# AN TOÀN MẠNG MÁY TÍNH

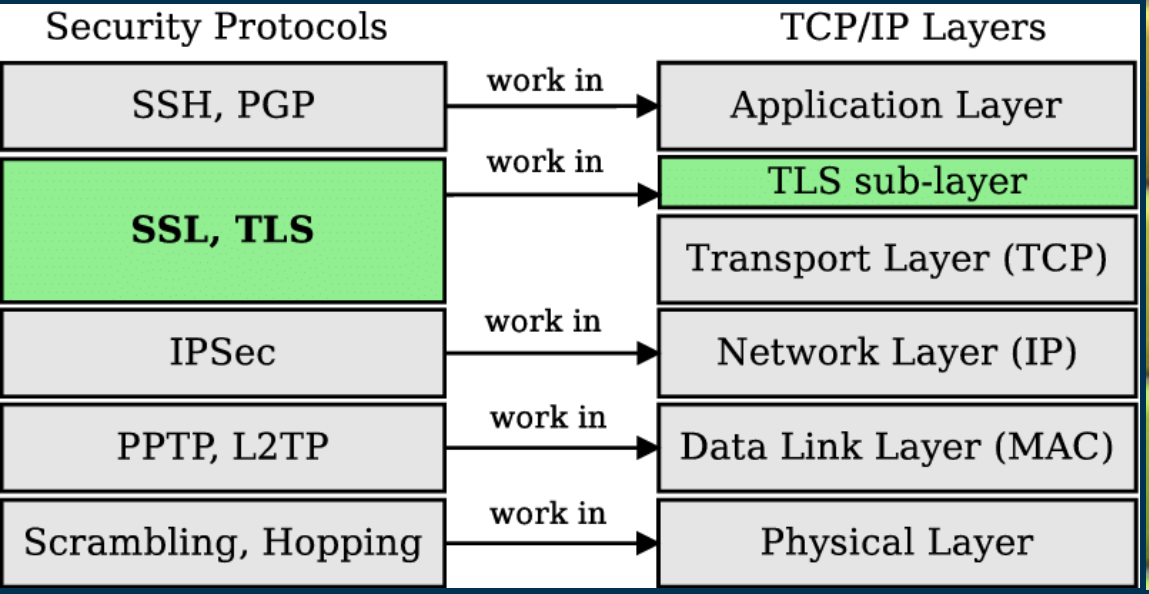
## #06: Security Protocols

ThS. Lê Đức Thịnh, UIT

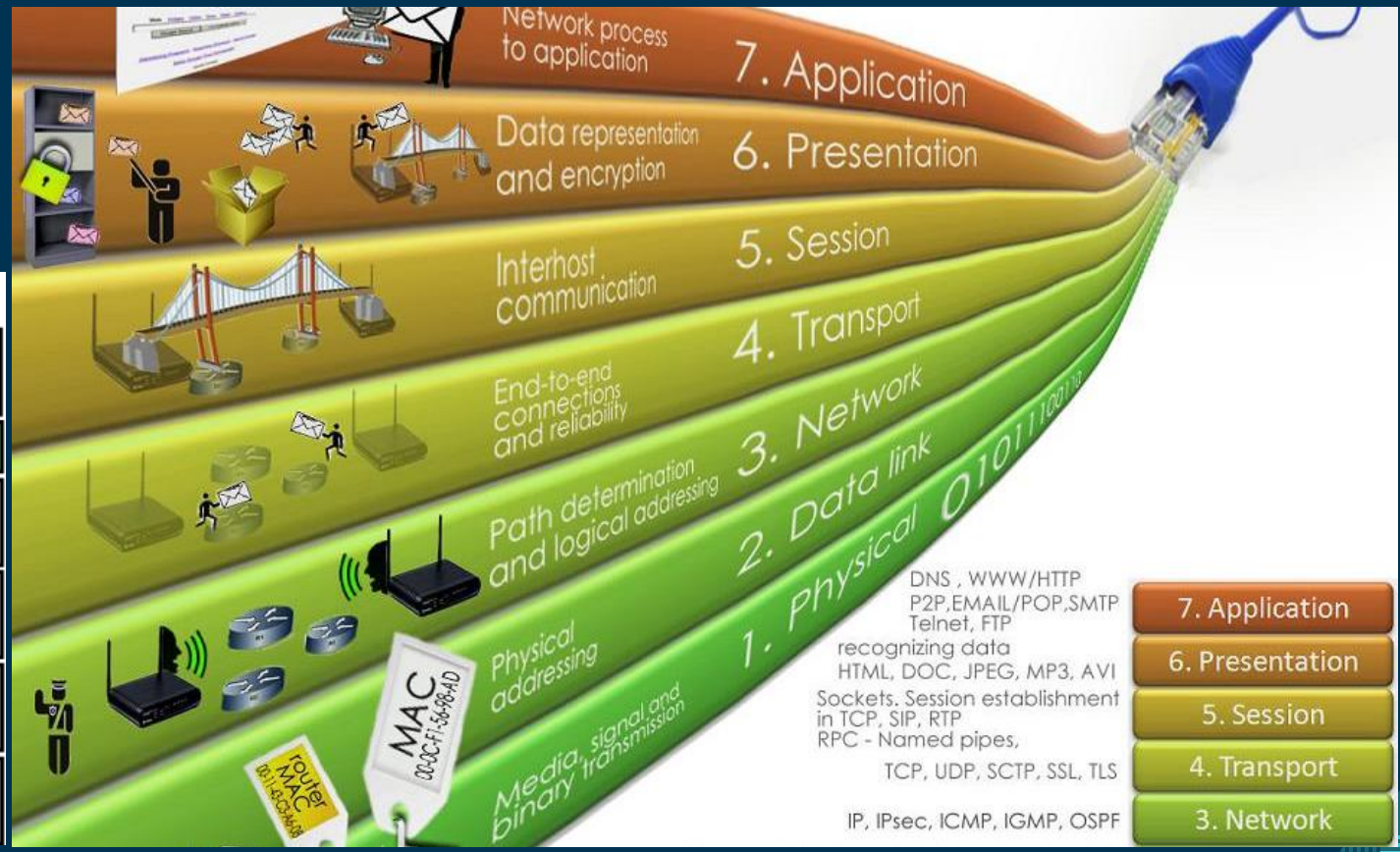
# Nội dung

1. Tổng quan
2. PKI
3. SSL/TLS
4. DNS
5. SSH
6. IPSec

# 1. Ứng dụng mật mã trong mạng máy tính

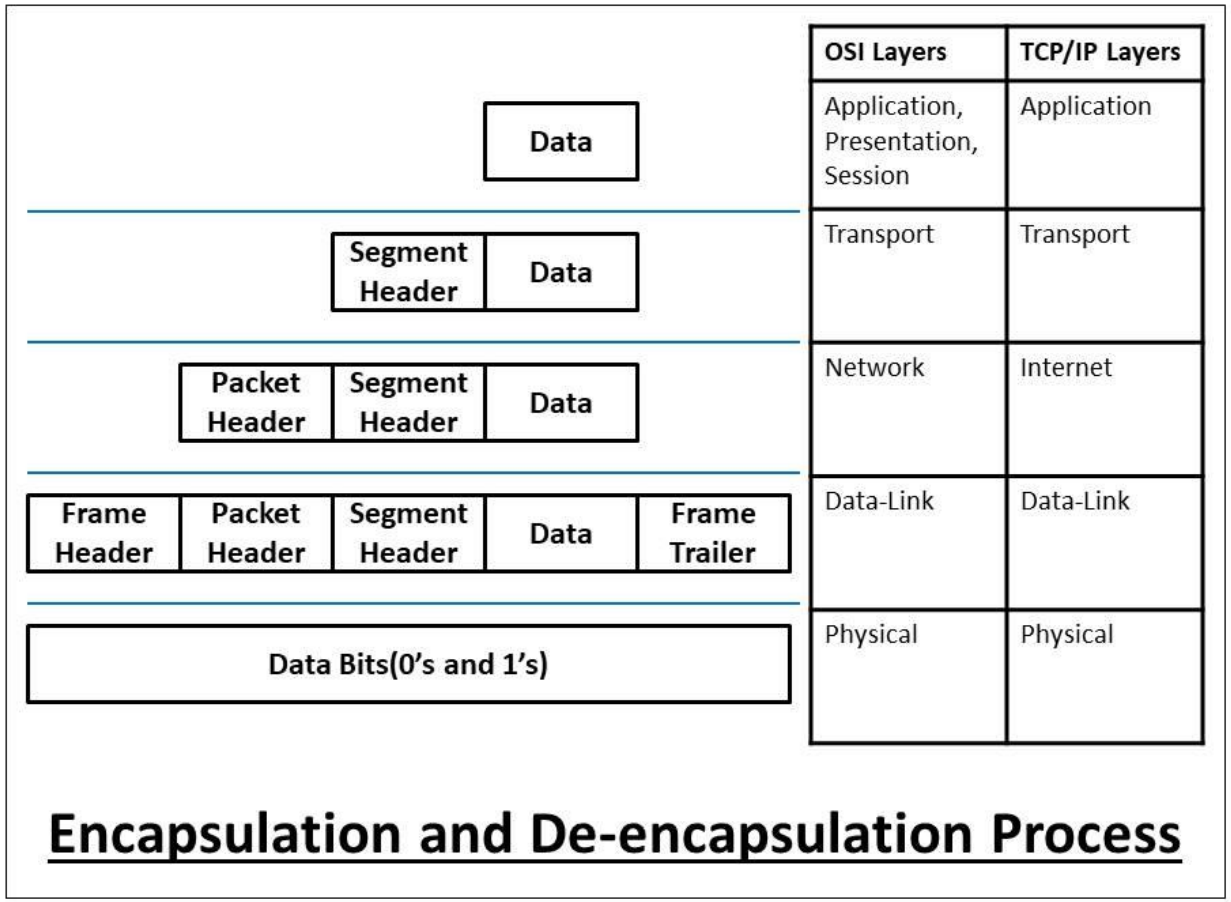



ResearchGate



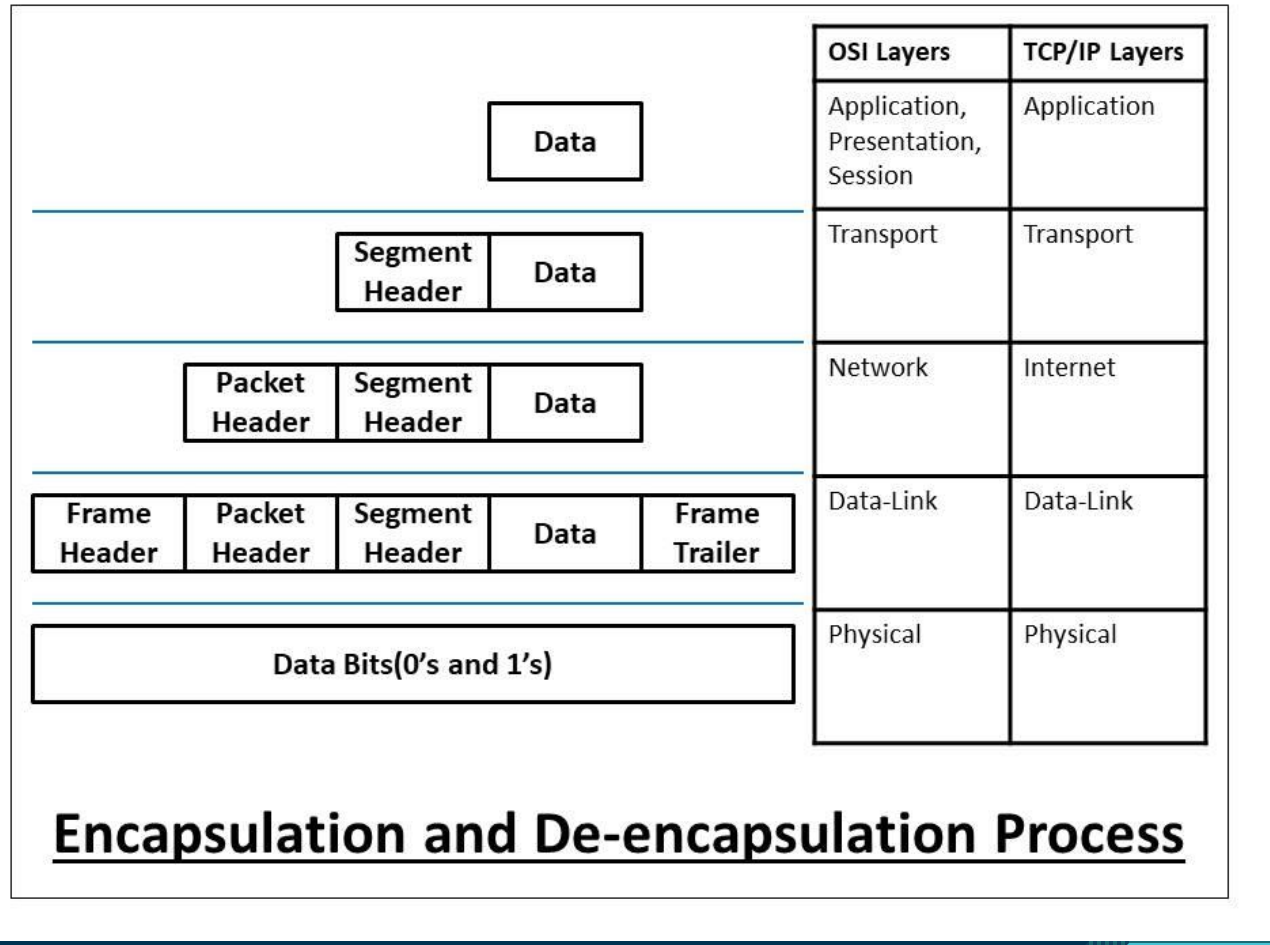
# 1. Ứng dụng mật mã trong mạng máy tính

- 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.



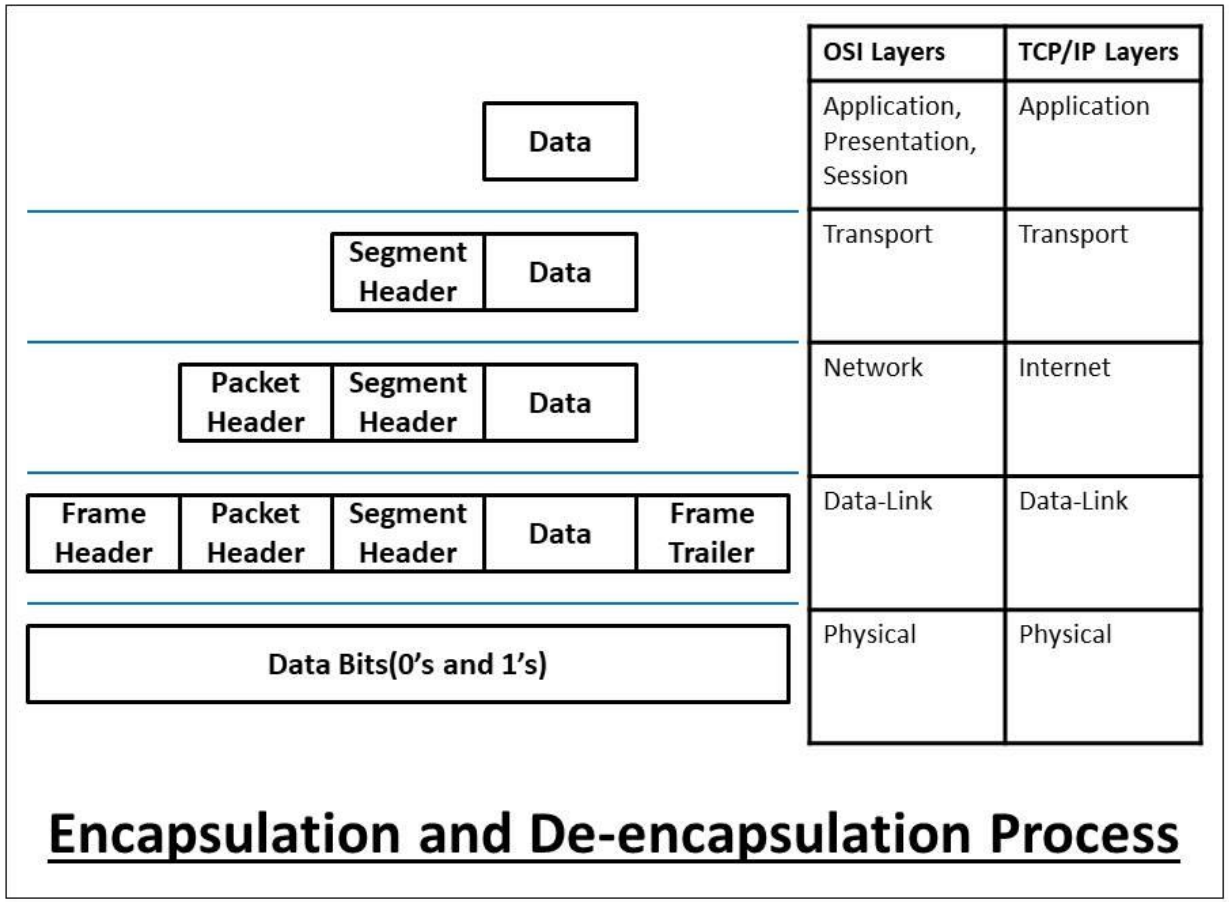
# 1. Ứng dụng mật mã trong mạng máy tính

- 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.



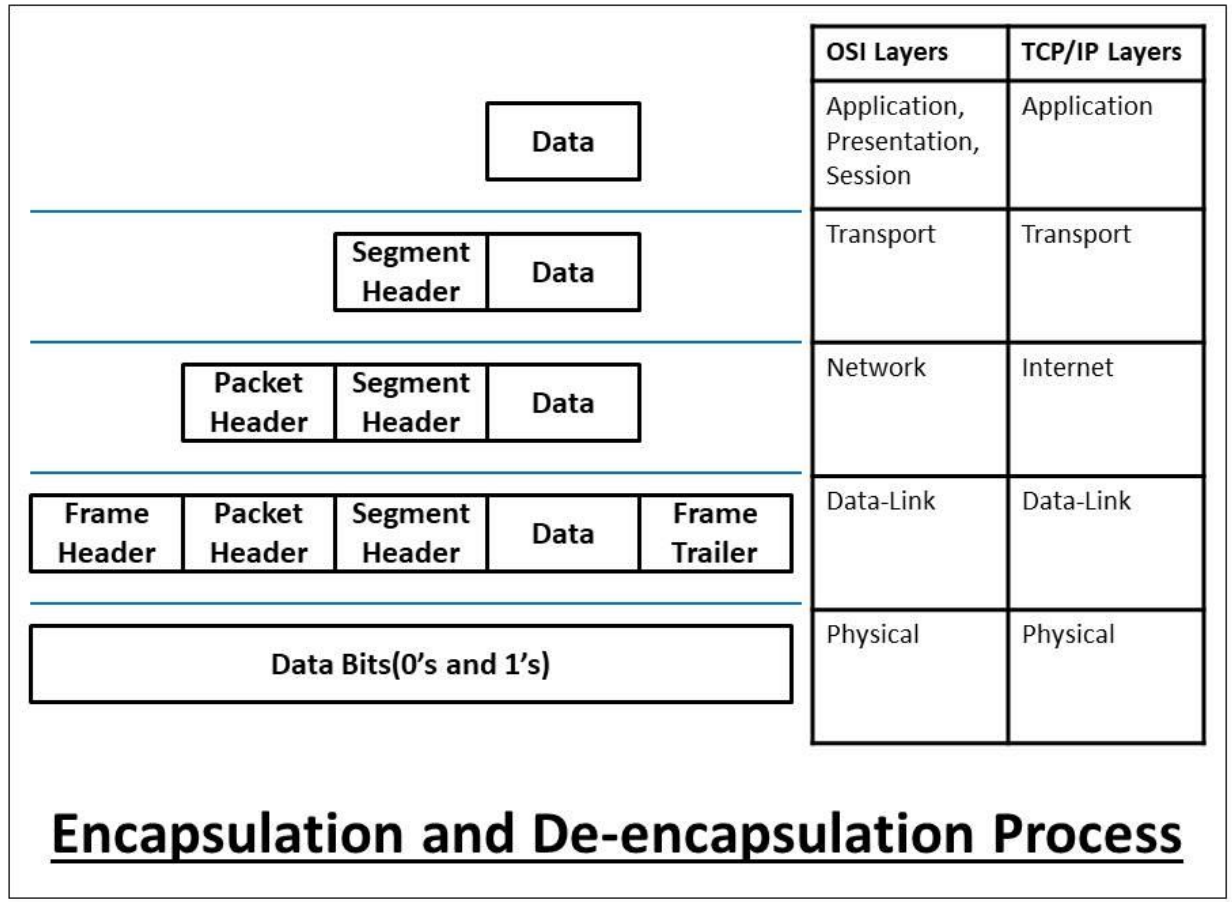
# 1. Ứng dụng mật mã trong mạng máy tính

- 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. Ứng dụng mật mã trong mạng máy tính

- 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.
  - VD: bảo mật mạng không dây

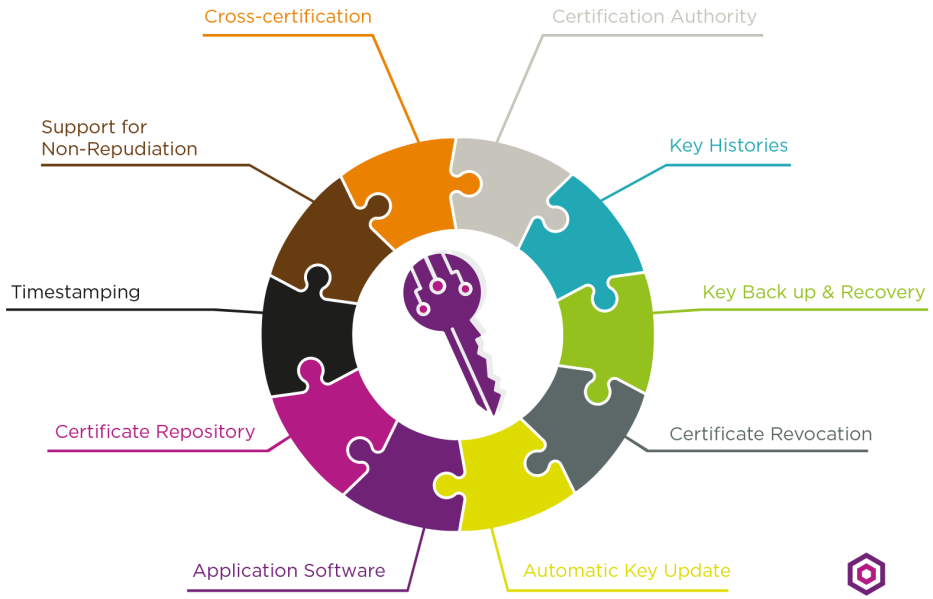


# 1. Ứng dụng mật mã trong mạng máy tính

- 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. PKI - Public Key Infrastructure

- *"A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption"* – Wikipedia.




https://www.entrust.com/resources/certificate-solutions/learn/what-is-pki

# 2. PKI - Public Key Infrastructure

- **Mục tiêu:**
  - PKI cho phép những người tham gia xác thực lẫn nhau và sử dụng thông tin từ các chứng thực khóa công khai để mật mã hóa và giải mã thông tin trong quá trình trao đổi.
  - Tạo điều kiện thuận lợi cho việc chuyển giao thông tin điện tử an toàn cho các hoạt động mạng như thương mại điện tử, ngân hàng trực tuyến và email bí mật, ...
- Một PKI đảm bảo các tính:
  - Confidentiality
  - Integrity
  - Authentication
  - Non-Repudiation

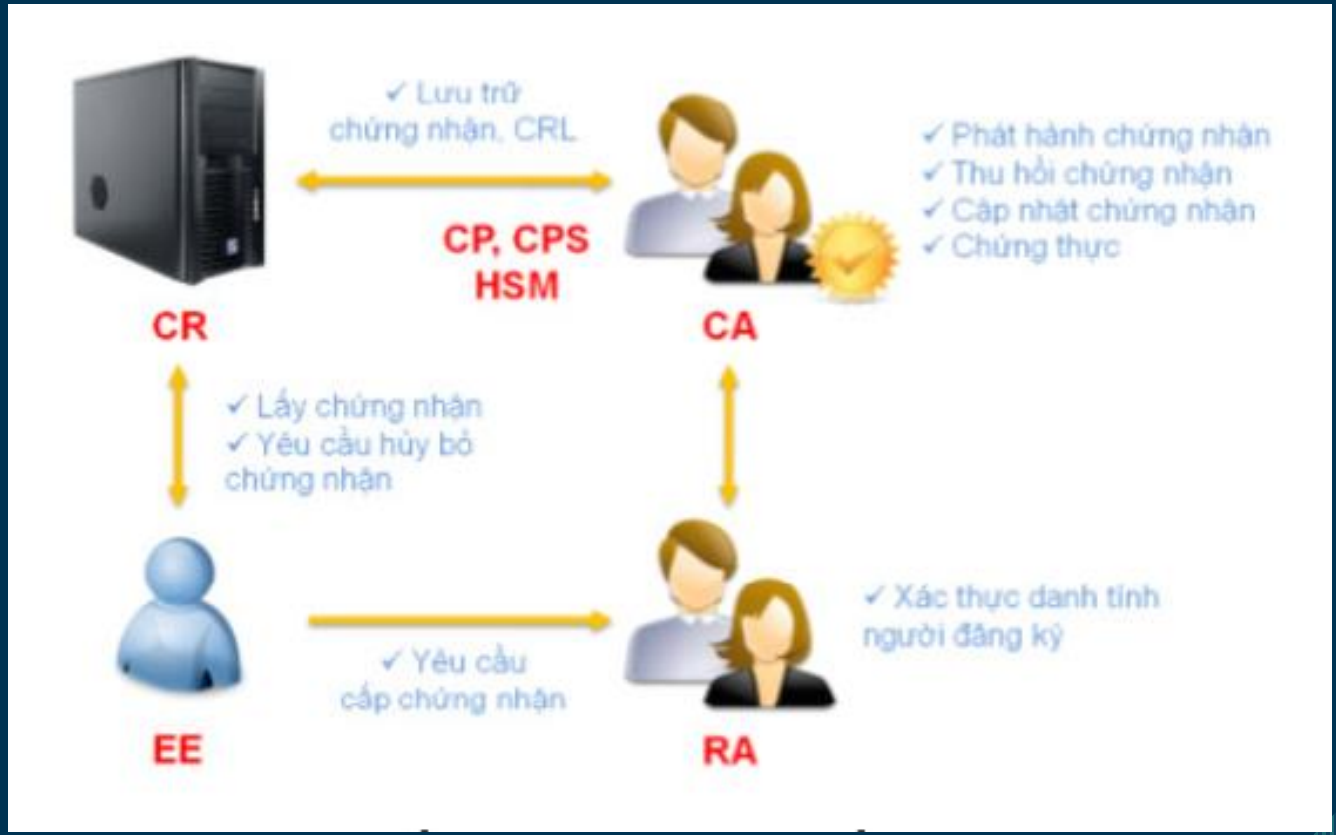
# 2. PKI - Public Key Infrastructure

- Các chức năng của PKI:
  - 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. PKI - Public Key Infrastructure

**Các thành phần chính của PKI:**

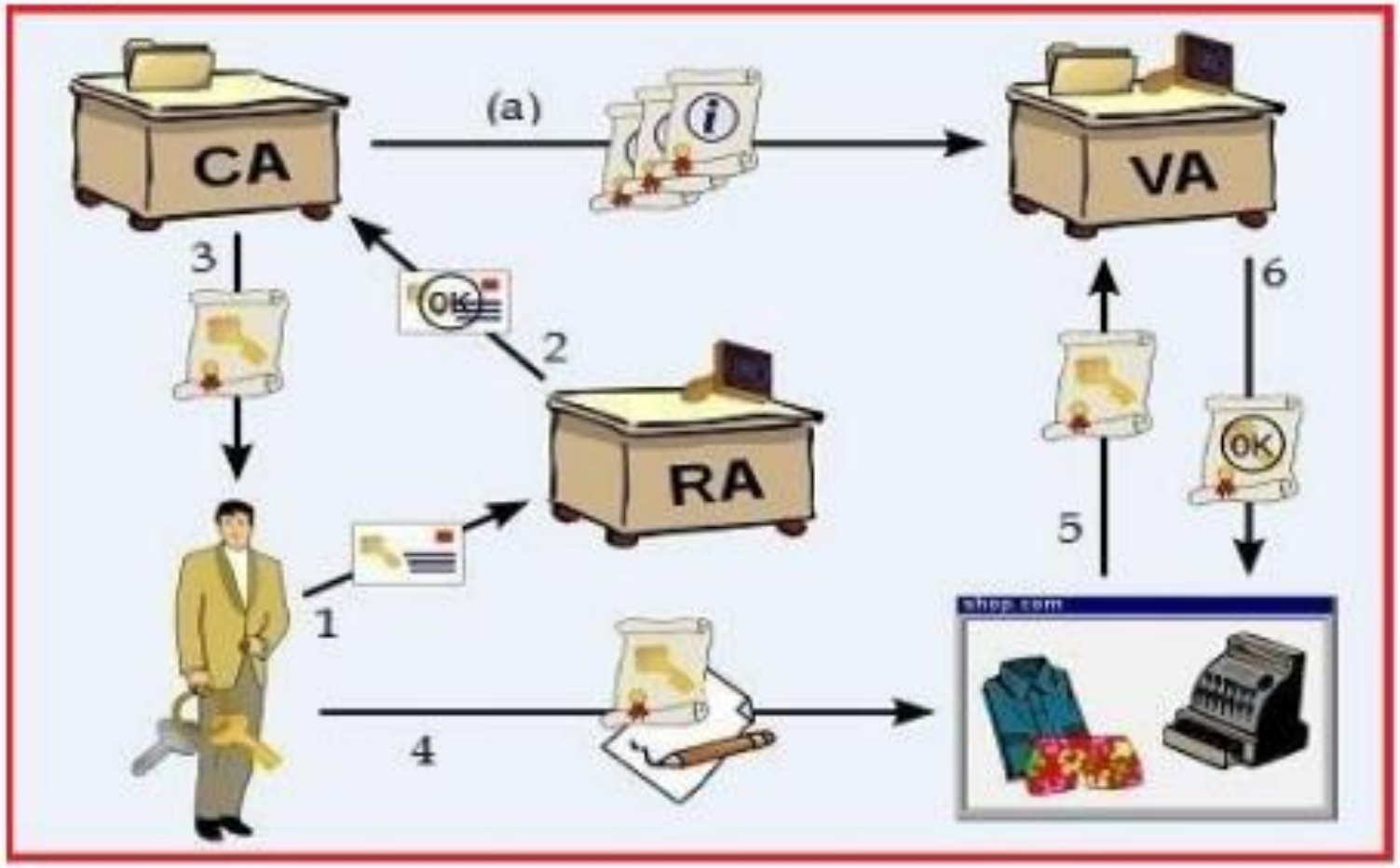
- End Entity – EE
- Certificate Authority – CA
- Registration Authority – RA
- Validation Authority – VA
- Certificate Repository – CR
- Public Key Certificate
- Software to manage
- ...




Viblo

# 2. PKI - Public Key Infrastructure

**Hoạt động:**




Viblo

# 2. PKI - Public Key Infrastructure

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

# 2.1. PKI - X.509

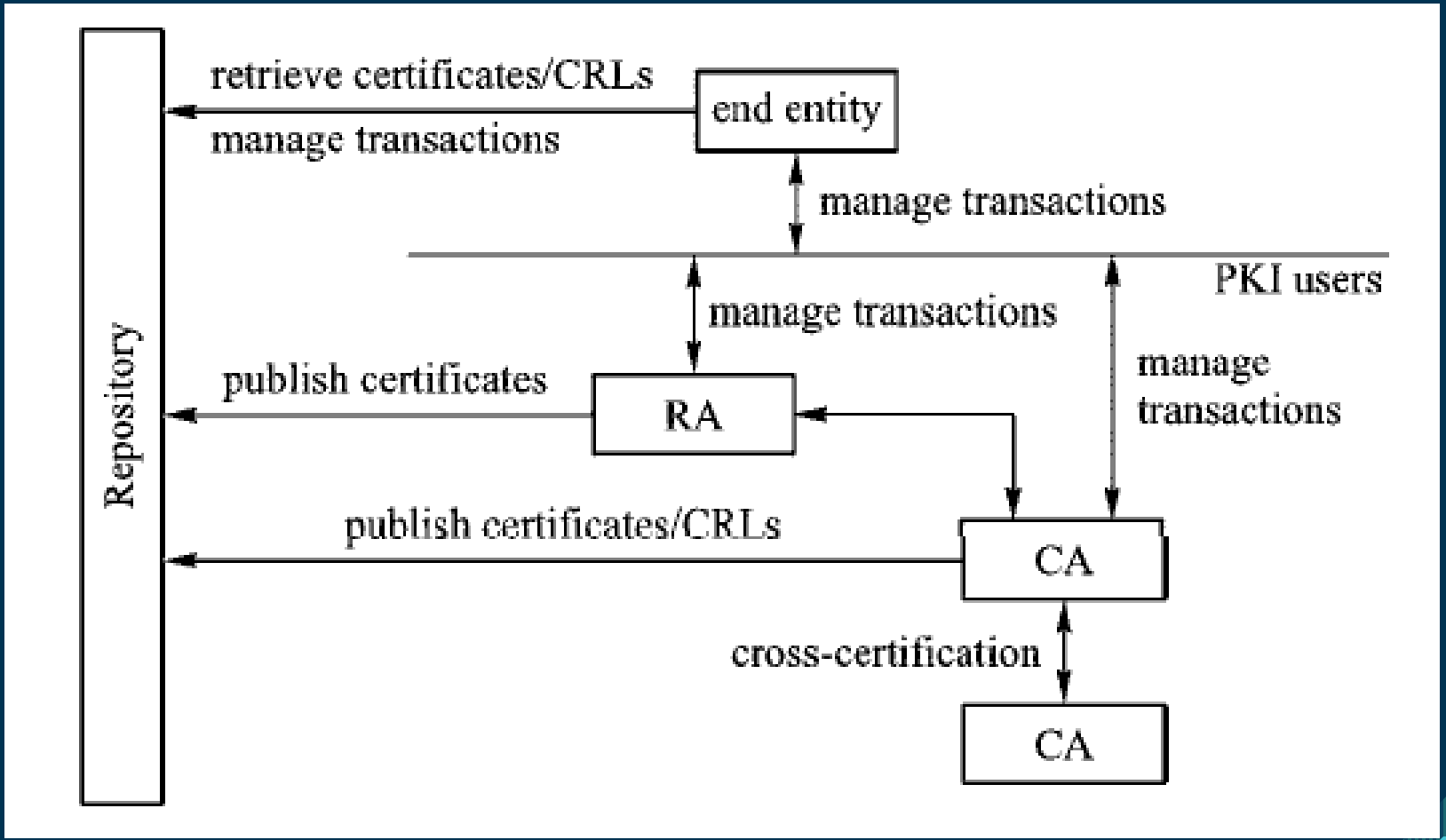
- Là một tiêu chuẩn định dạng chứng chỉ khóa công khai, được sử dụng phổ biến nhất
- Được thành lập theo các tiêu chuẩn ngành viễn thông của Liên minh Viễn thông Quốc tế (ITU) năm 1988.
- Gồm 3 phiên bản, phiên bản mới nhất, phổ biến nhất và được sử dụng đến ngày nay là phiên bản 3 (1997)

# 2.1. PKI - X.509

- 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.

# 2.1. PKI - X.509

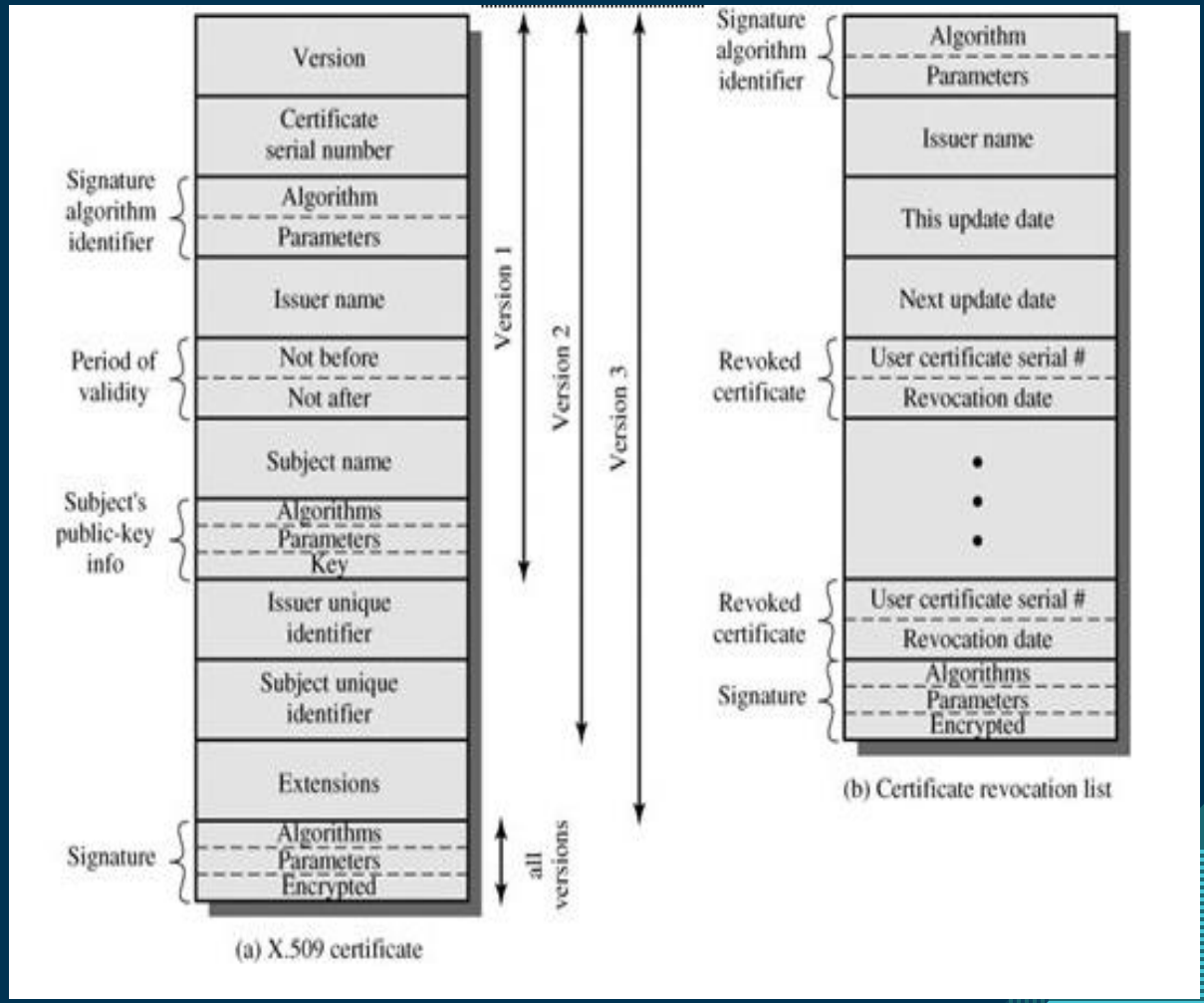
Kiến trúc PKIX



# 2.1. PKI - X.509

Chứng chỉ X.509 bao gồm các thành phần sau:

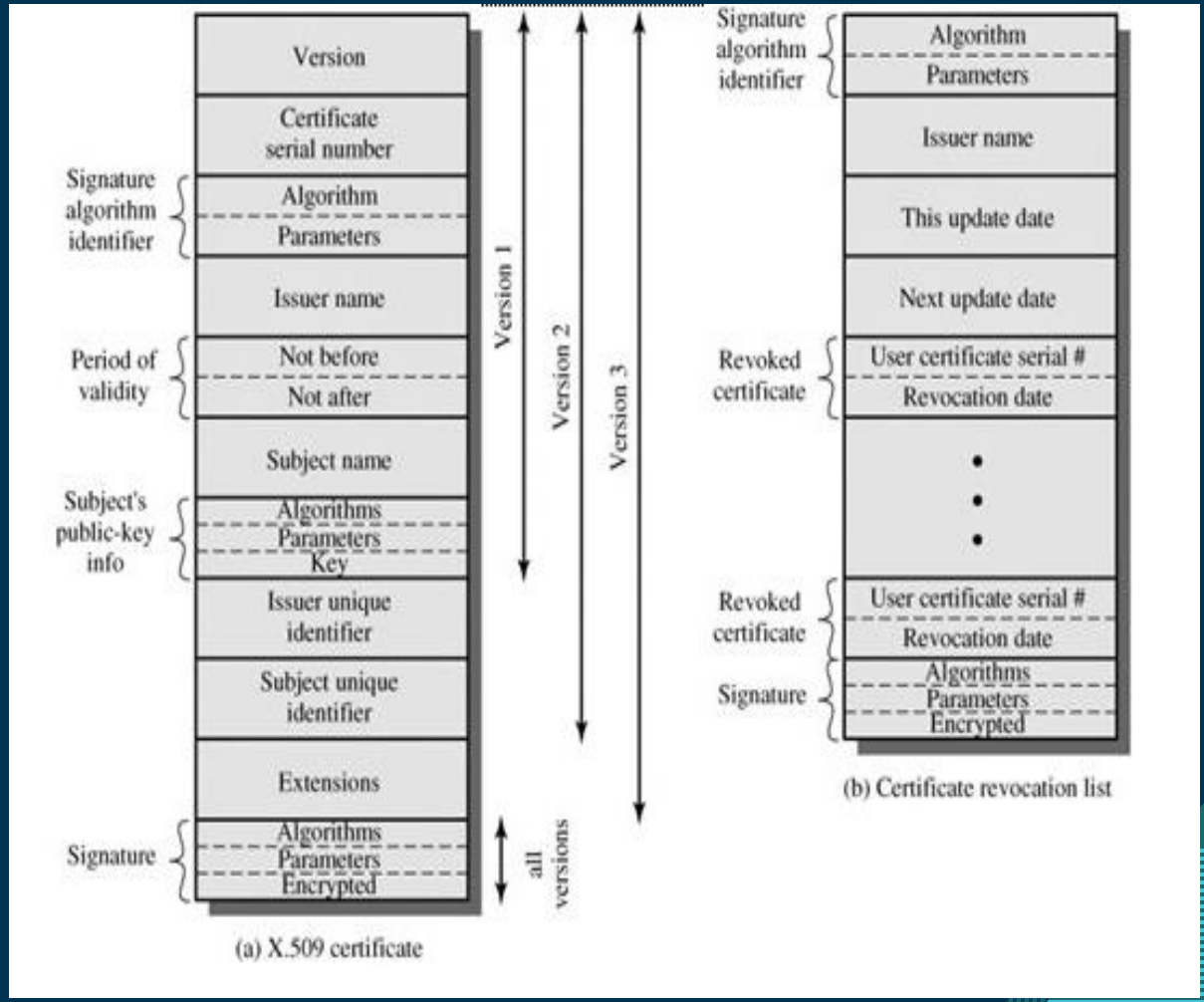
1. Version: chỉ ra phiên bản được sử dụng.
2. Serial number: số duy nhất được gán cho chứng chỉ.
3. Algorithm: liệt kê tên của hàm băm và giải thuật mã hoá khoá công khai dùng để sinh ra chữ ký cho chứng chỉ. Ví dụ: sha1RSA.



# 2.1. PKI - X.509

Chứng chỉ X.509 bao gồm các thành phần sau:

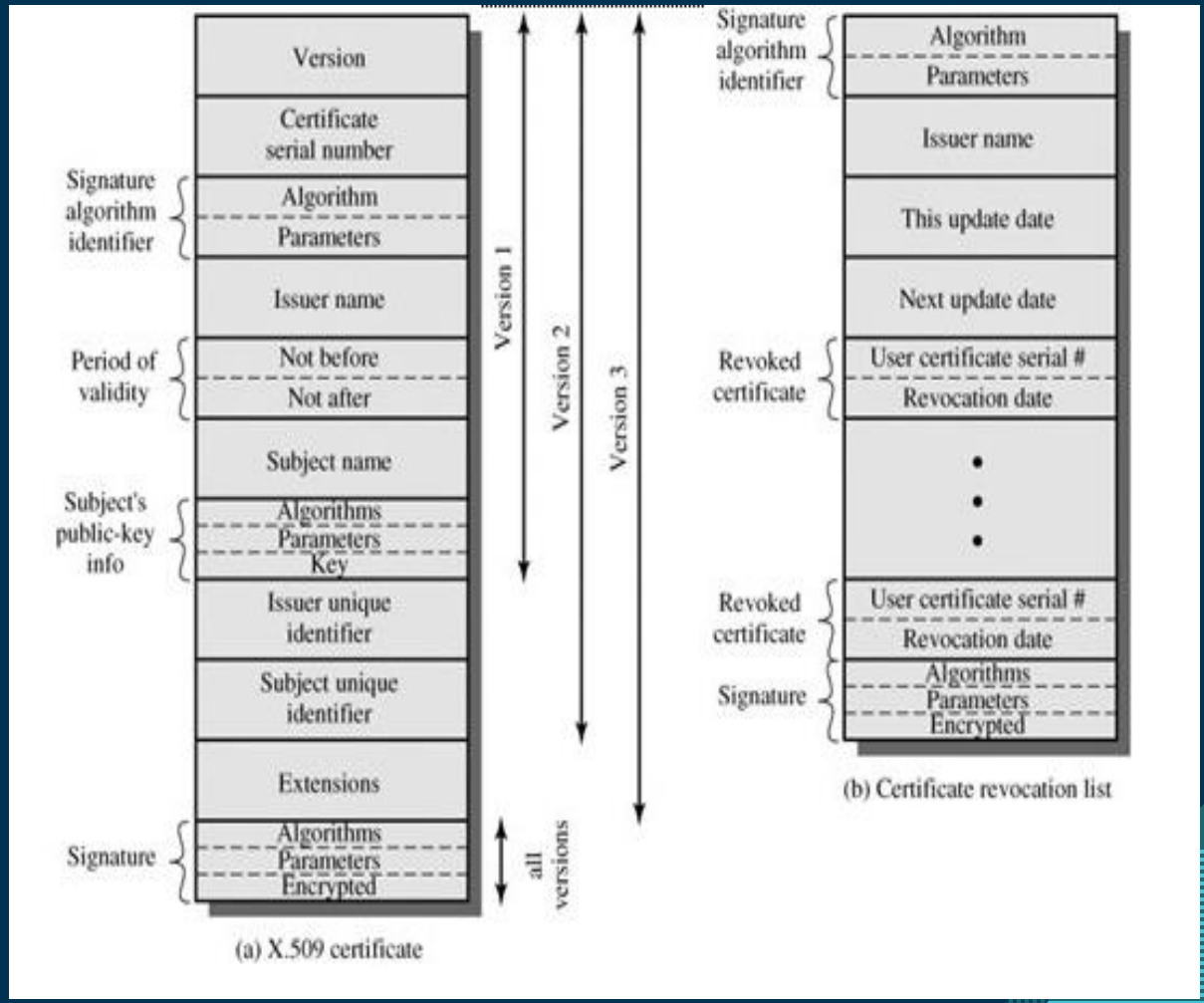
4. Issuer: tổ chức phát hành (CA ký và cấp chứng chỉ).
5. Validity period: thời hạn hiệu lực của chứng chỉ.
6. Subject: tên chủ sở hữu của chứng chỉ.



# 2.1. PKI - X.509

Chứng chỉ X.509 bao gồm các thành phần sau:

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.
10. Signature: CA áp dụng để ký cho tất cả các thành phần của giấy chứng nhận



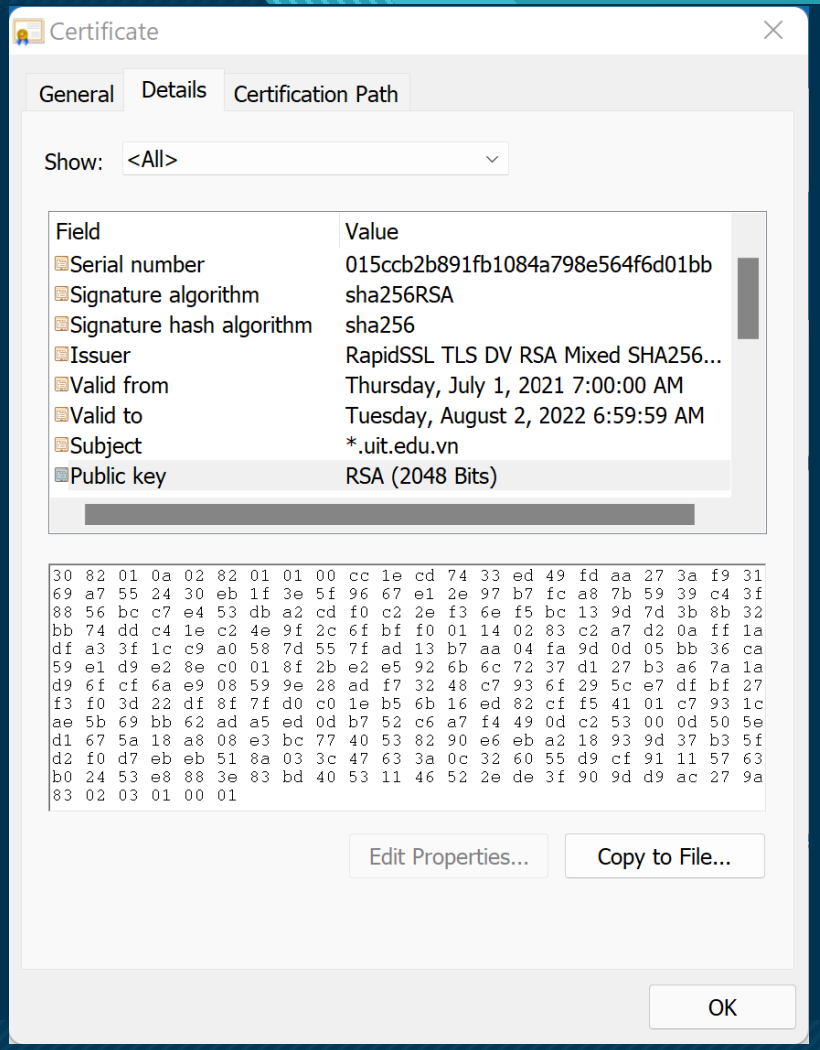
# 2.1. PKI - X.509

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. PKI

**Video**: https://www.youtube.com/watch?v=GwQuTKWvV1M

# 3. SSL/TLS

# 3. SSL/TLS

- 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.

# 3. SSL/TLS

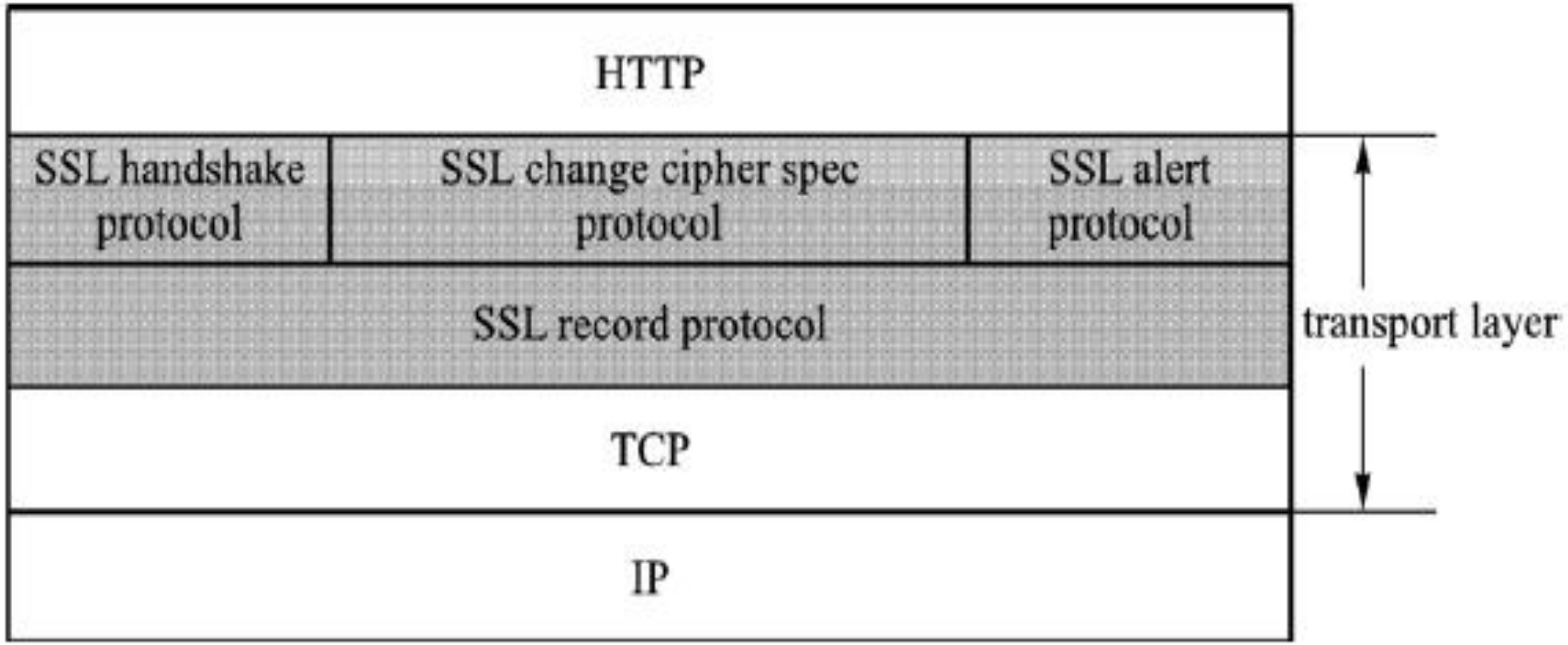
- SSL/TLS dùng để?
  - Xác thực server, client
  - Đảm bảo tính toàn vẹn của dữ liệu
  - Mã hóa dữ liệu đảm bảo tính bí mật
  - Nén dữ liệu

# 3. SSL/TLS

- 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

# 3. SSL/TLS

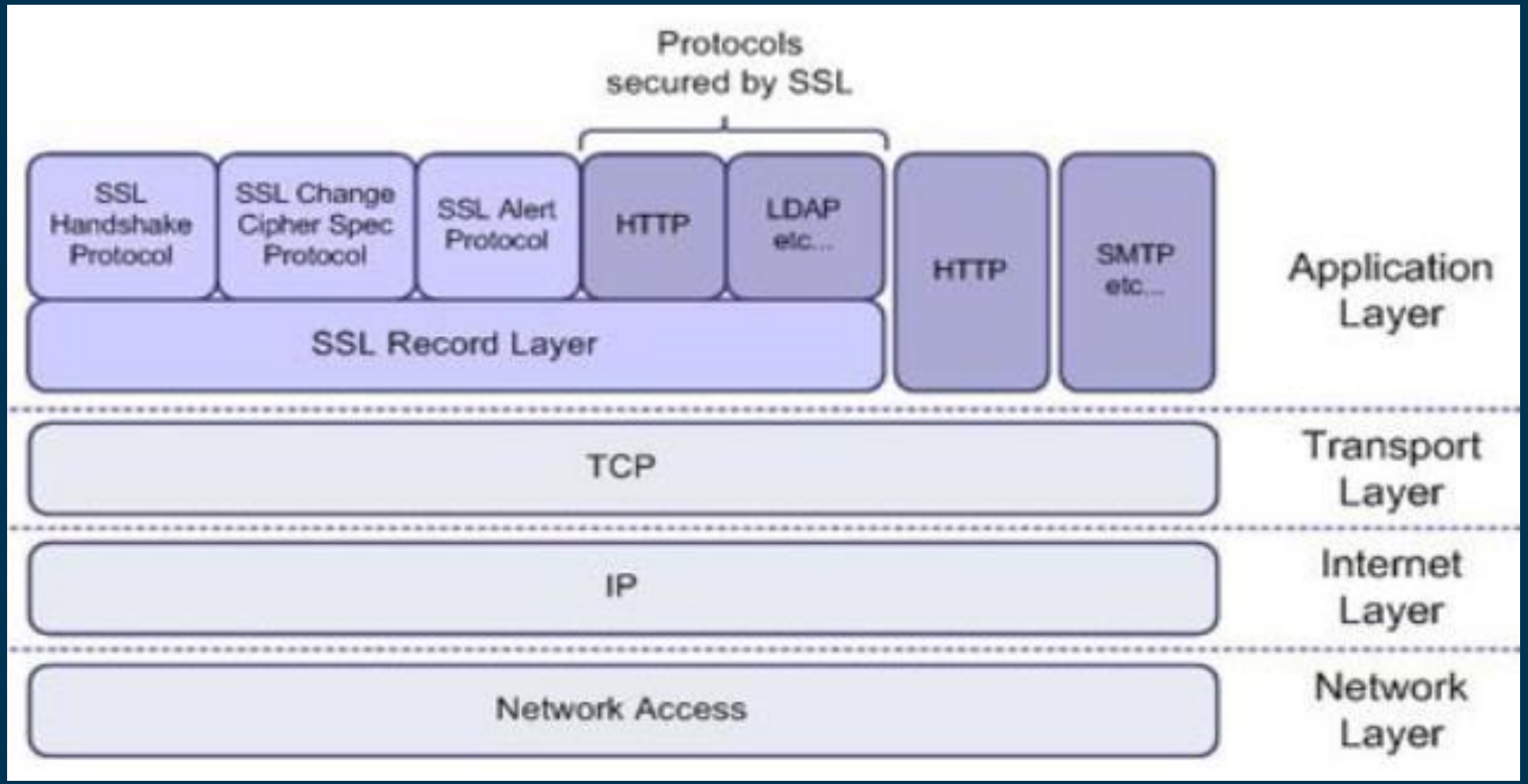
## Cấu trúc SSL




SSL structure

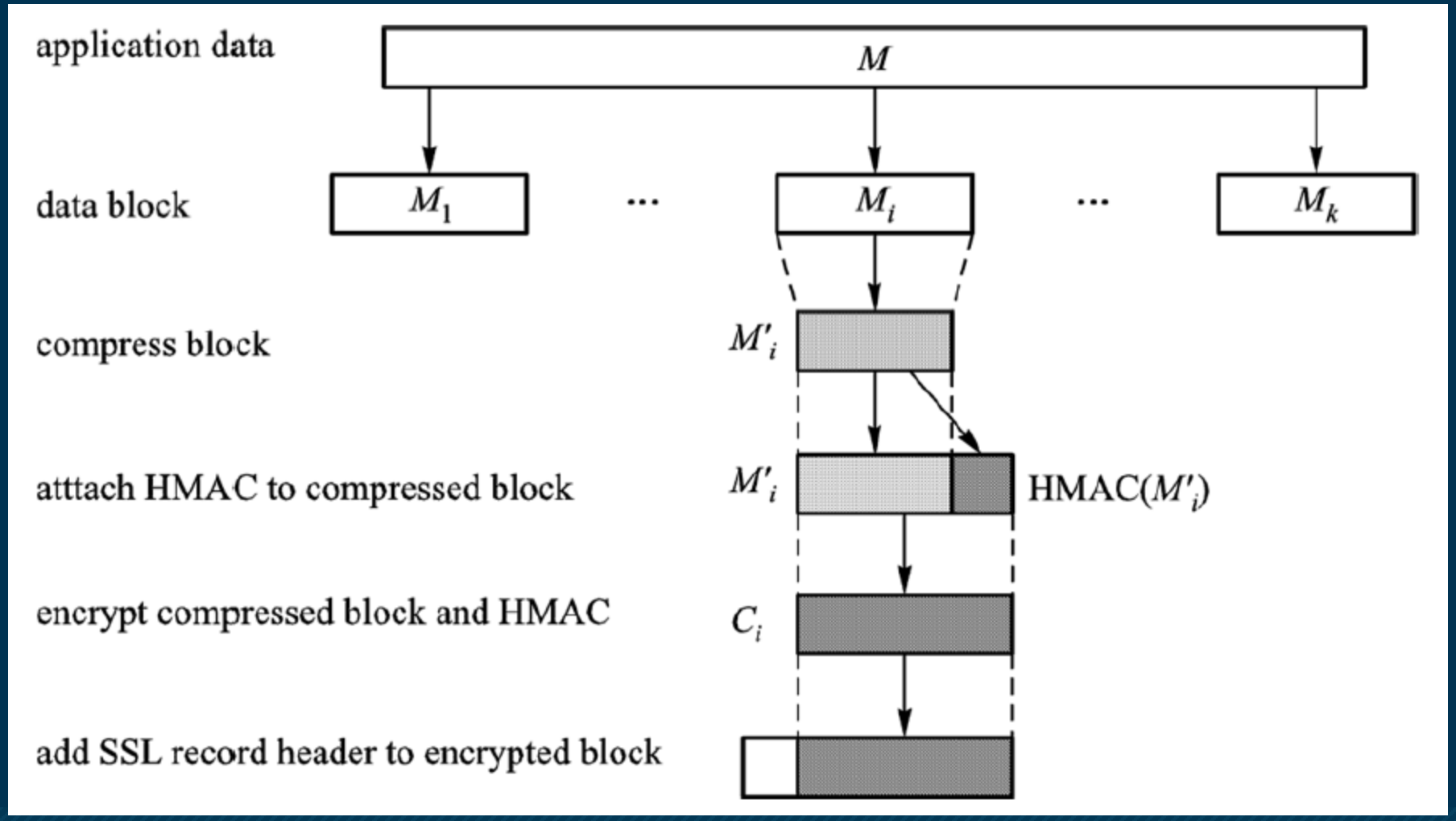
# 3. SSL/TLS

## Cấu trúc SSL



# 3. SSL/TLS

## Giao thức bản ghi (record protocol) của SSL



# 3. SSL/TLS

## Các giao thức của SSL

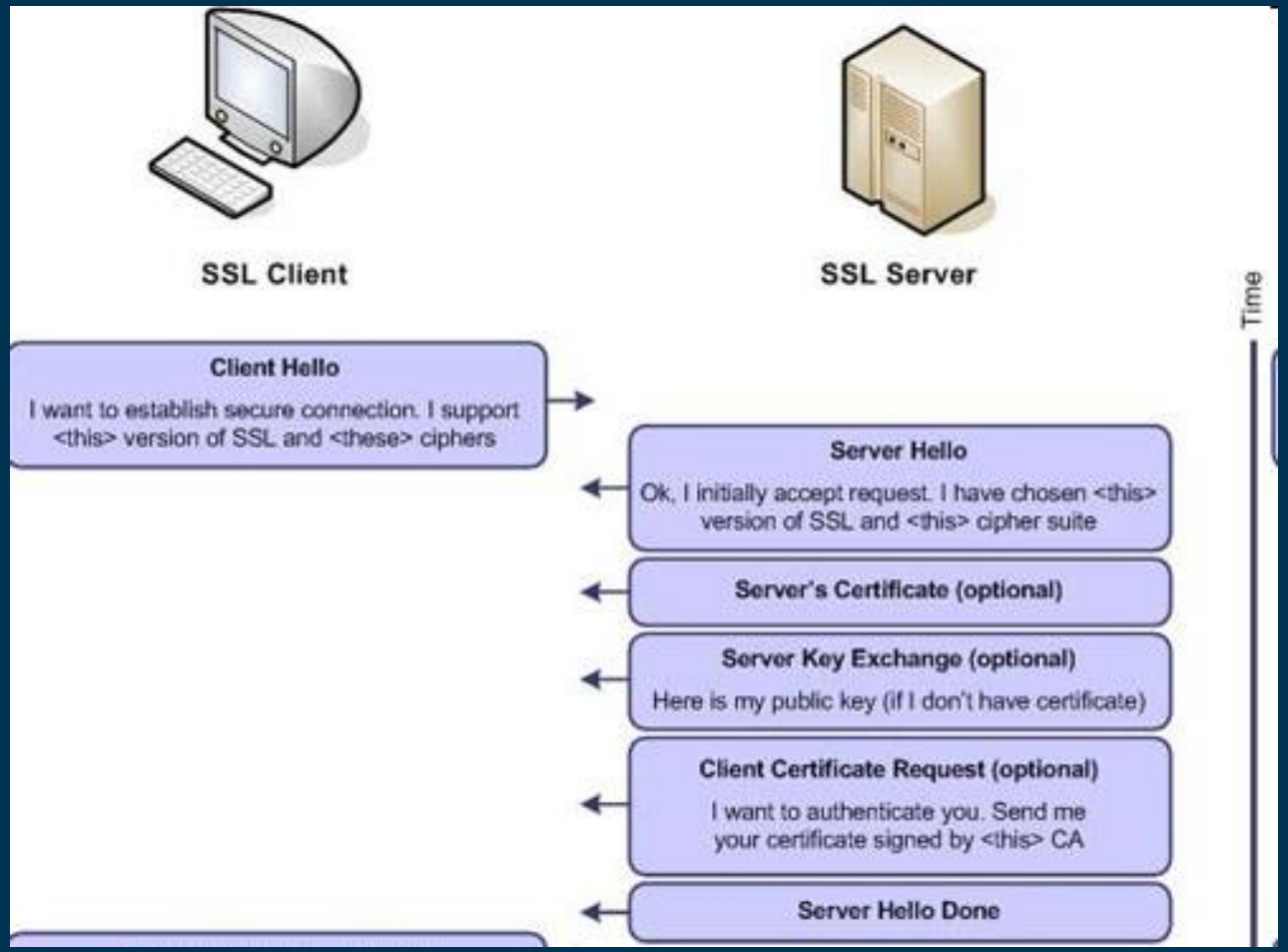
- Giao thức bắt tay (handshake protocol) thành lập các giải thuật mã hóa, giải thuật nén, và các thông số sẽ được sử dụng bởi cả hai bên trong việc trao đổi dữ liệu được mã hóa. Sau đó, các giao thức bản ghi (record protocol) chịu trách nhiệm phân chia thông điệp vào các khối, nén mỗi khối, chứng thực 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.

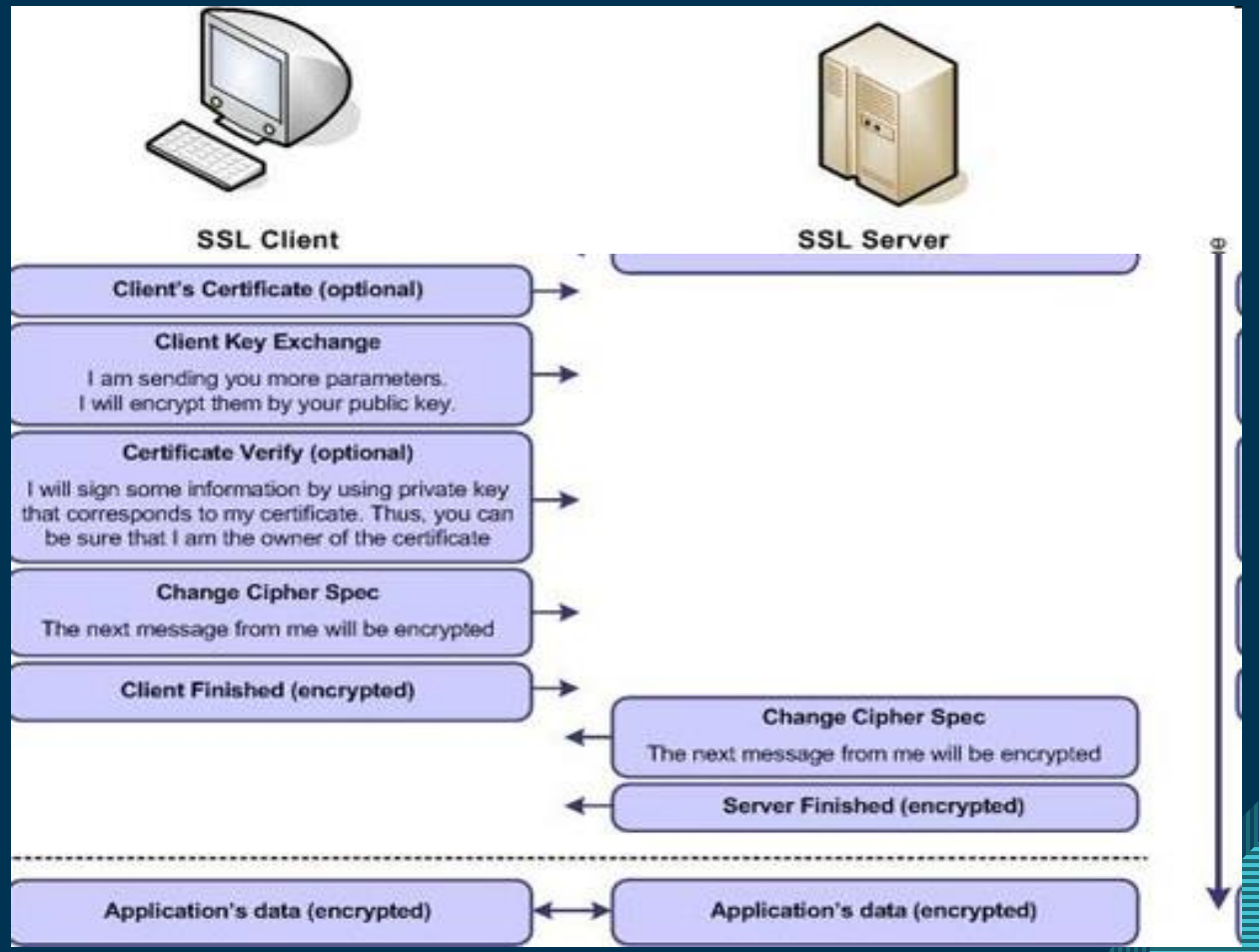
# 3. SSL/TLS

## Giao thức bắt tay của SSL

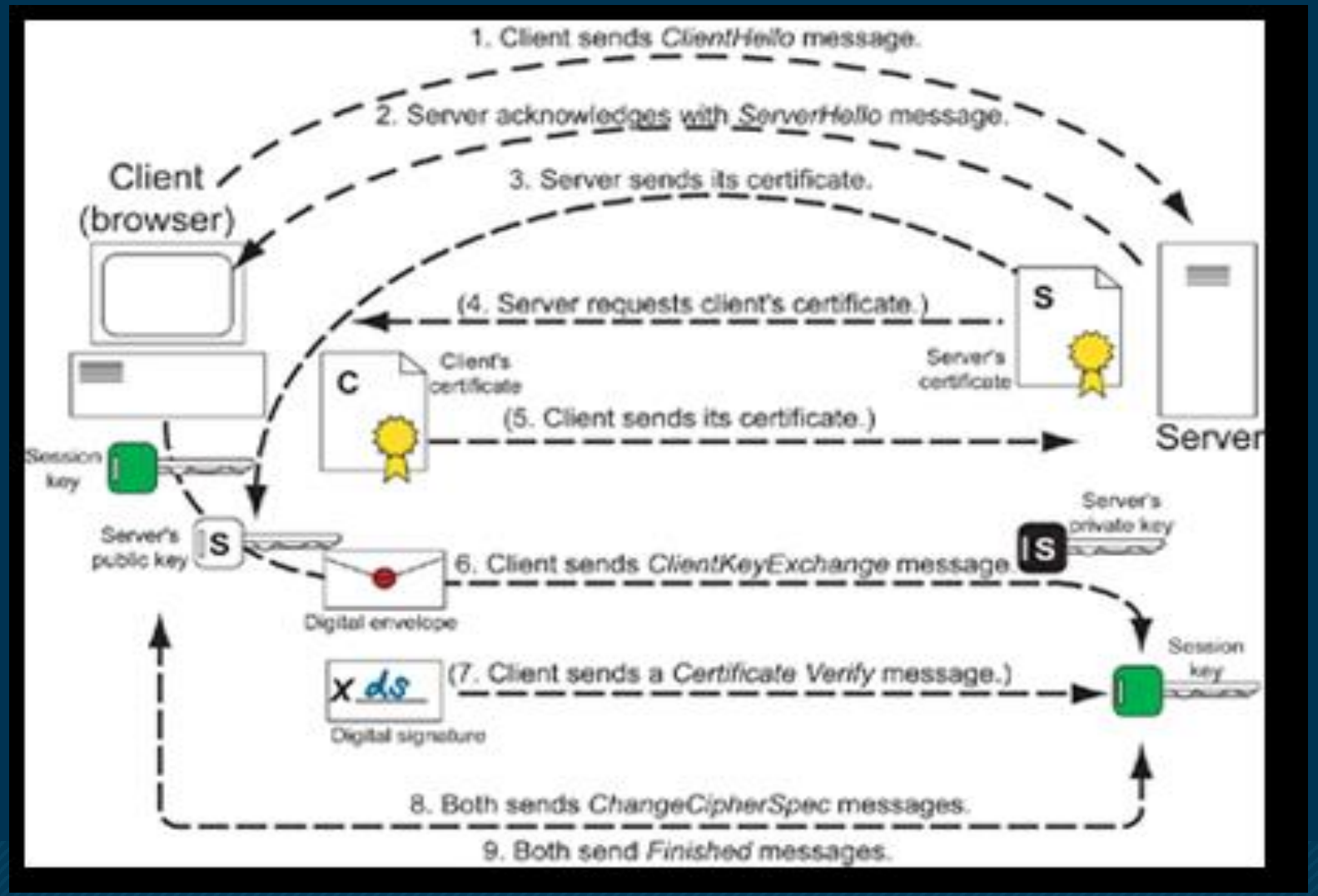
- Phase 1: chọn giải thuật mã hoá. Các giải thuật được chọn có thể là RSA, AES-128, 3DES, RC6, SHA-1… Client sẽ khởi tạo với một thông điệp client-hello.
- Phase 2: server xác thực và trao đổi khoá. Server sẽ gởi cho client:
  - Chứng chỉ khoá công khai của server
  - Thông tin trao đổi khoá của server
  - 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.

# 3. SSL/TLS
## Quá trình thiết lập kết nối SSL



# 3. SSL/TLS
## Quá trình thiết lập kết nối SSL



# 4. SSH

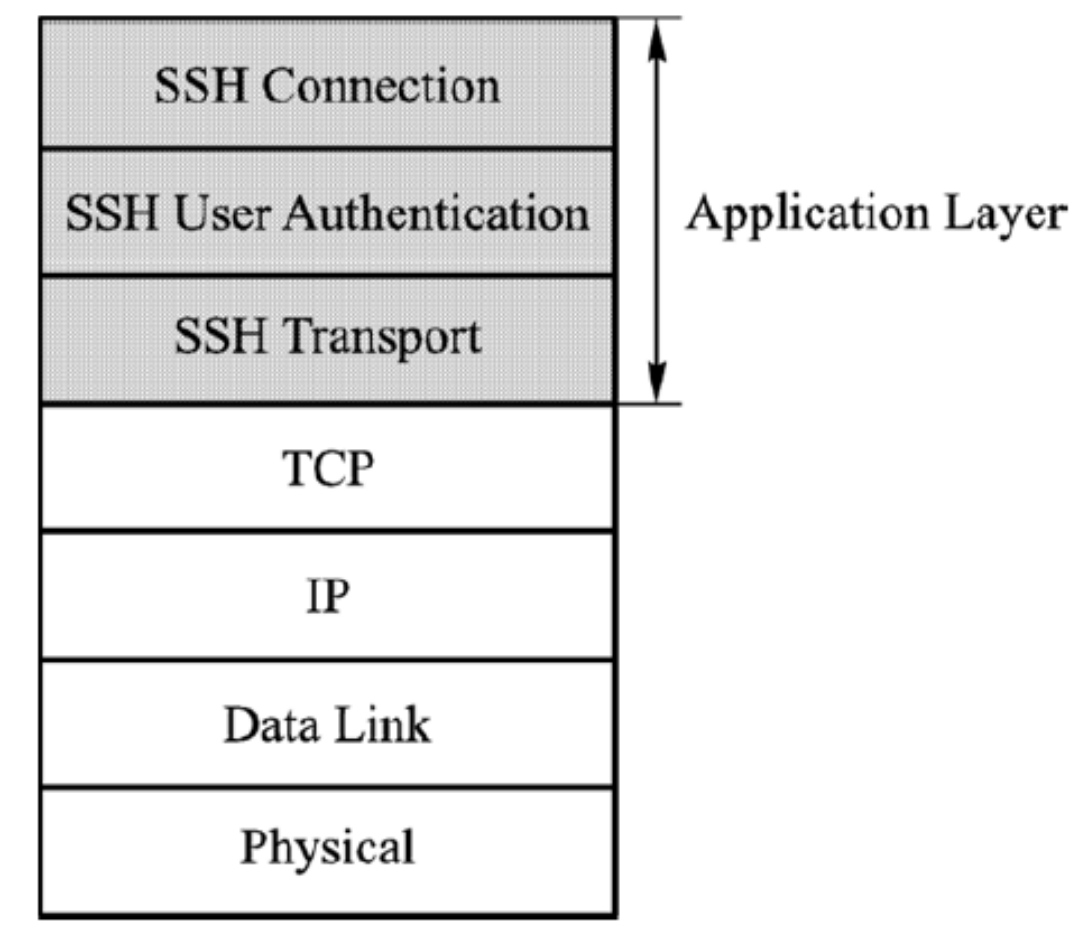
# 4. SSH
## Tổng quan

- 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.

# 4. 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.

## 4. 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

# 4. SSH
## Cách thức hoạt động

- SSH được thực hiện qua 3 bước:

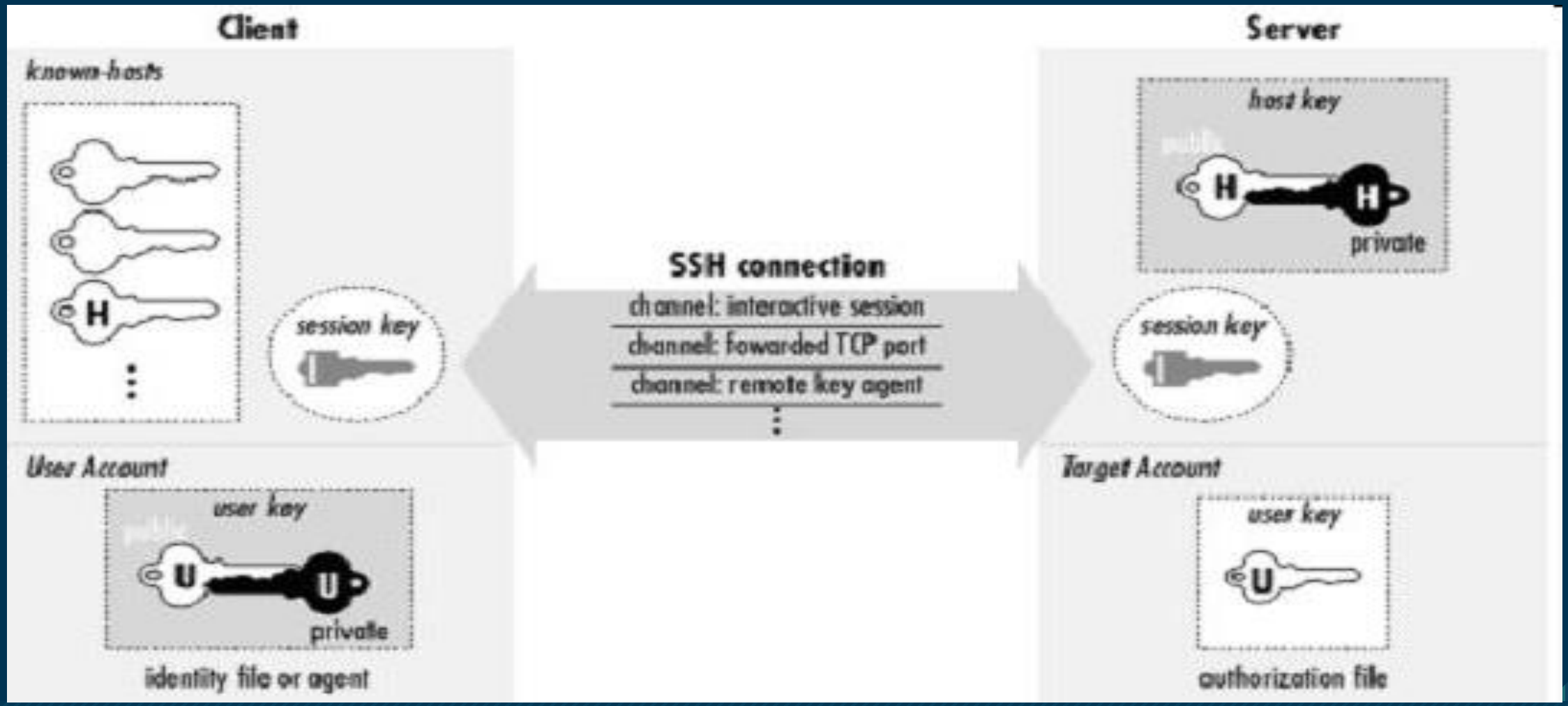
1. Định danh host:
    - Việc định danh host được thực hiện qua việc trao đổi khoá. Mỗi máy tính có hỗ trợ kiểu truyền thông SSH có một khoá định danh duy nhất. Khoá này gồm hai thành phần: khoá riêng và khoá công khai. Khoá công khai được sử dụng khi cần trao đổi giữa các máy chủ với nhau trong phiên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

# 4. 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.

# 4. SSH
## Cách thức hoạt động



# 4. 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.

# 4. SSH
## Cách thức hoạt động

- SSH được thực hiện qua 3 bước:

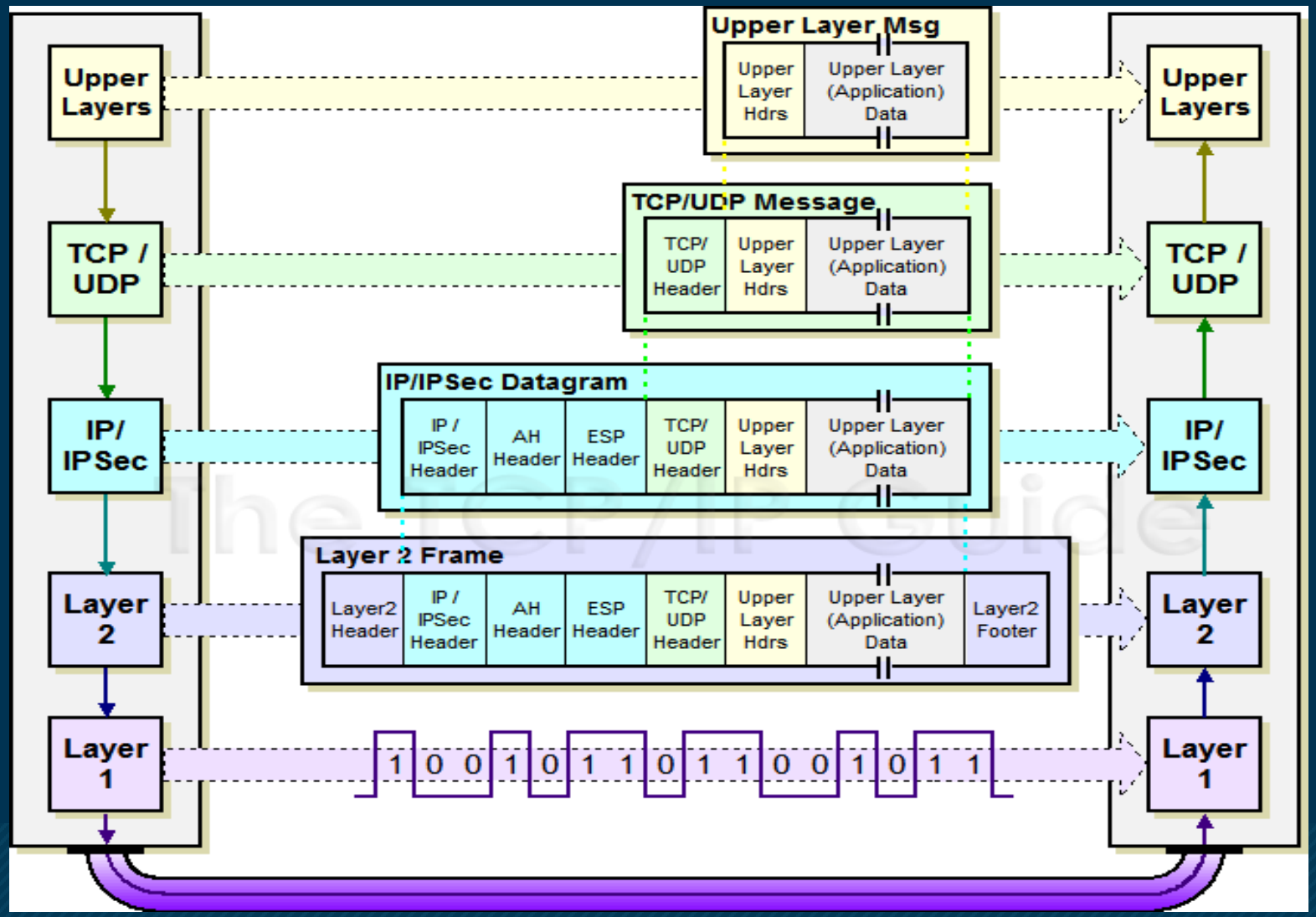
3. Chứng thực:
    - Mỗi định danh và truy nhập của người sử dụng có thể được cung cấp theo nhiều cách khác nhau. Chẳng hạn, kiểu chứng thực rhosts có thể được sử dụng, nhưng không phải là mặc định; nó đơn giản chỉ kiểm tra định danh của máy khách được liệt kê trong file rhost (theo DNS và địa chỉ IP).
    - 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.

# 5. IPSec

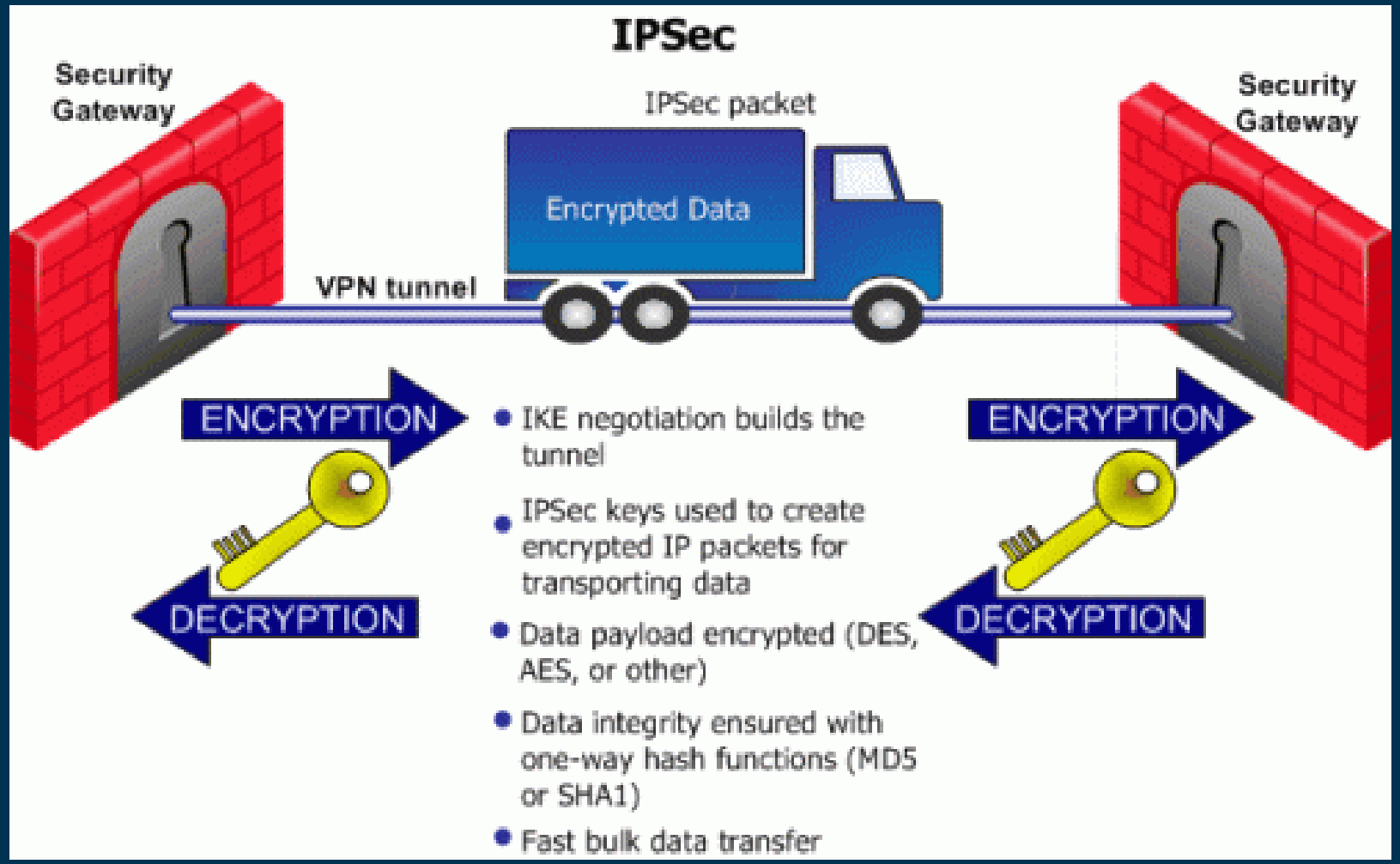
# 5. IPsec
## Tổng quan

- 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.

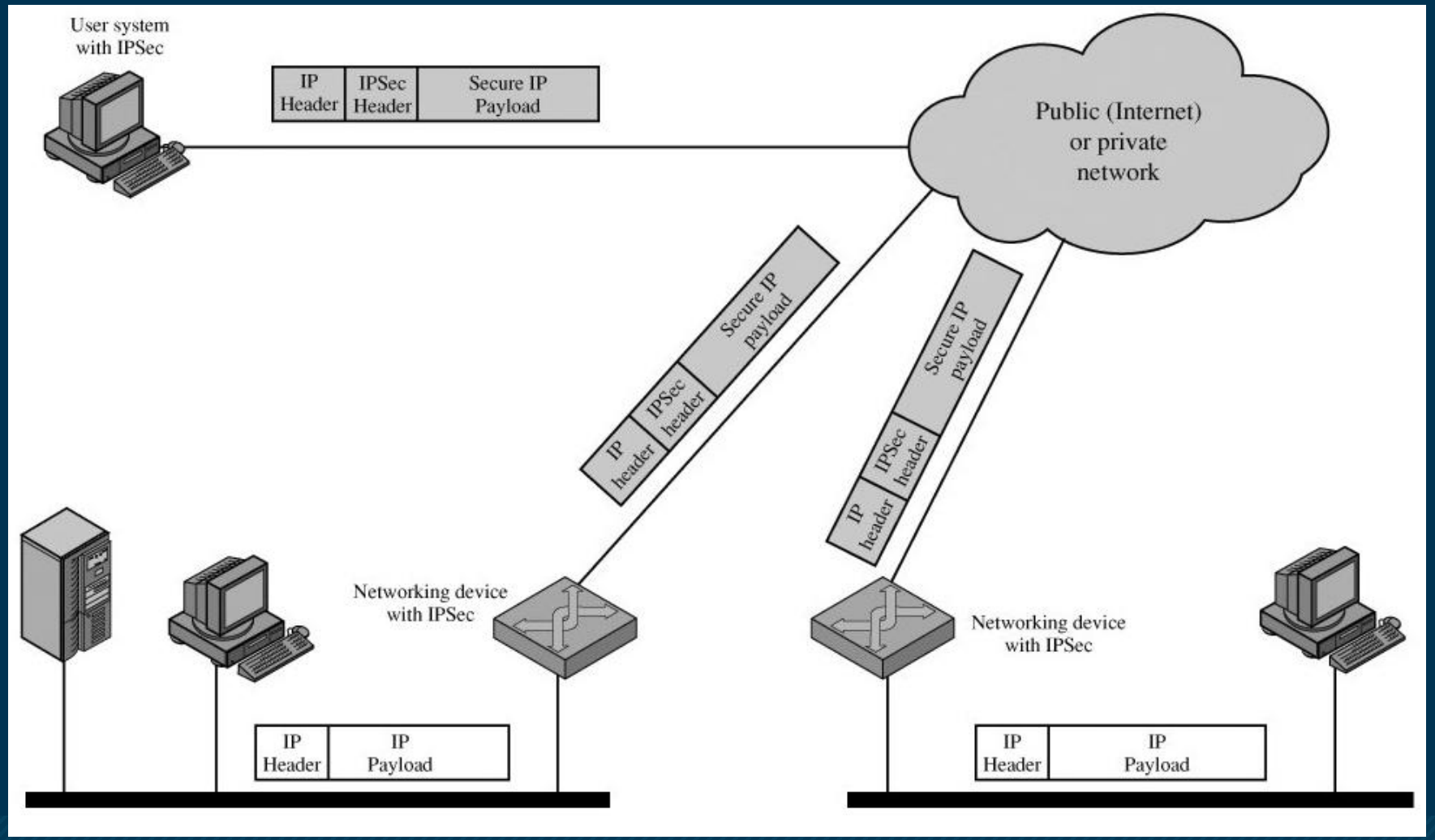
# 5. IPsec
## Tổng quan



# 5. IPsec
## Tổng quan



# 5. IPsec
## Tổng quan



# 5. IPsec
## Tổng quan

- Các phiên bản:
  - Phiên bản 1995: RFC 1825-1829
  - Phiên bản 1998: RFC 2401-2412
  - Phiên bản 2005: RFC 4301-4309
- 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.

# 5. IPsec
## Tổng quan

- IPsec cung cấp các dịch vụ bảo mật:
  - Mã hoá quá trình truyền thông tin
  - Đảm bảo tính nguyên vẹn của dữ liệu
  - Phải được xác thực giữa các giao tiếp
  - Chống quá trình replay trong các phiên bảo mật
- Thuật toán mã hoá được sử dụng trong IPsec bao gồm HMAC-SHA1 cho tính toàn vẹn dữ liệu (integrity protection), và thuật toán TripleDES-CBC và AES-CBC cho mã mã hoá và đảm bảo độ an toàn của gói tin. Toàn bộ thuật toán này được thể hiện trong RFC 4305.

# 5. 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.

# 5. IPsec

## Security Association (SA)

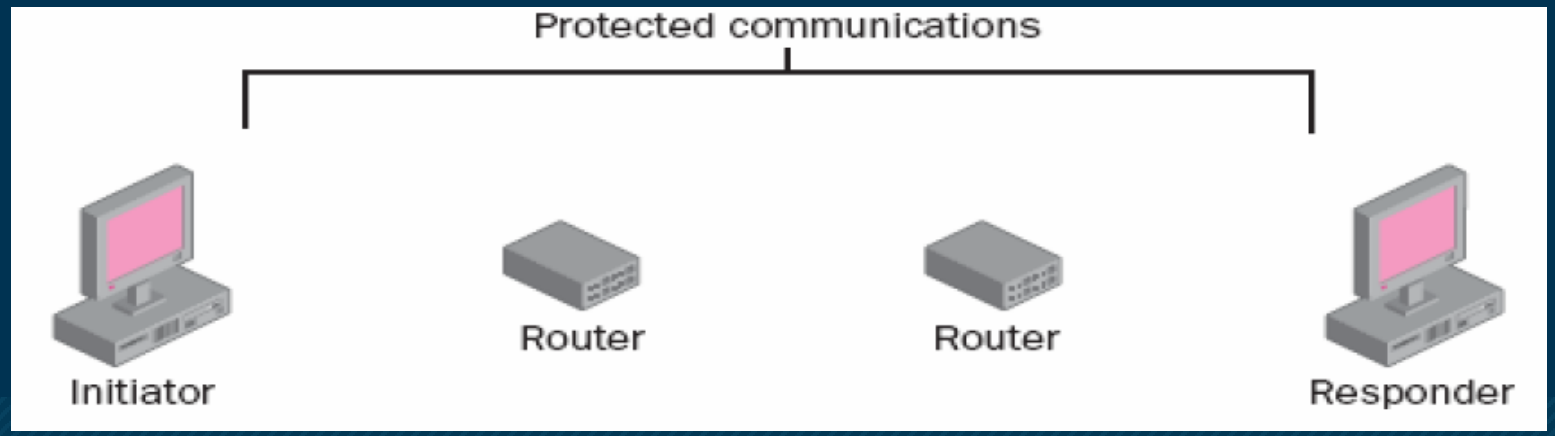
- Một SA cung cấp các thông tin sau:
  - Chỉ mục các thông số bảo mật (SPI - Security parameters index): là một chuỗi nhị phân 32 bit được sử dụng để xác định một tập cụ thể của các giải thuật và thông số dùng trong phiên truyền thông. SPI được bao gồm trong cả AH và ESP để chắc chắn rằng cả hai đều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

# 5. 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)

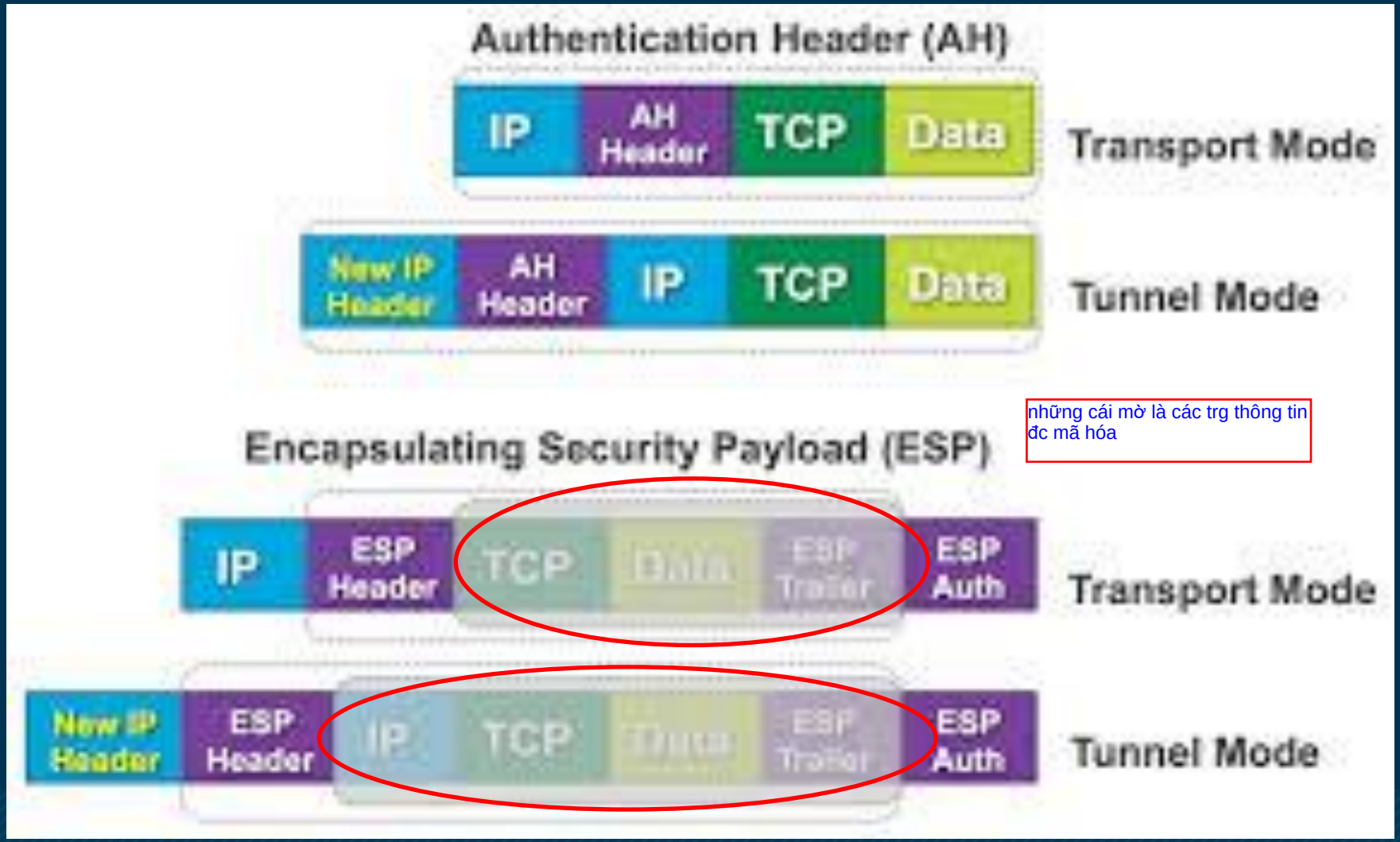


# 5. IPsec

## 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).

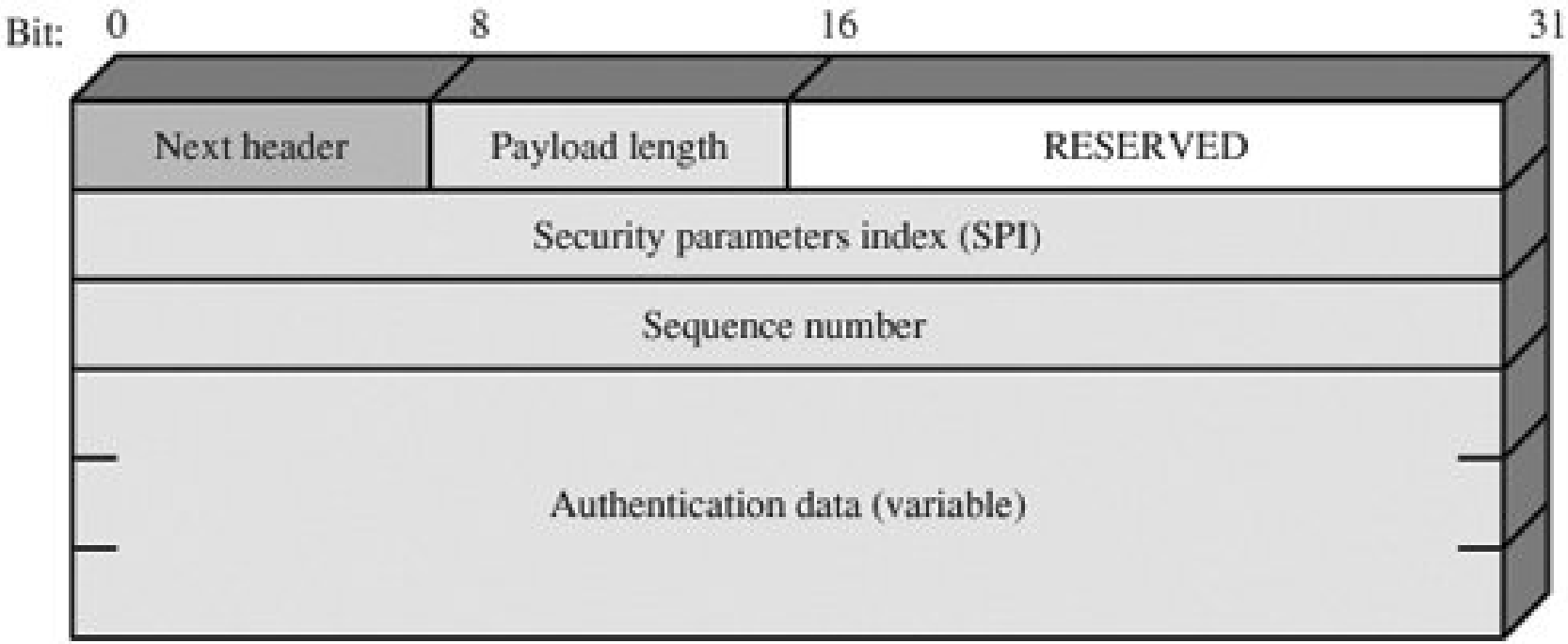
# 5. IPsec
## Các phương thức của IPsec



# 5. IPsec
## Định dạng AH

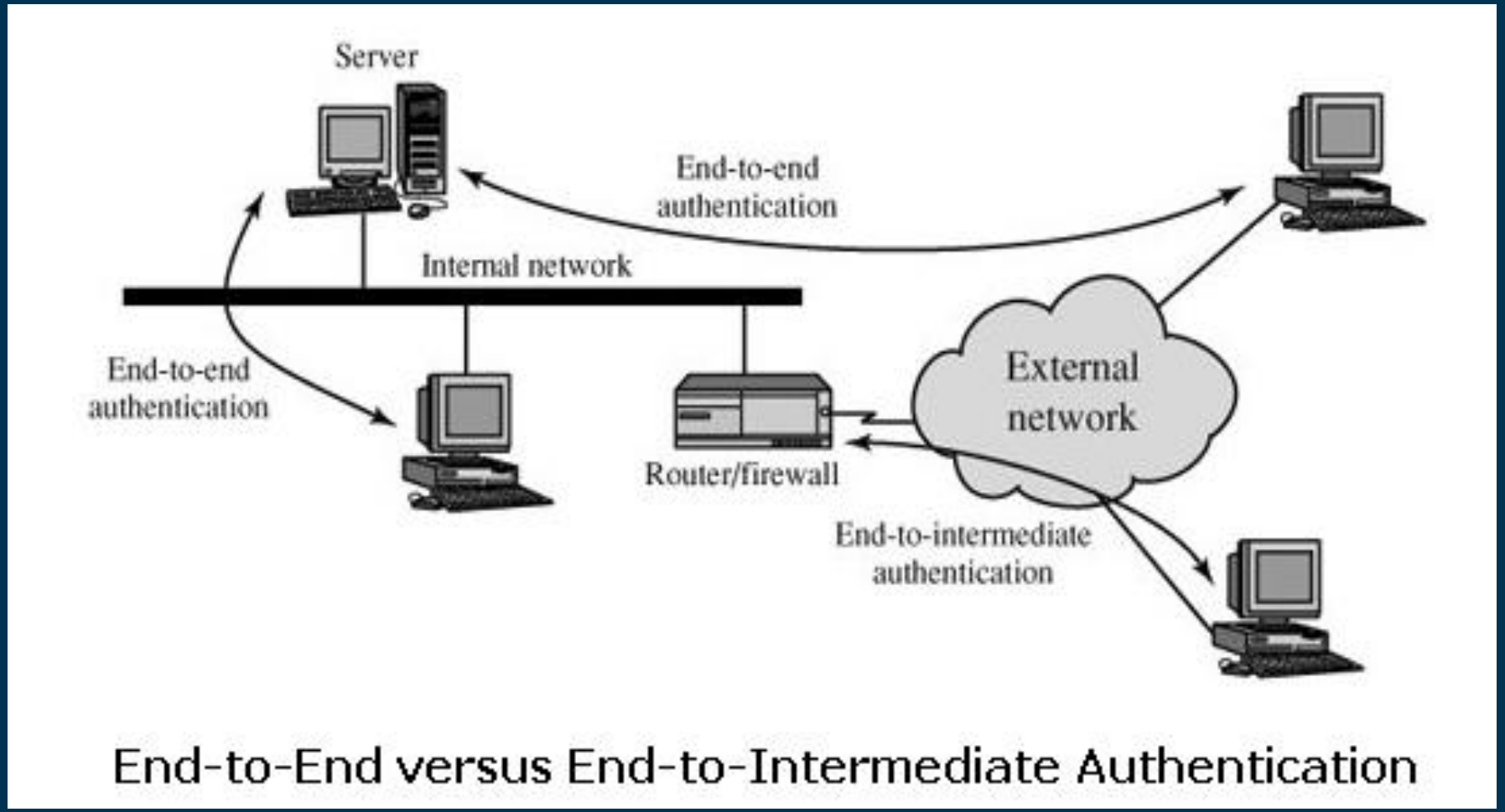
- Authentication Header (AH) bao gồm các vùng:
  - Next Header (8 bits): xác định header kế tiếp.
  - Payload Length (8 bits): chiều dài của Authentication Header theo từ 32-bit, trừ 2.
  - Reserved (16 bits): sử dụng cho tương lai.
  - Security Parameters Index (32 bits): xác định một SA.
  - Sequence 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.

# 5. IPsec
## Định dạng AH




IPSec Authentication Header

# 5. IPsec
## Các phương thức chứng thực

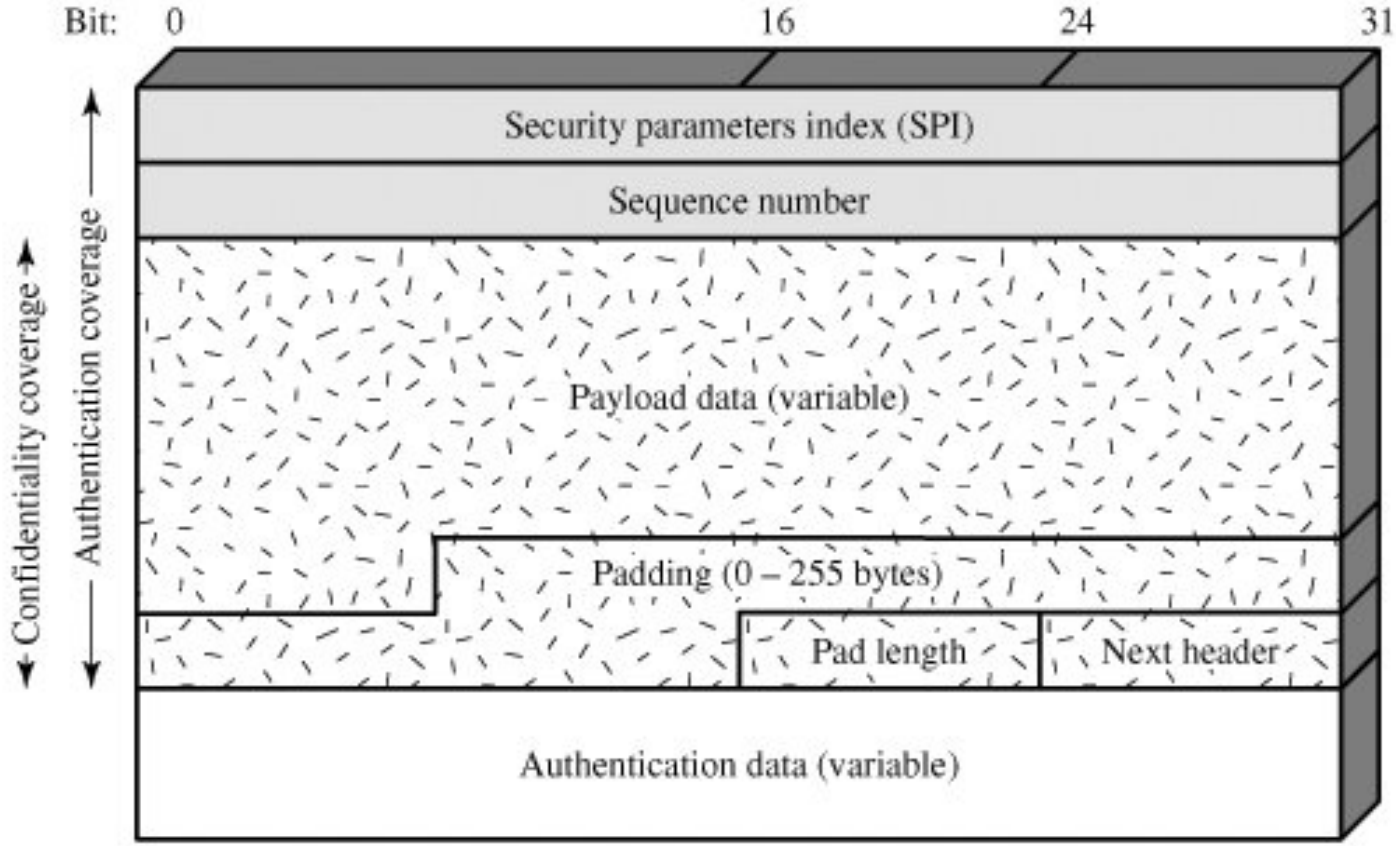



End-to-End versus End-to-Intermediate Authentication

# 5. IPsec
## Định dạng ESP

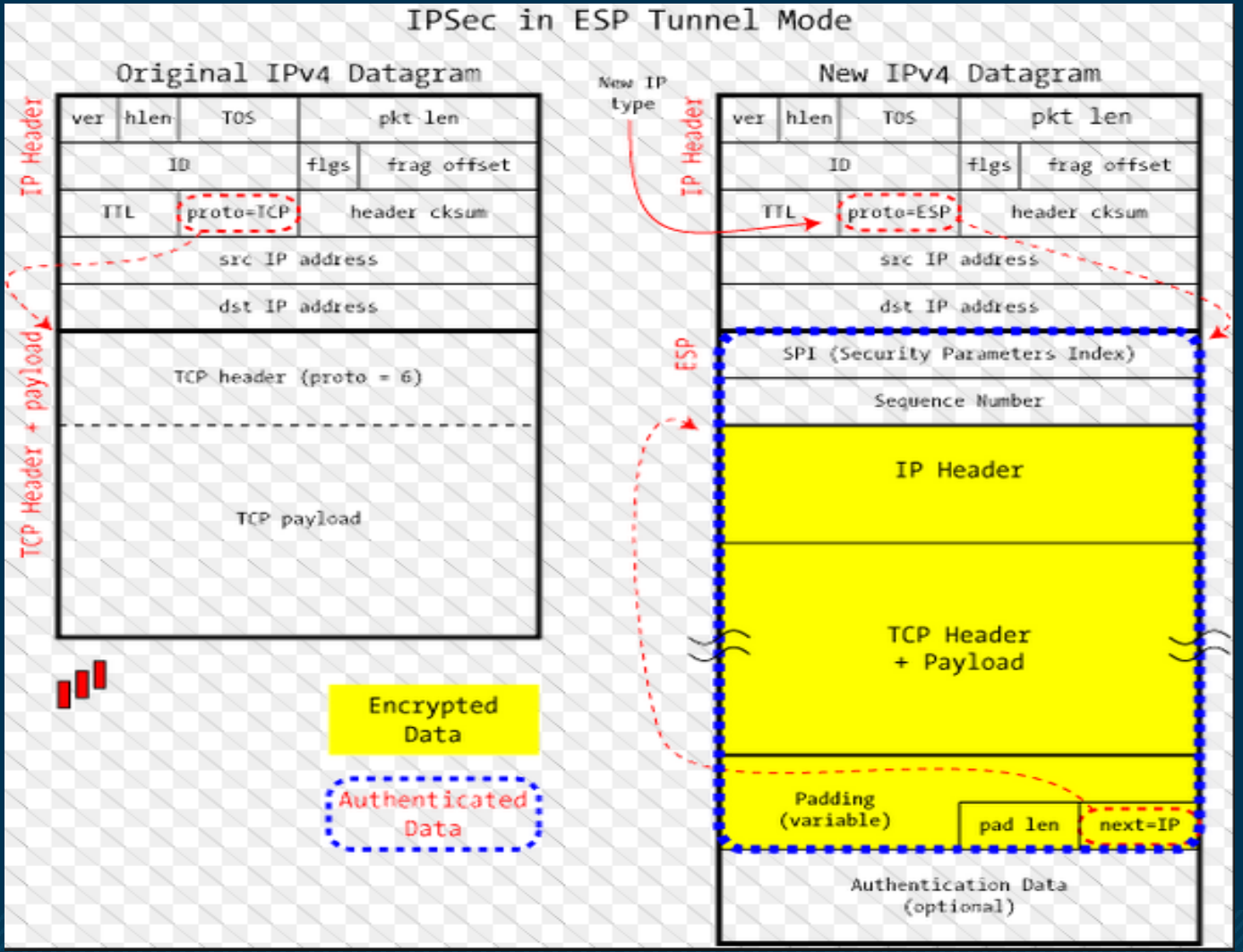
- Một gói ESP chứa các vùng sau:
  - Security Parameters Index (32 bits): xác định một SA.
  - Sequence Number (32 bits): một giá trị đếm tăng đơn điệu, cung cấp chức năng anti-replay (giống AH).
  - Payload Data (variable): đây là một segment ở transport-level (transport mode) hoặc gói IP (tunnel mode) 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.

# 5. IPsec
## Định dạng ESP

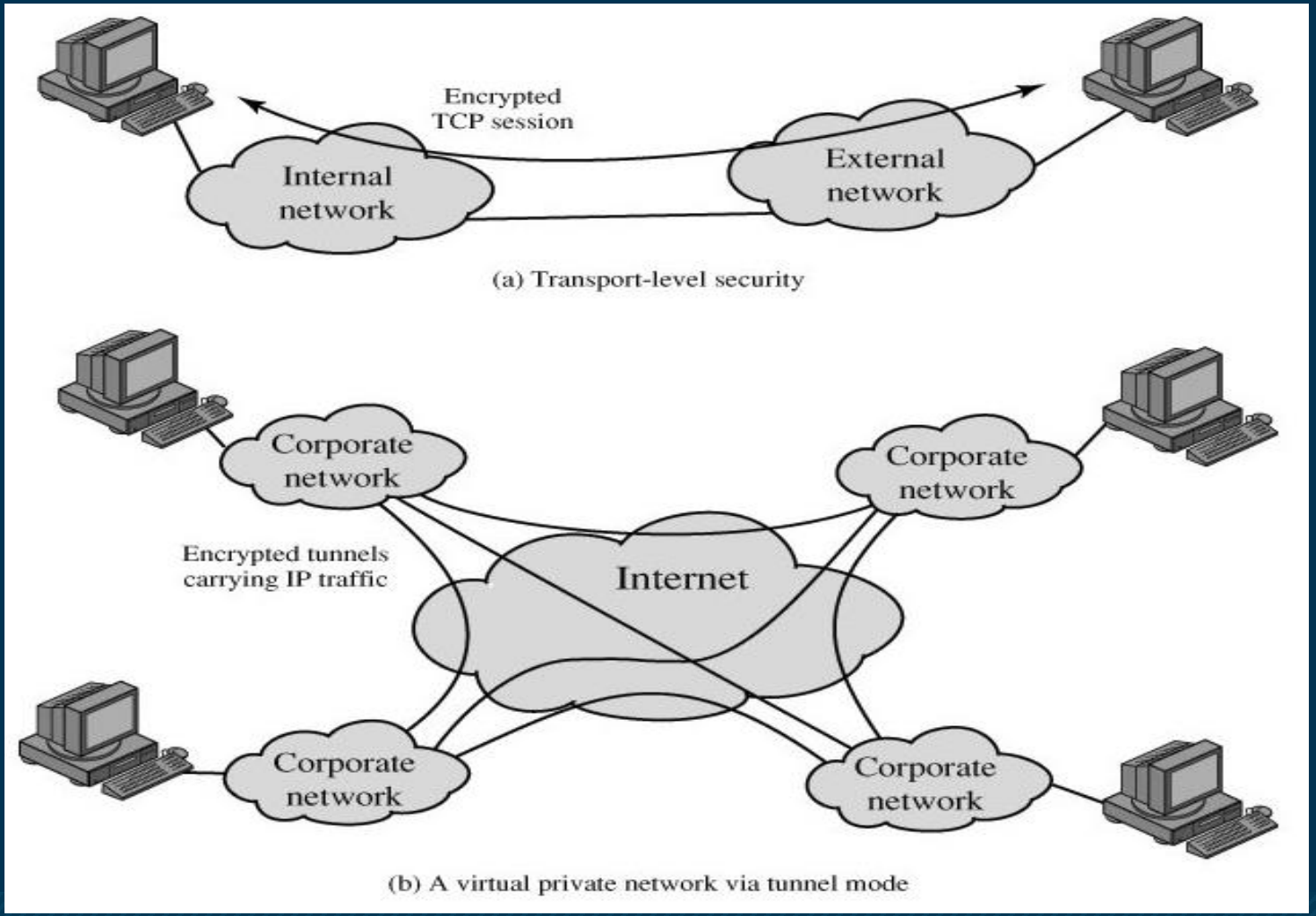



IPSec ESP format

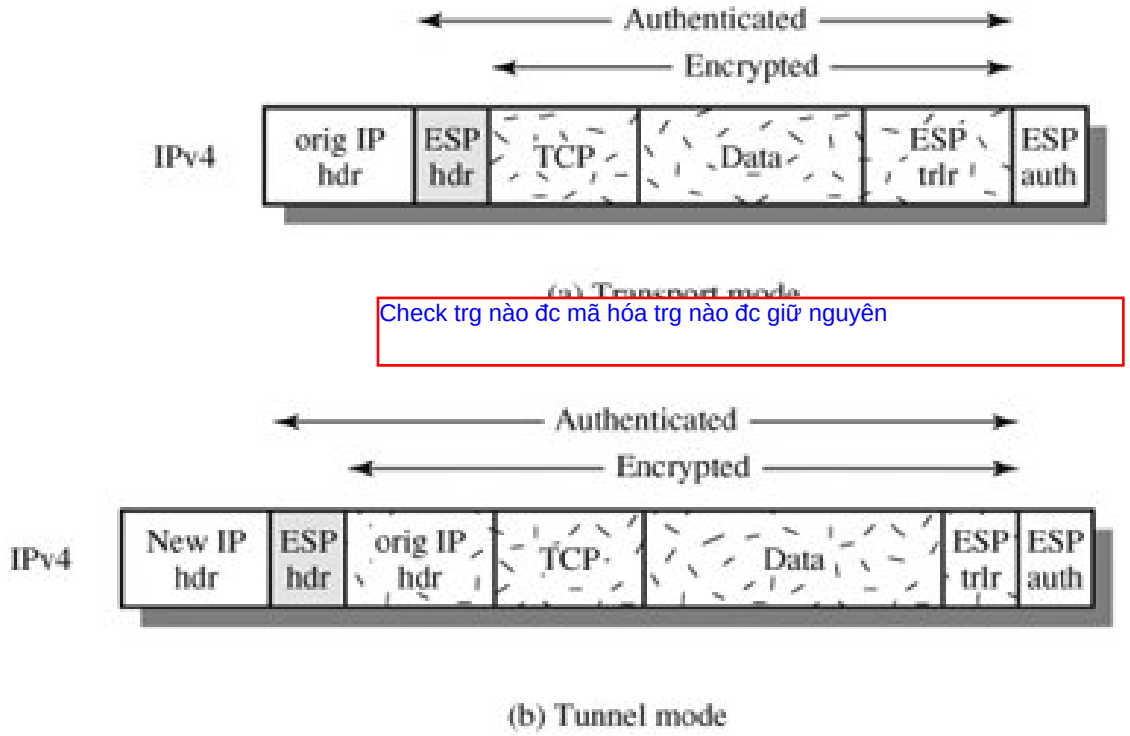
# 5. IPsec
## Định dạng ESP



# 5. IPsec
## Các phương thức mã hoá



# 5. IPsec
## Các phương thức mã hoá

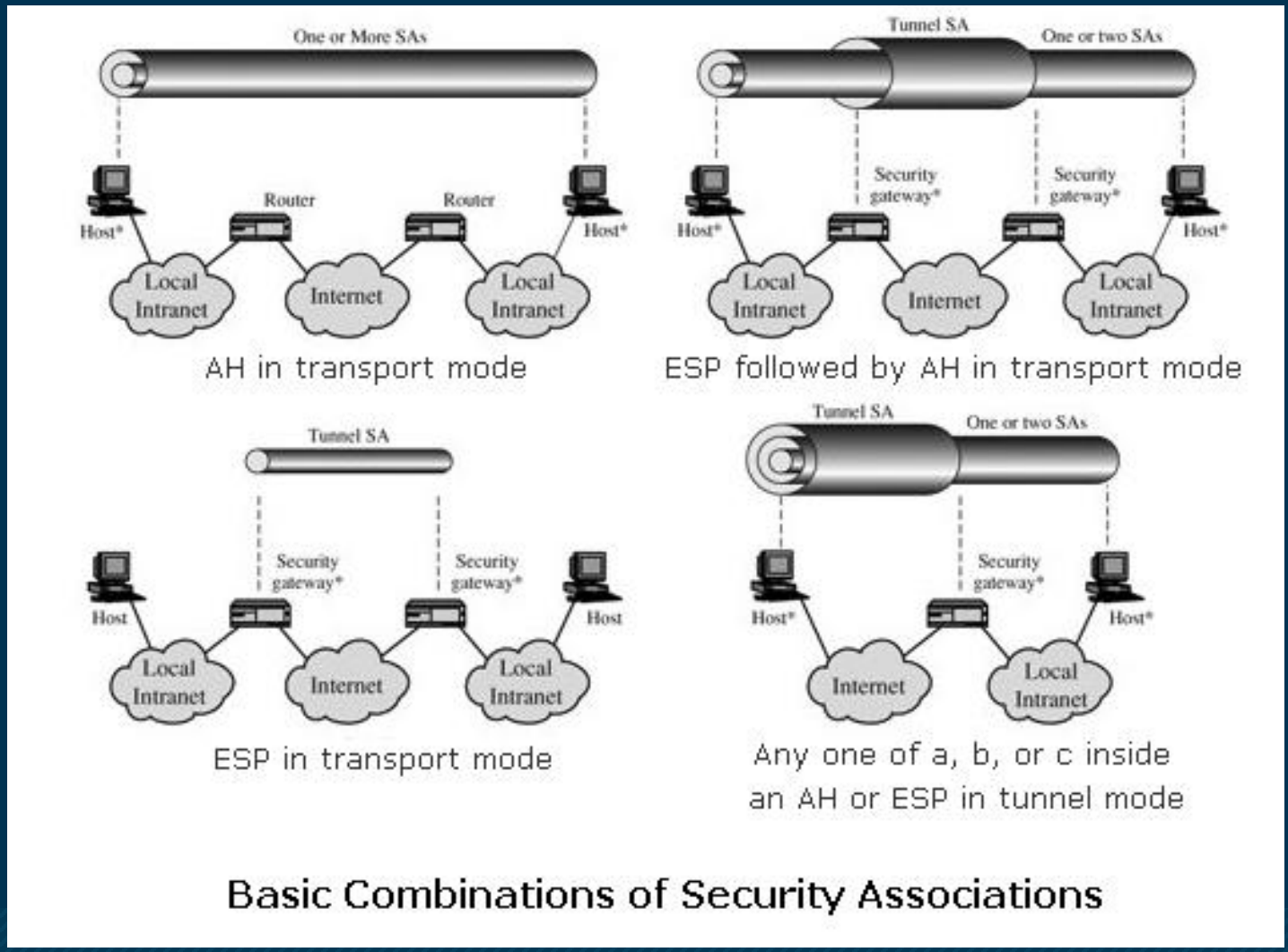



(b) Tunnel mode

Check trg nào đc mã hóa trg nào đc giữ nguyên

Scope of ESP Encryption and Authentication

# 5. IPsec
## Sự kết hợp của các SA



# 6. DNS

# . Bài tập


1. An toàn Mạng máy tính, Tô Nguyễn Nhật Quang, UIT
2. CISSP

# Thank You

# AN TOÀN MẠNG MÁY TÍNH

## #06: Security Protocols

ThS. Lê Đức Thịnh, UIT