# CHƯƠNG 5: AN NINH TRỰC TUYẾN VÀ HỆ THỐNG THANH TOÁN TRỰC TUYẾN


- TS. NGUYỄN THÀNH HUY
- KHOA CNTT KINH DOANH


# CYBERWAR:

## Mutually Assured Destruction 2.0

*Class Discussion*

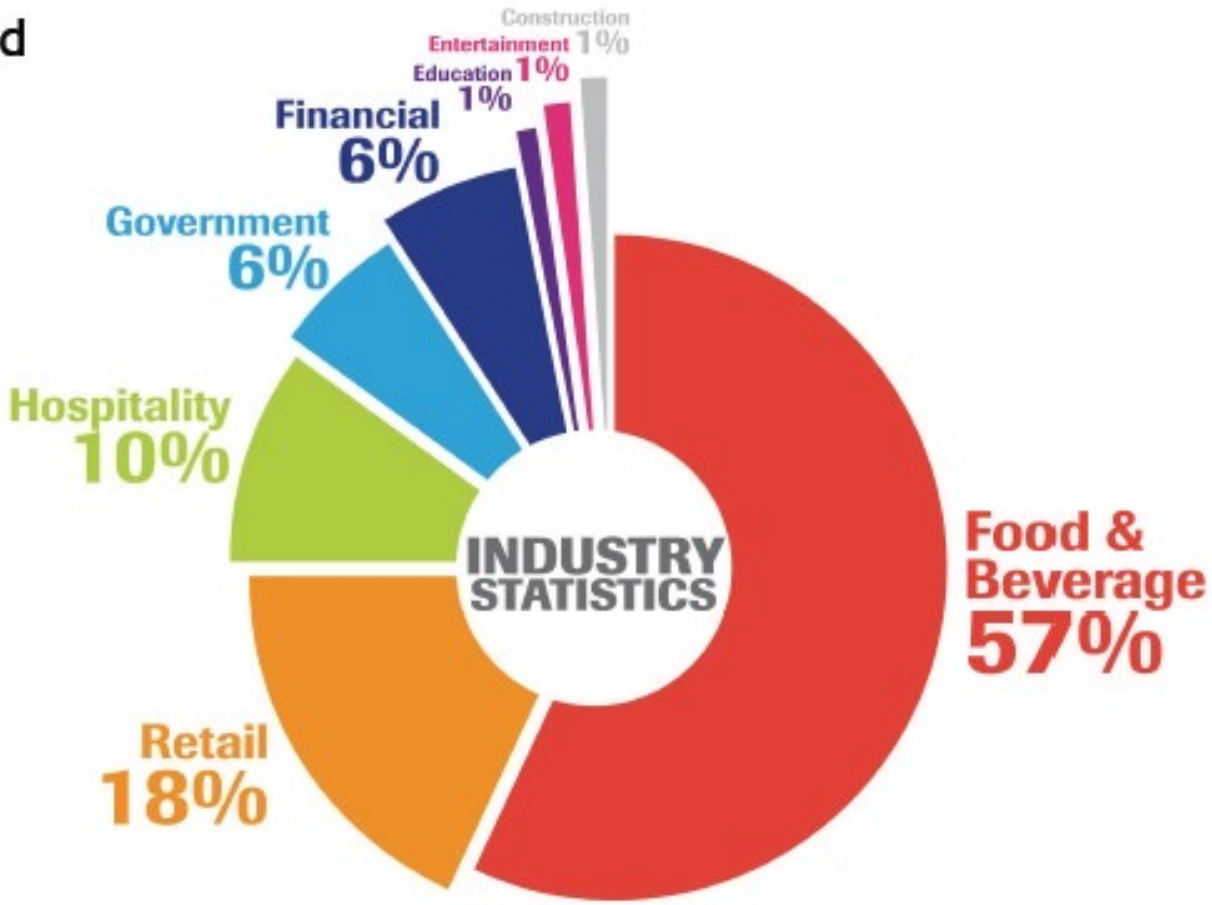
- Sự khác biệt giữa hack và chiến tranh mạng?
- Tại sao hiện nay chiến tranh mạng gây hậu quả nghiêm trọng hơn trước đây?
- Số lượng máy tính bị nhiễm mã độc hại?
- Giải pháp chính trị để MAD 2.0 đủ hiệu quả?

# MÔI TRƯỜNG AN NINH TMĐT

- Nhìn chung qui mô và những thiệt hại gây ra từ các cuộc tấn công không rõ ràng
  - Báo cáo công bố
- Theo nghiên cứu CSI 2013: 49% các doanh nghiệp khảo sát phát hiện ra các sự vi phạm trong năm ngoái
  - Thiệt hại trung bình khoảng $11.56 million/year
- Ăn cắp thông tin từ các server

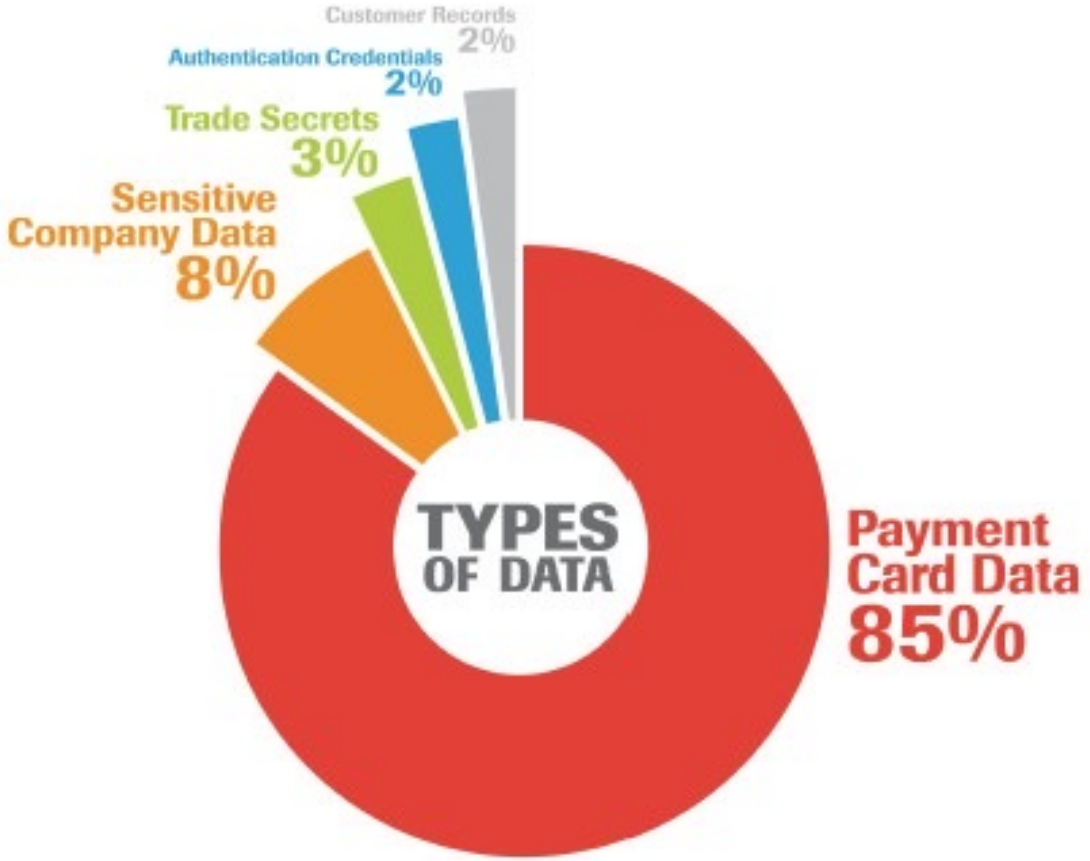
# Incident Response Investigations

- Industries Represented
  - 75% of cases - Food & Beverage and Retail
  - Less focus on hospitality than previous year
  - A group responsible for the majority increased their scope



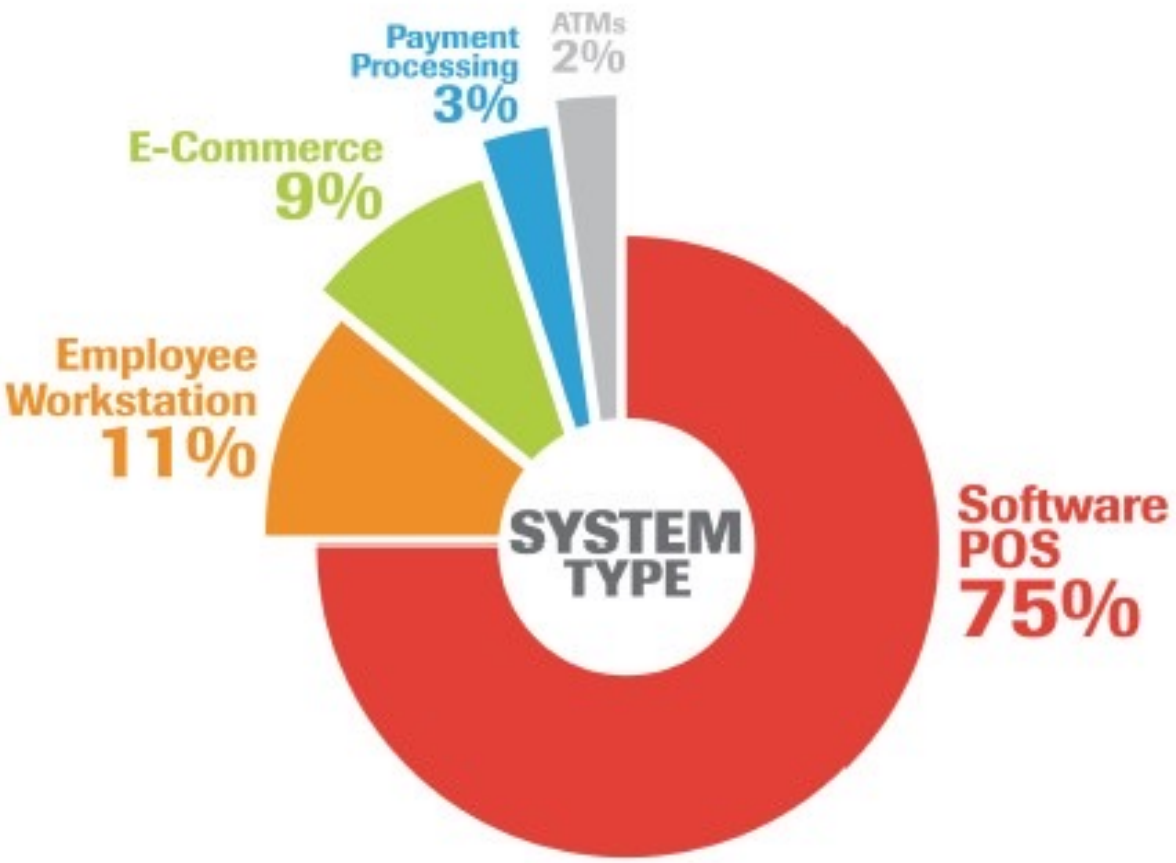
# Incident Response Investigations

- **Data at Risk**
  - Payment card data- simplest to monetize
  - Sensitive data
    - M&A activity
    - Board minutes
    - Intelligence
    - Proprietary data
    - Trade secrets



# Incident Response Investigations

- **Target Assets**
  - POS systems continue to be path of least resistance
  - Most relied on 3rd party integrators
  - EMV countries still a target
    - Focus on card present environments
    - As mag-reader POS still in use



## TABLE 5.2 THE CYBER BLACK MARKET FOR STOLEN DATA

| DATA | PRICE* |
|---|---|
| Individual U.S. card number with expiration date and CVV2 (the three-digit number printed on back of card) (referred to as a CVV) | $5–$8 |
| Individual U.S. card number with full information, including full name, billing address, expiration date, CVV2, date of birth, mother's maiden name, etc. (referred to as a Fullz or Fullzinfo) | $30 |
| Dump data for U.S. card (the term "dump" refers to raw data such as name, account number, expiration data, and CVV encoded on the magnetic strip on the back of the card) | $110–$120 |
| Online payment service accounts | $20–$300 |
| Bank account login credentials | $80–$700 |
| Online account login credentials (Facebook, Twitter, eBay) | $10–$15 |
| Medical information/health credentials | $10–$20 |
| 1,000 e-mail addresses | $1–$10 |
| Scan of a passport | $1–$2 |

SOURCES: Based on data from McAfee, 2016; Intel Security, 2015; Symantec, 2015; Maruca, 2015; Infosec Institute, 2015; RAND Corporation, 2014.

*Prices vary based on supply and quality (freshness of data, account balances, validity, etc.).

# AN NINH TMĐT NÀO LÀ TỐT?

- Đạt được chứng chỉ cao nhất về an ninh
  - Các công nghệ mới nhất
  - Những chính sách và thủ tục của tổ chức
  - Các tiêu chuẩn ngành và pháp luật
- Các yếu tố khác
  - Thời giờ là tiền bạc
  - Chi phí cho an ninh vs thiệt hại
  - An ninh thường bị phá vỡ tại những liên kết yếu nhất

# THE E-COMMERCE SECURITY ENVIRONMENT

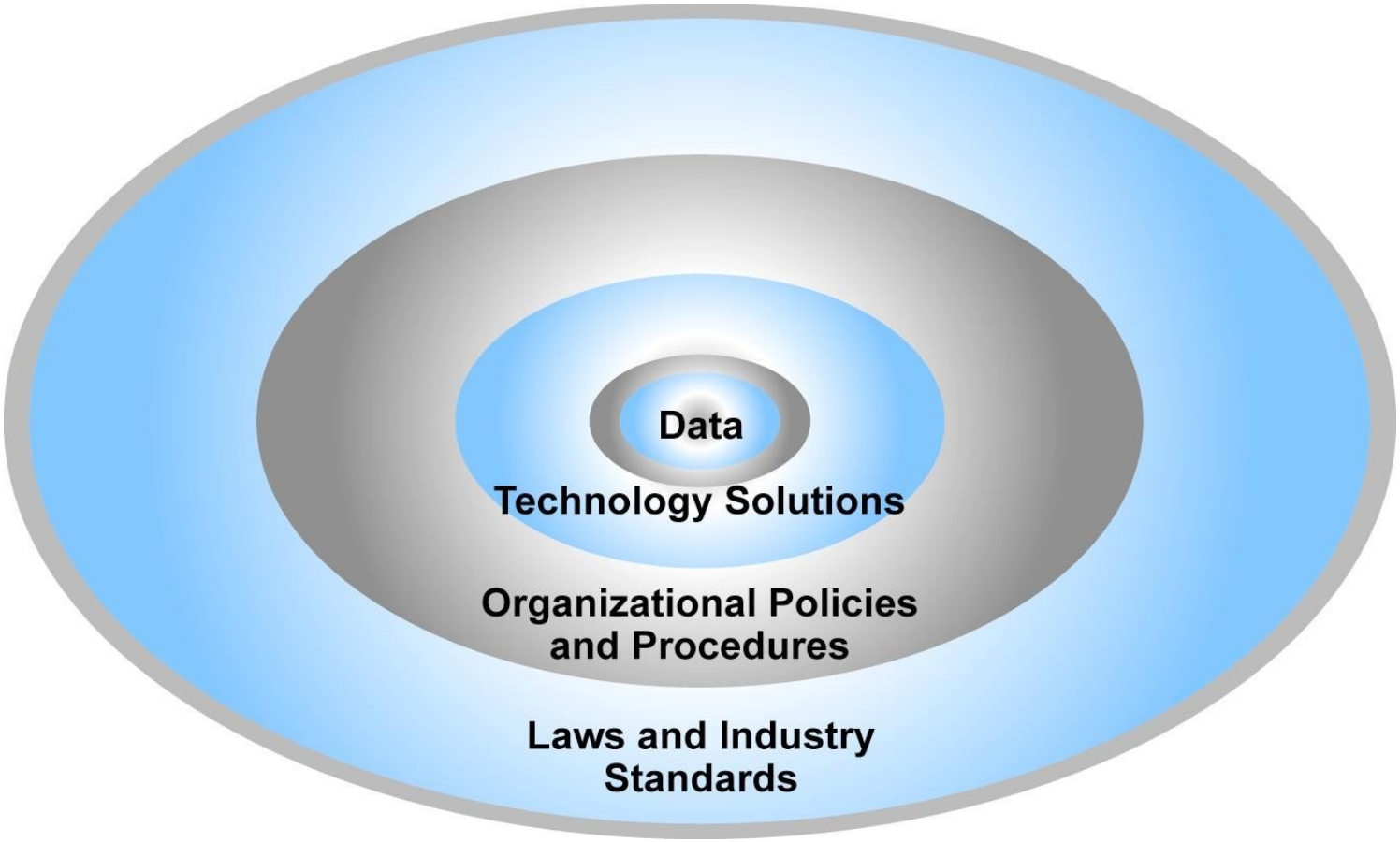



**Figure 5.2, Page 269**

# Sự bất đồng giữa an ninh và các giá trị khác

- Dễ sử dụng:
  - Càng nhiều tiêu chuẩn an ninh thêm vào càng khó sử dụng site, và việc truy cập ngày càng chậm
- An toàn chung và tội phạm trên Internet
  - Tội phạm sử dụng công nghệ lên kế hoạch tấn công, đe dọa các quốc gia

# CÁC ĐE DỌA AN NINH TRONG TMĐT

- 3 điểm yếu chính:

1. Kênh truyền thông Internet
2. Cấp Server
3. Cấp Client

# A TYPICAL E-COMMERCE TRANSACTION

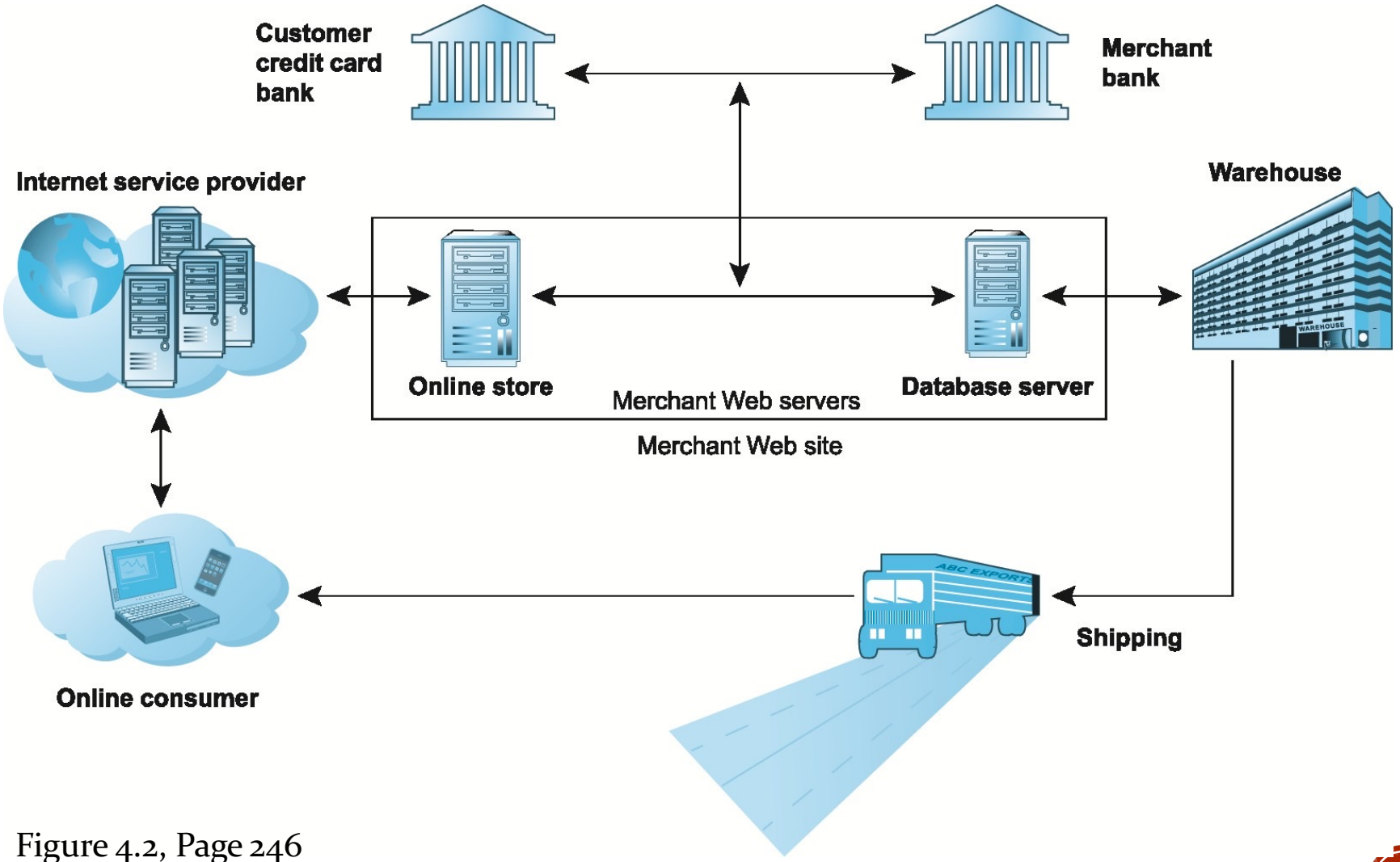



Figure 4.2, Page 246

# VULNERABLE POINTS IN AN E-COMMERCE TRANSACTION

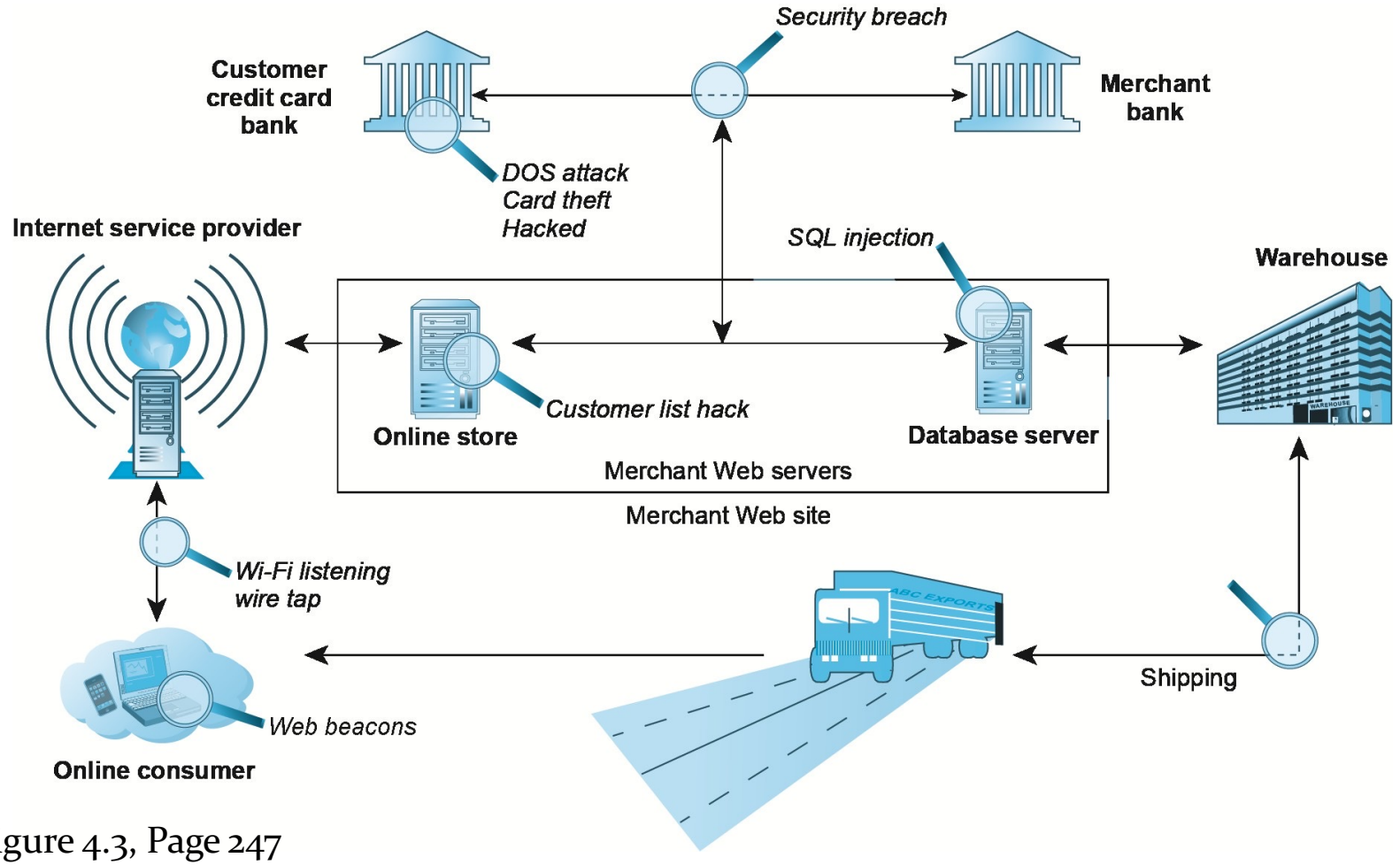



Figure 4.3, Page 247

# CÁC MỐI ĐE DỌA AN NINH PHỔ BIẾN TRONG TMĐT

- Mã độc hại
  - Viruses
  - Worms
  - Trojan horses
  - Bots, botnets
- Các chương trình không mong đợi
  - Browser parasites
  - Adware
  - Spyware

# MOST COMMON SECURITY THREATS (CONT.)

- Phishing
  - Social engineering
  - E-mail scams
  - Spear phishing
  - Identity fraud/theft

# MOST COMMON SECURITY THREATS (CONT.)

- Hacking
  - Hackers vs. crackers
  - Types of hackers: White, black, grey hats
  - Hacktivism
- Cybervandalism:
  - Disrupting, defacing, destroying Web site
- Data breach
  - Losing control over corporate information to outsiders

# HACKERS INFILTRATE TARGET

- What organizational and technological failures led to the data breach at Target?
- What technical solutions are available to combat data breaches?
- Have you or anyone you know experienced a data breach?

*Insight on Business: Class Discussion*

# CÁC MỐI ĐE DỌA AN NINH PHỔ BIẾN

- Gian lận thẻ tín dụng/ trộm cắp
- Spoofing
- Pharming
- Spam/junk Web sites
- Tấn công từ chối phục vụ - Denial of service (DoS)

# CÁC MỐI ĐE DỌA AN NINH PHỔ BIẾN

- Sniffing
- Tấn công từ bên trong (nhân viên - Insider jobs)
  - Single largest financial threat
- Phần mềm server & client thiết kế kém
- Các đe dọa từ Mobile

*Insight on Technology: Class Discussion*

# THINK YOUR SMARTPHONE IS SECURE?

- What types of threats do smartphones face?
- Are there any particular vulnerabilities to this type of device?
- What did Nicolas Seriot's "Spyphone" prove?
- Are apps more or less likely to be subject to threats than traditional PC software programs?

# CÁC GIẢI PHÁP CÔNG NGHỆ

- Bao vệ truyền thông Internet (encryption)
- Các kênh truyền thông an toàn (SSL, S-HTTP, VPNs)
- Bao vệ mạng (firewalls)
- Bao vệ servers và clients
  - OS security, anti-virus

# Tools Available to Achieve Site Security

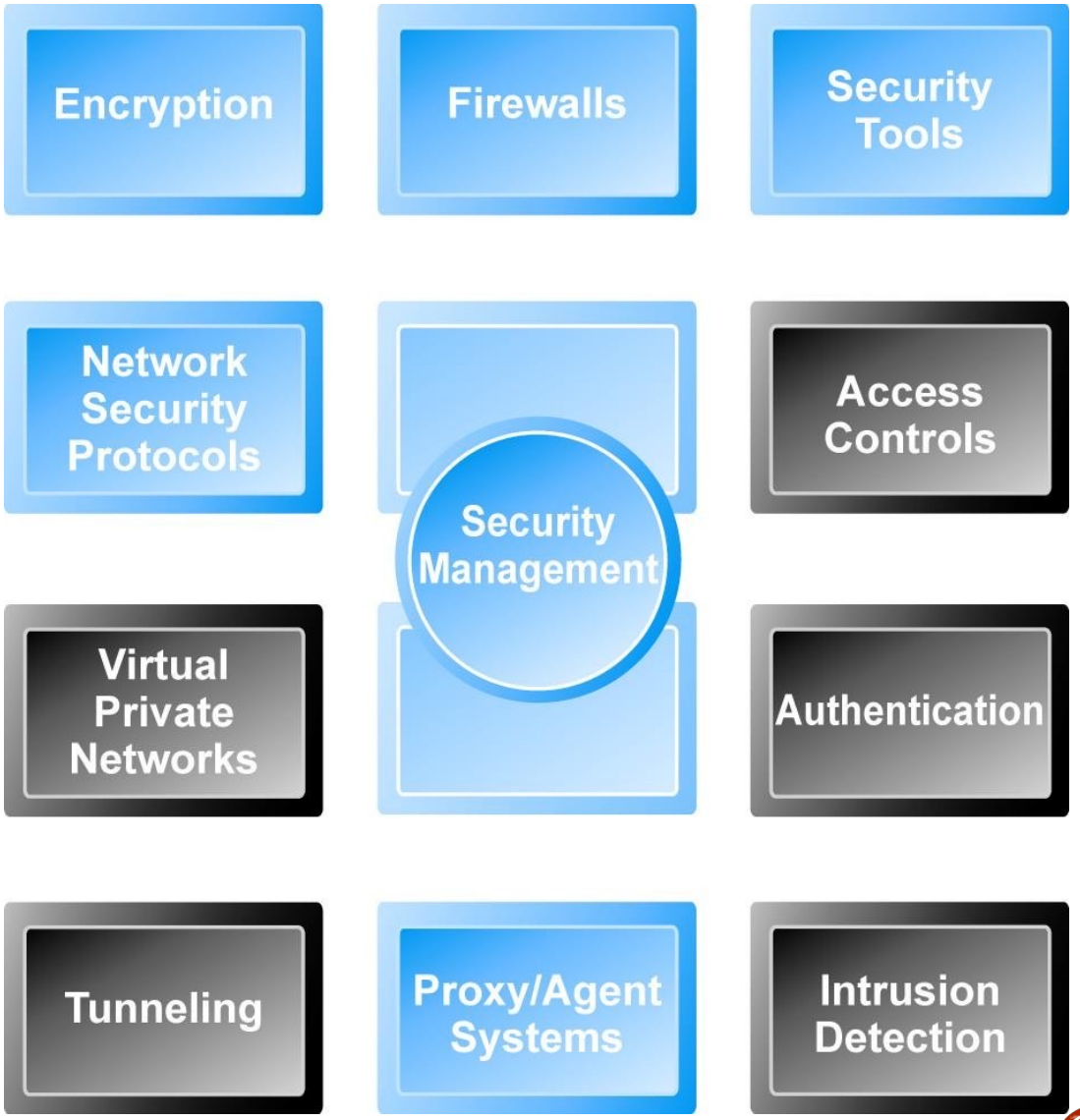



**Figure 5.7, Page 287**

# MÃ HÓA DỮ LIỆU

- Mã hóa dữ liệu
  - Chuyển dữ liệu thành dạng chỉ có thể đọc được bởi người gửi và người nhận
  - Đam bao an toàn cho thông tin khi lưu trữ và truyền tai
  - Nhằm đam bao an ninh TMĐT:
    1. Toàn vẹn thông điệp
    2. Chống chối bỏ
    3. Xác thực
    4. Cẩn mật, tin tưởng

# HASH CODING, PRIVATE-KEY, VÀ PUBLIC-KEY ENCRYPTION

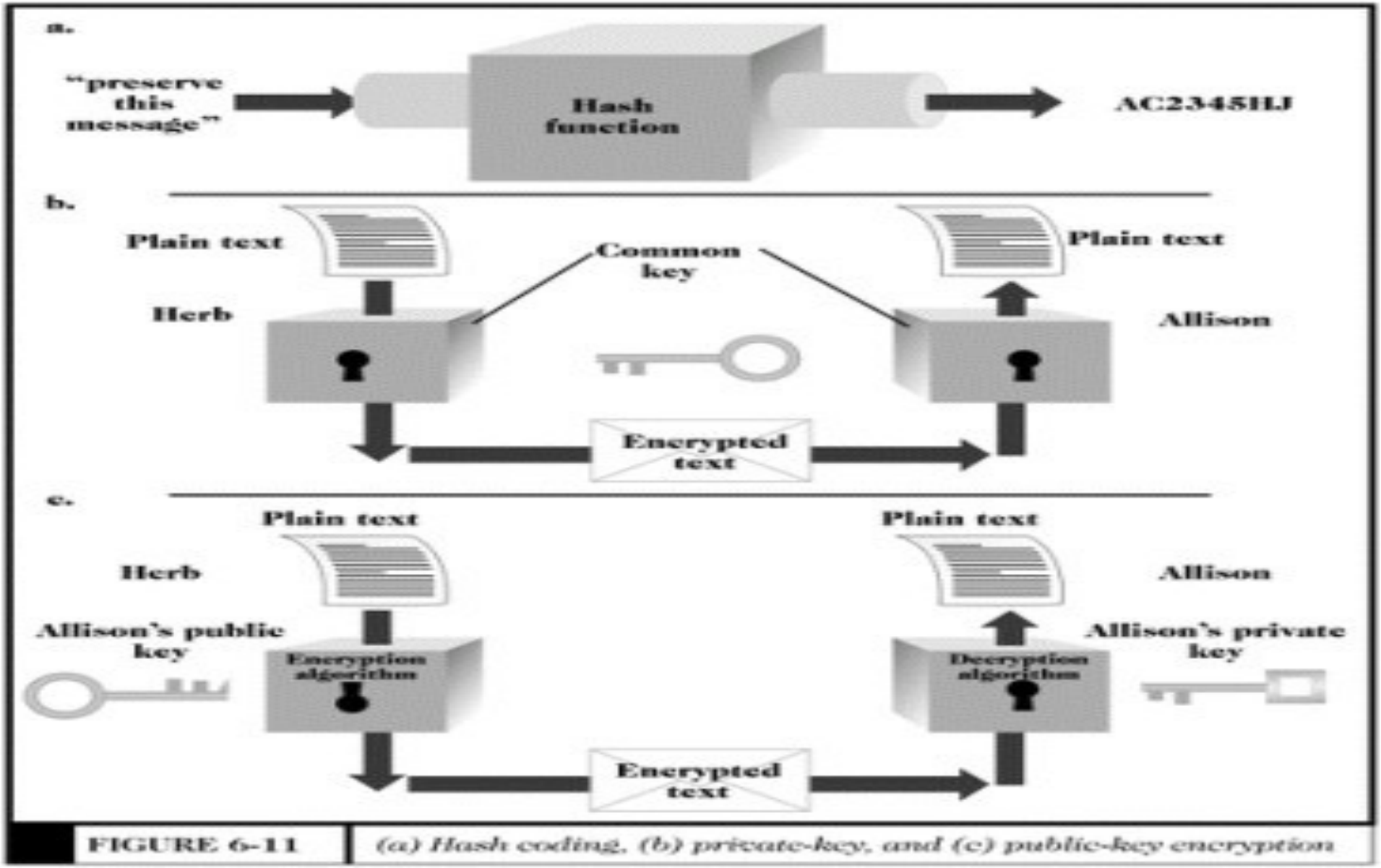



FIGURE 6-11 *(a) Hash coding, (b) private-key, and (c) public-key encryption*

# Mã hóa khóa đối xứng

- Người gửi và người nhận sử dụng cùng khóa số cho việc mã hóa và giai mã thông điệp
- Yêu cầu phai có khóa khác nhau cho mỗi giao dịch
- Sức mạnh của mã hóa phụ thuộc vào chiều dài của khóa mã hóa dữ liệu
- Advanced Encryption Standard (AES)
  - Được áp dụng rộng rãi
  - Sử dụng khóa mã hóa có chiều dài 128-, 192-, 256-bit
- Các chuẩn khác có thể sử dụng khóa 2,048 bits

# MÃ HÓA KHÓA CÔNG KHAI – KHÓA BẤT ĐỐI XỨNG

- Sử dụng 2 khóa số có quan hệ về mặt toán học với nhau
  - Public key (widely disseminated)
  - Private key (kept secret by owner)
- Ca 2 khóa đều có thể dùng cho quá trình mã hóa và giai mã thông điệp
- Mã hóa bằng khóa này chỉ có thể giai mã bằng khóa kia và ngược lại

# PUBLIC KEY CRYPTOGRAPHY – A SIMPLE CASE

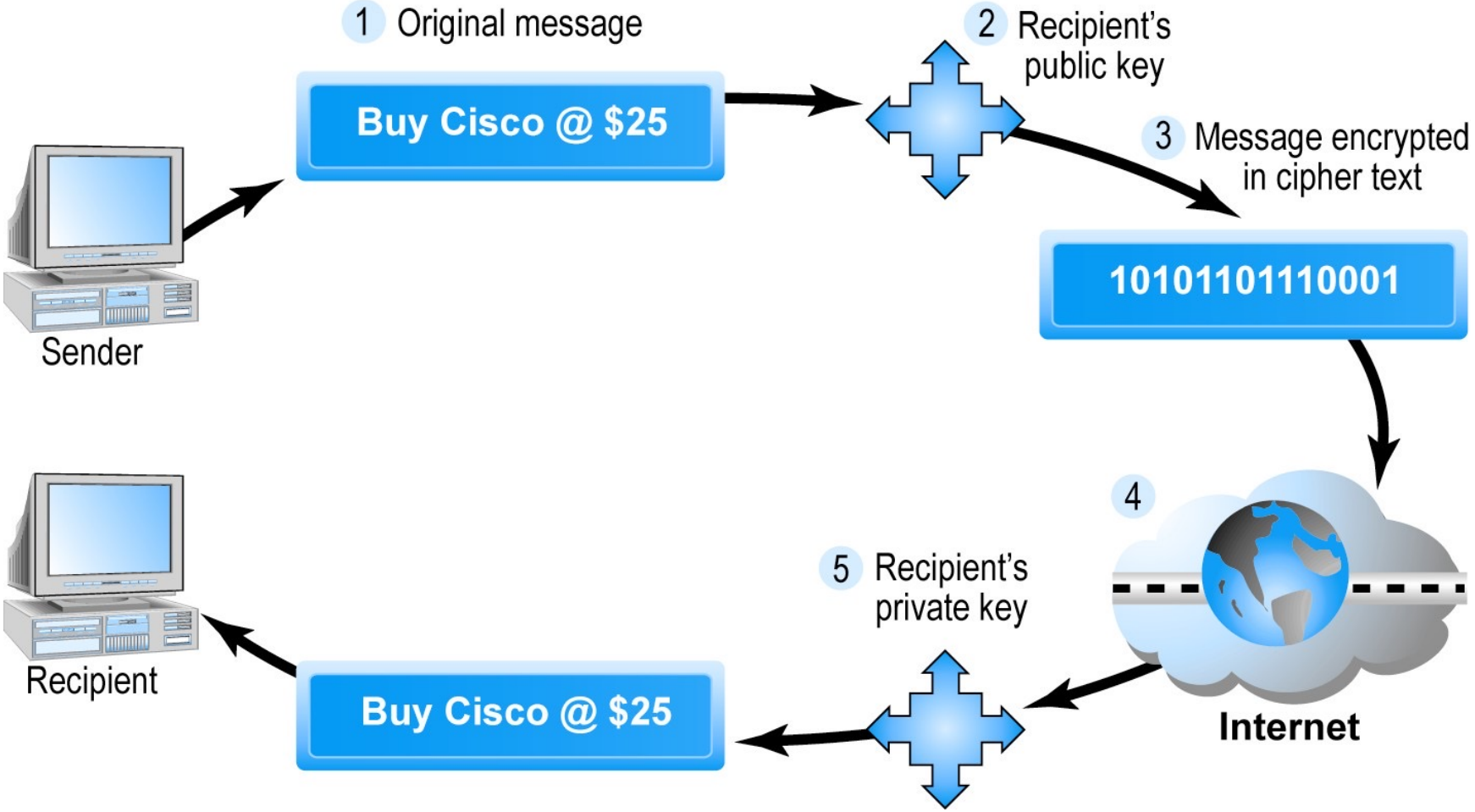



**Figure 5.8, Page 289**

# MÃ HÓA KHÓA CÔNG KHAI, CHỮ KÝ SỐ VÀ HASH DIGESTS

- Hàm Hash:
  - Thuật toán tạo ra dãy số có chiều dài cố định gọi là message hay hash digest
- Hash digest của thông điệp gửi đến người nhận nhằm kiểm tra tính toàn vẹn của thông điệp
- Hash digest và thông điệp được mã hóa với khóa công khai của người nhận
- Toàn văn ban mã hóa sau đó được mã hóa với khóa riêng của người gửi – tạo chữ ký số - nhằm xác thực và chống chối bỏ

# PUBLIC KEY CRYPTOGRAPHY WITH DIGITAL SIGNATURES

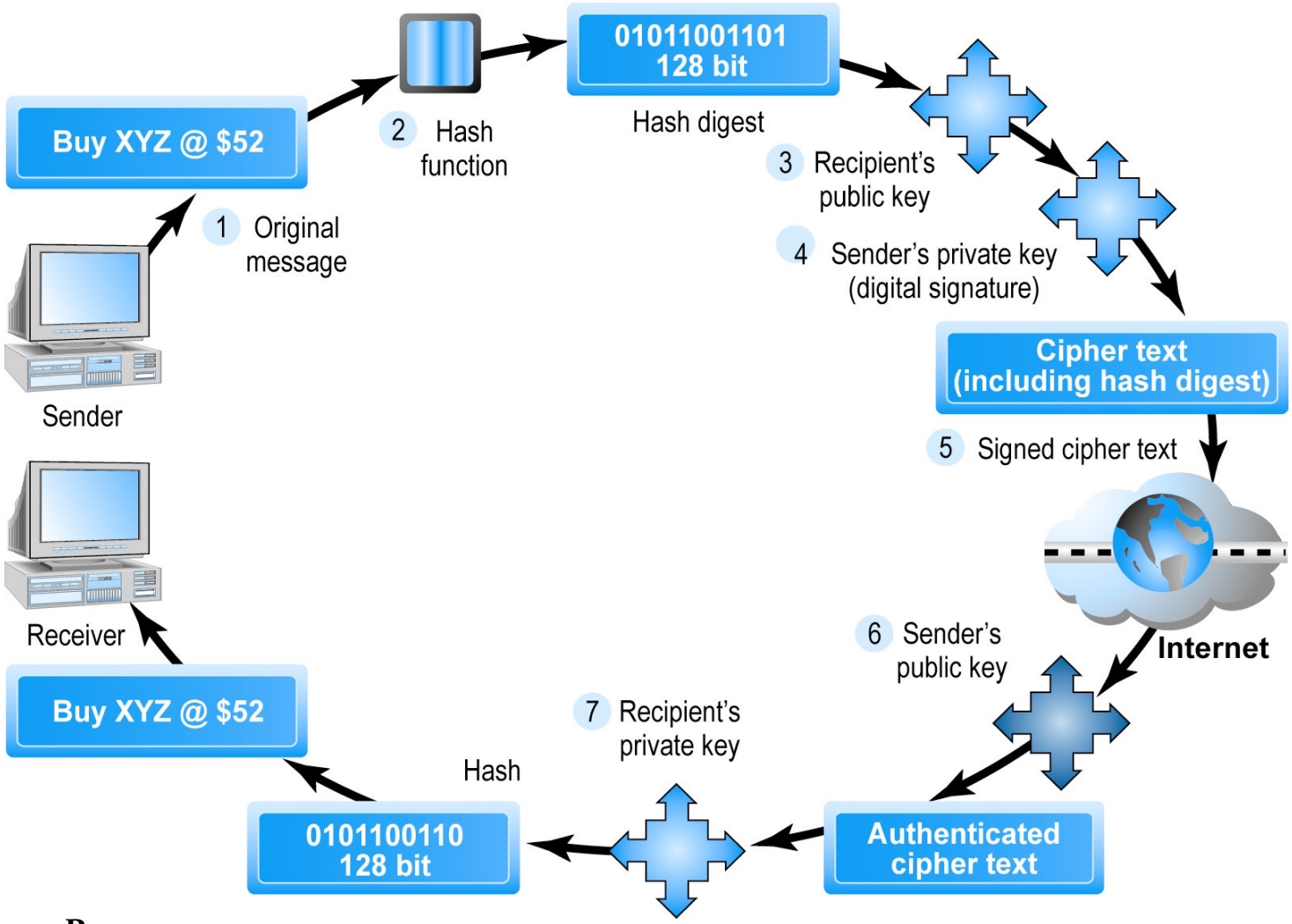



**Figure 5.9, Page 291**

# VĂN BẢN VỚI CHỮ KÝ ĐIỆN TỬ

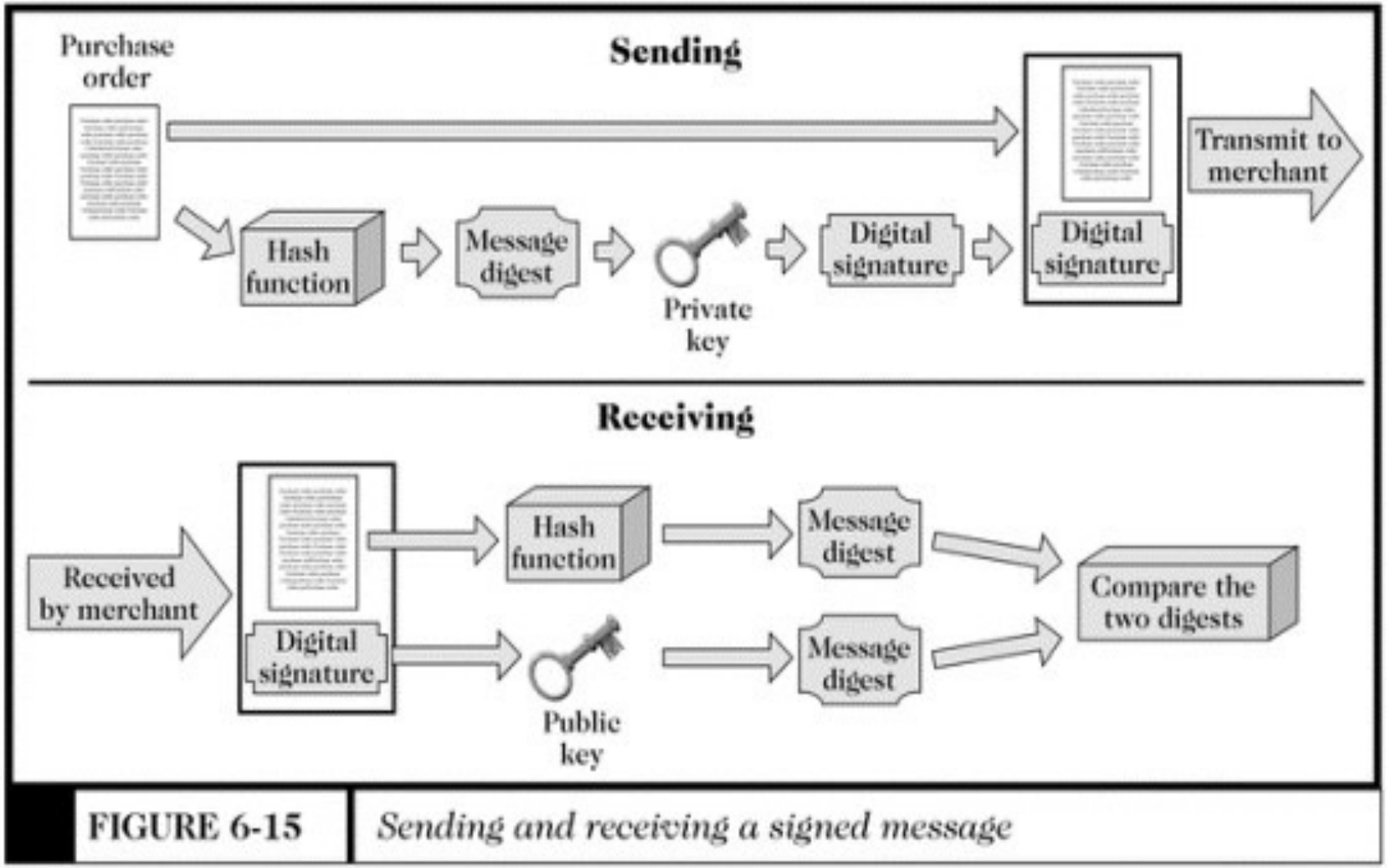



FIGURE 6-15 *Sending and receiving a signed message*

| STT | Gói sản phẩm | Nội dung | Thông số(độ dài khóa) | Giá / 1 năm(VND) | Giá / 2 năm(VND) | Giá / 3 năm(VND) |
|---|---|---|---|---|---|---|
| 01 | Kim Cương | - Kê khai thuế qua mạng,<br>- Quyết toán thuế.<br>- Khai hải quan điện tử<br>- Ký email, văn bản<br>- Giao dịch ngân hàng điện tử, chứng khoán điện tử…<br>- Mã hóa dữ liệu, bảo mật thông tin. | 1024bit | 4.990.000 | 8.980.000 | 11.970.000 |
| 02 | Vàng | - Kê khai thuế qua mạn<br>- Quyết toán thuế<br>- Khai hải quan điện tử<br>- Ký email, văn bản<br>- Giao dịch ngân hàng điện tử, chứng khoán điện tử … | 1024bit | 3.990.000 | 7.180.000 | 9.570.000 |
| 03 | Bạc | - Kê khai thuế qua mạng<br>- Quyết toán thuế<br>- Khai hải quan điện tử<br>- Ký email, văn bản | 1024bit | 990.000 | 1.790.000 | 2.480.000 |

-Giá FPT-CA Token (Chứa chữ ký số): 500,000 VND/ 1 chiếc
-Gói 3 năm được miễn phí sử dụng FPT CA Token
-Chi phí trên chưa bao gồm thuế VAT 10%

# PHONG BÌ SỐ

- Nhược điểm:
  - Mã hóa khóa công khai
    - Tính toán chậm, giam tốc độ truyền tai, tăng thời gian xử lý
  - Mã hóa khóa đối xứng
    - Không an toàn trong quá trình chuyển khóa
- Sử dụng mã hóa khóa đối xứng để mã hóa tài liệu
- Sử dụng mã hóa khóa chung để mã hóa và gửi khóa đối xứng

# CREATING A DIGITAL ENVELOPE

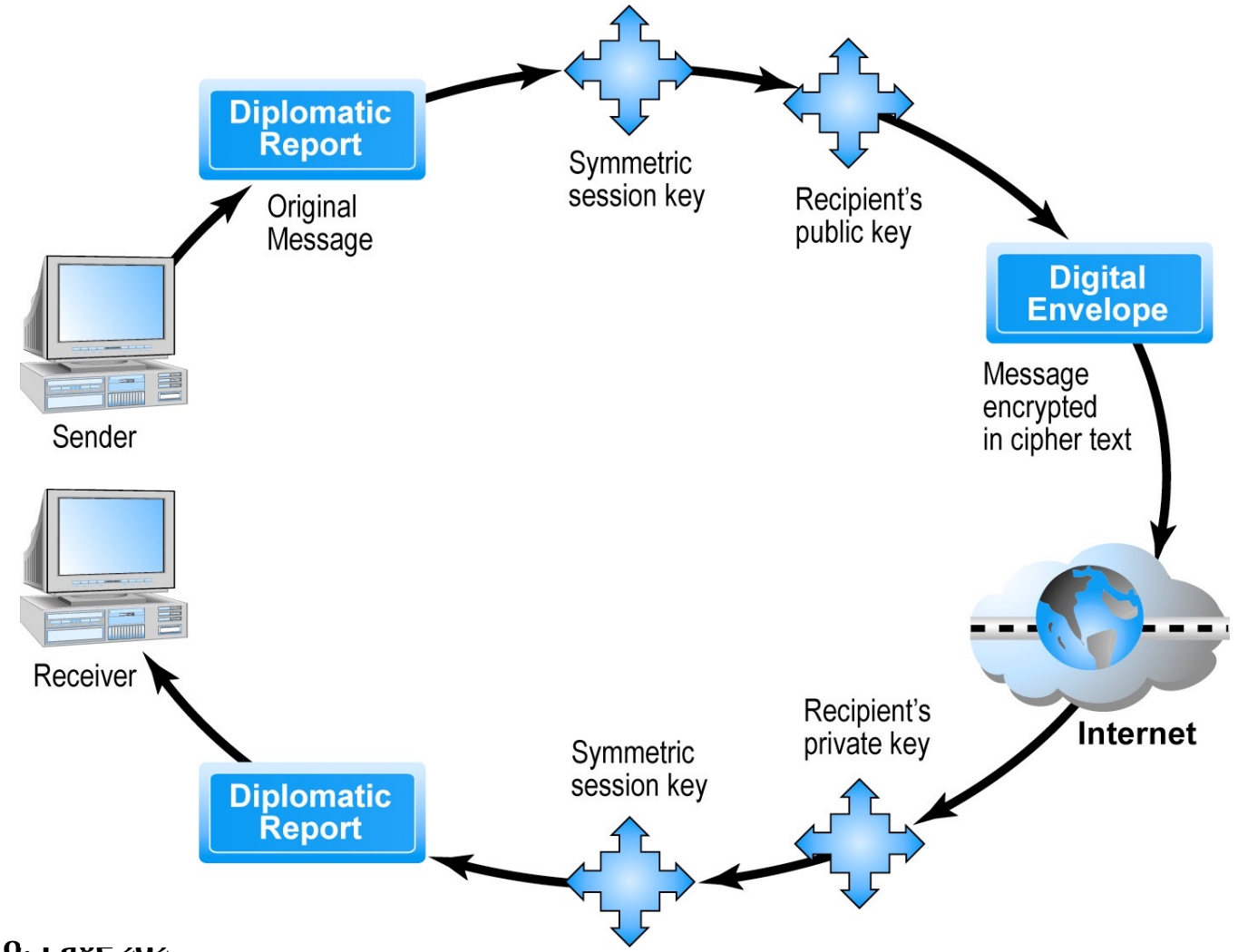
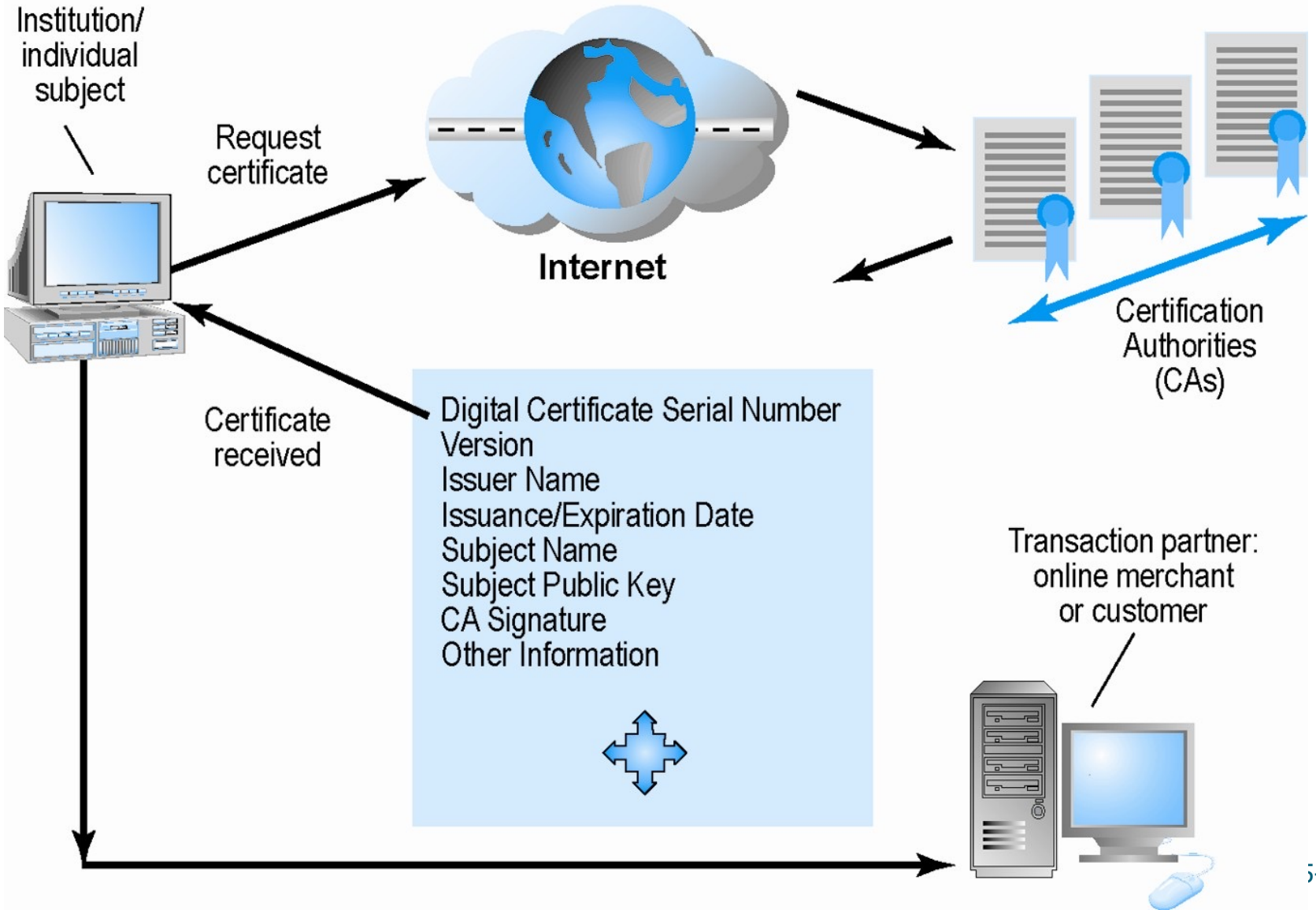



**Figure 5.10, Page 292**

# CHỨNG CHỈ SỐ VÀ CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI - PUBLIC KEY INFRASTRUCTURE (PKI)

- Chứng chỉ số bao gồm:
  - Tên của chủ thể / công ty
  - Khóa công khai của chủ thể
  - Dãy số của chứng chỉ số - Digital certificate serial number
  - Ngày cấp và ngày hết hiệu lực
  - Chữ ký số của CA
- Public Key Infrastructure (PKI):
  - CAs and digital certificate procedures
  - PGP "Pretty Good Privacy"", đây là phương pháp phổ biến nhất và mạnh nhất để mã hóa file hiện nay

# DIGITAL CERTIFICATES AND CERTIFICATION AUTHORITIES



# HẠN CHẾ CỦA CÁC GIẢI PHÁP MÃ HÓA

- Không đam bao trong việc lưu trữ khóa riêng
  - PKI không hiệu qua trong việc phòng chống trong nội bộ
  - Cá nhân không có ý thức trong việc bao vệ khóa riêng
- Các máy tính đã được kiểm tra cũng không đam bao an ninh
- Các CA không được kiểm soát, tự lựa chọn tổ chức

# TRUNG TÂM CHỨNG THỰC KỸ THUẬT SỐ - CA

- Cấp và quan lý chứng thực số cho tất ca các đối tượng tham gia trong môi trường giao dịch điện tử, như các giao dịch thương mại và trao đôi thông tin, gồm những cá nhân, những tổ chức và các hệ thống thương mại điện tử.
- Chứng thực số cho các cá nhân và tổ chức thực hiện an toàn các giao dịch trong môi trường điện tử, như gửi nhận e-mail, mua bán hàng hoá, trao đổi thông tin, phát triển phần mềm...

# TRUNG TÂM CHỨNG THỰC KỸ THUẬT SỐ

- **Các chức năng chính của Trung tâm chứng thực số**
  - Đăng ký xin cấp chứng thực số
  - Xác thực và cấp chứng thực số
  - Truy lục và tìm kiếm thông tin về chứng thực số
  - Yêu cầu thay đổi, gia hạn …
  - Quan lý chứng thực số

# TRUNG TÂM CHỨNG THỰC KỸ THUẬT SỐ

- Công cụ an toàn, bao mật và xác thực hợp pháp cho các hệ thống hoạt động thương mại điện tử: các web site giao dịch B2B, các web site bán hàng, hệ thống thanh toán trực tuyến…
- Sử dụng chứng thực số giúp cho bao đam an toàn các giao dịch điện tử. Tránh được các nguy cơ, gia mạo thông tin, lộ các thông tin nhậy cam, mạo danh, xuyên tạc và thay đổi nội dung thông tin.

# CÂU HỎI

- Xin cấp chứng thực số ở đâu ???
- Đã có cơ quan cấp chứng thực số tại VN???