Khoa CNTT - ĐHSG

Thương mại điện tử và ứng dụng

An toàn trong thương mại điện tử

GV: Phan Thị Kim Loan

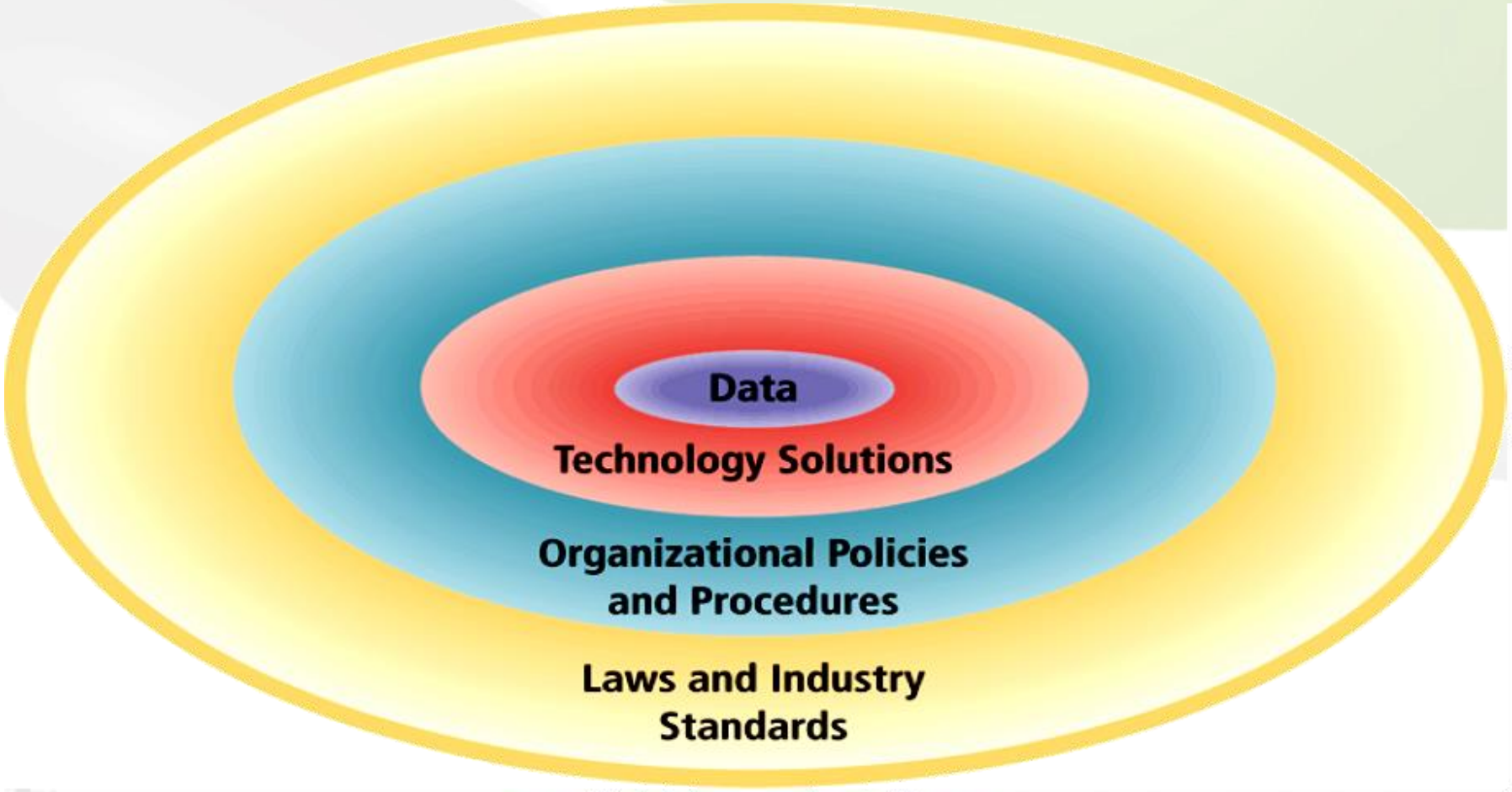
Nội Dung

- Khái niệm an toàn trong EC
- 6 khía cạnh của an toàn EC
- Các điểm có thể bị tấn công trong giao dịch EC
- Các hình thức tấn công thường gặp
- Các kỹ thuật bảo vệ an toàn: mã hóa, bảo vệ kênh truyền thông tin, an toàn mạng, an toàn máy tính

Khái niệm an toàn trong EC

- Tất cả các loại tội phạm diễn ra trong môi trường thương mại truyền thống đều diễn ra trong môi trường TMĐT
- Việc giảm các rủi ro trong TMĐT là một quá trình phức tạp liên quan đến công nghệ, thủ tục và chính sách của tổ chức, luật pháp và các tiêu chuẩn công nghiệp
- An toàn luôn chỉ mang tính tương đối, bất cứ hệ thống an toàn nào cũng có thể bị phá vỡ. An toàn là một chuỗi liên kết và thường bị đứt ở những điểm yếu nhất
- Một sự an toàn vĩnh viễn là không cần thiết
- Cần cân nhắc giữa an toàn và chi phí, an toàn và tiện dụng

Môi trường an toàn trong EC



6 khía cạnh của an toàn EC

- Tính tin cậy: khả năng đảm bảo không ai có thể truy cập các thông điệp và dữ liệu có giá trị

- Tính riêng tư: khả năng đảm bảo kiểm soát việc sử dụng các thông tin cá nhân mà khách hàng cung cấp về chính bản thân họ

- Tính sẵn dùng: khả năng đảm bảo các chức năng của một web site thương mại điện tửđược thực hiện đúng như mong đợi

6 khía cạnh an toàn EC

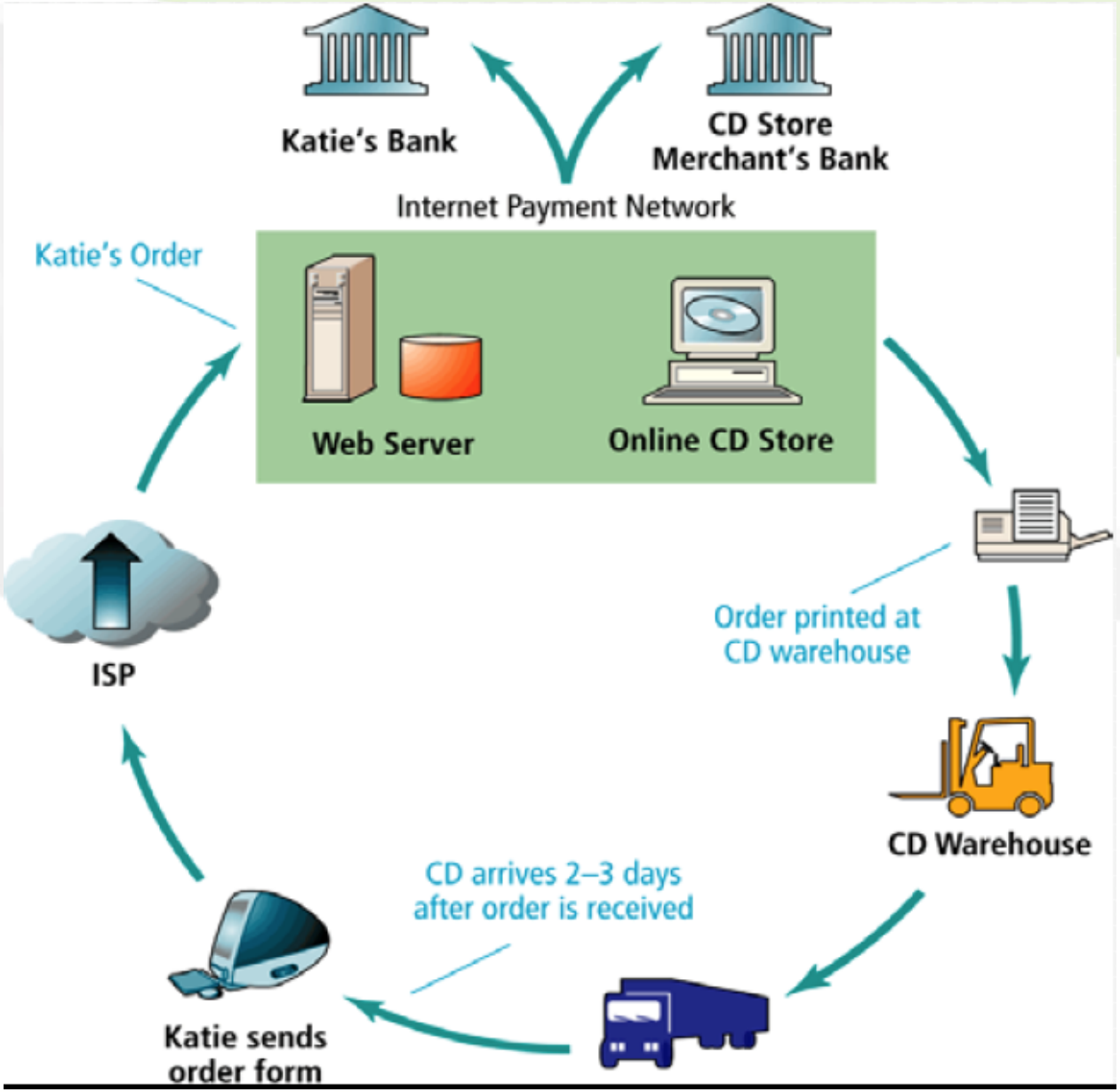
TABLE 5.1 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?

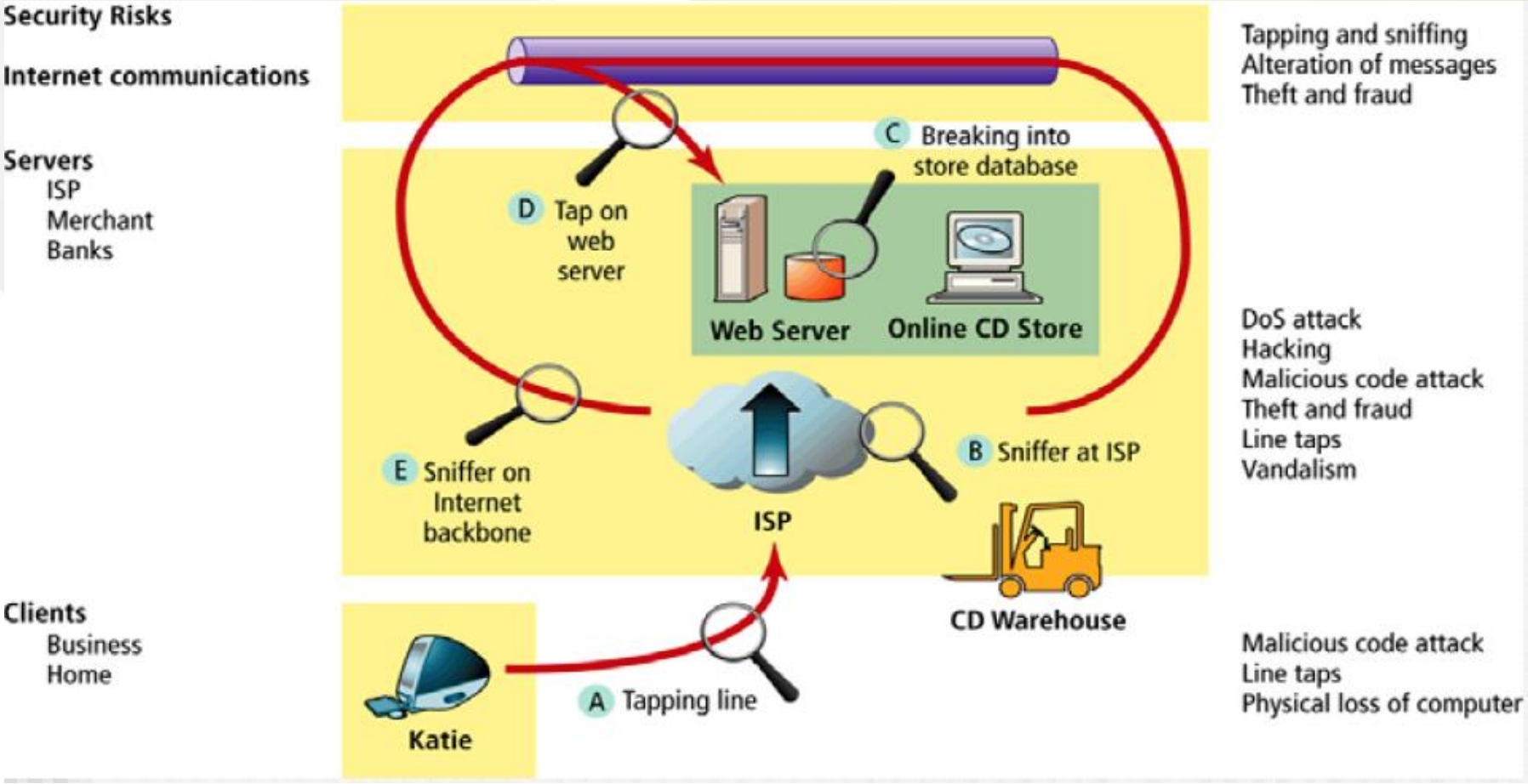
Các điểm cần bảo mật

- Ba điểm cần bảo mật
  - Client
  - Server
- Các hình thức tấn công thường gặp
  - Các đoạn mã nguy hiểm (malicious code)
  - Tin tặc và các chương trình phá hoại (hacking and cybervandalism)
  - Gian lận thẻ tín dụng (credit card fraud/theft)
  - Sự lừa đảo (spoofing)
  - Sự khước từ dịch vụ (DoS – Denial of service)
  - Kẻ trộm trên mạng (sniffing)
  - Sự tấn công từ bên ngoài tổ chức (insider jobs)

Các bước giao dịch



Các điểm dễ bị tấn công



Các đoạn mã nguy hiểm

- Virus: chương trình máy tính có khả năng tự nhân bản và lây lan đến các tập tin khác, hầu hết đều có mưu đồ (hiền từ hoặc hiểm độc); có3 loại macro virus, file-infecting virus và script virus
- Worm: có khả năng lây nhiễm từ máy tính này sang máy tính khác, tự nhân bản mà không cần kích hoạt, thường tìm kiếm và thay đổi mọi dữ liệu trong bộ nhớ hoặc đĩa cứng mà nó gặp
- Trojan horse: không phải là virus nhưng lại tạo cơ hội cho các virus nguy hiểm khác xâm nhập
- Bad applet (đoạn mã di động nguy hiểm): các Java applet hoặc ActiveX control trên Web site được download về client

Các đoạn mã nguy hiểm

TABLE 5.2 EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Melissa	Macro virus/worm	First spotted in March 1999. At the time, Melissa was the fastest spreading infectious program ever discovered. It attacked Microsoft Word's normal.dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook address book.
CodeRed	worm	Appeared in 2001. It spread to hundreds of thousands of systems and tried to flood the White House IP address with bogus information requests.
Chernobyl	File infecting virus	First appeared in 1998. It is very destructive: It wipes out the first megabyte of data on a hard disk (making the rest useless) every April 26, the anniversary of the nuclear disaster at Chernobyl.
Klez	E-mail worm	Most prolific virus of 2002. Klez comes in an e-mail with a random subject line and message body. Once launched, the worm sends itself to all addresses in the Windows address book, the database of instant-messaging program ICQ, and local files. A file from the user's system is randomly selected and sent along with the worm. Klez also attempts to disable anti-virus software and drops another virus in the user's system that tries to infect executable files there and across network filing systems.
Bugbear	Trojan horse/worm	Struck in 2002. It appeared as an e-mail attachment and random e-mail was infected in over 22,000 systems in 24 hours. It can intercept Web activity (i.e., credit card information) and can disable Windows and anti-virus software.

Tin tặc và các chương trình phá hoại

- Tin tặc là những người truy cập trái phép vào một hệ thống máy tính, sử dụng các chươngtrình phá hoại để gây ra sự cố làm mất uy tín của tổ chức
- Vd: ngày 01/4/2001 các tin tặc tấn công vàonhững web site dùng IIS của Microsoft
- Các loại tin tặc
  - Mũ trắng – giúp phát hiện và sửa chữa những kẻ hở trong một hệ thống an toàn
  - Mũđen – tấn công có chủđích không tốt
  - Mũ xám – giữa hai loại trên

Gian lận thẻ tín dụng

- Trong thương mại truyền thống, gian lận thẻ tín dụng có thể xảy ra trong trường hợp thẻ bị mất, bịđánh cắp; các thông tin về số thẻ, mã số định danh cá nhân (PIN), các thông tin về khách hàng bị tiết lộ và sử dụng bất hợp pháp
- Trong TMĐT, mối đe dọa lớn nhất là bị "mất" các thông tin liên quan đến thẻ hoặc các thôngtin về giao dịch sử dụng thẻ trong quá trìnhdiễn ra giao dịch
- Các tội phạm có thểđột nhập vào các website TMĐT và lấy cắp thông tin cá nhân khách hàngvà mạo danh khách hàng
- Một trong những đe dọa lớn nhất đối với người bán hàng là sự phủđịnh giao dịch đối với các đơn đặt hàng quốc tế

Sự lừa đảo

- Sử dụng các địa chỉ thư điện tử giả hoặc mạo danh một người nào đó để thực hiện những mưu đồ bất chính
- Thay đổi hoặc làm chệch hướng các liên kết Web tới một địa chỉ khác với địa chỉ thực hoặc tới một Web site giả mạo Web site cần liên kết
- Các hành vi lừa đảo đe dọa tính toàn vẹn và tính xác thực của các giao dịch TMĐT, khiến cho các giao dịch này trở thành "trắng đen lẫn lộn" và cả doanh nghiệplẫn khách hàng đều khó có thể xác định được đâu là thật và đâu là giả

Sự khước từ dịch vụ

- Tấn công vào một Web site gây nên sự quá tải về khả năng cung cấp dịch vụ của Web site này, khước từ dịch vụ
- Khiến cho Web site phải bị gián đoạn hoạt động
- Ảnh hưởng đến uy tín của doanh nghiệp,đối với những Web site náo nhiệt như eBay.com hay Amazon.com thì điều nàyđồng nghĩa với những khoản phí vô cùnglớn khi phải ngưng hoạt động một thời gian

Kẻ trộm trên mạng

- Một dạng của chương trình nghe trộm, giám sát sự di chuyển của thông tin trên mạng đểăn cắp các thông tin quan trọng từ bất cứ nơi nào trên mạng

- Xem lén thưđiện tử là một dạng mới của hành vi trộm cắp trên mạng. Kỹ thuật xem lén thưđiện tử một đoạn mã ẩn bí mật gắn vào thưđiện tử cho phép giám sát toàn bộ các thông điệp chuyển tiếp được gởi đi cùng với thông điệp ban đầu

Sự tấn công từ bên trong tổ chức

- Những mối đe dọa an toàn không chỉđến từ bên ngoài mà có thể bắt nguồn từ chính những thành viên trong tổ chức

- Trong nhiều trường hợp, hậu quả của những đe dọa loại này còn nghiêm trọnghơn những vụ tấn công từ bên ngoài

Giải pháp kỹ thuật

Mã hóa thông tin

- Mã hóa thông tin là quá trình chuyển các văn bản hay tài liệu gốc thành các văn bản dưới dạng mật mã không ai, ngoài người gởi và người nhận, có thểđọc được
- Mục đích
  - Đảm bảo an toàn các thông tin được lưu trữ
  - Đảm bảo an toàn các thông tin được truyền nhận
- Đáp ứng 4 trong 6 khía cạnh an toàn TMĐT
  - Tính toàn vẹn
  - Chống phủđịnh
  - Tính xác thực
  - Tính tin cậy
- Mã hóa dựa trên cơ sở khóa (mã), là phương pháp để chuyển văn bản gốc thành văn bản mã hóa

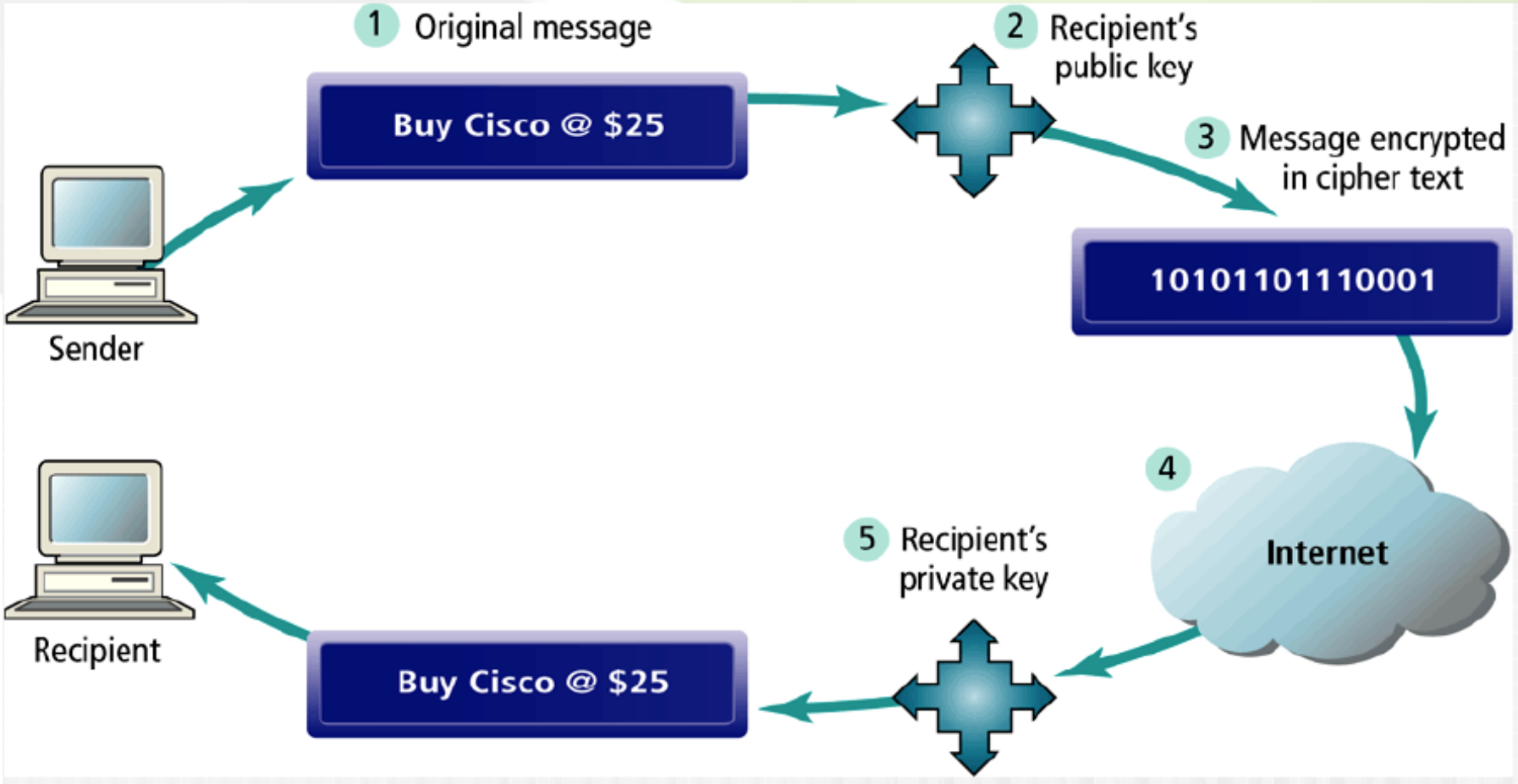
Mã hóa khóa bí mật

- Còn được gọi là mã hóa đối xứng hay mã hóa khóa riêng
- Sử dụng cùng một khóa cho cả quá trình mã hóa(được thực hiện bởi người gởi) và quá trình giải mã (được thực hiện bởi người nhận)
- Tiêu chuẩn mã hóa dữ liệu (Data EncryptionStandard -DES): dùng 56, 128 hoặc 2048 bit
- Hạn chế:
  - Các bên tham gia mã hóa phải tin tưởng nhau và chắc chắn rằng khóa được đối tác bảo vệ cẩn mật
  - Mỗi giao dịch TMĐT khác nhau cần có khóa khác nhau → chi phí lớn tạo, chuyển và quản lý khóa cho mỗi khách hàng

Mã hóa công khai

- Còn được gọi là mã hóa không đối xứng
- Sử dụng hai khóa trong quá trình mã hóa: một khóa dùng để mã hóa và một khóa dùng để giải mã thông điệp. Hai khóa này có quan hệ với nhau về thuật toán sao cho dữ liệu được mã hóa bằng khóa này sẽđược giải mã bằng khóa kia
- Mỗi đối tác có một cặp khóa duy nhất: một khóa chung và một khóa riêng. Khóa chung dùng để mã hóa và khóa riêng để giải mã thông điệp.Khóa chung mọi đối tác đều biết còn khóa riêngchỉ một người chủ khóa biết
- Như vậy, A muốn gởi thông điệp cho B thì sẽ lấykhóa chung của B để mã hóa thông điệp, sau đó gởi đi. B sẽ dùng khóa riêng của B để giải mã

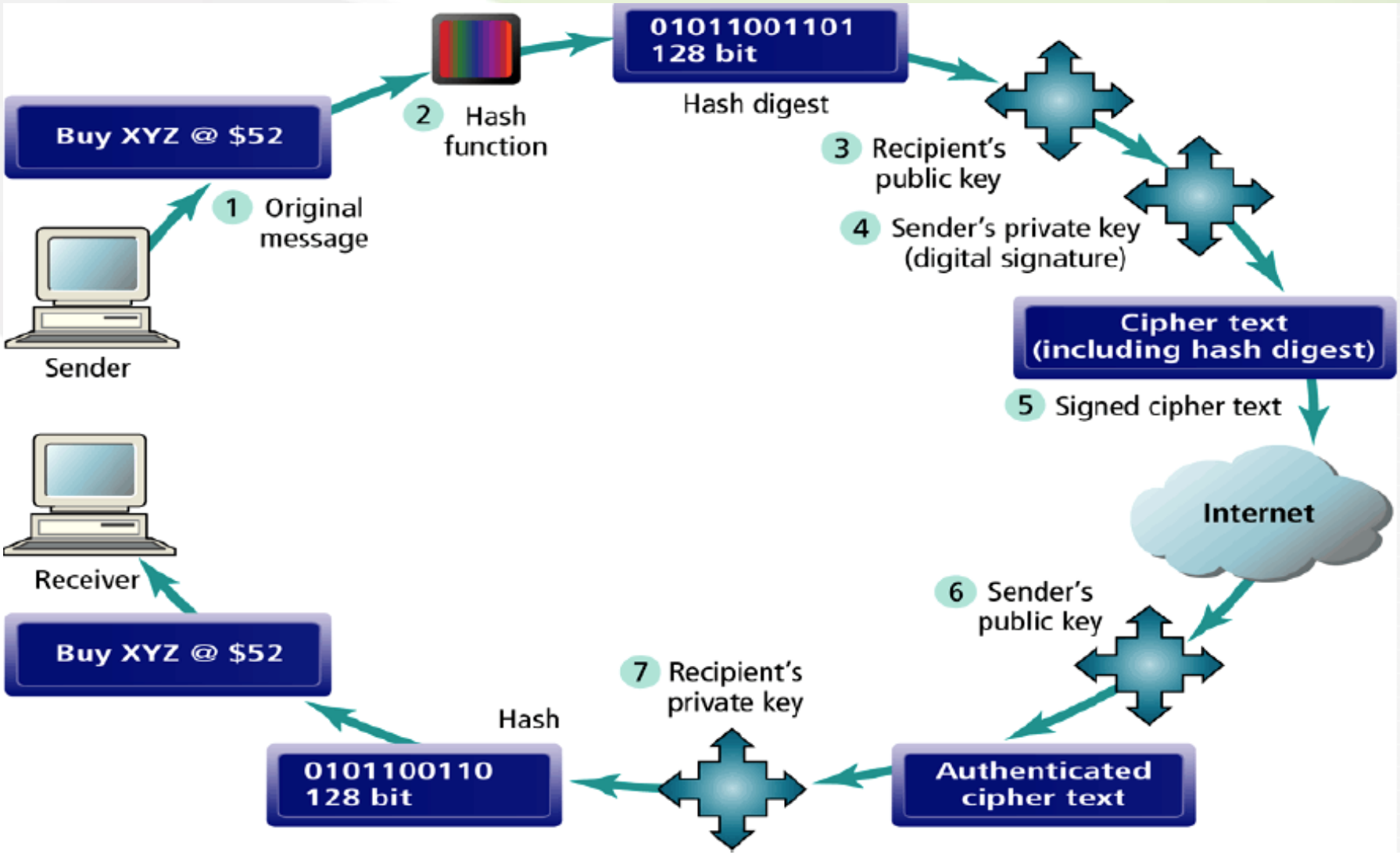
Mã hóa công khai



Mã hóa công khai

- Dùng hàm băm để tạo ra giá trị duy nhất cho mỗi thông điệp dùng để kiểm tra tính toàn vẹn của thông điệp
- Kết hợp với chữ ký số (digital signature thực chất là khóa riêng của người gởi) vào thông điệp đểđảm bảo tính xác thực và chống phủđịnh
- Chữ ký điện tử là ký hiệu điện tửđược gắn với văn bản điện tử khác theo một nguyên tắc nhất định và được người ký văn bản đó áp dụng

Mã hóa khóa công khai với chữ ký số và hàm băm

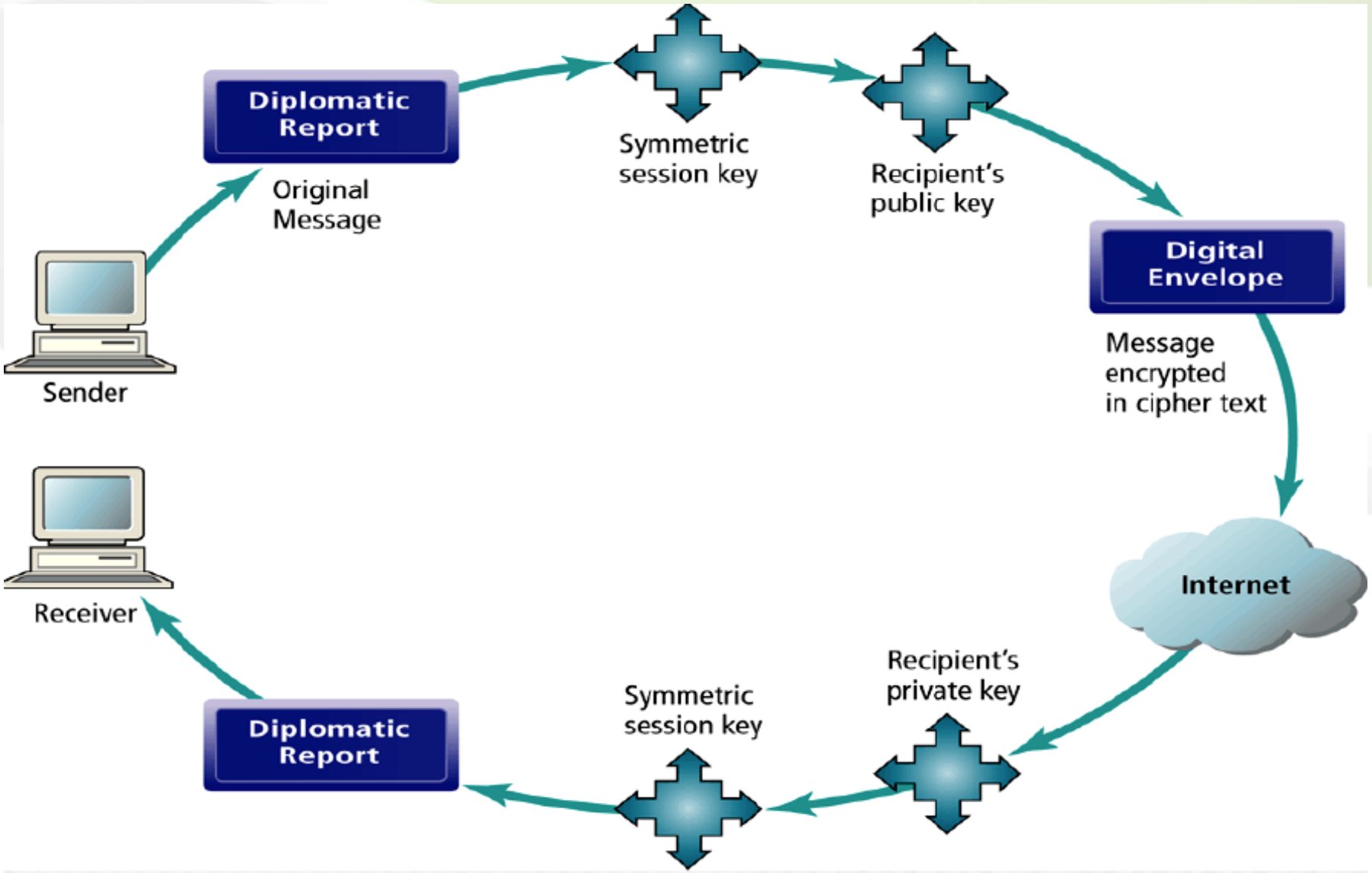


Mã hóa khóa công khai với phong bì số

- Khắc phục nhược điểm của mã hóa khóa công khai (thời gian tính toán dài, giảm tốc độ) và ưu điểm của mã hóa khóa bí mật (nhanh hơn, bảo mật hơn)

- Dùng khóa bí mật để mã hóa thông điệp và khóa công khai để mã hóa và gởi khóa bí mật

Mã hóa khóa công khai với phong bì số



Chứng thực điện tử

- Các bên giao dịch TMĐT đều muốn chắc chắn rằng đối tác của mình là xác thực, khóa côngkhai và chữ ký điện tửđúng là của đối tác, không ai có thể giả danh đối tác để thực hiện giao dịch
- Các cơ quan chứng thực (Certificate Authority – CA) sẽđứng ra xác thực chữ ký điện tử (haykhóa công khai) là của cá nhân hay tổ chức cụ thể và duy nhất
- Đểđược xác thực, cá nhân hay tổ chức phải cung cấp cho cơ quan chứng nhận chứng cớ định danh của mình

Chứng thực điện tử

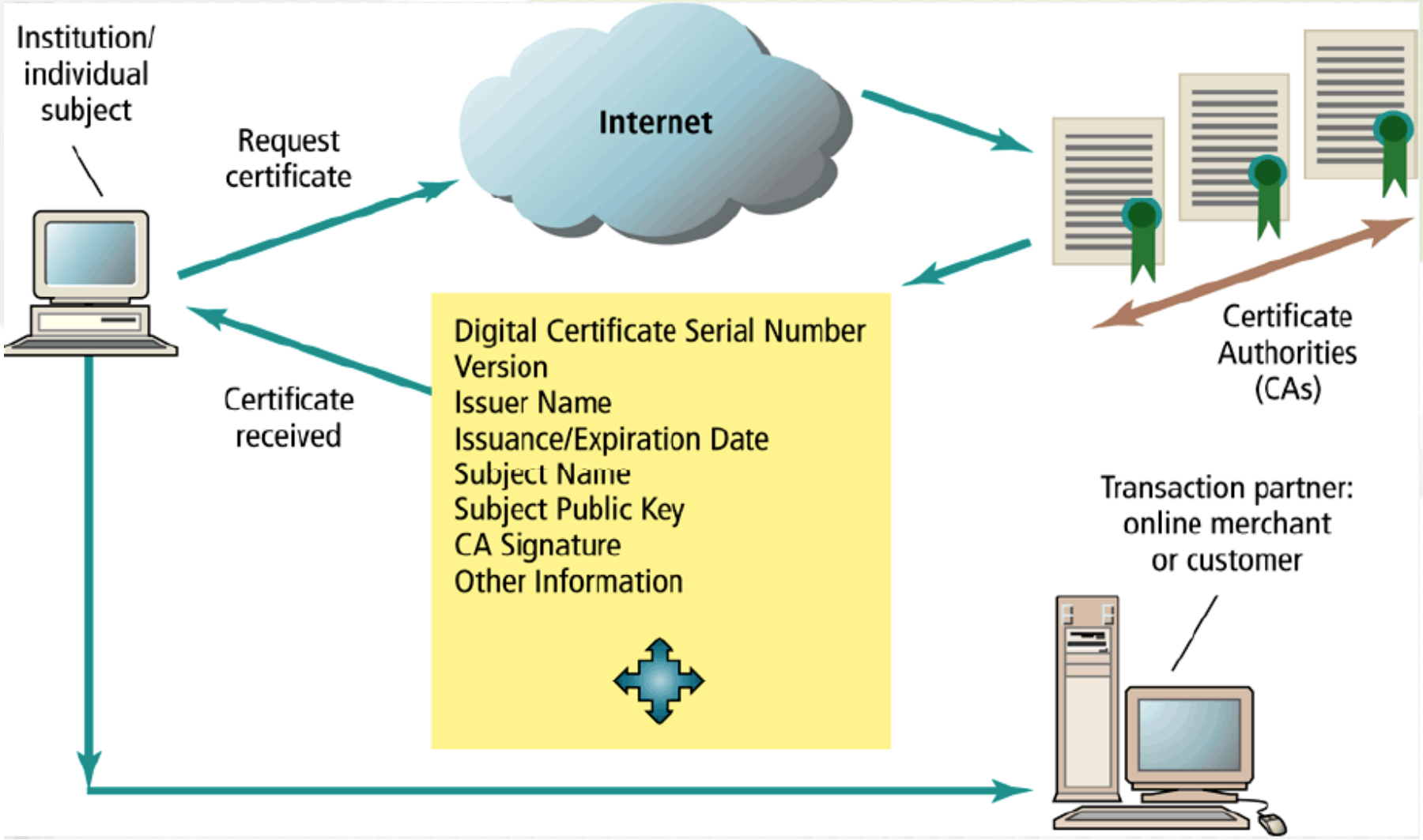
- Cơ quan chứng nhận căn cứ vào đó tạo một thông điệp gọi là chứng thực điện tử (digital-certificate) bao gồm các thông tin:
  - Tên của cá nhân hoặc tổ chức
  - Khóa công khai
  - Sốđịnh danh của chứng thực điện tử
  - Thời hạn hiệu lực
  - Ngày cấp
  - Chữ ký của cơ quan chứng nhận
  - Các thông tin nhận dạng khác

Chứng thực điện tử

- Các chứng thực điện tử là cơ sở của giao thức an toàn giao dịch điện tử

- Tập hợp hệ thống các cơ quan chứng nhận và các thủ tục chứng thực điện tửđược tất cả các đối tượng tham gia TMĐT chấp nhận hình thành cơ sở hạ tầng khóa công khai (PublicKey Infrastructure – PKI)

Chứng thực điện tử



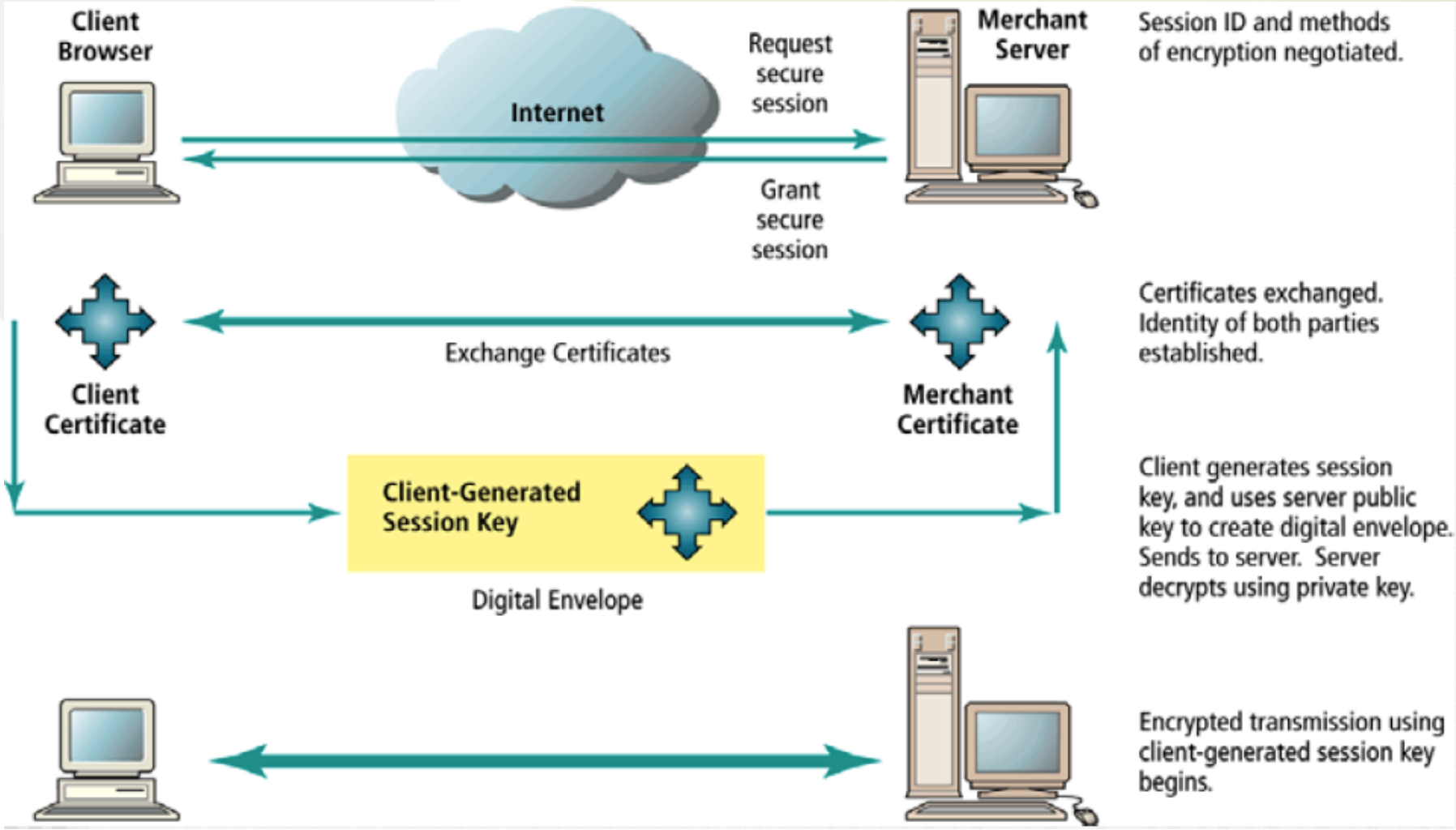
Khuyết điểm của mã hóa

- CSHT khóa công khai áp dụng chủ yếu cho việc bảo vệ các thông điệp được truyền nhận
- CSHT khóa công khai không ngăn chặn được tấn công từ bên trong nội bộ tổ chức
- Việc tự bảo vệ khóa riêng của các cá nhân không được bảo đảm
- Không có gì đảm bảo an toàn của các máy tính được sử dụng cho giao dịch
- Các cơ quan chứng nhận không được kiểm soát

SSL

- Lớp ổ cắm an toàn (Secure Sockets Layer – SSL): bảo vệ các kênh thông tin trong quátrình trao đổi dữ liệu giữa máy chủ và các máy khách thay vì từng thông điệp
- Với việc sử dụng phương pháp mã hóa khóacông khai và các chứng thực điện tử, SSL yêu cầu xác thực các đối tác và bảo vệ các thông tin gởi từđối tác này đến đối tác khác
- Khuyết điểm: SSL chỉ bảo vệ thông tin được chuyển đi, không bảo vệ thông tin đã được giải mã và lưu trữ trên máy tính. Nếu máy tính không được đảm bảo an toàn thì có thể bị truy cập trái phép và mất đi dữ liệu

SSL


Client Browser
Internet
Request secure session
Merchant Server
Session ID and methods of encryption negotiated.
Grant secure session
Client Certificate
Exchange Certificates
Merchant Certificate
Certificates exchanged. Identity of both parties established.
Client-Generated Session Key
Digital Envelope
Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.
Encrypted transmission using client-generated session key begins.

An toàn các kênh truyền thông

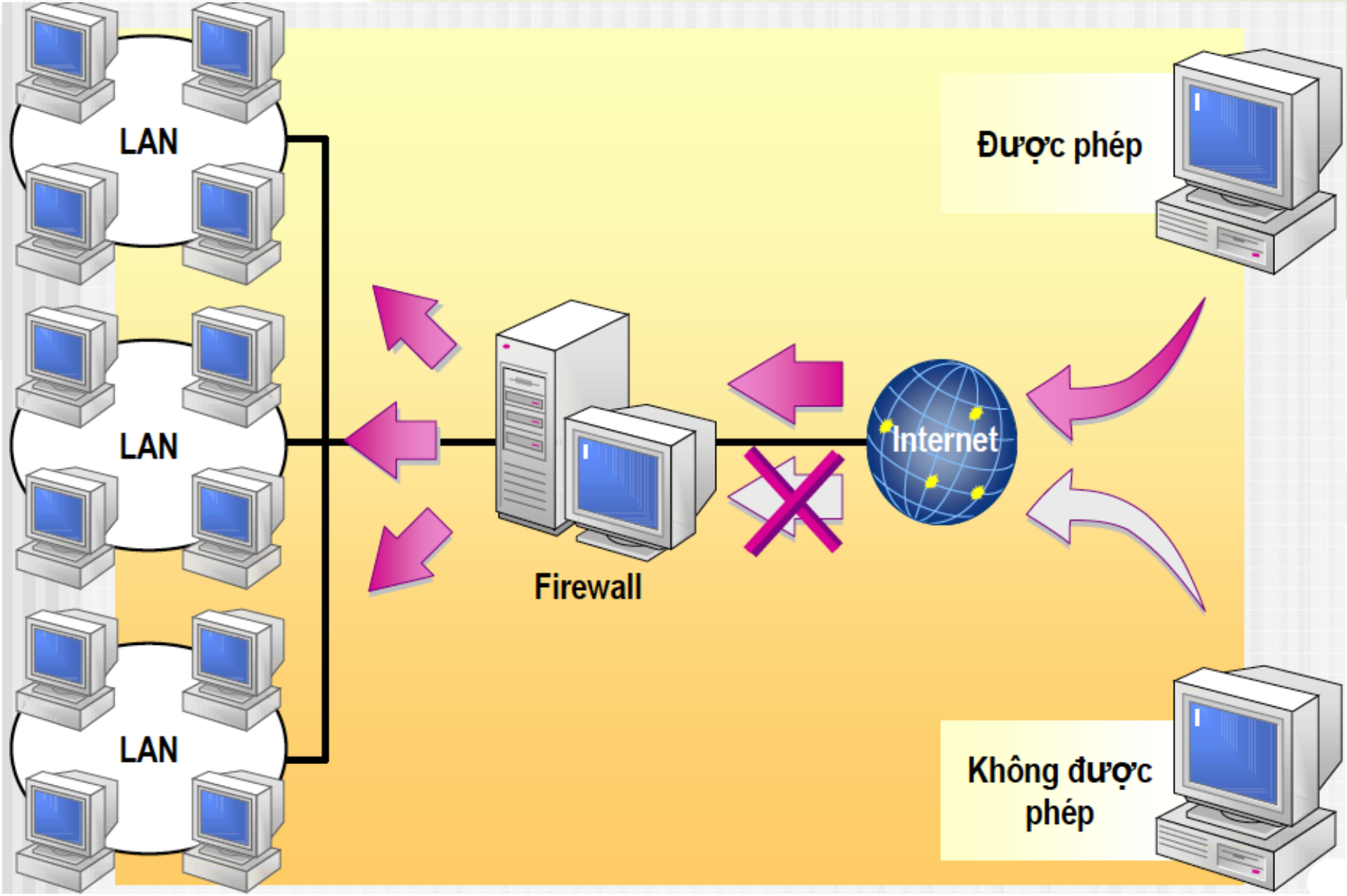
- Secure HyperText Transfer Protocol – SHTTP: một kỹ thuật khác cung cấp an toàn truyền thông dùng với HTTP

- Virtual Private Network (VPN): cho phép các user kết nối vào mạng nội bộ một cách an toàn thông qua Internet, dùng giao thức Point-to-Point Tunneling Protocol (PPTP)

An toàn mạng – tường lửa

- Bức tường lửa (firewall): là một ứng dụng phần mềm hoặc phần cứng thiết lập một rào chắn giữa mạng máy tính của tổ chức và bên ngoài
- Bảo vệ mạng máy tính của tổ chức:
  - Tất cả thông điệp từ bên trong tổ chức ra ngoài và ngược lại đều phải qua tường lửa
  - Chỉ những thông điệp đảm bảo được các yêu về an toàn của tổ chức mới được tiếp tục phân phối (qua tường lửa), nếu không sẽ bị chặn đứng lại ở tường lửa
  - Không được phép thâm nhập vào chính hệ thống

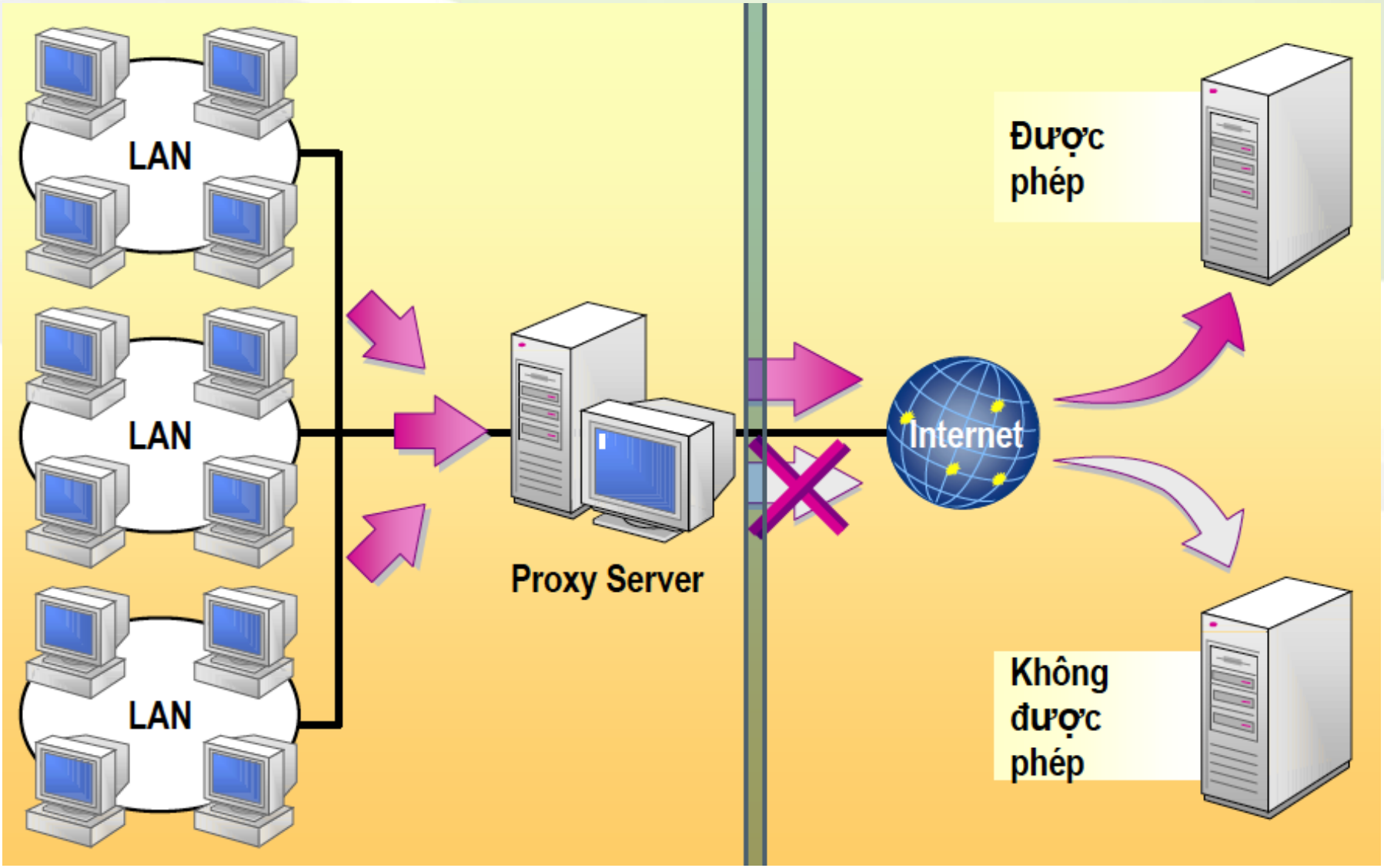
An toàn mạng – tường lửa



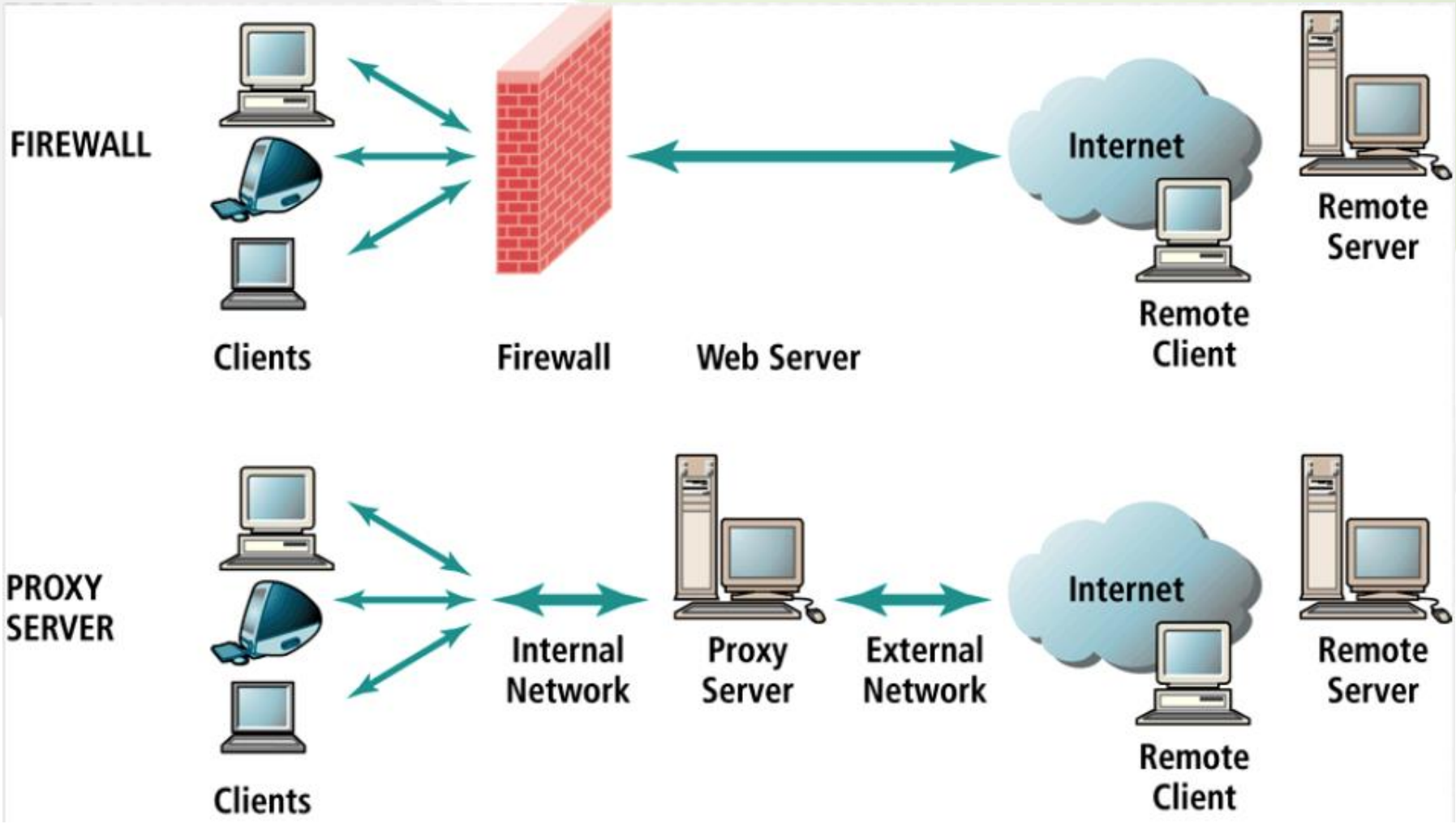
An toàn mạng – proxy server

- Proxy server (máy phục vụủy quyền) cung cấp các dịch vụ trung gian, đóng vai trò là "người thông ngôn" giữa mạng nội bộ của tổ chức với bên ngoài
- Khi một người trong mạng nội bộ muốn "nói chuyện" với một người ở ngoài thì phải nói chuyện với proxy, sau đó proxy sẽ nói chuyện với người ngoài kia. Tương tự cho chiều giao tiếp ngược lại
- Ưu điểm:
  - Các thông tin bên trong được bảo vệ vì chỉ có proxy liên lạc trực tiếp với bên ngoài
  - Lọc được các nguồn thông tin bên ngoài
  - Tăng khả năng đáp ứng bằng cách lưu trữ các trang Web thường được yêu cầu
  - Theo dõi các giao tiếp giữa bên trong và bên ngoài

An toàn mạng – proxy server



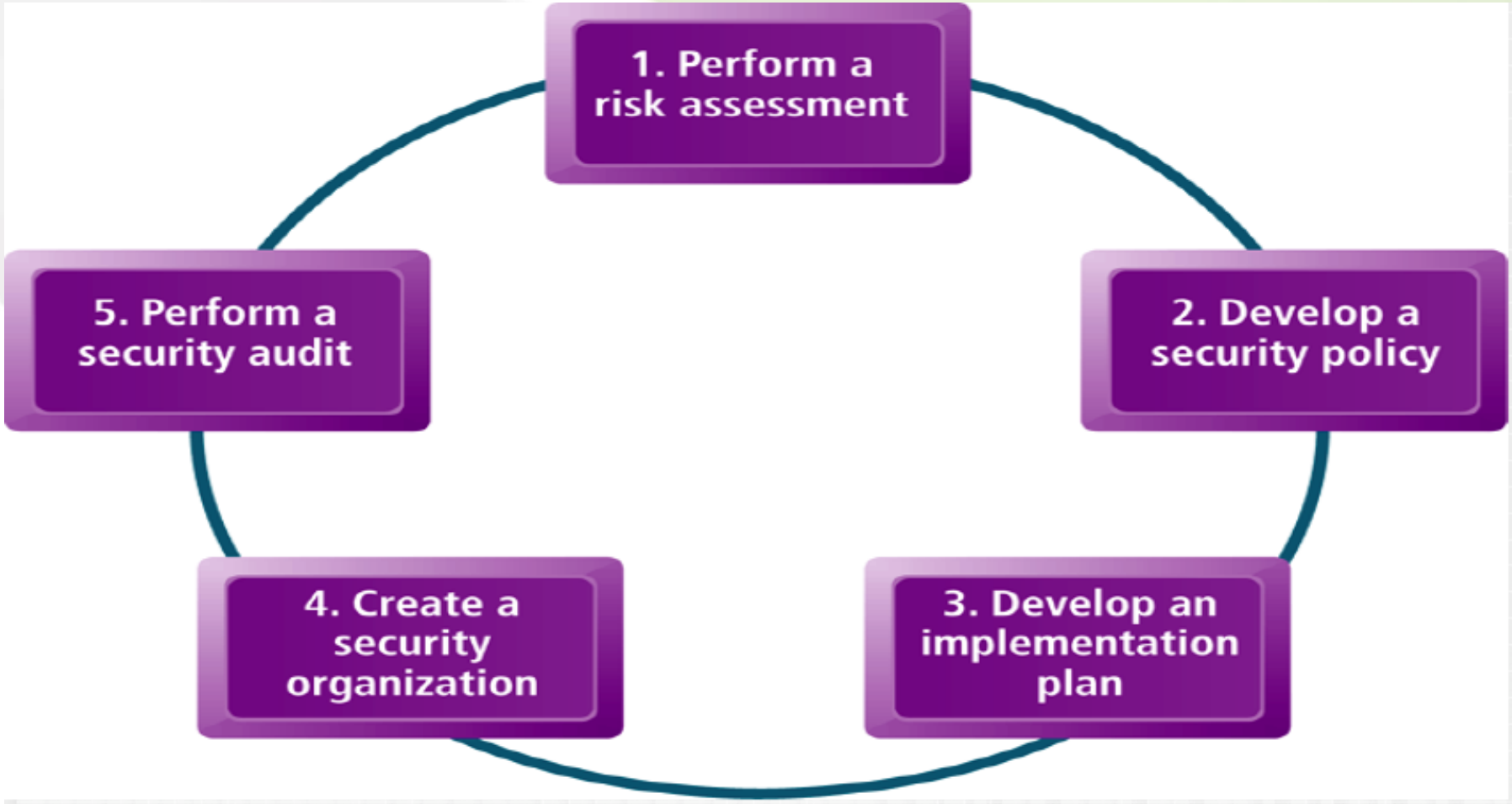
Firewall & Proxy server



Bảo vệ máy tính

- **Chức năng tự bảo vệ của hệđiều hành**
  - Authentication: kiểm tra username, password của user đăng nhập
  - Authorization: cấp phép sử dụng các tài nguyên cho user
  - Accounting: ghi lại nhật ký truy cập của user
- **• Phần mềm diệt virus**
  - Nhận biết và tiêu diệt hầu hết các loại virus thông thường ngay khi chúng xâm nhập vào máy tính hoặc ẩn nấp trên đĩa cứng
  - Phải được cập nhật thường xuyên mới có khả năng phát hiện và tiêu diệt các loại virus mới liên tục xuất hiện
- **Phần mềm hệ thống phát hiện xâm nhập**
  - Dò tìm và nhận biết những công cụ mà tin tặc thường dùng hoặc các hành động khả nghi

Lập kế hoạch bảo mật



Lập kế hoạch bảo mật

- Tiger team: công việc chủ yếu là phát hiện các lỗ hổng có thể tấn công vào các hệ thống máy tính
  - Bắt đầu từ thập niên 1970 với U.S. Air Force
  - Chỉ dùng tin tặc "mũ trắng"
- Vai trò của chính phủ và luật pháp

Practice 5

- ASP.NET:
- Bài thực hành 4: Tạo trang sản phẩm và chi tiết sản phẩm sử dụng kỹ thuật MasterPage của ASPX
- Additional chapter material : COMPUTER.SECURITY.SURVEY.PDF
- Topic project:
  - Kiểm tra phần ứng dụng của End- user trong đồ án

THANK YOU !

Contact : kimloanpt@gmail.com