Máy chủ cung cấp dịch vụ cho người sử dụng.

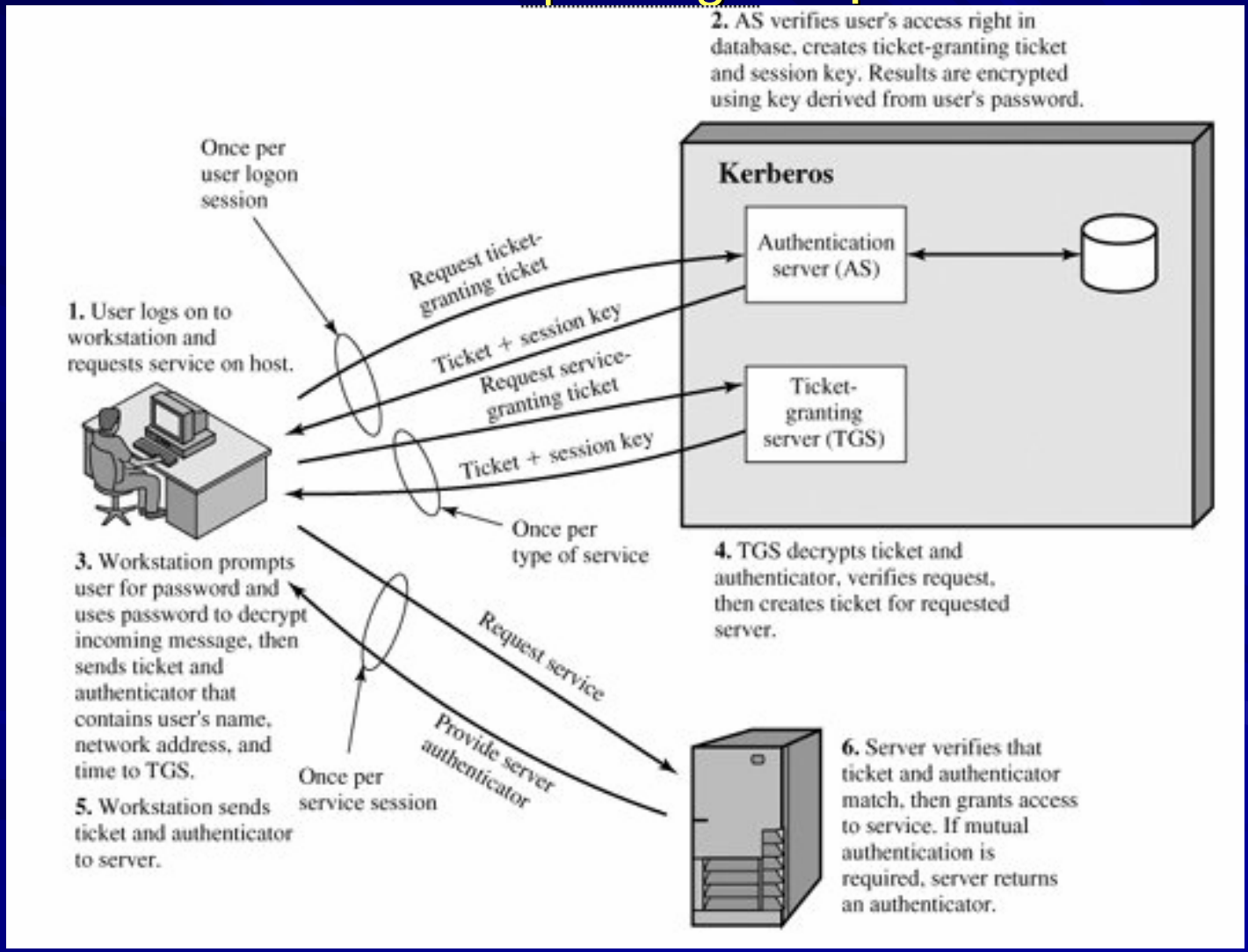
6. Kerberos

Mô tả phiên giao dịch



6. Kerberos

Mô tả phiên giao dịch



7. SSH

Tổng quan

- Telnet, rlogin, rsh, rcp, và FTP đã từng là những giao thức lớp ứng dụng phổ biến giúp người dùng đăng nhập vào một máy tính từ xa và truyền file giữa các máy tính trên mạng.
- Tuy nhiên, các giao thức này truyền tải dữ liệu thô mà không có bất kỳ sự bảo vệ nào, nên dễ bị đánh cắp mật khẩu, nghe trộm, giả mạo IP, và các loại tấn công khác.
- Năm 1995, nhà nghiên cứu người Phần Lan Tatu Ylonen đưa ra giải thuật Secure Shell (SSH) để bảo vệ việc đăng nhập từ xa đối với các cuộc tấn công bảo mật.

7. SSH
Tổng quan

- SSH được định nghĩa trong RFC 4251.
- SSH sử dụng cổng TCP 22.
- SSH có thể hoạt động trên các flatform khác nhau:
  - Kết nối đến một máy chủ SSH trên một router của Cisco từ một máy khách chạy Windows
  - Kết nối đến một máy chủ Linux từ một router Cisco hay có thể kết nối đến một máy chủ Windows 2008 từ một máy khách sử dụng hệ điều hành Linux.

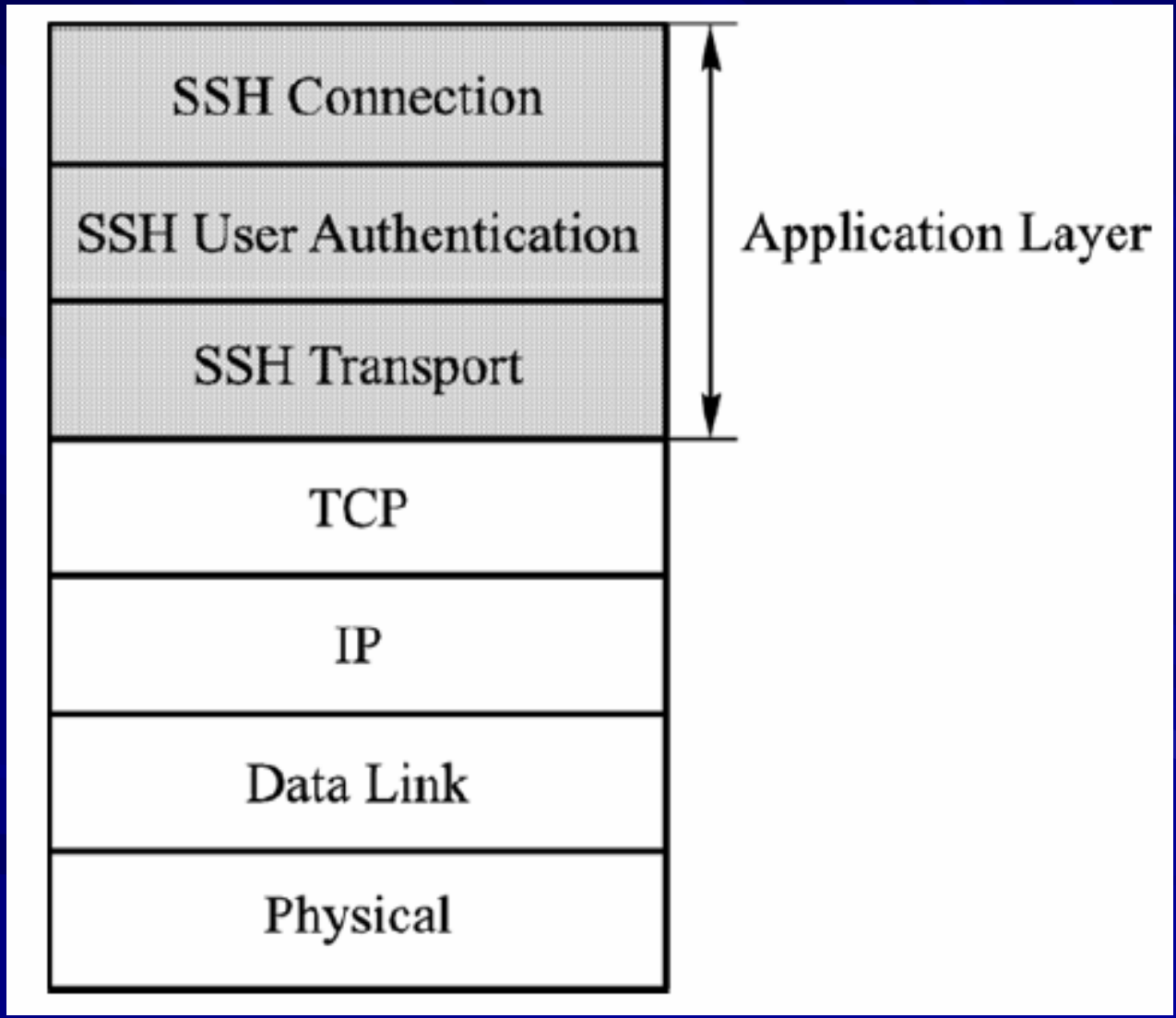
7. SSH

Tổng quan

- SSH tạo ra một kết nối bảo mật giữa hai máy tính sử dụng các giải thuật mã hoá và chứng thực.
- Có khả năng nén dữ liệu, bảo mật cho dữ liệu truyền (SFTP) và sao chép file (SCP).
- Là giao thức ứng dụng client-server. SSH được chia thành 3 lớp trong lớp ứng dụng của mô hình mạng TCP/IP:
  - Connection Layer
  - User Authentication Layer
  - Transport Layer

7. SSH

Tổng quan



7. SSH

Cách thức hoạt động

- SSH được thực hiện qua 3 bước:

1. Định danh host:
   - Việc định danh host được thực hiện qua việc trao đổi khoá. Mỗi máy tính có hỗ trợ kiểu truyền thông SSH có một khoá định danh duy nhất. Khoá này gồm hai thành phần: khoá riêng và khoá công khai. Khoá công khai được sử dụng khi cần trao đổi giữa các máy chủ với nhau trong phiên làm việc SSH, dữ liệu sẽ được mã hoá bằng khoá công khai và chỉ có thể giải mã bằng khoá riêng.

7. SSH

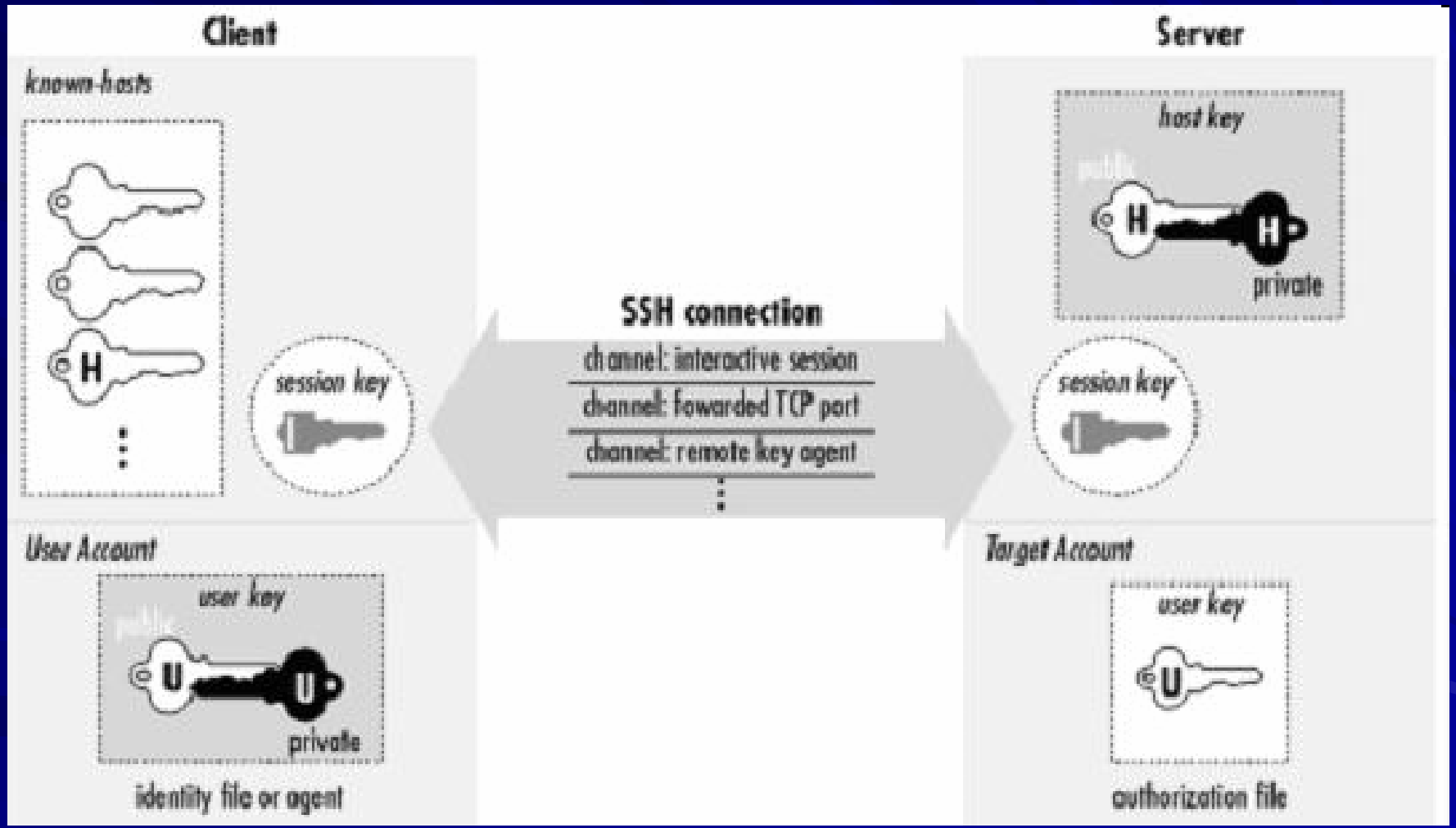
Cách thức hoạt động

- SSH được thực hiện qua 3 bước:

1. Định danh host:
   - Khi hai hệ thống bắt đầu một phiên làm việc SSH, máy chủ sẽ gửi khoá công khai của nó cho máy khách. Máy khách sinh ra một khoá phiên ngẫu nhiên và mã hoá khoá này bằng khoá công cộng của máy chủ, sau đó gửi lại cho máy chủ. Máy chủ sẽ giải mã khoá phiên này bằng khoá riêng của mình và nhận được khoá phiên. Khoá phiên này sẽ là khoá sử dụng để trao đổi dữ liệu giữa hai máy. Quá trình này được xem như các bước nhận diện máy chủ và máy khách.

7. SSH

Cách thức hoạt động



7. SSH

Cách thức hoạt động

- SSH được thực hiện qua 3 bước:

2. Mã hoá:
   - Sau khi hoàn tất việc thiết lập phiên làm việc bảo mật (trao đổi khoá, định danh), quá trình trao đổi dữ liệu diễn ra thông qua một bước trung gian đó là mã hoá/giải mã. Dữ liệu gửi/nhận trên đường truyền đều được mã hoá và giải mã theo cơ chế đã thoả thuận trước giữa máy chủ và máy khách.
   - Việc lựa chọn cơ chế mã hoá thường do máy khách quyết định. Các cơ chế mã hoá thường được chọn bao gồm: 3DES, IDEA, và Blowfish. Khi cơ chế mã hoá được lựa chọn, máy chủ và máy khách trao đổi khoá mã hoá cho nhau.

7. SSH

Cách thức hoạt động

- SSH được thực hiện qua 3 bước:

3. Chứng thực:
   - Mỗi định danh và truy nhập của người sử dụng có thể được cung cấp theo nhiều cách khác nhau. Chẳng hạn, kiểu chứng thực rhosts có thể được sử dụng, nhưng không phải là mặc định; nó đơn giản chỉ kiểm tra định danh của máy khách được liệt kê trong file rhost (theo DNS và địa chỉ IP).
   - Việc chứng thực mật khẩu là một cách rất thông dụng để định danh người sử dụng, nhưng ngoài ra cũng có các cách khác: chứng thực RSA, sử dụng ssh-keygen và ssh-agent để chứng thực các cặp khoá.

8. Bài tập

1. Trình bày cơ chế Anti-Replay của giao thức AH trong IPsec.
2. Nêu các ứng cụng của Ipsec.
3. Replay attack là gì?
4. Sử dụng ví dụ để trình bày chi tiết cơ chế hoạt động của SSL.
5. Mô tả chi tiết hoạt động của giao thức SSH.

8. Bài tập

6. Nêu sự khác biệt giữa transport mode và tunnel mode.
7. Nêu các yêu cầu cần thiết khi triển khai Kerberos.
8. Trình bày mục tiêu của chuẩn X.509.
9. X.509 thu hồi các chứng chỉ bằng cách nào?
10. Xây dựng một bảng tổng hợp về vai trò, công dụng, đặc điểm… của các giao thức nêu trong bài.

Thank You !