HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN HỌC
AN TOÀN MẠNG NÂNG CAO

CHƯƠNG 2 – CÁC KỸ THUẬT BẢO MẬT THÔNG TIN TRUYỀN

Giảng viên: PGS.TS. Hoàng Xuân Dậu

E-mail: dauhx@ptit.edu.vn

Khoa: An toàn thông tin

NỘI DUNG CHƯƠNG 2

1. Các yêu cầu bảo mật thông tin truyền
2. Các giải pháp bảo mật thông tin dựa trên mật mã
3. Các giao thức bảo mật thông tin.

2.1 Các yêu cầu bảo mật thông tin truyền

- Giới thiệu về các yêu cầu bảo mật
- Các yêu cầu bảo mật thông tin truyền
- Các lĩnh vực ứng dụng của bảo mật thông tin truyền

Giới thiệu về các yêu cầu bảo mật

- Thông tin lưu trên các thiết bị lưu trữ, lưu trong CSDL --> thông tin tĩnh;
- Thông tin truyền / trên đường truyền / lưu thông là thông tin động, được vận chuyển trên hệ thống truyền thông, như mạng máy tính hoặc mạng Internet.
- Các yêu cầu bảo mật:
  - Tính bí mật (Confidentiality)
  - Tính toàn vẹn (Integrity)
  - Tính sẵn dùng (Availability)
  - Tính xác thực (Authenticity)
  - Tính chống chối bỏ (Non-repudiation).

Các yêu cầu bảo mật thông tin truyền

- Tính bí mật đảm bảo rằng thông tin truyền không bị tiết lộ cho các bên không có thẩm quyền.
  - Các kỹ thuật phổ biến được sử dụng để duy trì tính bí mật bao gồm mã hóa, kiểm soát truy cập và che giấu dữ liệu.
- Tính toàn vẹn đảm bảo rằng thông tin không bị giả mạo hoặc sửa đổi một cách trái phép.
  - Điều này bao gồm việc bảo vệ dữ liệu khỏi bị sửa đổi, xóa hoặc bổ sung trái phép;
  - Các kỹ thuật phổ biến được sử dụng để duy trì tính toàn vẹn bao gồm chữ ký số, mã xác thực thông điệp và băm dữ liệu.

Các yêu cầu bảo mật thông tin truyền

- Tính xác thực đảm bảo rằng thông tin đến từ một nguồn đáng tin cậy.
  - Điều này bao gồm việc bảo vệ chống mạo danh, giả mạo và các hình thức gian lận danh tính khác;
  - Các kỹ thuật phổ biến được sử dụng để thiết lập tính xác thực bao gồm xác thực, chứng chỉ số và nhận dạng sinh trắc học.

Các yêu cầu bảo mật thông tin truyền

- Tính xác thực đảm bảo rằng thông tin đến từ một nguồn đáng tin cậy.
  - Điều này bao gồm việc bảo vệ chống mạo danh, giả mạo và các hình thức gian lận danh tính khác;
  - Các kỹ thuật phổ biến được sử dụng để thiết lập tính xác thực bao gồm xác thực, chứng chỉ số và nhận dạng sinh trắc học.

Các yêu cầu bảo mật thông tin truyền

- Tính chống chối bỏ đảm bảo rằng một bên không thể phủ nhận việc đã gửi hoặc nhận một thông điệp hoặc giao dịch.
  - Điều này bao gồm việc bảo vệ chống lại các cuộc tấn công giả mạo và phát lại thông điệp;
  - Các kỹ thuật phổ biến được sử dụng để thiết lập tính chống chối bỏ bao gồm chữ ký số, mã xác thực thông điệp và tem thời gian.

Các lĩnh vực ứng dụng của bảo mật thông tin truyền

- Các dịch vụ mạng
- Trao đổi thông tin
- Thương mại điện tử
- Thanh toán, dịch vụ tài chính, ngân hàng.

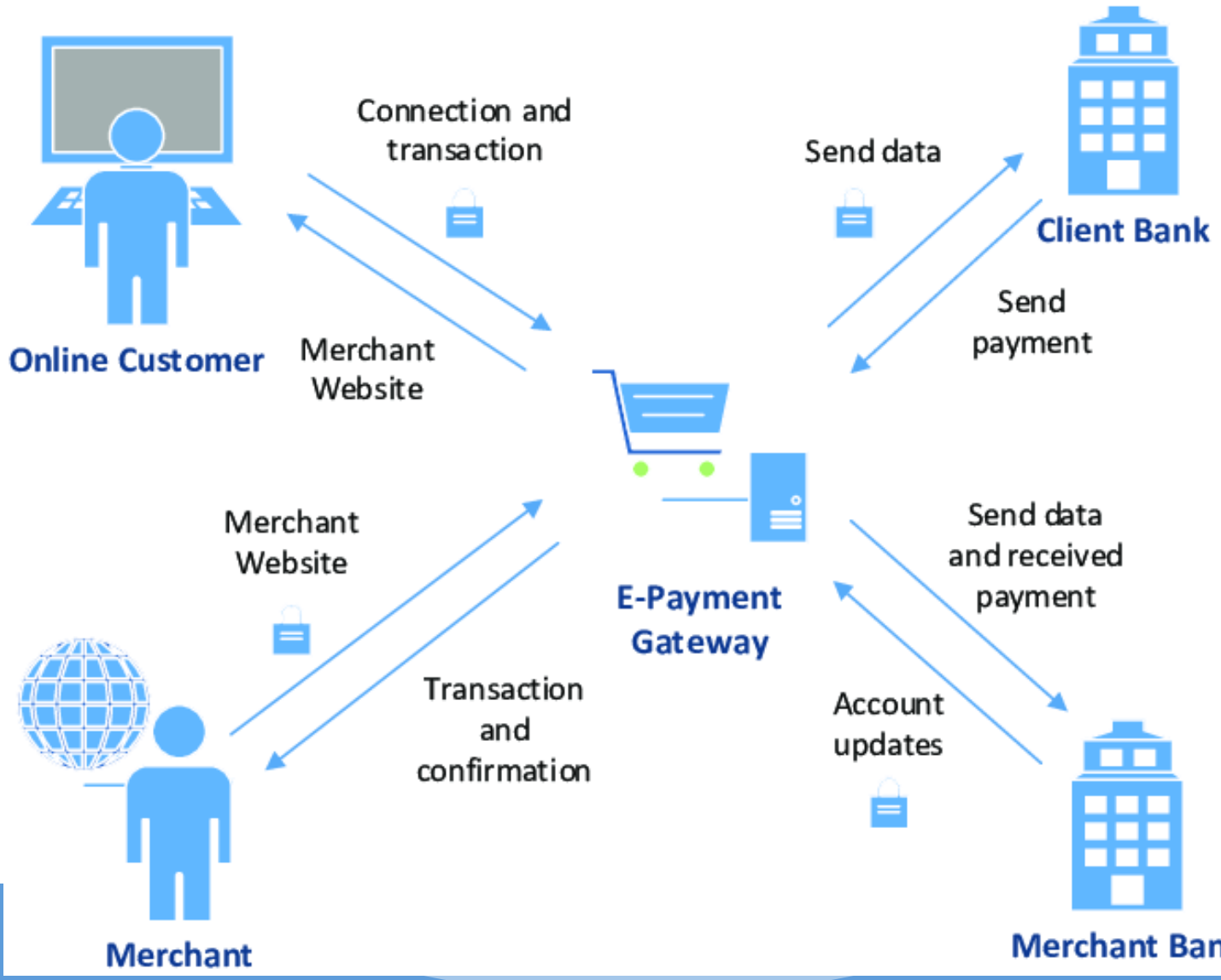
Các lĩnh vực ứng dụng của bảo mật thông tin truyền

- Các dịch vụ mạng
  - Các hệ thống dịch vụ công, các cổng thông tin điện tử
  - Các trang thông tin điện tử
  - Các hệ thống học tập, đào tạo trực tuyến
  - Các mạng xã hội
  - Truyền hình trực tuyến, kho nội dung số
  - Thư viện trực tuyến...

Các lĩnh vực ứng dụng của bảo mật thông tin truyền

- Trao đổi thông tin
  - Các ứng dụng nhắn tin, như Zalo, Skype, Messager...
  - Các ứng dụng dạy học trực tuyến, như Zoom, Google Meet, MS Teams...
- Thương mại điện tử
  - Sàn thương mại điện tử, như Amazon, Tiki, Shopee...
  - Các website thương mại điện tử.
- Thanh toán, dịch vụ tài chính, ngân hàng
  - Ngân hàng trực tuyến
  - Dịch vụ tài chính trực tuyến
  - Thanh toán trực tuyến.

Hệ thống thanh toán trực tuyến



2.2 Các giải pháp bảo mật thông tin dựa trên mật mã

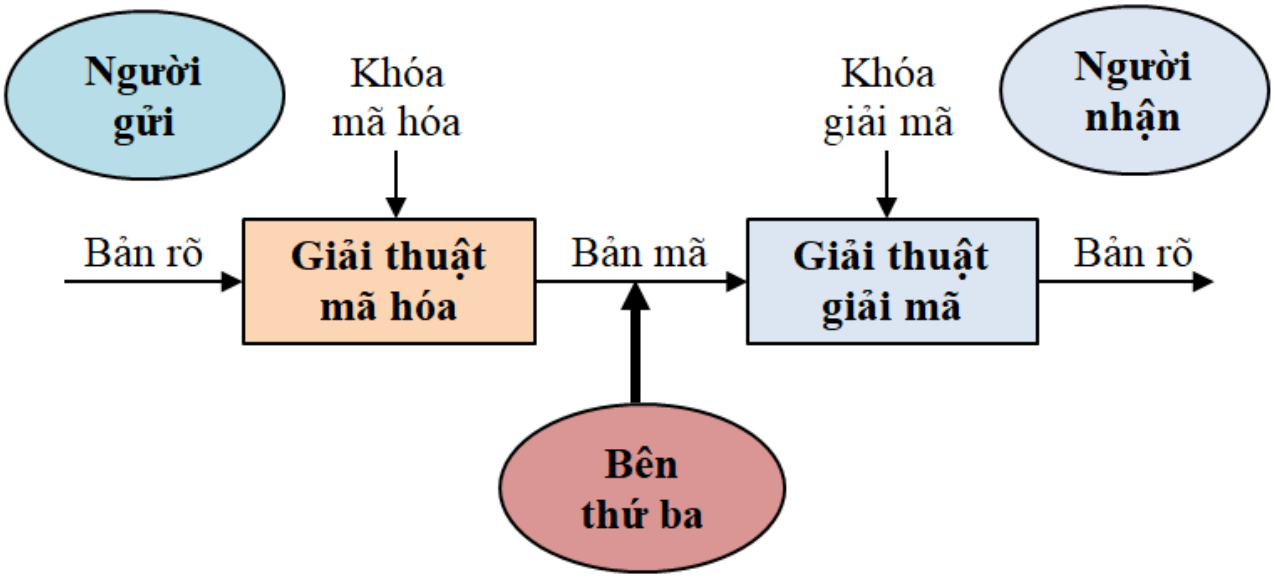
- Mã hóa dữ liệu
- Hàm băm
- Các hệ mật mã lai
- Chữ ký số
- Chứng chỉ số
- Hạ tầng khóa công khai
- Giấu tin

Mã hóa dữ liệu

- Giới thiệu
- Một số hệ mật mã

Mã hóa dữ liệu - Giới thiệu

- Các giải pháp mã hóa dữ liệu được sử dụng để đảm bảo *tính bí mật* của thông tin truyền.



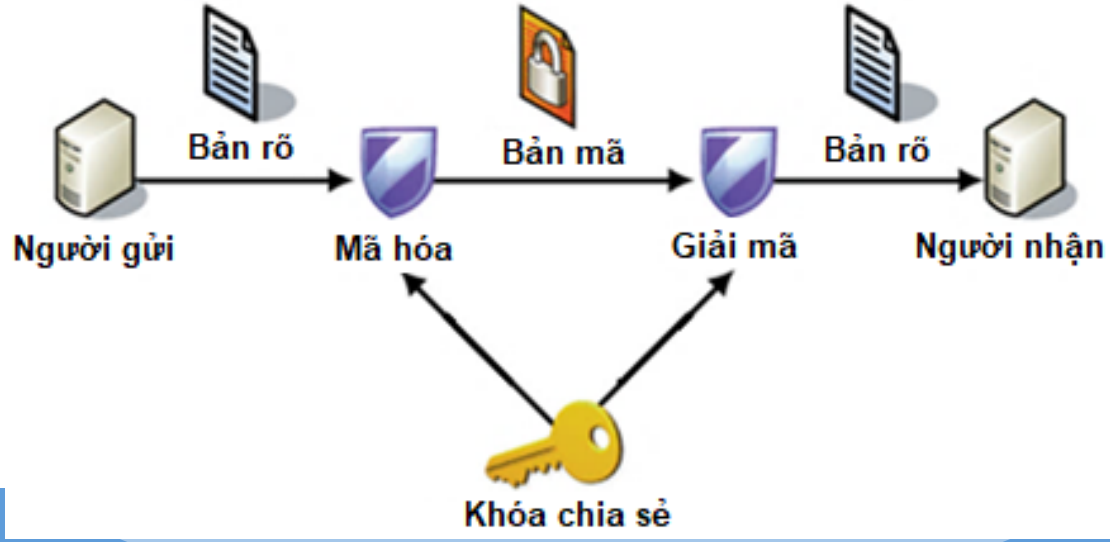
Mã hóa dữ liệu - Giới thiệu

- Các hệ mật mã thường được sử dụng để mã hóa - giải mã thông điệp bao gồm:
  - Các hệ mật mã khóa đối xứng
    - DES, 3-DES
    - AES, IDEA, Twofish, Blowfish...
  - Các hệ mật mã khóa bất đối xứng
    - RSA
    - Elgamal
    - Elliptic curve cryptosystem (ECC)...

Một số hệ mật mã

❖ Các hệ mật mã khóa đối xứng:

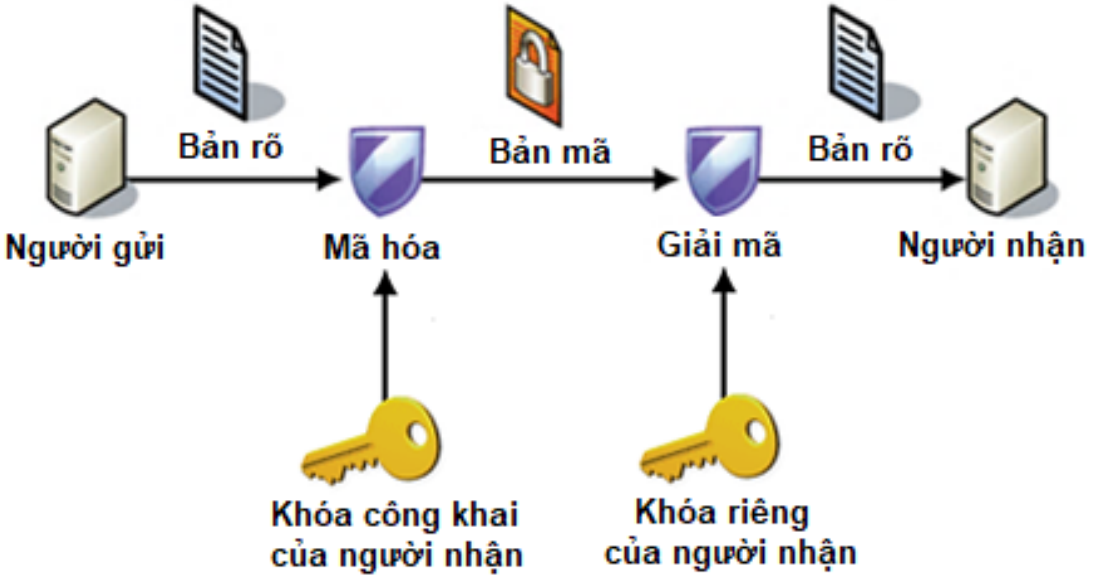
- Sử dụng chung 1 khóa (khóa bí mật / khóa chia sẻ) cho cả khâu mã hóa và giải mã
- Kích thước khóa nhỏ, tốc độ cao, độ bảo mật cao
- Thích hợp cho mã hóa và giải mã lượng lớn dữ liệu
- Khó khăn trong trao đổi khóa dùng chung.



Một số hệ mật mã

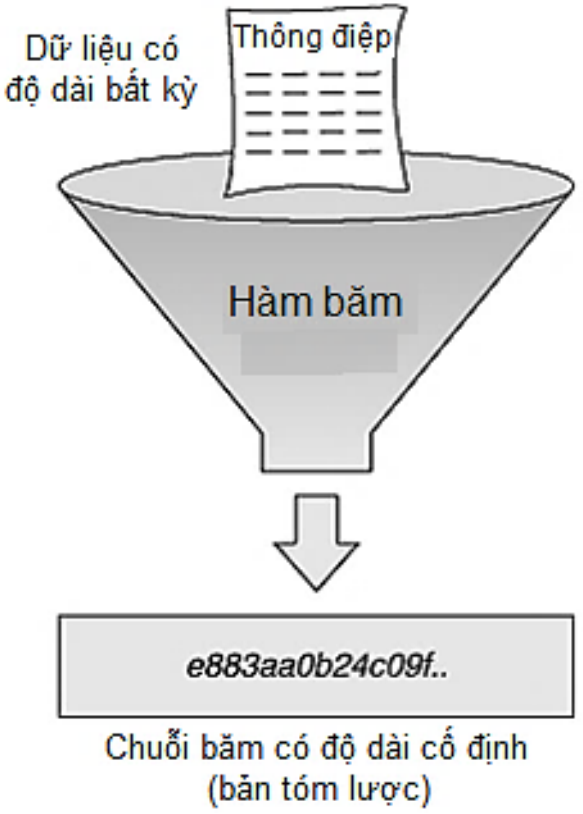
❖ Các hệ mật mã khóa bất đối xứng:

- Sử dụng chung 1 khóa (khóa công khai) cho khâu mã hóa và 1 khóa khác (khóa riêng) cho khâu giải mã
- Kích thước khóa lớn, tốc độ thấp (trừ các hệ mật ECC), độ bảo mật cao
- Thích hợp cho mã hóa và giải mã lượng nhỏ dữ liệu (như trao đổi khóa bí mật, hoặc ký số).
- Trao đổi khóa dễ dàng hơn cho khóa mã hóa là công khai.



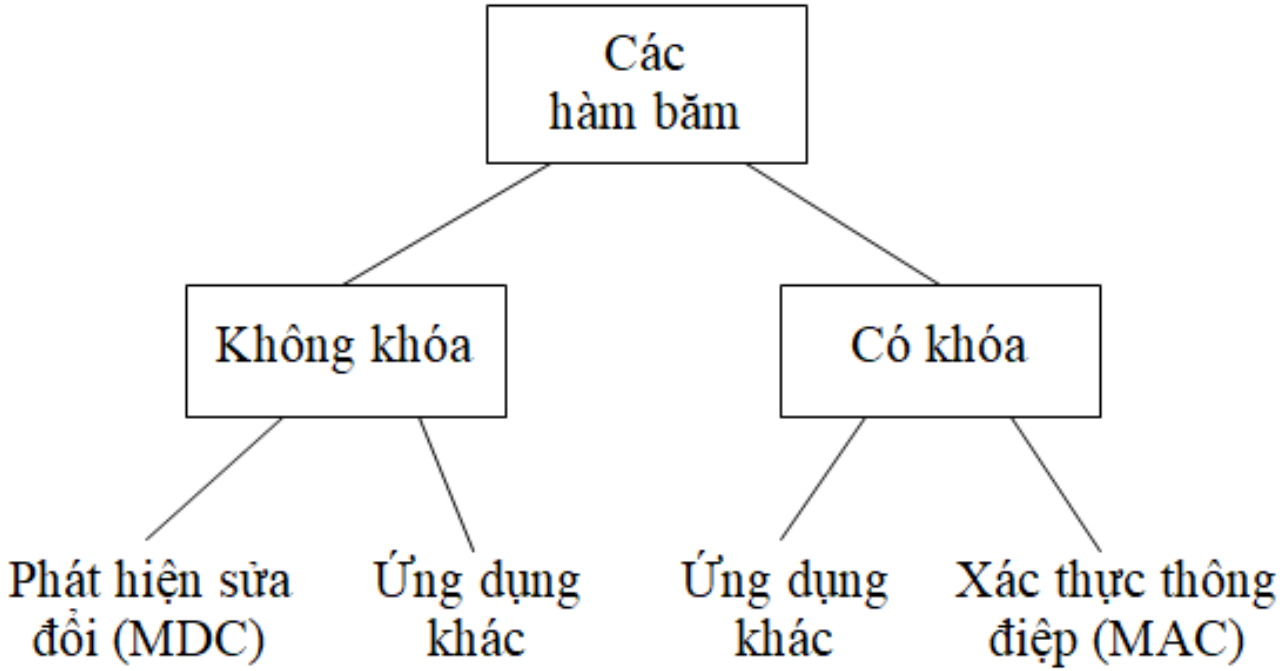
Hàm băm

- Hàm băm (Hash function) là một ánh xạ chuyển đổi dữ liệu có kích thước thay đổi về dữ liệu có kích thước cố định.
  - Do chuỗi băm đầu ra thường có kích thước cố định và nhỏ hơn nhiều lần so với thông điệp đầu vào, nó thường được gọi là chuỗi đại diện, hay bản tóm lược (digest) của thông điệp.
- Hàm băm thường được sử dụng để:
  - Mã hóa mật khẩu
  - Tạo chuỗi xác thực thông điệp (MAC)
  - Sử dụng trong tạo và kiểm tra chữ ký số.



Hàm băm

❖ Các loại hàm băm:



Hàm băm

- Một số hàm băm thông dụng:
  - CRC-32 (đầu ra 32 bít)
  - Họ MD:
    - MD2, MD4, MD5 (đầu ra 128 bít)
    - MD6 (đầu ra từ 0-512 bit)
  - Họ SHA:
    - SHA0 (đầu ra 160 bít)
    - SHA1 (đầu ra 160 bít)
    - SHA2 (đầu ra 224, 256, 384, 512 bít)
    - SHA3 (đầu ra từ 0-512 bit)

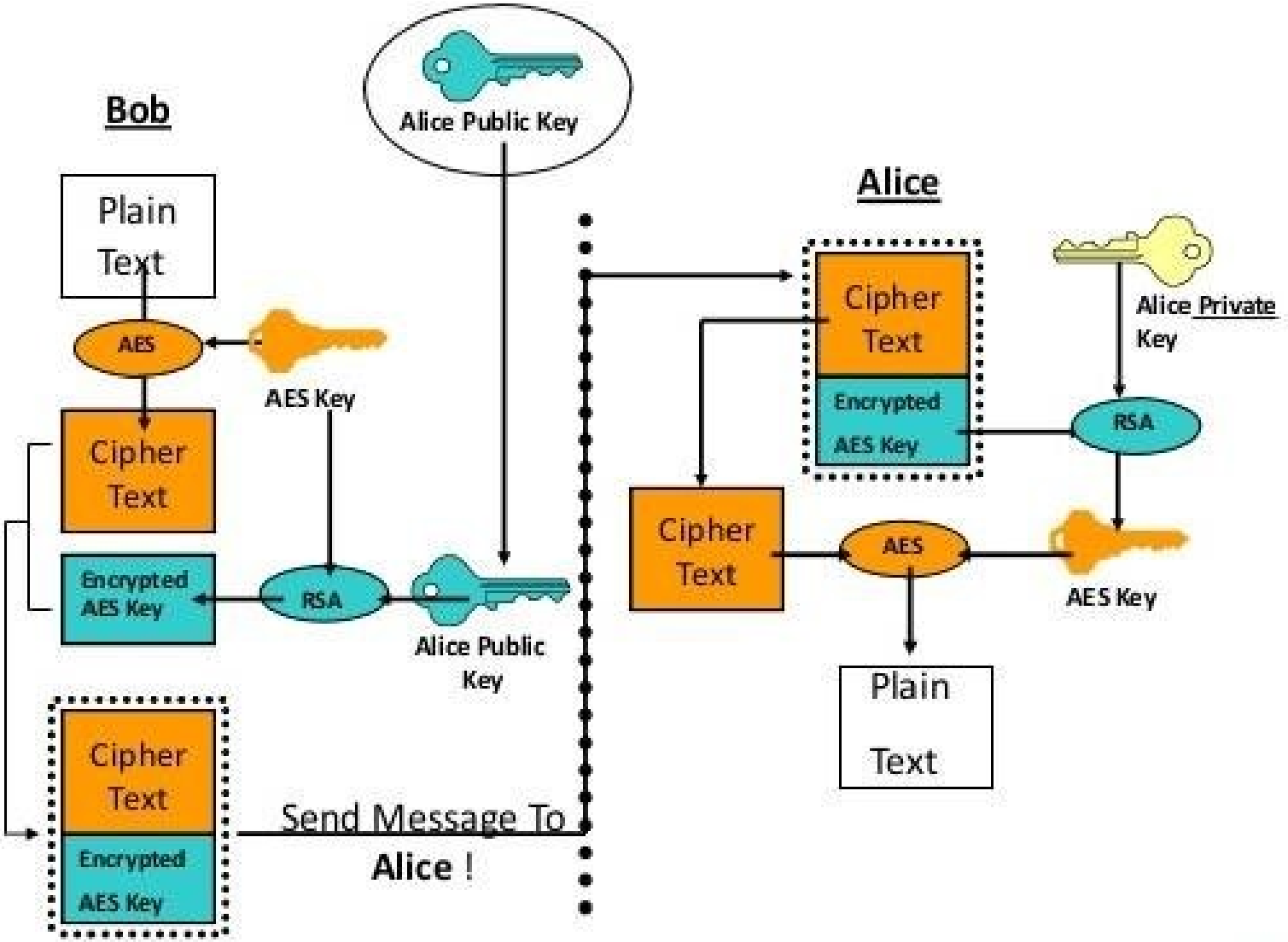
Các hệ mật mã lai

- Hệ mật mã lai (hybrid cryptosystem) là hệ mật mã kết hợp giữa hệ mật khóa công khai (public-key cryptosystem) và hệ mật khóa bí mật (secret-key cryptosystem) để khai thác điểm mạnh của cả 2 hệ mật mã:
  - Hệ mật khóa công khai hỗ trợ trao đổi khóa dễ dàng: sử dụng để trao đổi khóa bí mật cho mã hóa/giải mã dữ liệu;
  - Hệ mật khóa bí mật có tốc độ mã hóa/giải mã cao: sử dụng để mã hóa/giải mã dữ liệu truyền.

Các hệ mật mã lai

- Các hệ mật mã lai có thể được xây dựng bằng cách kết hợp 2 hệ mật độc lập:
  - 1 hệ mật khóa công khai
  - 1 hệ mật khóa bí mật.
- Ví dụ:
  - RSA + AES
  - Diffie-Hellman + AES
  - RSA + 3-DES...

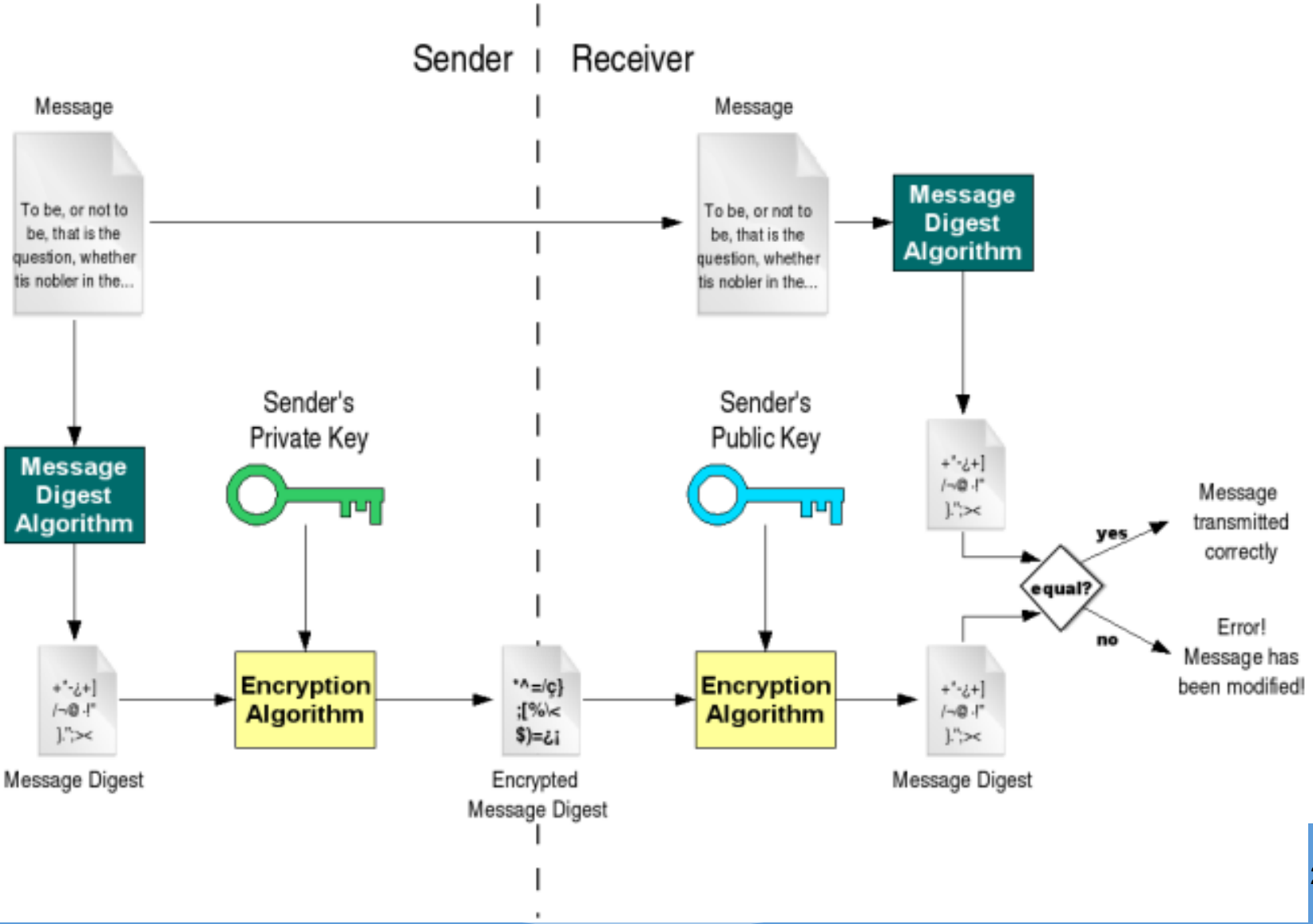
Mã hóa/giải mã sử dụng hệ mật mã lai



Chữ ký số

- Chữ ký số (Digital signature) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp.
- Chữ ký số thường được sử dụng để đảm bảo tính toàn vẹn của thông điệp.
- Các giải thuật mật mã khóa khóa bất đối xứng / khóa công khai thường được sử dụng để tạo và kiểm tra chữ ký số:
  - Khóa riêng của người gửi thông điệp được sử dụng để tạo chữ ký số
  - Khóa công khai của người gửi thông điệp được sử dụng để kiểm tra chữ ký số.

Chữ ký số - Quá trình ký và kiểm tra



Chữ ký số - Quá trình ký và kiểm tra

- Các bước của quá trình ký một thông điệp (bên Sender / Người gửi):
  - Tính toán chuỗi đại diện (message digest/hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm);
  - Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và một giải thuật tạo chữ ký (Signature/Encryption algorithm). Kết quả là chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encrypted message digest);
  - Thông điệp ban đầu (message) được ghép với chữ ký số (Digital signature) tạo thành thông điệp đã được ký (Signed message);
  - Thông điệp đã được ký (Signed message) được gửi cho người nhận.

Chữ ký số - Quá trình ký và kiểm tra

- Các bước của quá trình kiểm tra chữ ký (bên Receiver / Người nhận):
  - Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
  - Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký);
  - Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số → chuỗi đại diện thông điệp MD2;
  - So sánh MD1 và MD2:
    - Nếu MD1 = MD2 → chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
    - Nếu MD1 <> MD2 → chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.

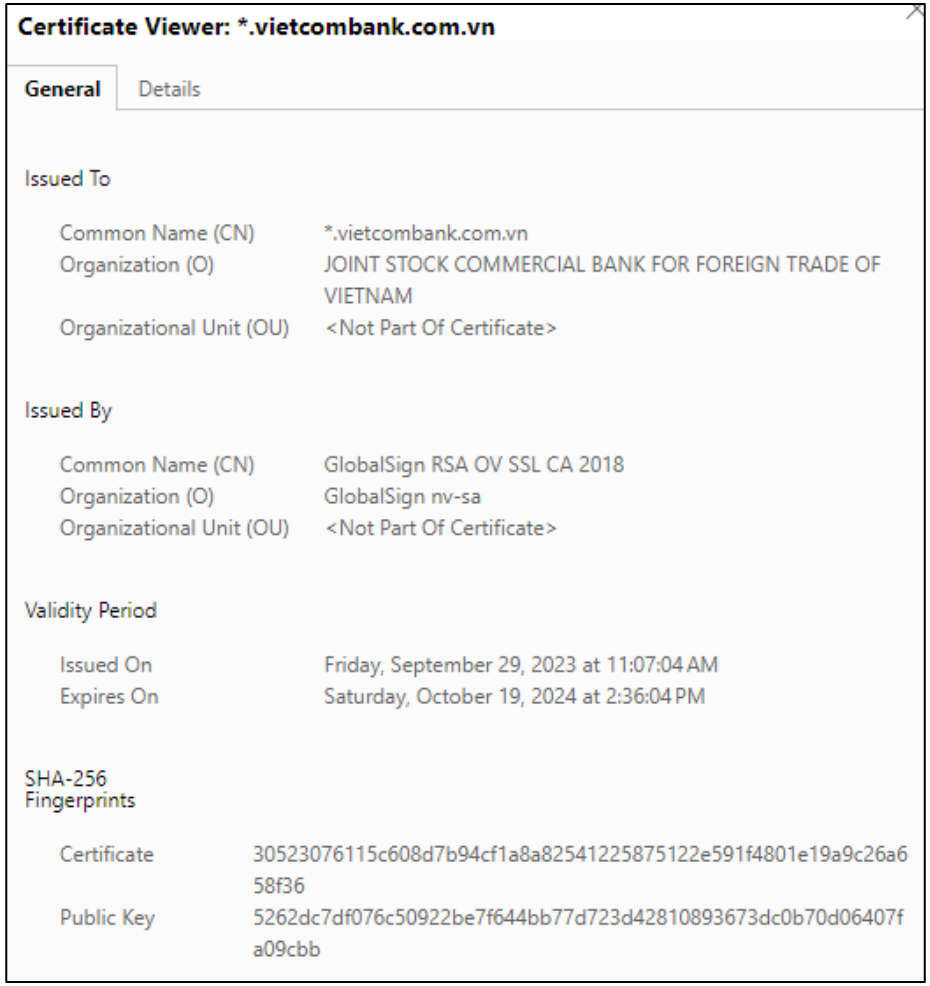
Chữ ký số - Một số giải thuật chữ ký số

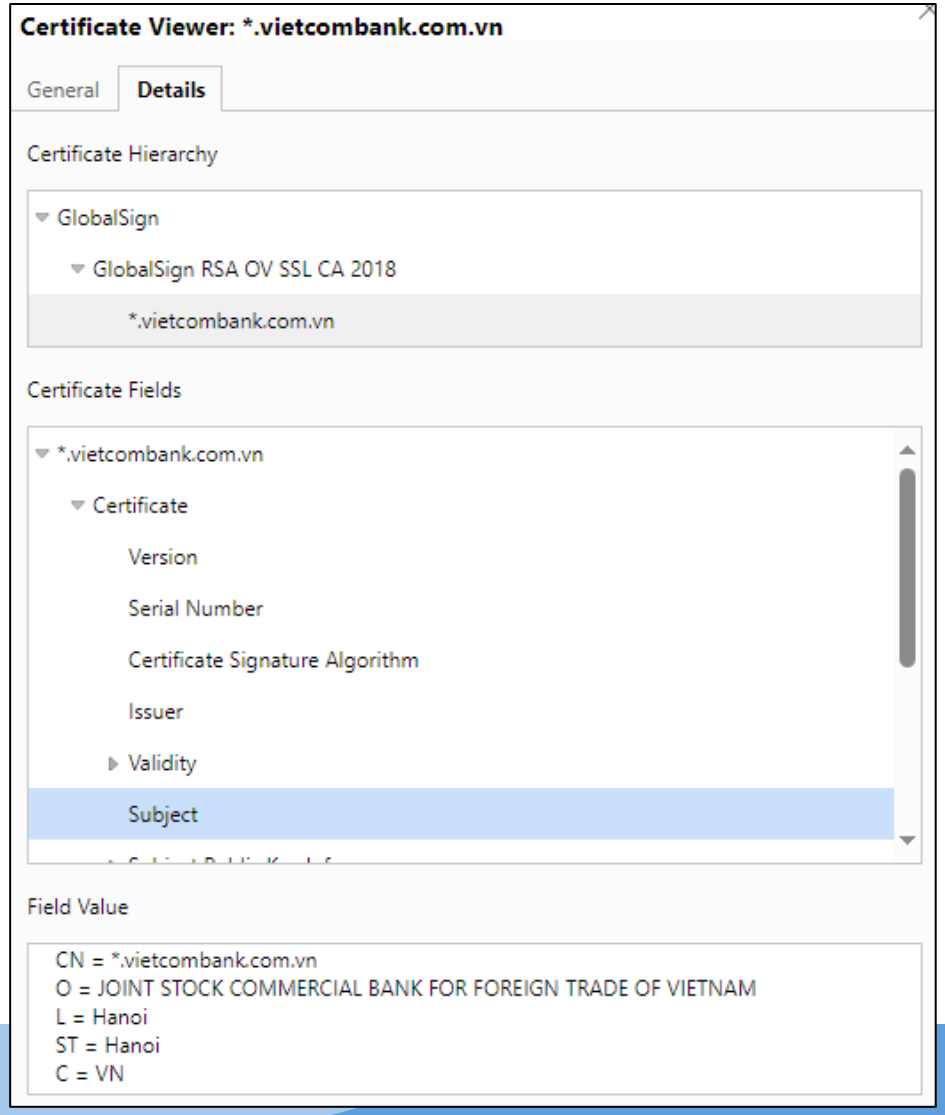
- Chữ ký số RSA
  - Giải thuật RSA được sử dụng rộng rãi cho ký số: khóa riêng RSA để tạo chữ số và khóa công khai (thường được tích hợp trong chứng chỉ số) để kiểm tra chữ ký số.
- Chữ ký số DSA (Digital Signature Algorithm)
  - DSA được phát triển từ ElGamal Signature Algorithm
- Chữ ký số ECDSA (Elliptic Curve Digital Signature Algorithm)
  - Là chữ ký số DSA dựa trên đường cong Elliptic.
- Chữ ký số EdDSA (Edward Curve Digital Signature Algorithm)
  - Là chữ ký số DSA dựa trên đường cong Edward.

Chứng chỉ số - Giới thiệu

- Chứng chỉ số (Digital certificate), còn gọi là chứng chỉ khóa công khai (Public key certificate), hay chứng chỉ nhận dạng (Identity certificate) là một tài liệu điện tử sử dụng một ***chữ ký số*** để liên kết một ***khóa công khai*** và ***thông tin nhận dạng*** của một thực thể:
  - Chữ ký số: là chữ ký của một bên thứ 3 tin cậy, thường gọi là CA – Certificate Authority;
  - Khóa công khai: là khóa công khai trong cặp khóa công khai của thực thể;
  - Thông tin nhận dạng: là tên, địa chỉ, tên miền hoặc các thông tin định danh của thực thể.
- Chứng chỉ số có thể được sử dụng để xác minh chủ thể thực sự của một khóa công khai.

Chứng chỉ số - Nội dung





Chứng chỉ số - Nội dung

- Chứng chỉ số gồm các trường chính sau (chuẩn X.509 V3):
  - Version: Phiên bản
  - Serial Number: Số nhận dạng của chứng chỉ số;
  - Certificate Signature Algorithm: Giải thuật tạo/kiểm tra chữ ký;
  - Issuer: Người/tổ chức có thẩm quyền/tin cậy cấp chứng chỉ;
  - Validity: Thời hạn sử dụng hợp lệ (Not before / Not after)
  - Subject: Thông tin nhận dạng một cá nhân hoặc một tổ chức;
  - Subject Public Key Info: Thông tin khóa công khai của chủ thể
  - SHA-256 Fingerprints: thông tin chữ ký của nhà cung cấp:
    - Certificate: Chứng chỉ của nhà cung cấp
    - Public Key: khóa công khai của nhà cung cấp.

Chứng chỉ số - Nội dung

- Nội dung của trường Subject:
  - CN (Common Name): Tên chung, nhưng một tên miền được gán chứng chỉ;
  - OU (Organisation Unit): Tên bộ phận/phòng ban;
  - O (Organisation): Tổ chức/Cơ quan/công ty;
  - L (Location): Địa điểm/Quận huyện;
  - ST (State/Province): Bang/Tỉnh/Thành phố;
  - C (Country): Đất nước.

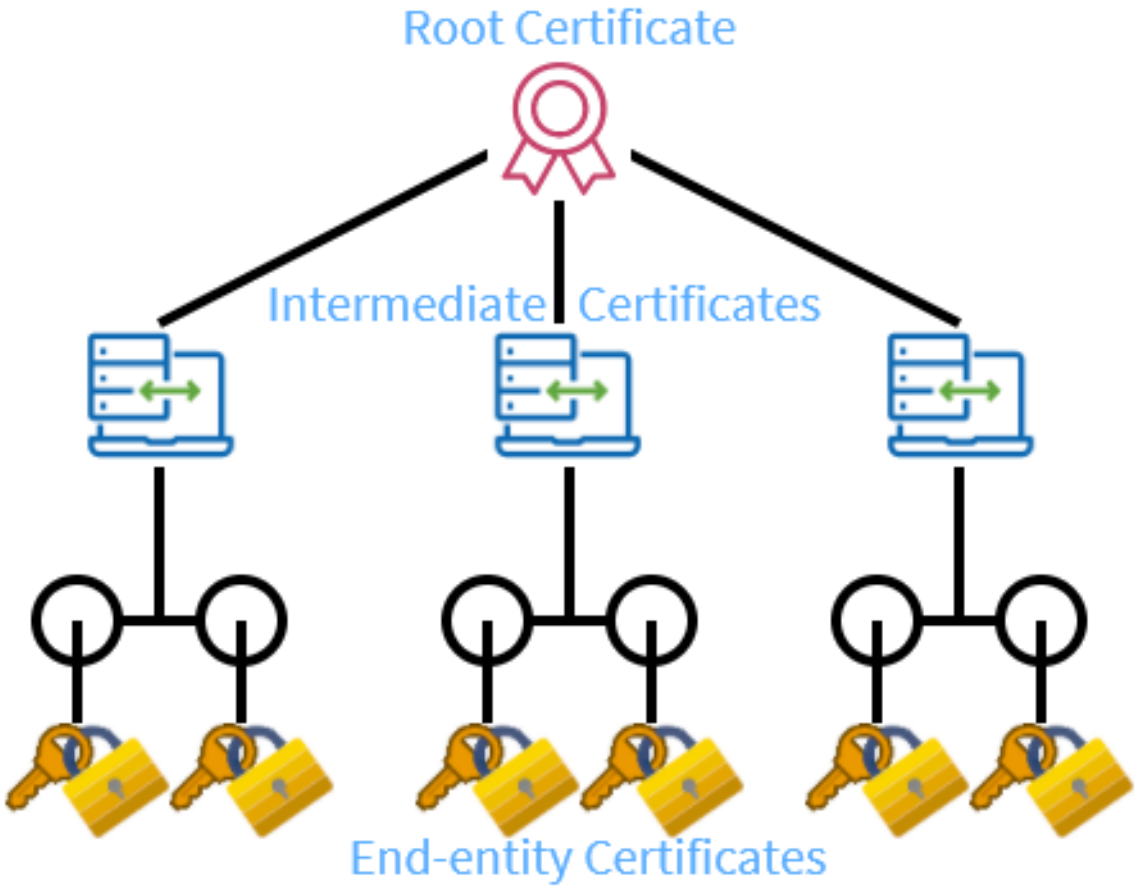
Chứng chỉ số - Sử dụng

- Đảm bảo an toàn cho giao dịch trên nền web:
  - Dùng chứng chỉ số cho phép website chạy trên SSL (tối thiểu máy chủ phải có chứng chỉ số): HTTP → HTTPS: toàn bộ thông tin chuyển giữa server và client được đảm bảo tính bí mật (sử dụng mã hóa khóa đối xứng), toàn vẹn và xác thực (sử dụng hàm băm có khóa MAC);
  - Chứng chỉ số để các bên xác thực thông tin nhận dạng của nhau.
- Chứng chỉ số có thể được sử dụng cho nhiều ứng dụng:
  - Email;
  - FTP;
  - Các ứng dụng khác.

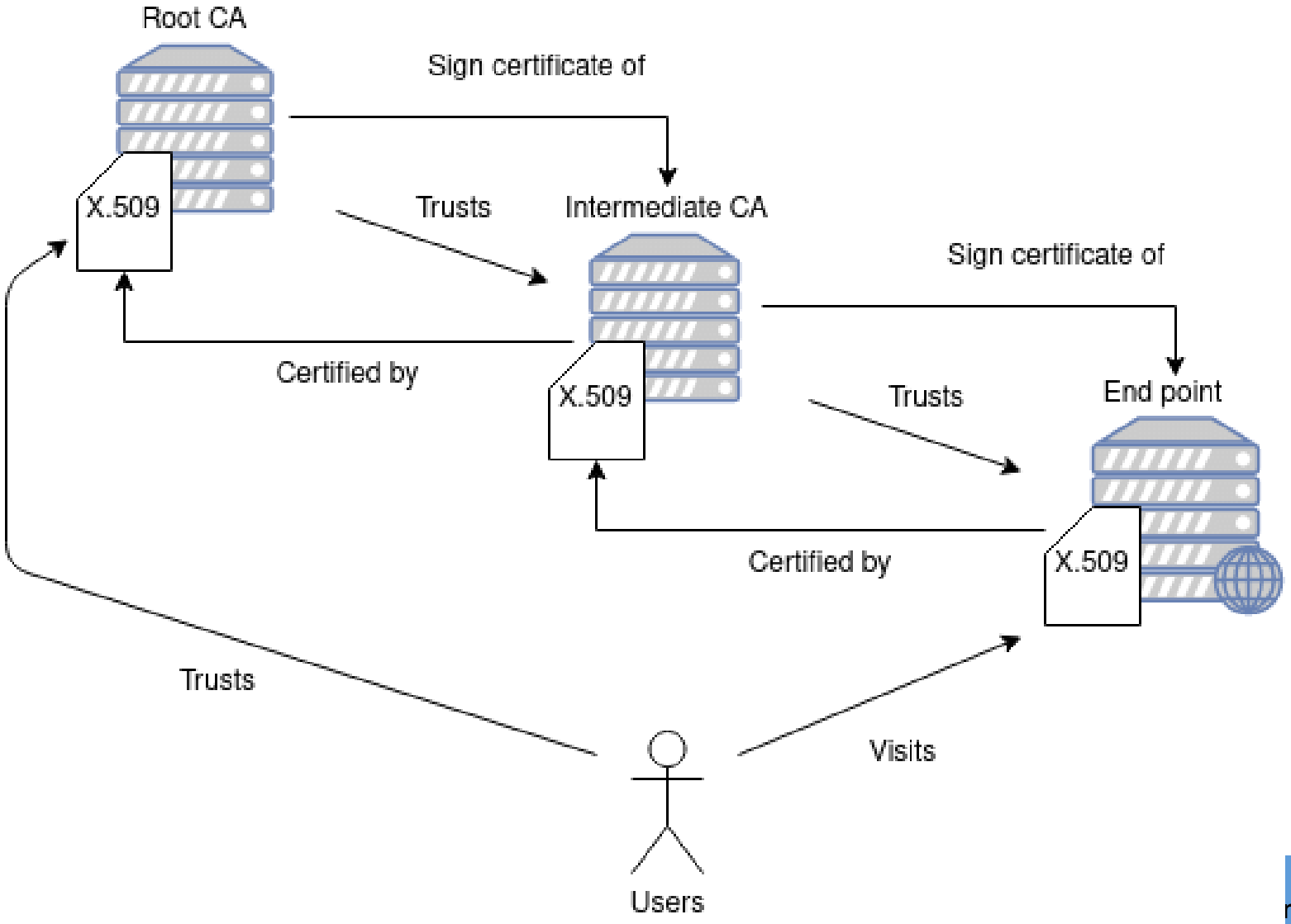
Chuẩn chứng chỉ số khóa công khai - X.509

- X.509 là chuẩn chứng chỉ số khóa công khai do Liên minh Viễn thông Quốc tế ban hành;
  - X.509 được sử dụng rộng rãi trong nhiều giao thức Internet, như SSL/TLS;
  - X.509 được sử dụng trong nhiều ứng dụng tạo chữ ký điện tử offline.
- Các loại chứng chỉ theo X.509:
  - Root certificate: là dạng chứng chỉ tự ký của 1 CA, cũng là điểm kết thúc của chuỗi chữ ký. Root certificate được lưu trong Trust Store của ứng dụng kiểm tra, như trình duyệt.
  - Intermediate certificate: là dạng chứng chỉ nhánh của CA, được ký bởi Root certificate.
  - End-entity certificate: là chứng chỉ cấp cho người / tổ chức sử dụng.

Chuỗi chứng chỉ X.509



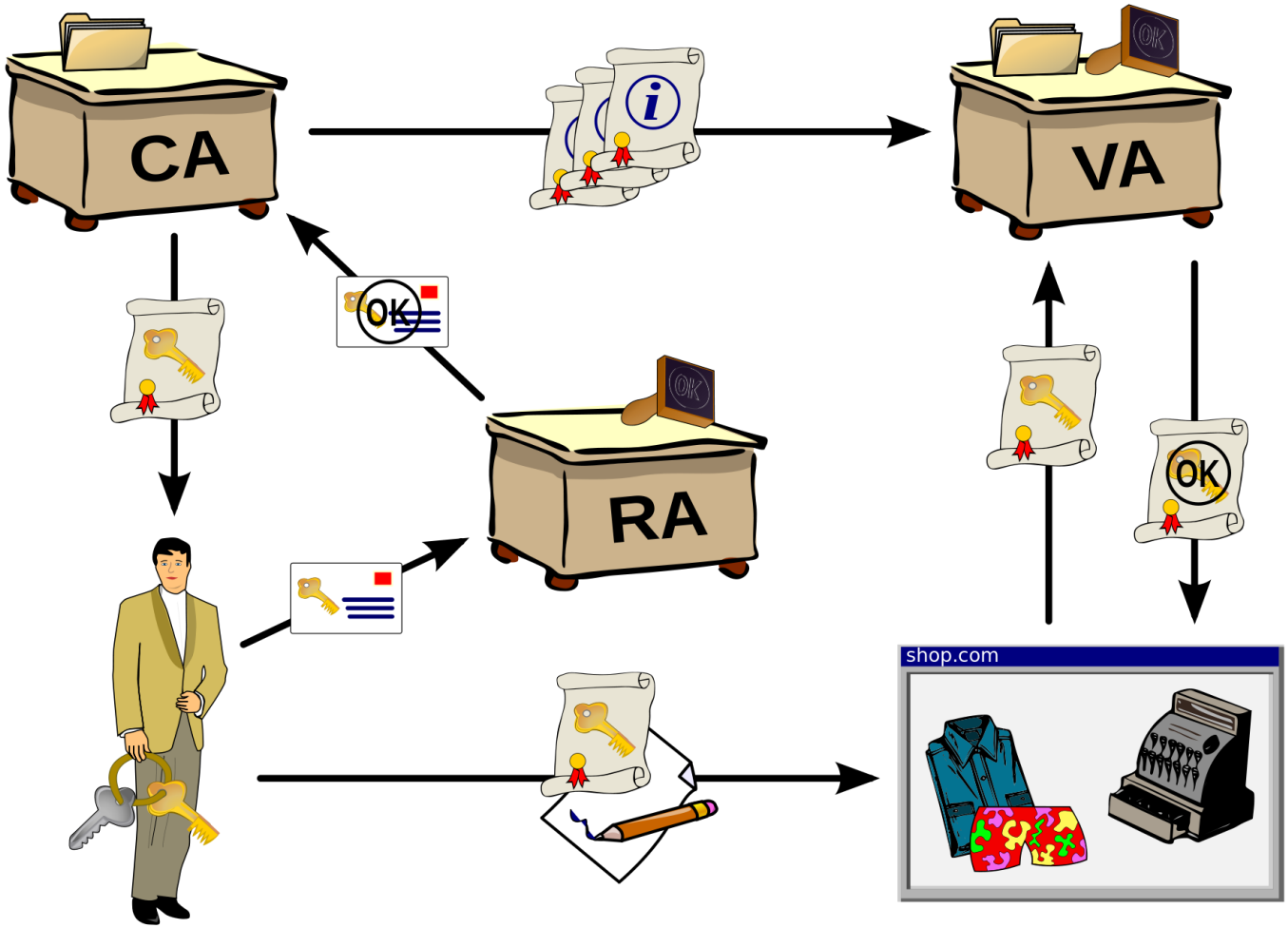
Chuỗi chứng chỉ X.509 - Xác minh



Hạ tầng khóa công khai - PKI

- Hạ tầng khóa công khai (Public-key infrastructure - PKI) là một tập các phần cứng, phần mềm, nhân lực, chính sách và các thủ tục để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng chỉ số;
- Một PKI gồm:
  - Certificate Authority (CA): Cơ quan cấp và kiểm tra chứng chỉ số;
  - Registration Authority (RA): Bộ phận kiểm tra thông tin nhận dạng của người dùng theo yêu cầu của CA;
  - Validation Authority (VA): Cơ quan xác nhận thông tin nhận dạng của người dùng thay mặt CA;
  - Central Directory (CD): Là nơi lưu danh mục và lập chỉ số các khóa;
  - Certificate Management System: Hệ thống quản lý chứng chỉ;
  - Certificate Policy: Chính sách về chứng chỉ;

Hạ tầng khóa công khai – Lưu đồ cấp và sử dụng



Hạ tầng khóa công khai – Lưu đồ cấp và sử dụng

- Đăng ký, xét duyệt và cấp chứng chỉ số:
  - Người dùng có yêu cầu cấp chứng chỉ số tạo một cặp khóa, gồm 1 khóa công khai và 1 khóa riêng;
  - Người dùng tạo yêu cầu cấp chứng chỉ số (Certificate request), trong đó tích hợp khóa công khai và thông tin định danh của mình. Yêu cầu cấp chứng chỉ số thường được lưu dưới dạng 1 file văn bản theo định dạng của chuẩn X.509;
  - Người dùng gửi yêu cầu cấp chứng chỉ số đến Bộ phận tiếp nhận (RA). RA kiểm tra các thông tin trong yêu cầu cấp chứng chỉ số, nếu hợp lệ thì chuyển yêu cầu đến Cơ quan cấp chứng chỉ (CA);

Hạ tầng khóa công khai – Lưu đồ cấp và sử dụng

❖ Đăng ký, xét duyệt và cấp chứng chỉ số:

- CA sẽ thực hiện việc xác minh các thông tin nhận dạng của chủ thể và nếu xác minh thành công thì cấp chứng chỉ số cho người yêu cầu. Chứng chỉ số được CA ký bằng khóa riêng của mình để đảm bảo tính xác thực và toàn vẹn và thường được lưu dưới dạng 1 file văn bản theo định dạng của chuẩn X.509;
- Sau khi phát hành chứng chỉ số cho người dùng, CA chuyển thông tin về chứng chỉ số đã cấp cho thành phần VA để xác nhận thông tin nhận dạng theo yêu cầu;
- Người dùng cài đặt chứng chỉ số vào hệ thống và có thể bắt đầu sử dụng trong các ứng dụng của mình.

Hạ tầng khóa công khai – Lưu đồ cấp và sử dụng

- Sử dụng và kiểm tra chứng chỉ số:
  - Người dùng tạo đơn hàng, ký vào đơn hàng bằng khóa riêng, gửi đơn hàng đã ký và chứng chỉ số cho nhà cung cấp;
  - Nhà cung cấp chuyển chứng chỉ số của người dùng cho VA để kiểm tra, nếu chứng chỉ số hợp lệ thì tiến hành xác thực chữ ký số của người dùng sử dụng khóa công khai của người dùng lấy từ chứng chỉ số. Nếu chữ ký của người dùng xác thực thành công thì đơn hàng được duyệt.

Một số nền tảng PKI mã mở

- EJBCA CE
- Dogtag PKI
- OpenXPKI
- step-CA

Một số nền tảng PKI mã mở

	EJBCA	Dogtag PKI	OpenXPKI	step-CA
Ease of use	Easy	Moderate	Easy-Moderate	Advanced (No GUI)
Language	Java	Java	Perl	Go
Extensibility	SCEP, CMP, REST API	ACME, SCEP, REST API	SCEP, EST, REST API	ACME, SCEP
Revocation	CRL, OCSP	CRL, OCSP	CRL	"Passive Revocation"
Key types	RSA, ECDSA	RSA	RSA, ECDSA	RSA, ECDSA, EdDSA
PKCS #11 interface	Yes	Yes	Yes	Yes
Web interface / GUI	Yes	Yes	Yes	No (Only CLI)
Updates / releases	See GitHub	See GitHub	See GitHub	See GitHub
Initial release	2001	2008	2005	2018
Enterprise edition	EJBCA Enterprise	RedHat Certificate System	Not available	Smallstep Certificate Manager

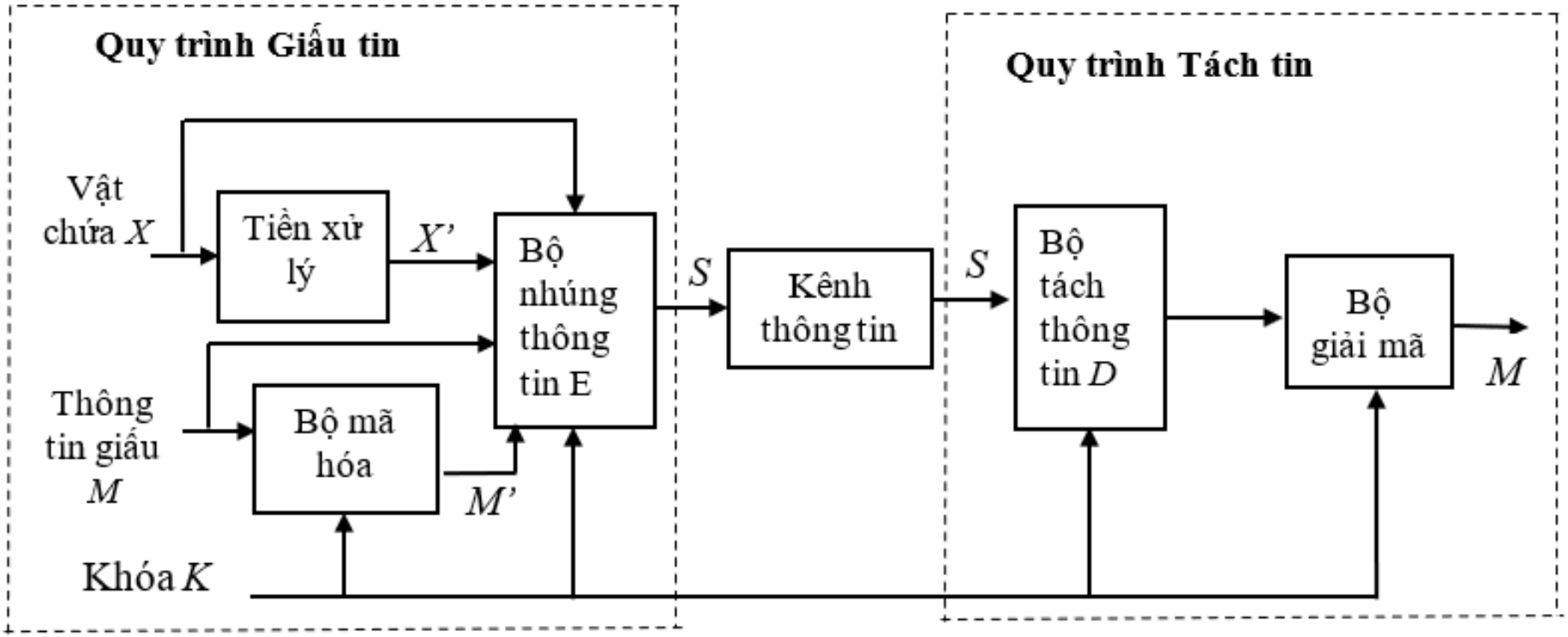
Giấu tin

- Giấu tin mật (Steganography) là kỹ thuật giấu một lượng thông tin nhất định vào 1 vật mang mà không làm thay đổi đáng kể về hình thức và nội dung của vật mang.
  - Giấu tin có thể được sử dụng để truyền thông tin nhạy cảm bằng cách nhúng chúng vào các vật mang, như ảnh, video...
  - Giấu tin cũng có thể được sử dụng kết hợp với mật mã để tăng cường độ an toàn bằng cách mã hóa thông tin mật trước khi nhúng vào vật mang.

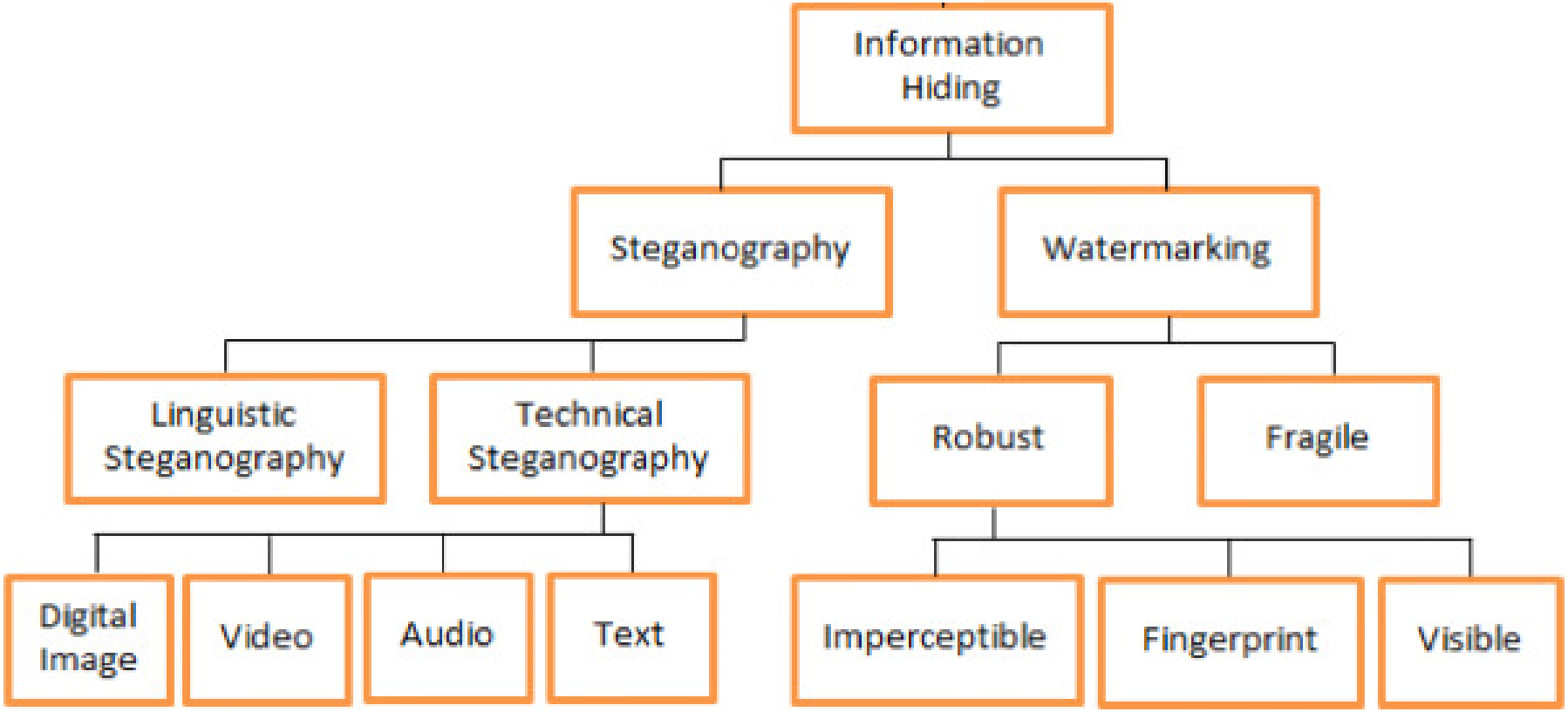
Giấu tin vs Mật mã

- Sự khác biệt của giấu tin và mật mã:
  - Giấu tin: bên thứ ba không biết sự tồn tại của thông tin mật nếu chỉ quan sát vật mang;
  - Mật mã: bên thứ ba biết sự tồn tại của thông tin mật trong bản mã.

Quy trình giấu và tách tin



Phân loại giấu tin



Phân loại giấu tin

- Hai loại giấu tin:
  - Giấu tin mật (steganography)
    - Giấu tin dựa trên ngôn ngữ (Linguistic)
    - Giấu tin dựa trên kỹ thuật (Technical)
      - Giấu trong ảnh số (digital image)
      - Giấu trong video
      - Giấu trong audio
      - Giấu trong văn bản (text)
  - Thủy vân số (watermarking)
    - Bền vững (Robust)
      - Ẩn (Imperceptible)
      - Dấu vân tay (Fingerprint)
      - Hiện (Visible)
    - Dễ vỡ (Fragile)

2.3 Các giao thức bảo mật thông tin

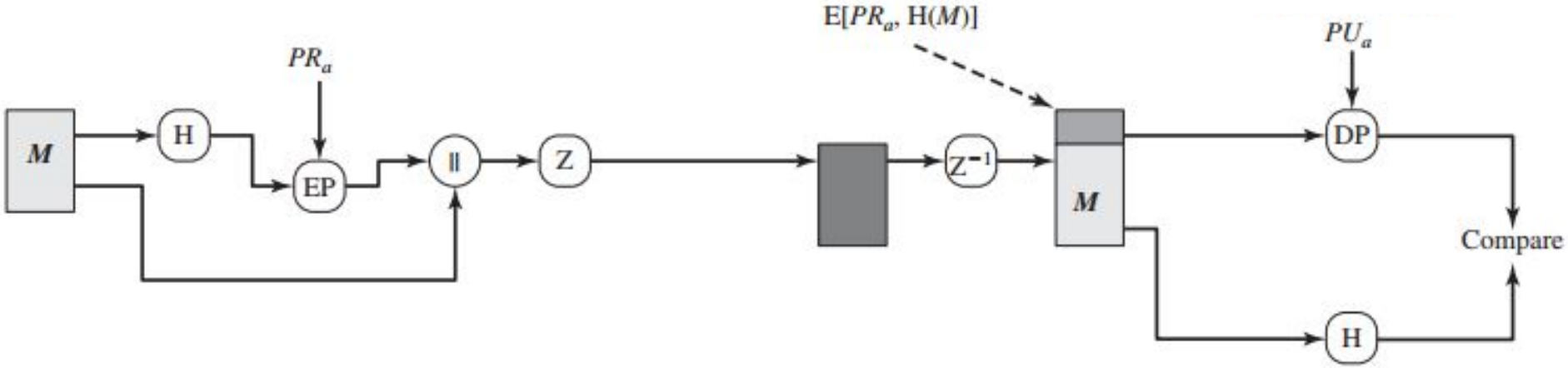
- PGP
- SSL/TLS
- IPSec
- HTTPS
- SSH
- S/MIME.

Giao thức PGP (Pretty Good Privacy)

- PGP do Philip Zimmermann phát triển năm 1991:
  - Cung cấp tính riêng tư (bí mật)
  - Cung cấp tính xác thực
- PGP được sử dụng rộng rãi và đã được thừa nhận thành chuẩn (RFC 3156).
- PGP cho phép:
  - Mã hoá dữ liệu sử dụng kết hợp mã hoá khoá bí mật và mã hóa khoá công khai
    - Mã hóa khoá công khai được sử dụng để trao đổi khóa bí mật
    - Mã hoá khoá bí mật dùng để mã hóa/giải mã thông điệp.
  - Tạo và kiểm tra chữ ký số.

Giao thức PGP

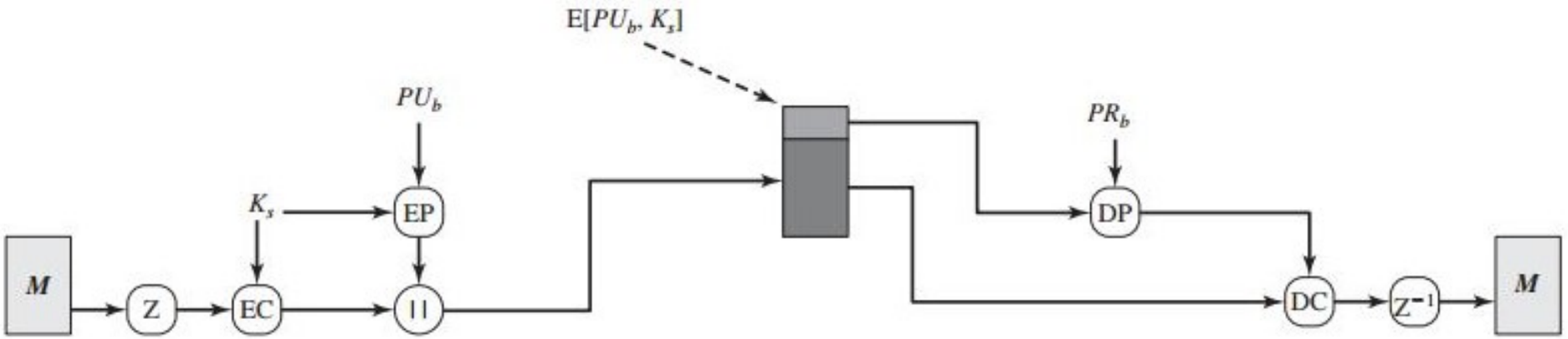
Bên gửi =====> Bên nhận



Mô hình PGP chỉ đảm bảo tính xác thực thông điệp sử dụng tạo và kiểm tra chữ ký số

Giao thức PGP

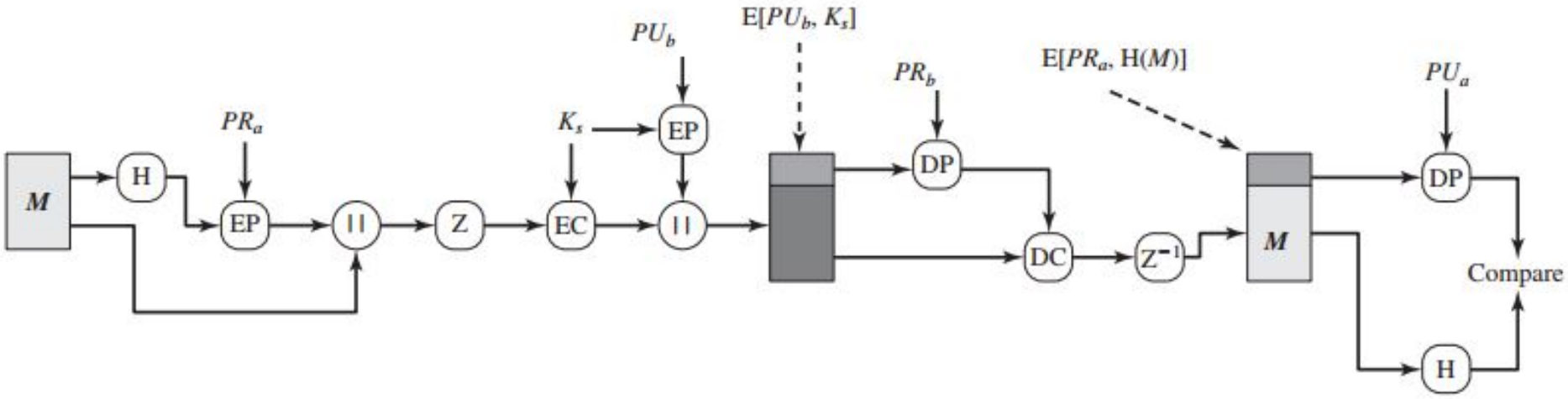
Bên gửi =====> Bên nhận



Mô hình PGP chỉ đảm bảo tính bí mật thông điệp sử dụng kết hợp mã hoá khoá bí mật và mã hóa khoá công khai

Giao thức PGP

Bên gửi =====> Bên nhận



Mô hình PGP đảm bảo tính bí mật và xác thực/toàn vẹn thông điệp sử dụng mã hóa và ký số

Giao thức bảo mật SSL/TLS

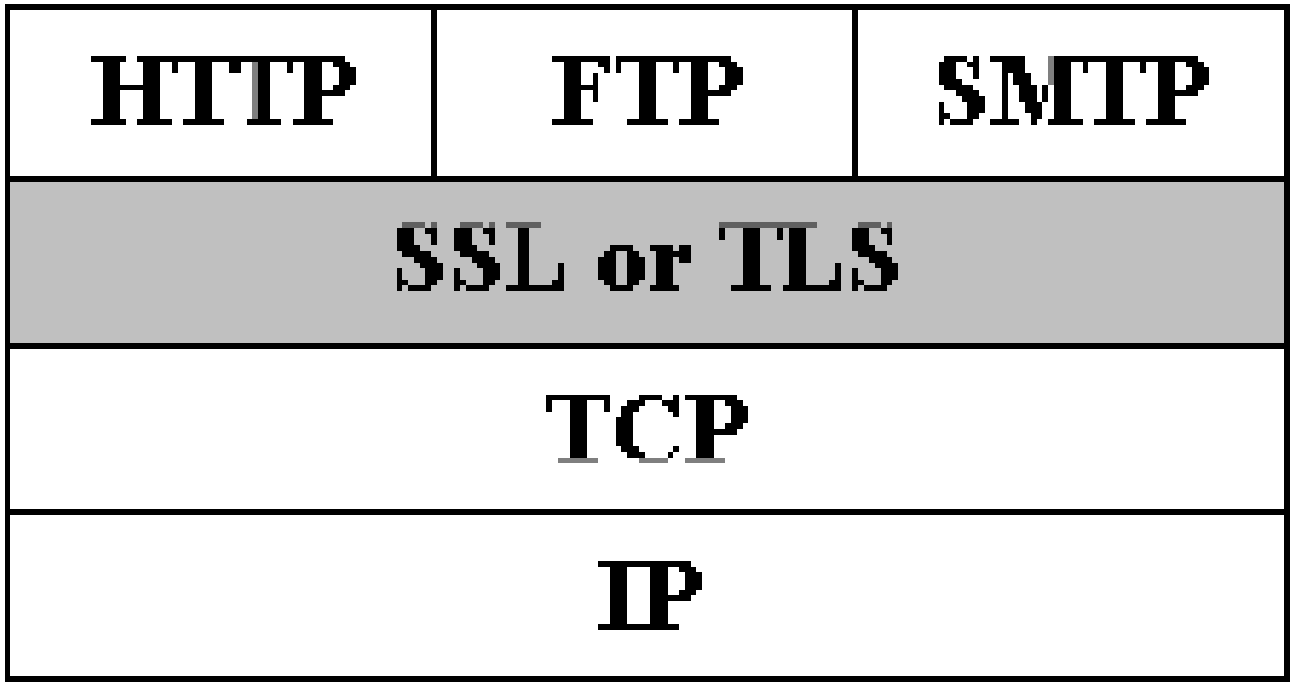
- SSL do công ty Netscape phát minh năm 1993;
  - Các phiên bản 1.0 (1993), 2.0 (1995) và 3.0 (1996);
  - SSL hiện ít được sử dụng do có nhiều lỗi và không được cập nhật.
- TLS được xây dựng vào năm 1999 dựa trên SSL 3.0 và do IETF phê chuẩn.
  - Các phiên bản của TLS: 1.0 (1999), 1.1 (2005), 1.2 (2008), 1.3 (2015).

Giao thức bảo mật SSL/TLS

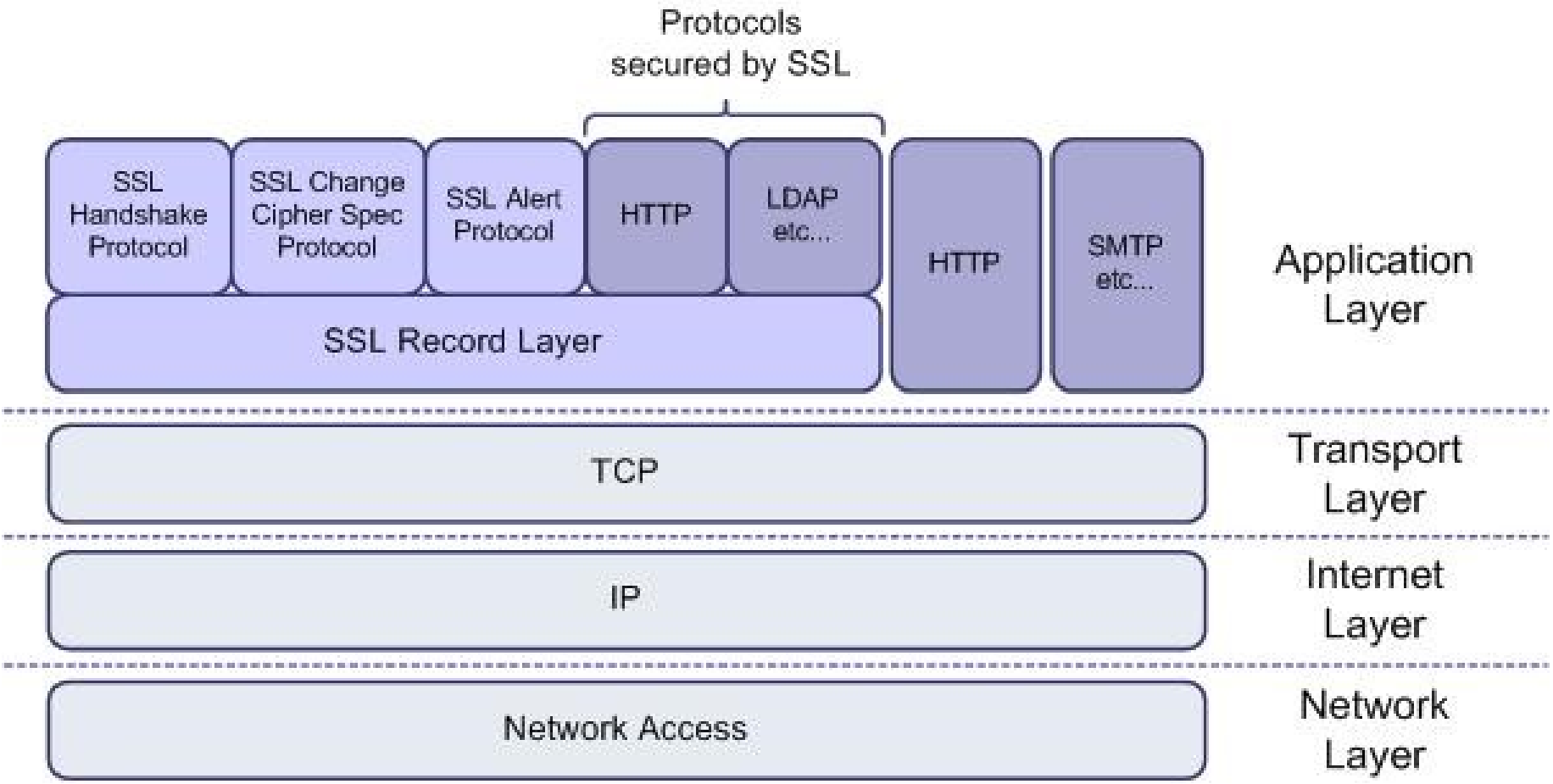
❖ Đặc điểm của SSL/TLS:

- Sử dụng mã hoá khoá công khai để trao đổi khoá phiên. Mỗi khoá phiên chỉ được sử dụng trong 1 phiên làm việc.
- Sử dụng khoá phiên và mã hoá khoá bí mật để mã hoá toàn bộ dữ liệu trao đổi.
- Sử dụng hàm băm có khóa (MAC) để đảm bảo tính toàn vẹn và xác thực thông điệp.
- Ít nhất một thực thể (thường là server) phải có chứng chỉ số cho khoá công khai (Public key certificate).

Giao thức bảo mật SSL/TLS



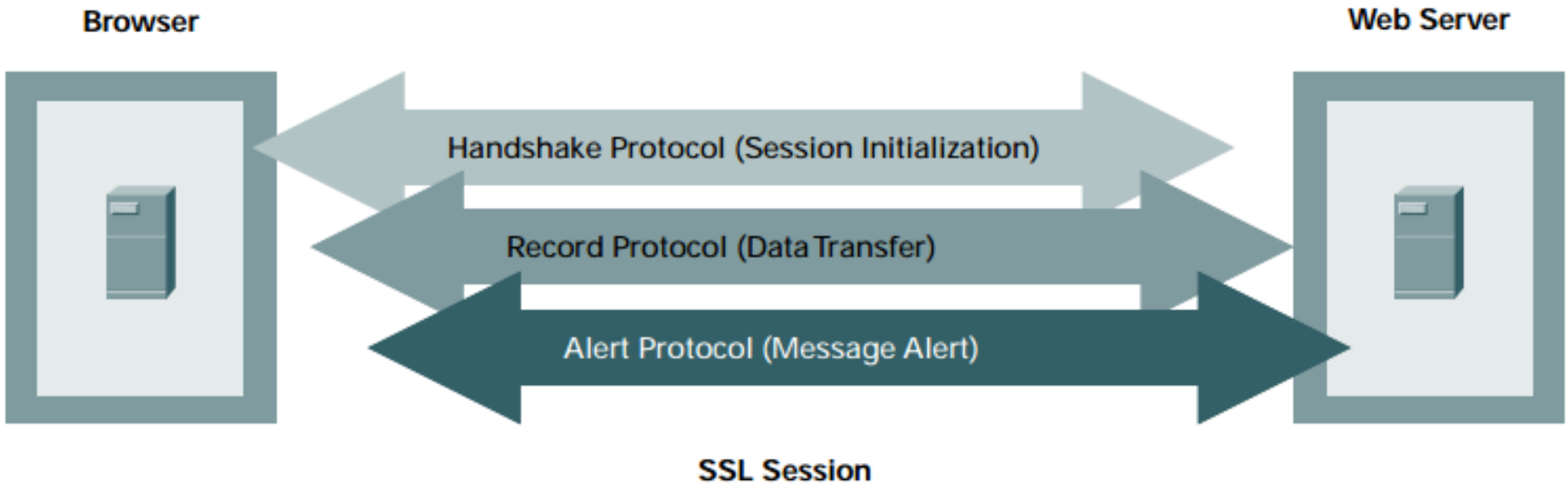
Giao thức bảo mật SSL/TLS



Giao thức bảo mật SSL/TLS

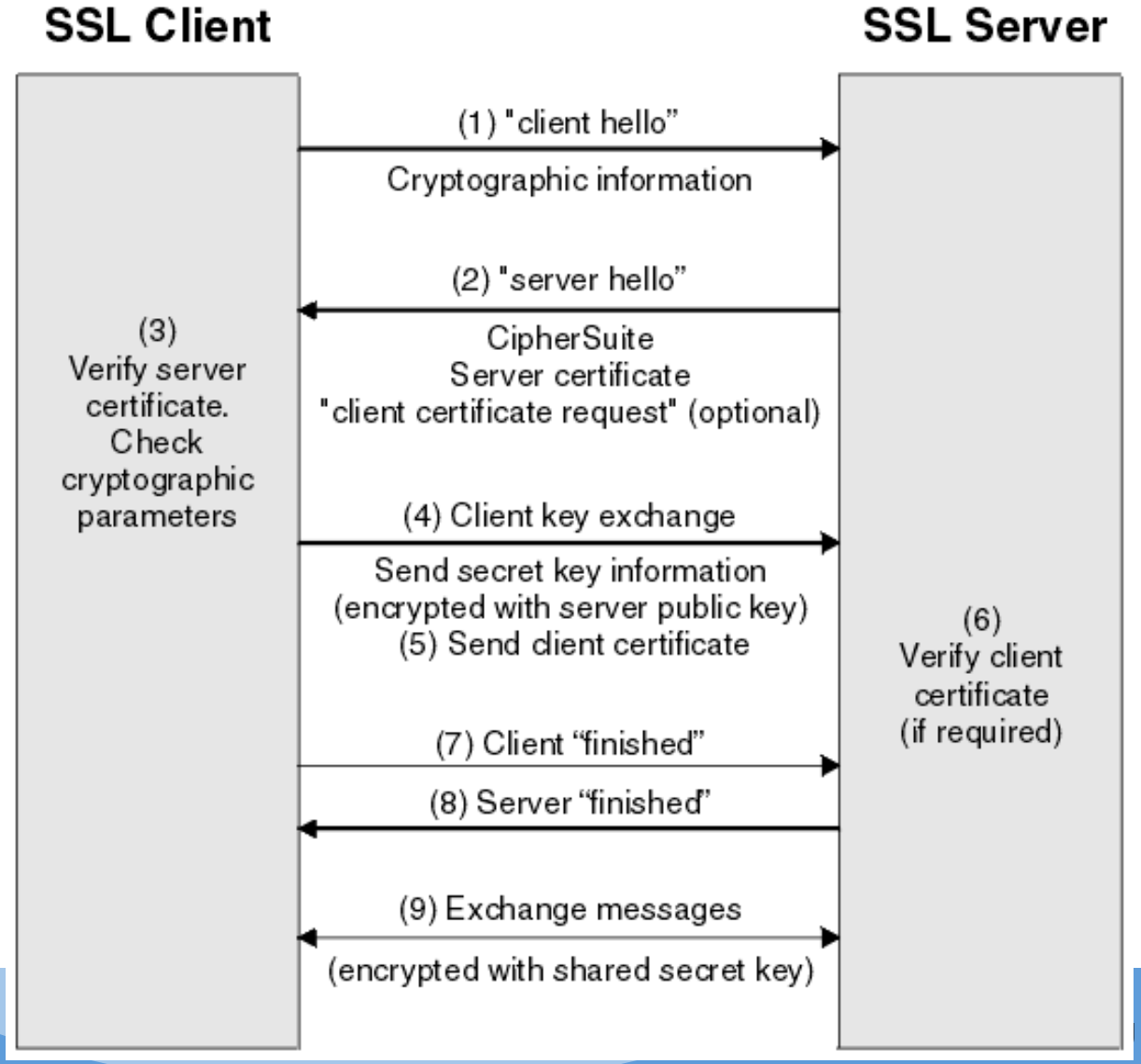
- Các giao thức con của SSL:
  - SSL Handshake Protocol: Giao thức bắt tay của SSL, có nhiệm vụ trao đổi các thông điệp xác thực thực thể và thiết lập các thông số cho phiên làm việc;
  - SSL Change Cipher Spec Protocol: Giao thức thiết lập việc sử dụng các bộ mã hóa được hỗ trợ bởi cả 2 bên tham gia truyền thông;
  - SSL Alert Protocol: Giao thức cảnh bảo của SSL
  - SSL Record Protocol: Giao thức bản ghi của SSL có nhiệm vụ tạo đường hầm an toàn để chuyển thông tin đảm bảo tín bí mật, toàn vẹn và xác thực.

Giao thức bảo mật SSL/TLS



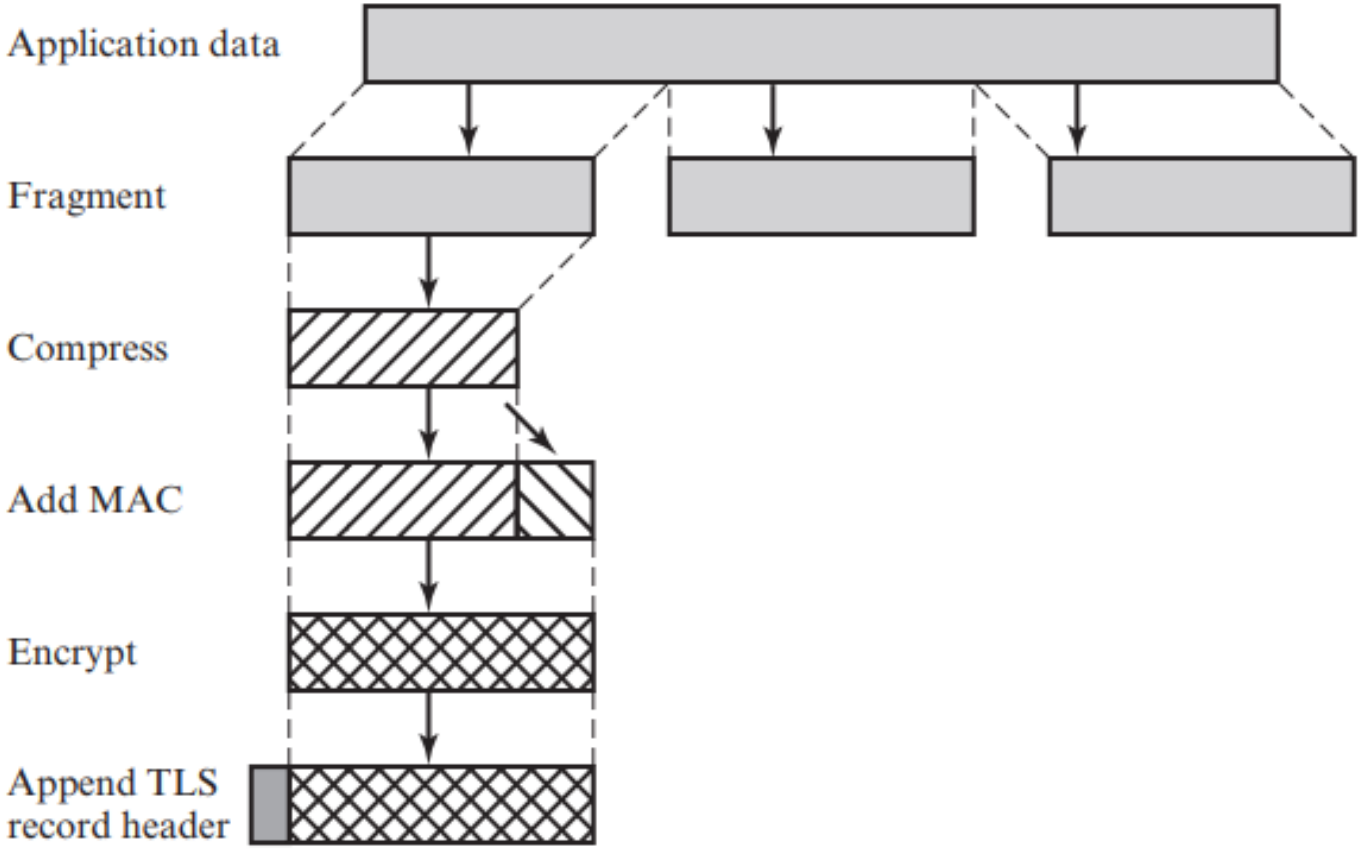
Giao thức bảo mật SSL/TLS

- SSL Handshake Protocol:



Giao thức bảo mật SSL/TLS

- SSL Record Protocol:



Giao thức bảo mật SSL/TLS

❖ Tính toán giá trị MAC/HMAC:

$$\text{HMAC}_K(M) = \text{H}[(K^+ \oplus \text{opad}) \| \text{H}[(K^+ \oplus \text{ipad}) \| M]]$$

where

H = embedded hash function (for TLS, either MD5 or SHA-1)

M = message input to HMAC

K^+ = secret key padded with zeros on the left so that the result is equal to the block length of the hash code (for MD5 and SHA-1, block length = 512 bits)

ipad = 00110110 (36 in hexadecimal) repeated 64 times (512 bits)

opad = 01011100 (5C in hexadecimal) repeated 64 times (512 bits)

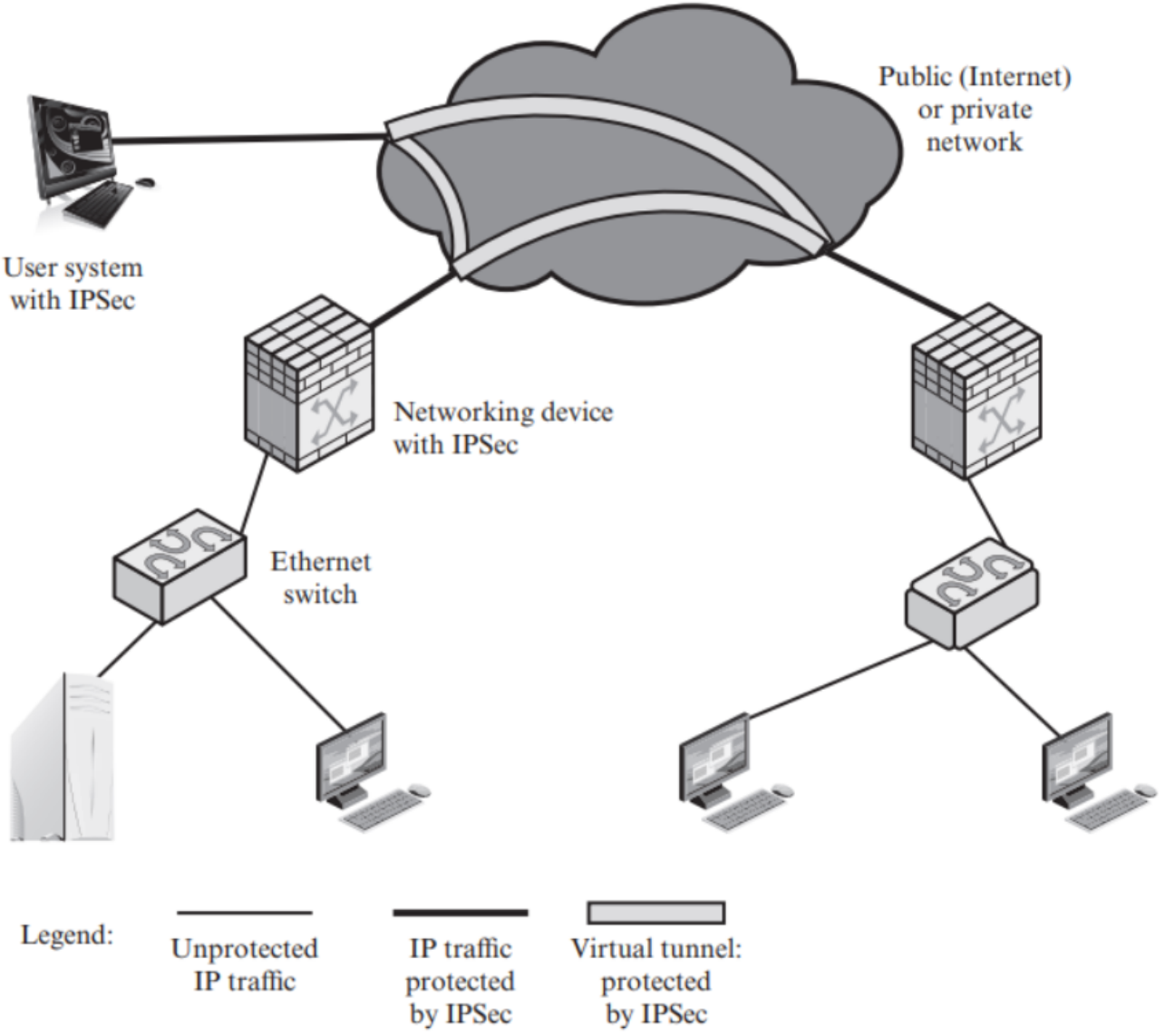
IPSec - IP Security

- Giới thiệu IPSec
- Kiến trúc và các thành phần của IPSec
- Các chế độ hoạt động của IPSec.

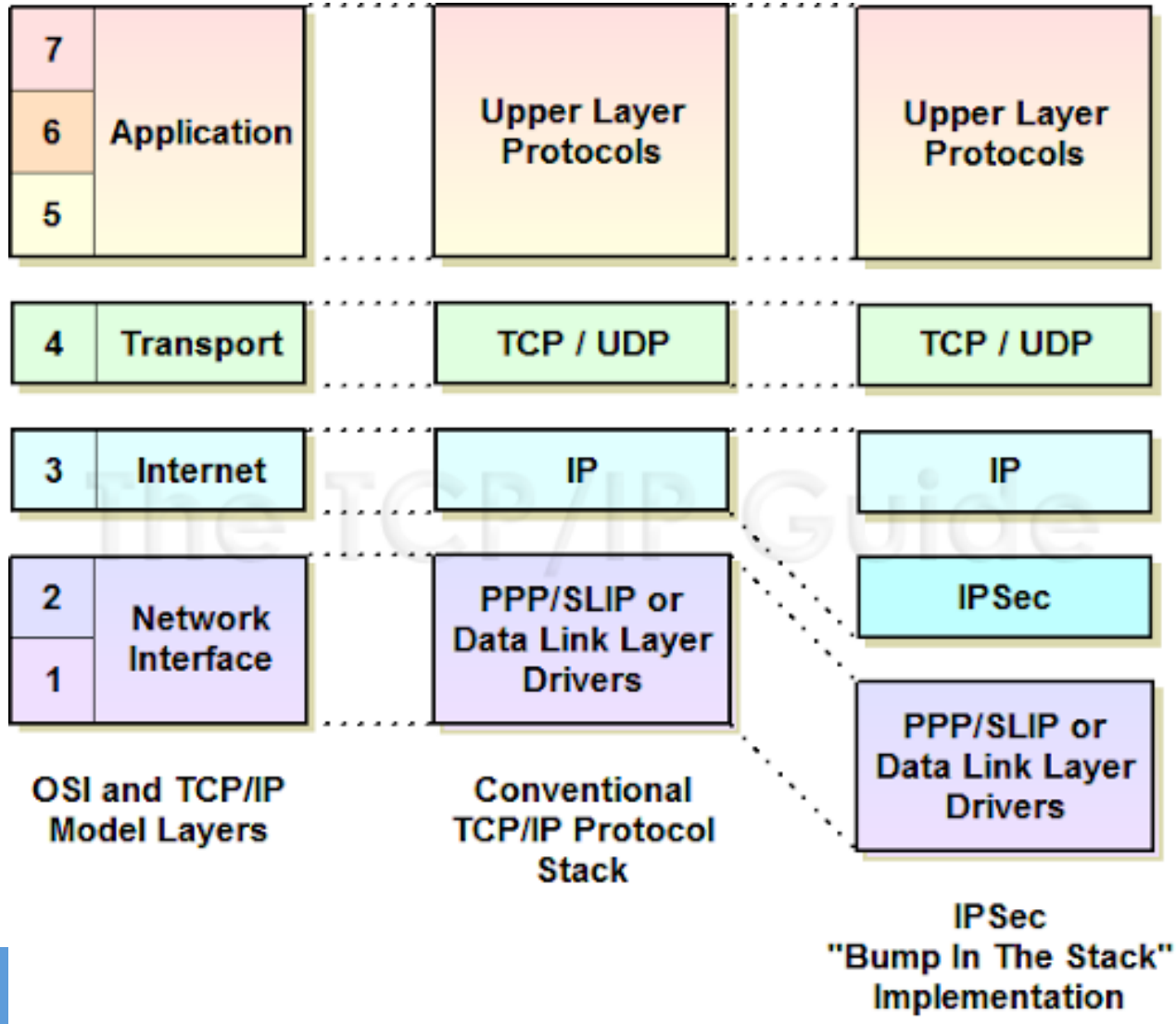
Giới thiệu IPSec

- IPSec (Internet Protocol Security) là một bộ chuẩn gồm các giao thức do IETF phê duyệt nhằm cung cấp tính bí mật, toàn vẹn và xác thực thông tin giao tiếp giữa 2 điểm trên mạng IP.
  - IPSec được sử dụng để bảo mật dữ liệu truyền tại lớp 3 (Network) trong mô hình OSI, hoặc lớp IP trong mô hình TCP/IP.
  - IPSec được sử dụng rộng rãi trong các mạng riêng ảo (VPN).
- IPSec cũng bao gồm các giao thức cho trao đổi và quản lý khóa an toàn.

IPSec VPN


Public (Internet)
or private
network
User system
with IPSec
Networking device
with IPSec
Ethernet
switch
Legend:
Unprotected
IP traffic
IP traffic
protected
by IPSec
Virtual tunnel:
protected
by IPSec

IPSec trong quan hệ với mô hình OSI và TCP/IP



Đặc điểm của IPSec

- IPSec có các đặc điểm sau:
  - Xác thực: IPSec cung cấp xác thực các gói IP bằng chữ ký số hoặc bí mật chung. Điều này giúp đảm bảo rằng các gói không bị giả mạo.
  - Bí mật: IPSec cung cấp tính bí mật bằng cách mã hóa các gói IP, ngăn chặn việc nghe lén lưu lượng mạng.
  - Toàn vẹn: IPSec cung cấp tính toàn vẹn bằng cách đảm bảo rằng các gói IP không bị sửa đổi hoặc bị hỏng trong quá trình truyền.

Đặc điểm của IPSec

- IPSec có các đặc điểm sau:
  - Quản lý khóa: IPSec cung cấp các dịch vụ quản lý khóa, bao gồm trao đổi khóa và thu hồi khóa, đảm bảo rằng các khóa mật mã được quản lý an toàn.
  - Đường hầm: IPSec hỗ trợ tạo đường hầm, cho phép các gói IP được đóng gói trong một giao thức khác, chẳng hạn như GRE hoặc L2TP.
  - Linh hoạt: IPSec có thể được cấu hình để cung cấp bảo mật cho nhiều cấu trúc liên kết mạng, bao gồm kết nối điểm-điểm, site-to-site và truy cập từ xa.
  - Khả năng tương tác: IPSec là một bộ chuẩn mở, có nghĩa là nó được hỗ trợ bởi nhiều nhà cung cấp và có thể được sử dụng trong các môi trường không đồng nhất.

Ưu điểm và Nhược điểm của IPSec

❖ Ưu điểm của IPSec:

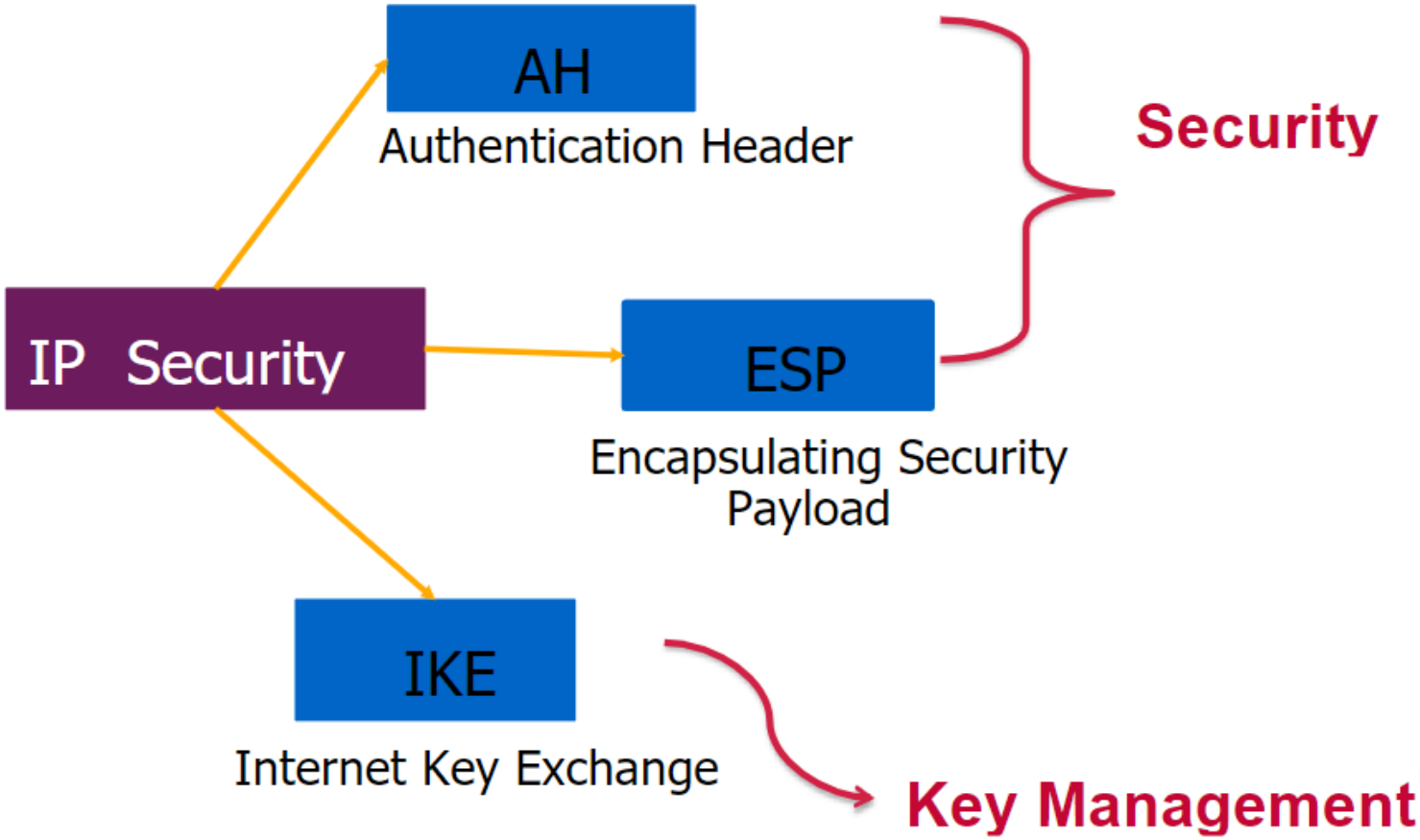
- Bảo mật mạnh mẽ: IPSec cung cấp các dịch vụ bảo mật mật mã mạnh mẽ giúp bảo vệ dữ liệu nhạy cảm và đảm bảo quyền riêng tư và tính toàn vẹn của dữ liệu truyền.
- Khả năng tương thích rộng: IPSec là bộ chuẩn mở được các nhà cung cấp hỗ trợ rộng rãi và có thể được sử dụng trong các môi trường không đồng nhất.
- Tính linh hoạt: IPSec có thể được cấu hình để cung cấp bảo mật cho nhiều cấu trúc liên kết mạng, bao gồm các kết nối điểm-điểm, site-to-site và truy cập từ xa.
- Khả năng mở rộng: IPSec có thể được sử dụng để bảo mật các mạng quy mô lớn và có thể tăng hoặc giảm quy mô khi cần.
- Cải thiện hiệu suất mạng: IPSec có thể giúp cải thiện hiệu suất mạng bằng cách giảm tắc nghẽn mạng và cải thiện hiệu quả mạng.

Ưu điểm và Nhược điểm của IPSec

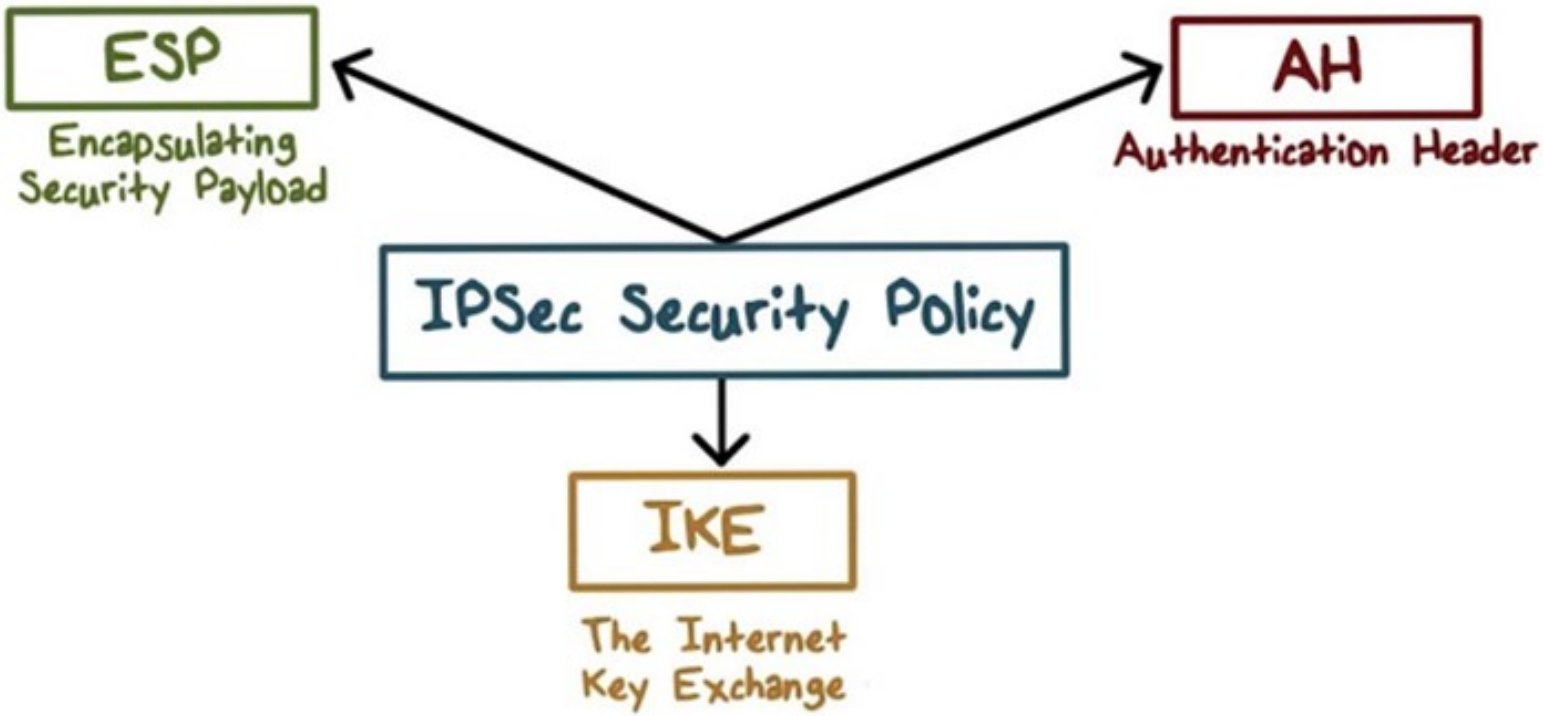
❖ Nhược điểm của IPSec:

- Độ phức tạp của cấu hình: IPSec có thể phức tạp trong việc cấu hình và đòi hỏi kiến thức và kỹ năng chuyên môn.
- Sự cố tương thích: IPSec có thể gặp sự cố tương thích với một số thiết bị và ứng dụng mạng. Điều này có thể dẫn đến sự cố về khả năng tương tác.
- Tác động đến hiệu suất: IPSec có thể ảnh hưởng đến hiệu suất mạng do chi phí mã hóa và giải mã các gói IP.
- Quản lý khóa: IPSec yêu cầu quản lý khóa hiệu quả để đảm bảo tính bảo mật của khóa mật mã được sử dụng để mã hóa và xác thực.
- Hạn chế miền bảo vệ: IPSec chỉ cung cấp khả năng bảo vệ cho lưu lượng IP. Các giao thức khác như ICMP, DNS và giao thức định tuyến vẫn có thể bị tấn công.

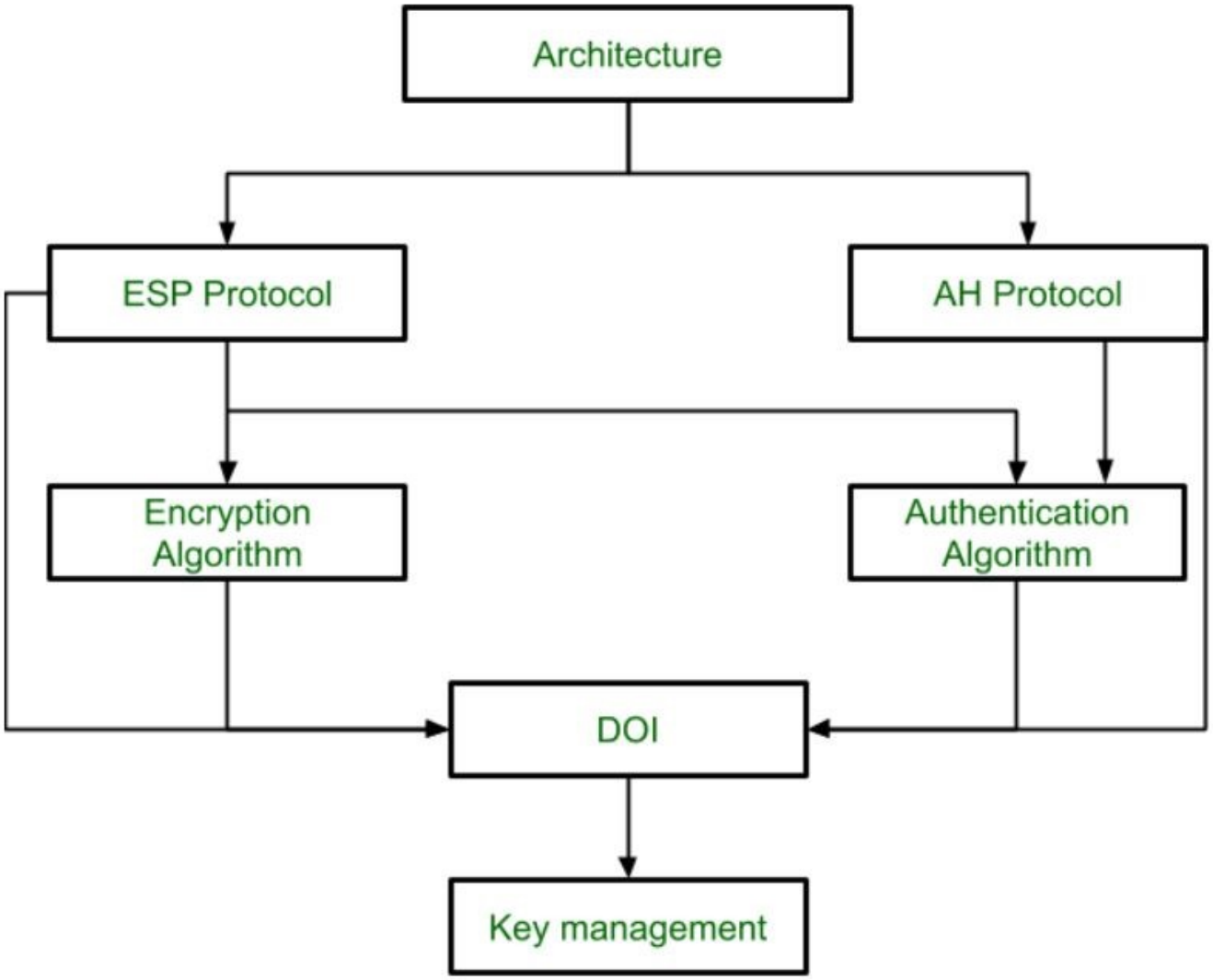
Kiến trúc của IPSec - Kiến trúc rút gọn



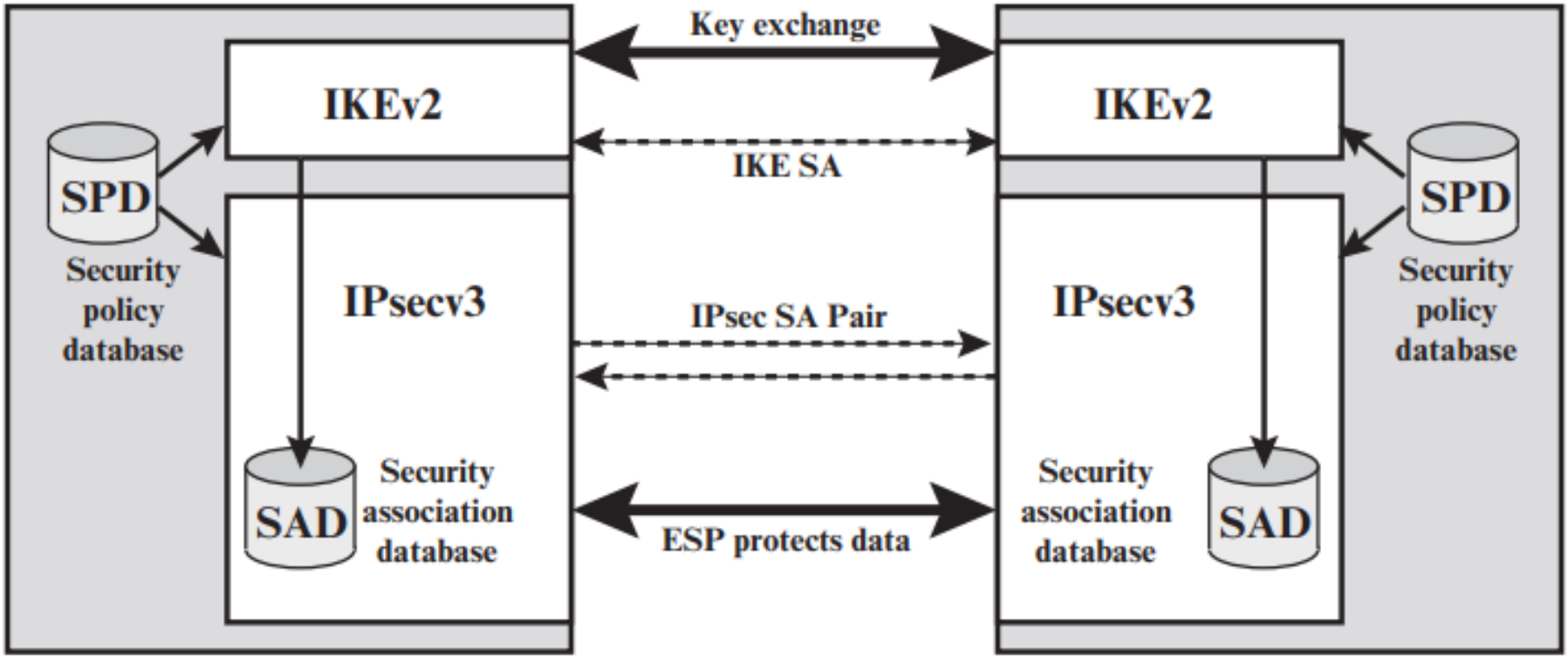
Kiến trúc của IPSec - Kiến trúc rút gọn



Kiến trúc của IPSec - Kiến trúc khối



Kiến trúc của IPSec - Kiến trúc tương tác



Các thành phần của IPSec

- IP security policy
- Giao thức trao đổi khóa IKE
- Giao thức bảo mật AH
- Giao thức bảo mật ESP
- Các chế độ hoạt động của IPSec
- Các thuật toán mật mã.

IP security policy

- Chính sách bảo mật IP (IP security policy) là nền tảng của việc vận hành IPSec, áp dụng cho từng gói tin chuyển từ điểm nguồn đến điểm đích;
- IP security policy gồm các thành phần:
  - Security Association (SA)
  - Security Association Database (SAD)
  - Security Policy Database (SPD)

Security Association (SA)

- Security Association (SA) - *Liên kết bảo mật* là một kết nối logic 1 chiều giữa người gửi và người nhận nhằm cung cấp các dịch vụ bảo mật cho lưu lượng truy cập được thực hiện trên đó;
  - Nếu cần có một mối quan hệ ngang hàng để trao đổi an toàn hai chiều thì cần có hai liên kết bảo mật.
- Security Association là một trong các khái niệm quan trọng trong đảm bảo tính bí mật và xác thực của IPSec.

Security Association (SA)

- Security Association (SA) được nhận dạng bởi 3 tham số:
  - Security Parameters Index (SPI): Chỉ mục tham số bảo mật là số nguyên không dấu 32 bit được gán cho SA này và chỉ có ý nghĩa cục bộ. SPI được mang trong các tiêu đề AH và ESP để cho phép hệ thống nhận chọn SA mà theo đó gói nhận được sẽ được xử lý;
  - IP Destination Address: Địa chỉ đích IP: Đây là địa chỉ của điểm cuối đích của SA, có thể là hệ thống người dùng cuối hoặc hệ thống mạng như tường lửa hoặc bộ định tuyến;
  - Security Protocol Identifier: Mã định danh giao thức bảo mật là trường này trong tiêu đề IP bên ngoài cho biết liên kết đó là liên kết bảo mật AH hay ESP.

Security Association Database (SAD)

- Security Association Database - CSDL liên kết bảo mật định nghĩa các tham số liên quan đến mỗi SA. Mỗi SA được định nghĩa bằng các tham số trong 1 bản ghi của SAD:
  - Security Parameter Index
  - Sequence Number Counter: Bộ đếm số trình tự
  - Sequence Counter Overflow: cờ báo nếu Bộ đếm số trình tự bị tràn
  - Anti-Replay Window: tham số cửa sổ để chống phát lại.

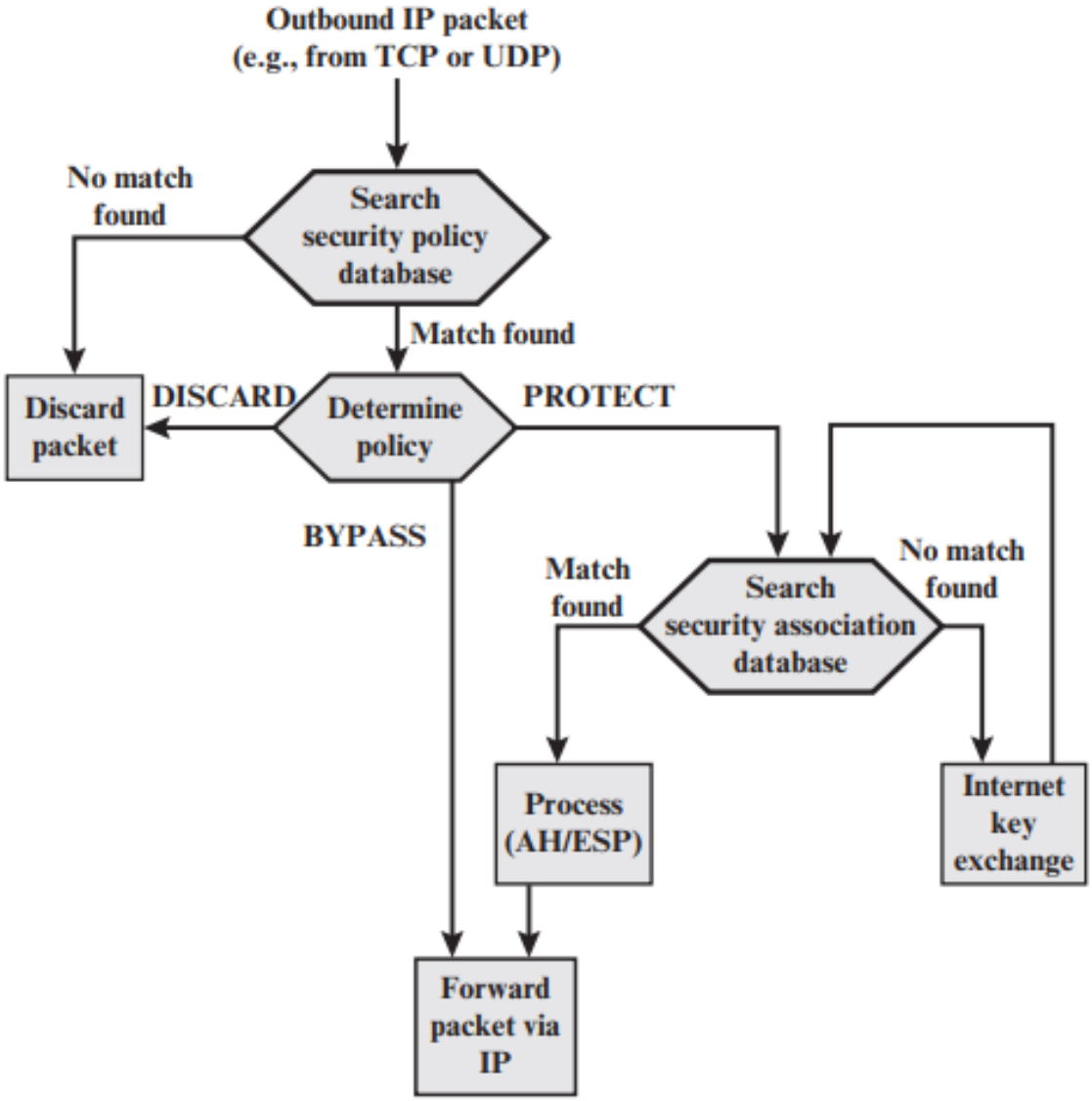
Security Association Database (SAD)

- Mỗi SA được định nghĩa bằng các tham số trong 1 bản ghi của SAD:
  - AH Information: thuật toán xác thực, các khóa, thời gian sống của khóa và các tham số khác của AH.
  - ESP Information: thuật toán xác thực và mã hóa, các khóa, các giá trị khởi tạo, thời gian sống của khóa và các tham số khác của ESP.
  - Lifetime of this Security Association: thời gian sống của SA
  - IPsec Protocol Mode: chế độ hoạt động (đường hầm hoặc vận chuyển)
  - Path MTU (maximum transmission unit).

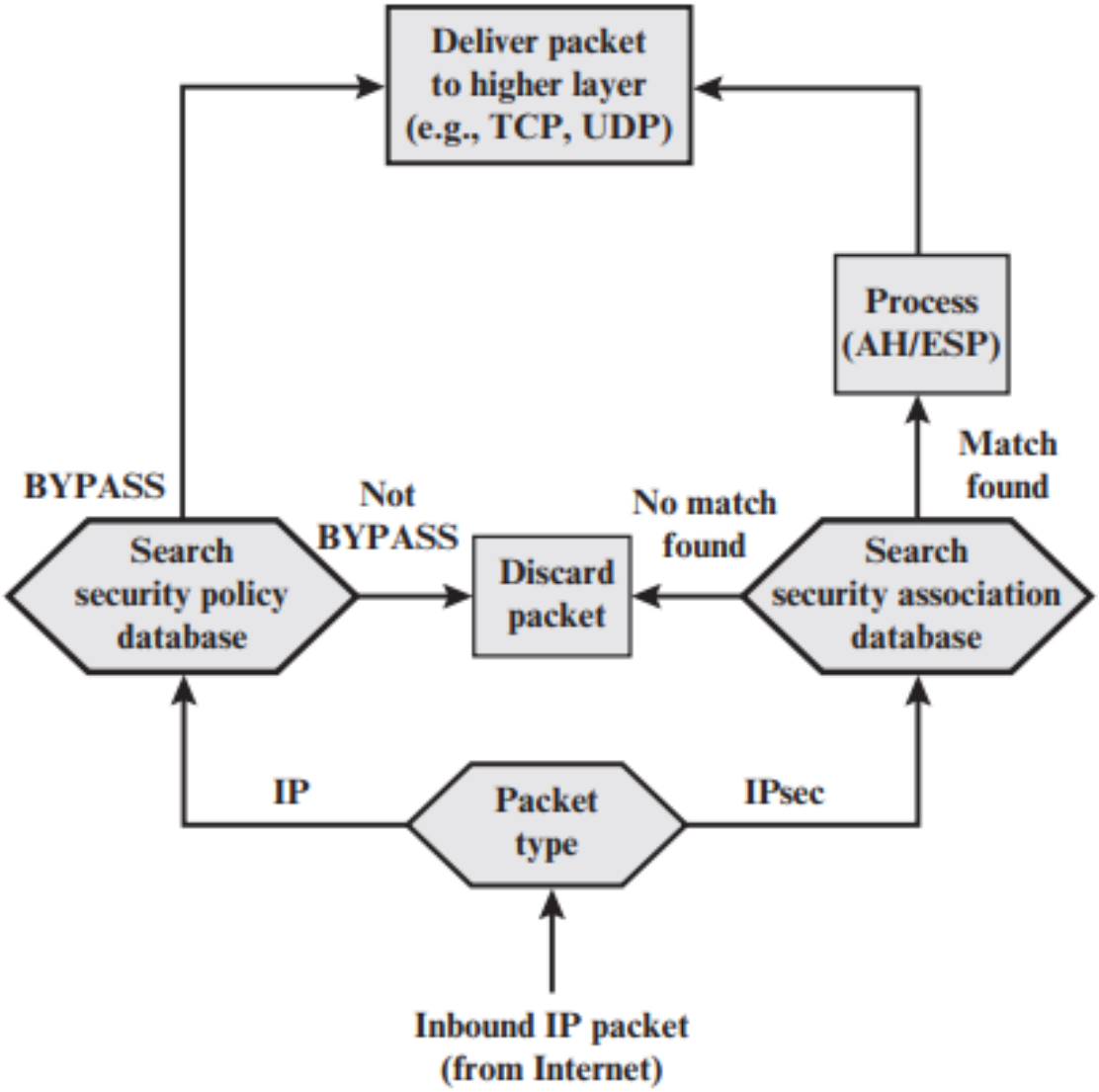
Security Policy Database (SPD)

- Security Policy Database - CSDL chính sách bảo mật là phương tiện hỗ trợ để xác định SA phù hợp cho lưu lượng IP cụ thể.
  - Ở dạng đơn giản nhất, SPD chứa các mục, mỗi mục xác định một tập hợp con lưu lượng IP và trỏ đến SA cho lưu lượng đó.
  - Trong các môi trường phức tạp hơn, có thể có nhiều mục có khả năng liên quan đến một SA hoặc nhiều SA được liên kết với một mục SPD.

Mô hình xử lý gói outbound trong IPSec



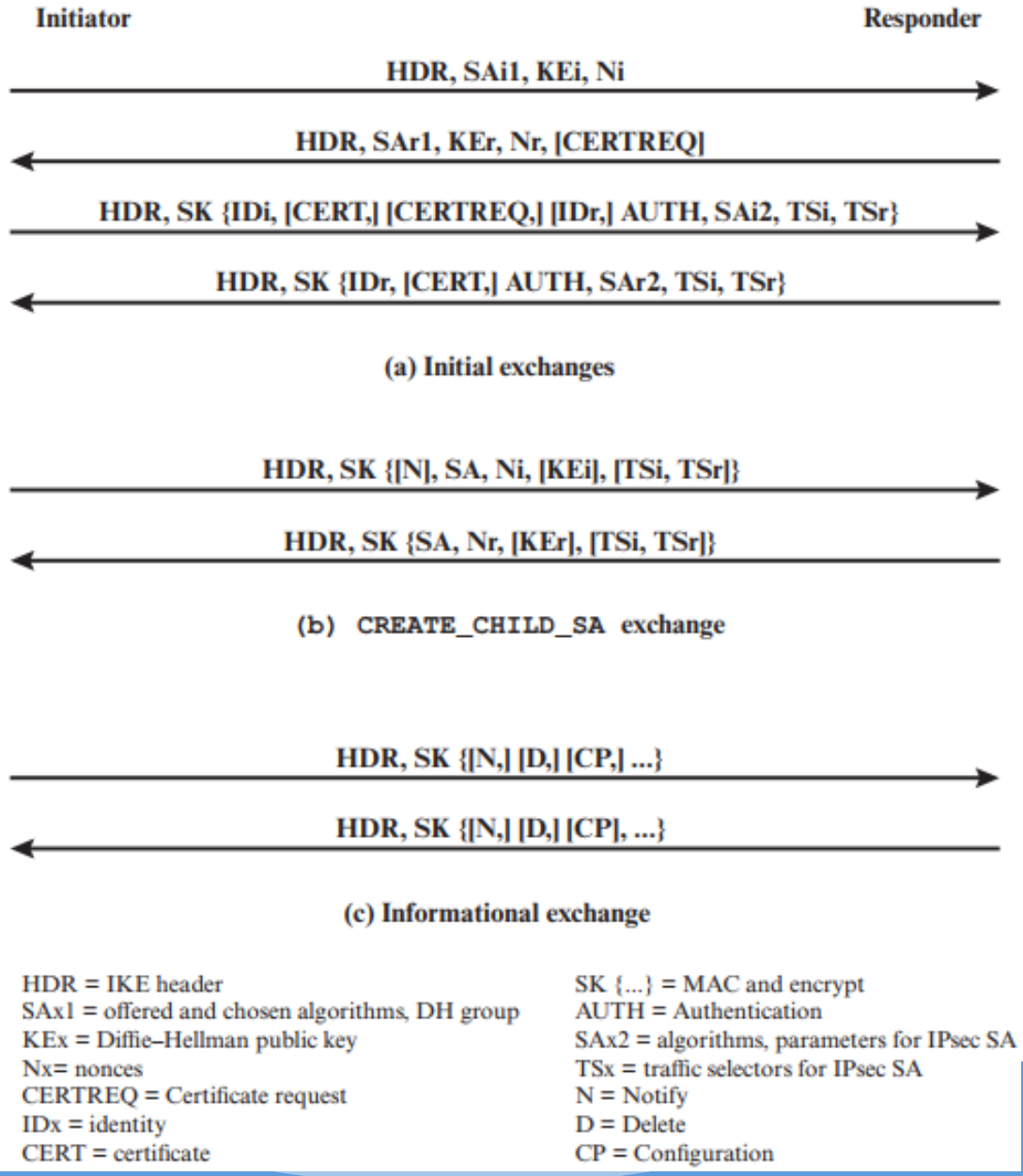
Mô hình xử lý gói inbound trong IPSec



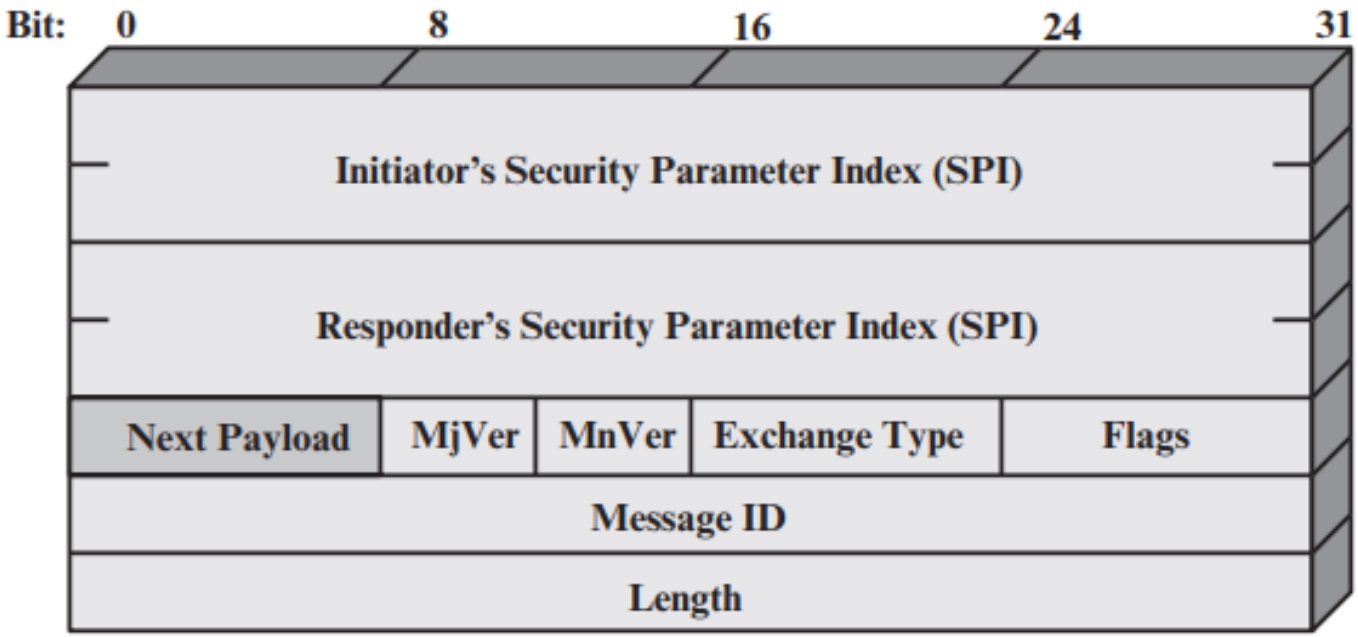
Giao thức trao đổi khóa IKE

- IKE (Internet Key Exchange) - Giao thức trao đổi khóa Internet được sử dụng để sinh, trao đổi và duy trì khóa trong IPSec;
- IKE sử dụng 1 biến thể của thuật toán trao đổi khóa Diffie-Hellman;
- IKE có 2 phiên bản:
  - IKEv1
  - IKEv2.

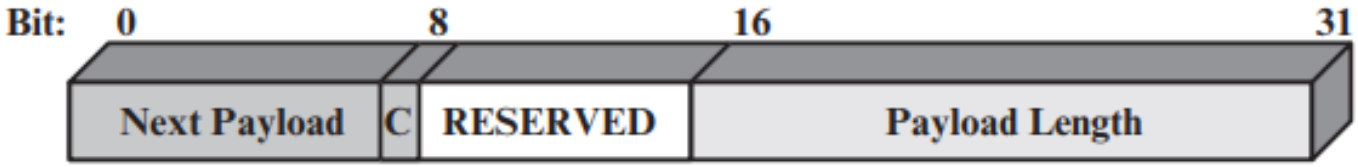
Trao đổi các thông điệp trong IKEv2



Định dạng gói tin IKE



(a) IKE header



(b) Generic Payload header

Định dạng gói tin IKE

- Initiator SPI (64 bits): SPI của bên khởi tạo
- Responder SPI (64 bits): SPI của bên tiếp nhận
- Next Payload (8 bits): Cho biết loại tải trọng đầu tiên trong thông điệp
- Major Version (4 bits): Phiên bản chính của IKE hiện sử dụng
- Minor Version (4 bits): Phiên bản phụ của IKE hiện sử dụng
- Exchange Type (8 bits): Cho biết loại trao đổi thông tin

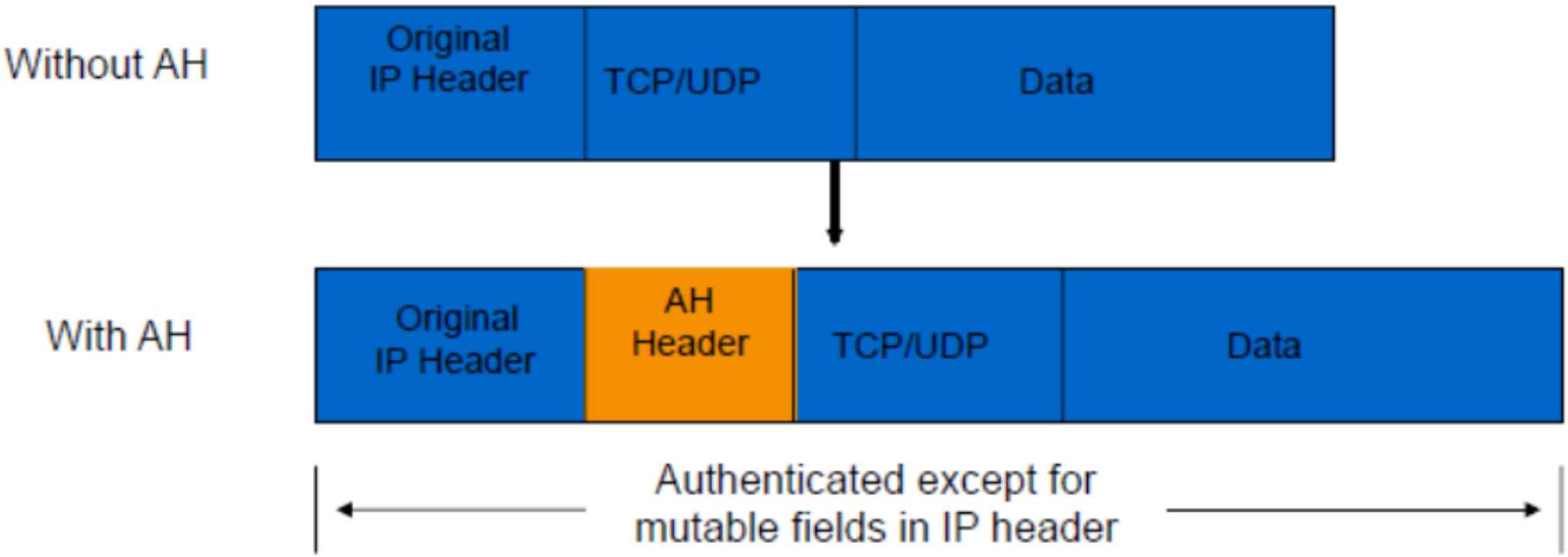
Định dạng gói tin IKE

- Flags (8 bits): Các cờ cho biết các tùy chọn cụ thể được đặt cho trao đổi IKE. Ba bit cờ được xác định cho đến phiên bản IKE hiện tại.
  - Bit khởi tạo cho biết gói này có được gửi bởi bộ khởi tạo SA hay không.
  - Bit phiên bản cho biết liệu bộ phát có khả năng sử dụng số phiên bản chính cao hơn số phiên bản hiện được chỉ định hay không.
  - Bit phản hồi cho biết đây có phải là phản hồi cho tin nhắn có cùng ID tin nhắn hay không.
- Message ID (32 bits): Được sử dụng để kiểm soát việc truyền lại các gói bị mất và khớp các yêu cầu và phản hồi.
- Length (32 bits): Độ dài của tổng số tin nhắn (tiêu đề cộng với tất cả tải trọng) tính bằng octet.

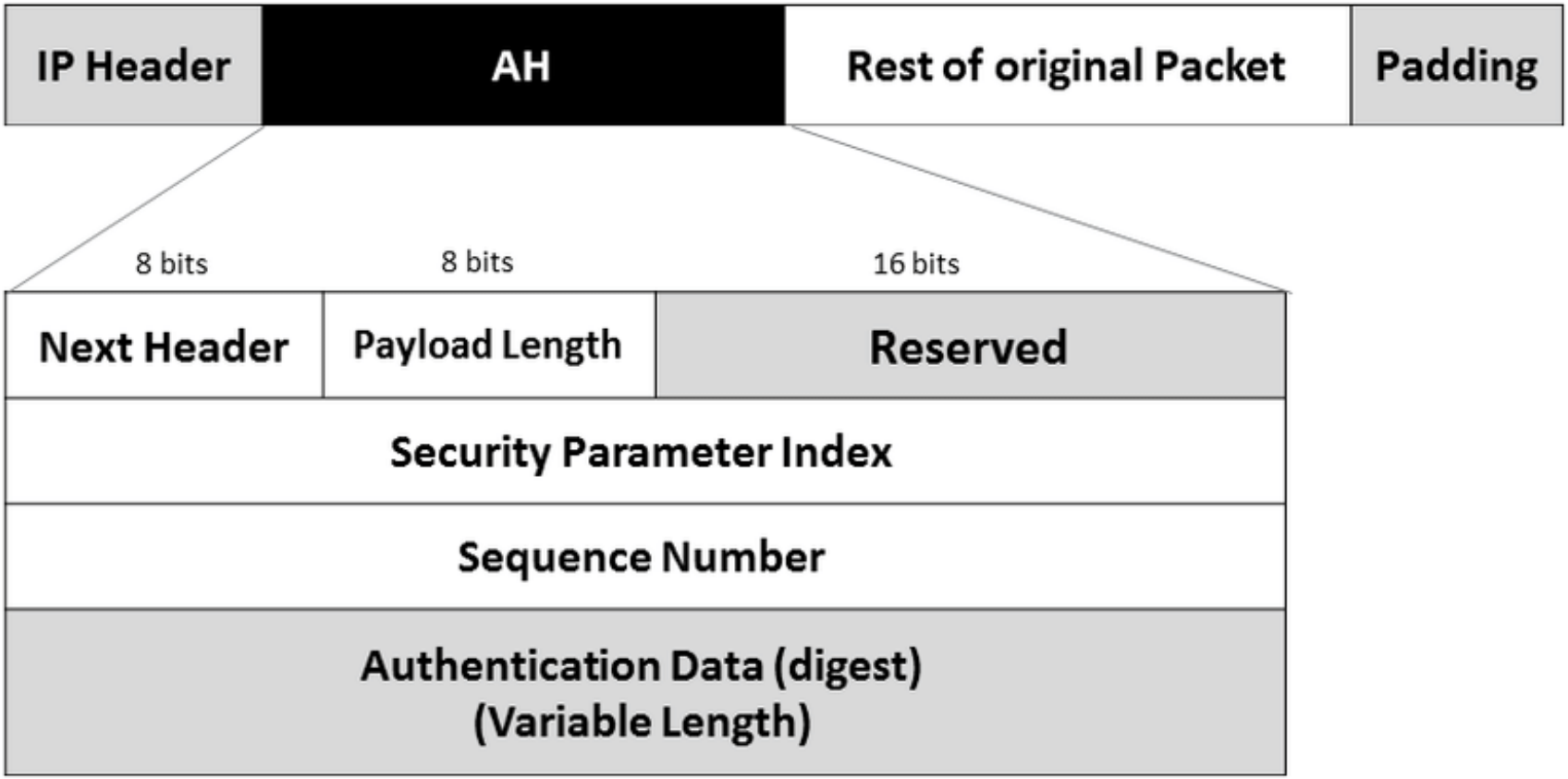
Giao thức bảo mật AH

- Giao thức AH chỉ cung cấp cơ chế xác thực:
  - AH cung cấp tính toàn vẹn dữ liệu, xác thực nguồn gốc dữ liệu và dịch vụ bảo vệ chống phát lại (tùy chọn);
  - Tính toàn vẹn dữ liệu được đảm bảo bằng cách sử dụng chuỗi đại diện thông điệp được tạo bằng các thuật toán băm như HMAC-MD5 hoặc HMAC-SHA;
  - Xác thực nguồn gốc dữ liệu được đảm bảo bằng cách sử dụng khóa bí mật chung để tạo chuỗi đại diện thông điệp.
  - Bảo vệ chống phát lại được cung cấp bằng cách sử dụng trường số thứ tự với tiêu đề AH.

Giao thức bảo mật AH - Cấu trúc gói



Giao thức bảo mật AH - Cấu trúc gói



Giao thức bảo mật AH - HMAC

$$\mathrm{HMAC}(K, m) = \mathrm{H}\left((K' \oplus opad) \parallel \mathrm{H}\left((K' \oplus ipad) \parallel m \right) \right)$$

$$K' = \begin{cases} \mathrm{H}(K) & \text{if } K \text{ is larger than block size} \\ K & \text{otherwise} \end{cases}$$

where

H is a cryptographic hash function.

m is the message to be authenticated.

K is the secret key.

K' is a block-sized key derived from the secret key, K; either by padding to the right with 0s up to the block size, or by hashing down to less than or equal to the block size first and then padding to the right with zeros.

$\parallel$ denotes concatenation.

$\oplus$ denotes bitwise exclusive or (XOR).

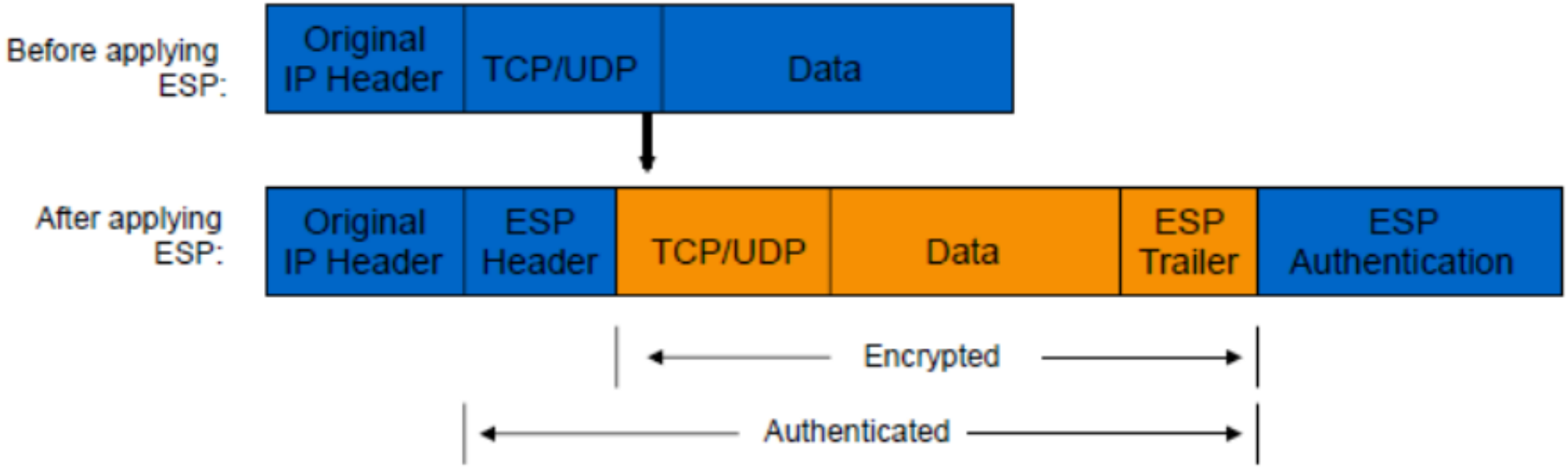
$opad$ is the block-sized outer padding, consisting of repeated bytes valued 0x5c.

$ipad$ is the block-sized inner padding, consisting of repeated bytes valued 0x36.[3]

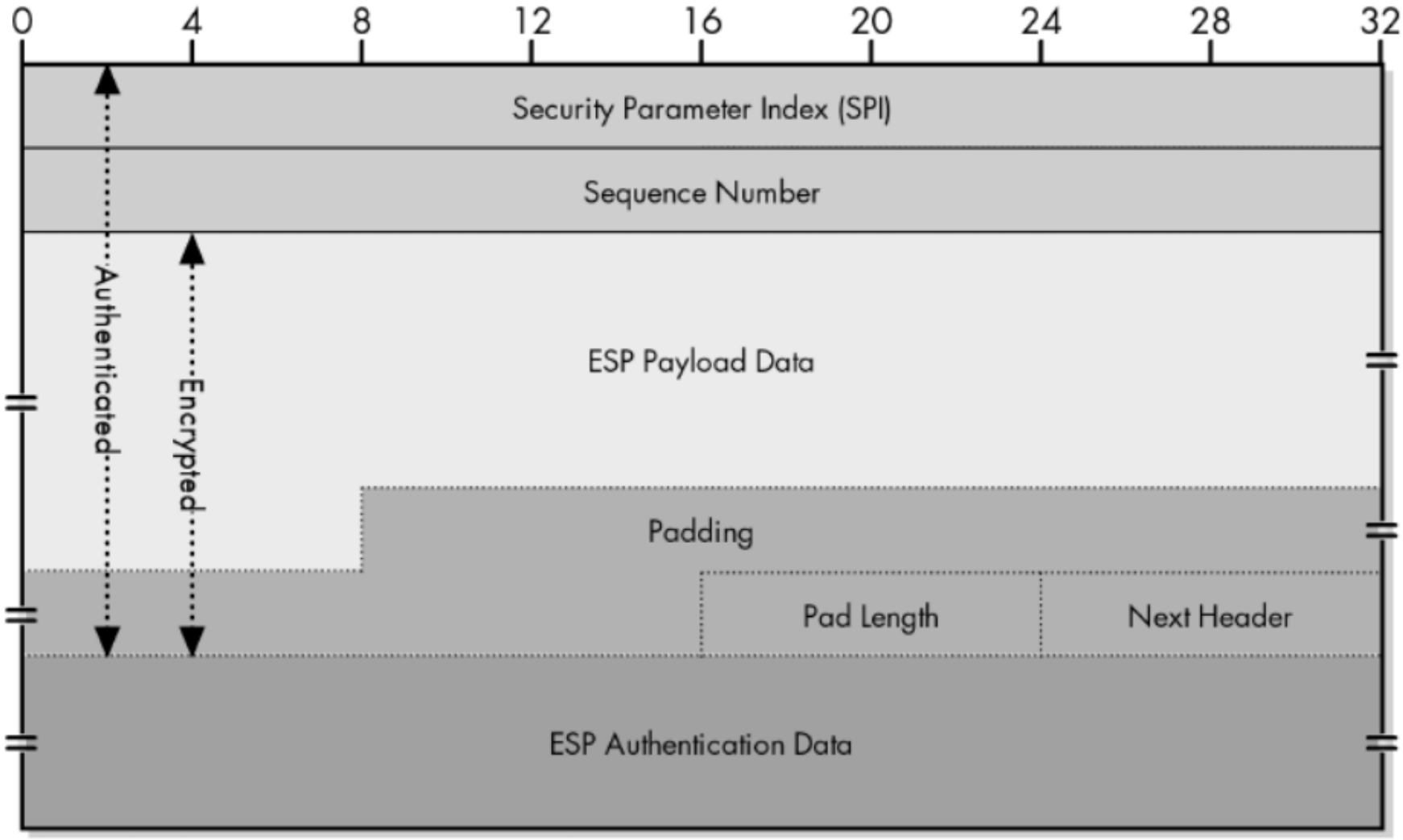
Giao thức bảo mật ESP

- Giao thức ESP cung cấp:
  - Tính bí mật dữ liệu (mã hóa) sử dụng các hệ mã hóa khóa đối xứng như DES, 3-DES và AES;
  - Xác thực (toàn vẹn dữ liệu, xác thực nguồn gốc dữ liệu và bảo vệ chống phát lại) sử dụng hàm băm HMAC.
- ESP có thể được sử dụng chỉ với tính bí mật, chỉ xác thực hoặc cả tính bí mật và xác thực.
  - Khi ESP cung cấp chức năng xác thực, nó sử dụng các thuật toán tương tự như AH, nhưng phạm vi bao phủ khác nhau.
    - Xác thực kiểu AH xác thực toàn bộ gói IP, bao gồm cả tiêu đề IP bên ngoài
    - Xác thực ESP chỉ xác thực phần datagram IP của gói IP.

Giao thức bảo mật ESP



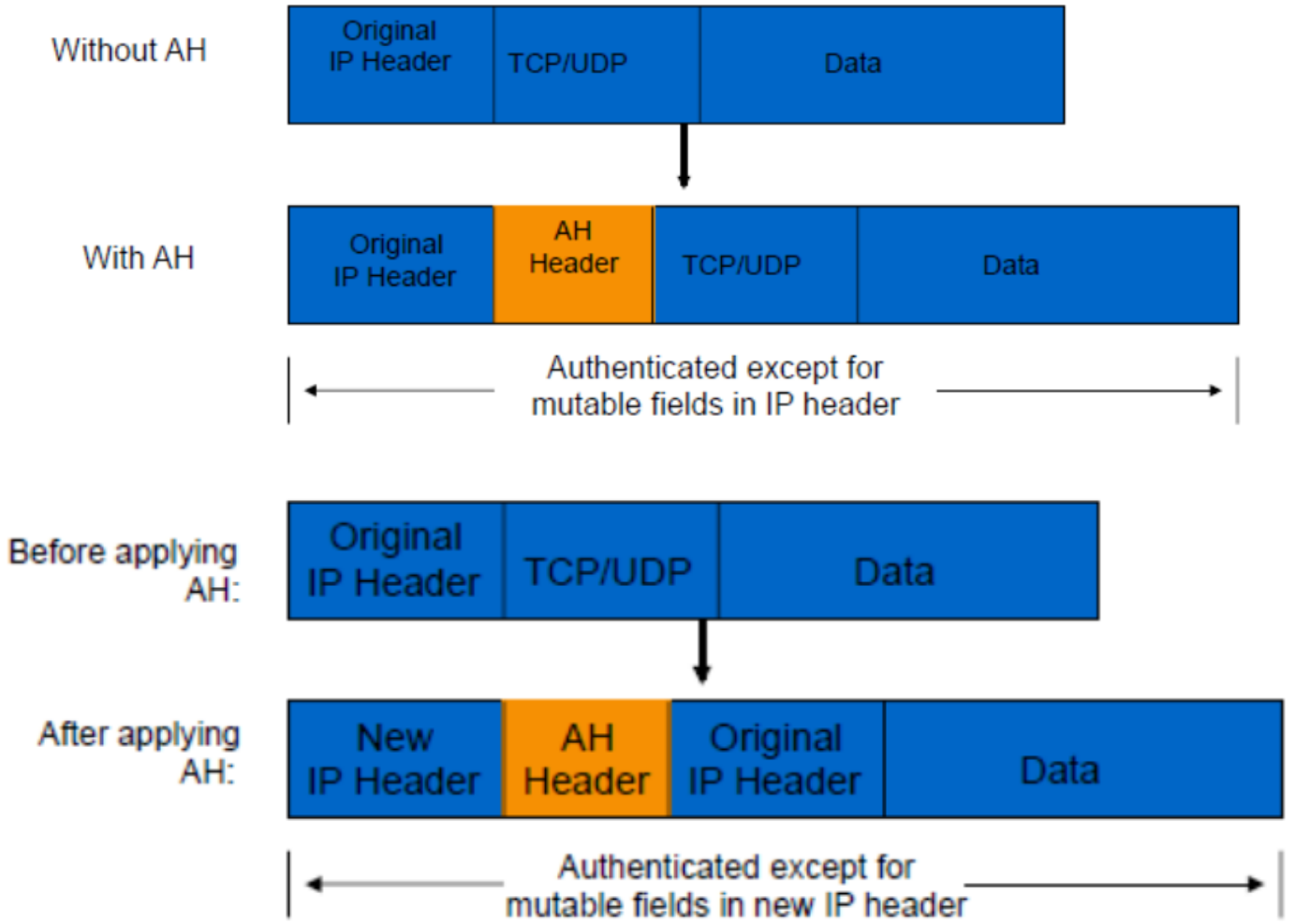
Giao thức bảo mật ESP: Cấu trúc gói tin



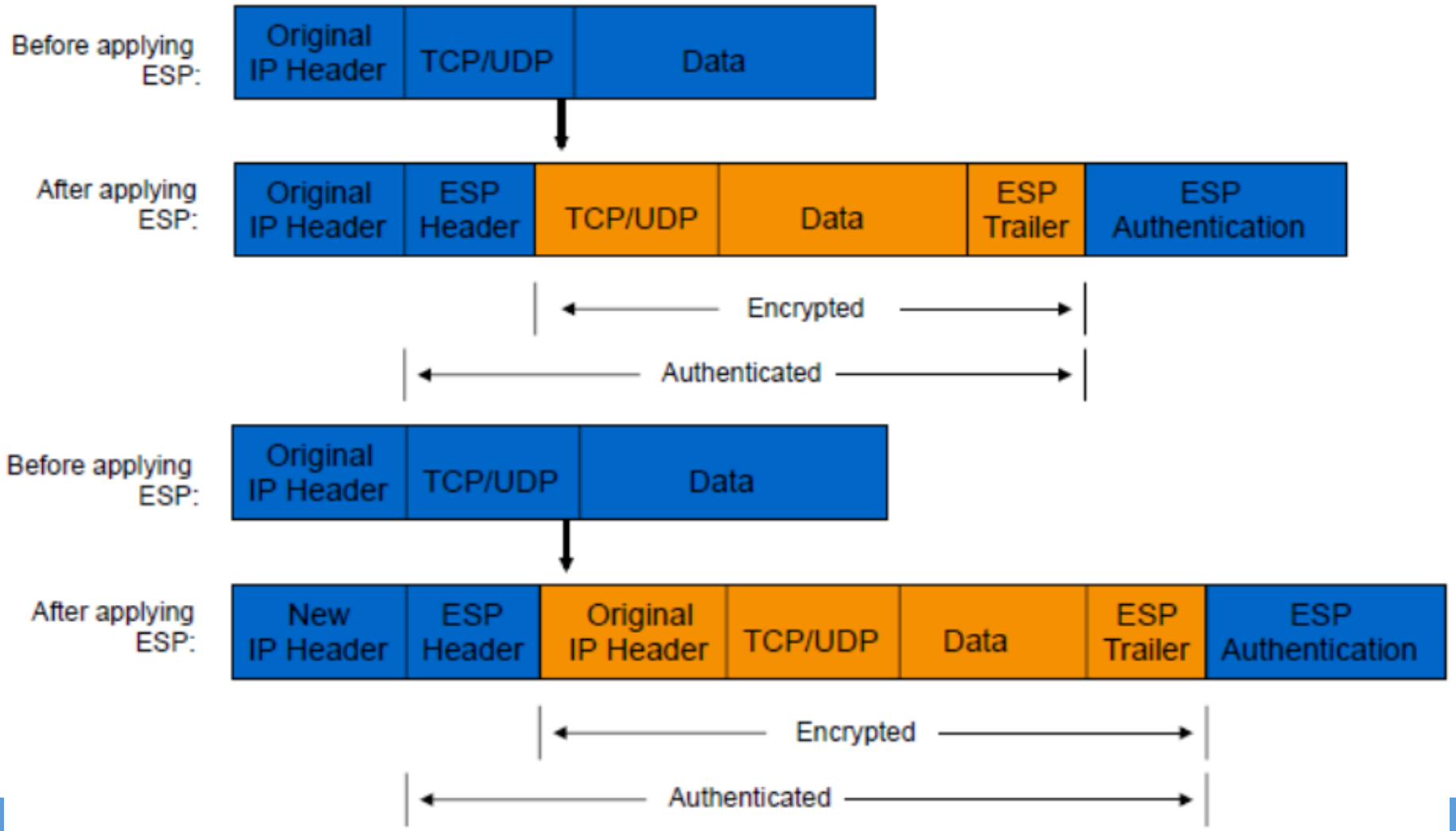
Các chế độ hoạt động của IPSec

- IPSec có thể hoạt động ở 1 trong 2 chế độ (mode):
  - Chế độ vận chuyển (transport mode): Chỉ hỗ trợ bảo vệ dữ liệu (payload) của gói tin vận chuyển;
    - Kém an toàn hơn
    - Nhanh hơn do lượng dữ liệu cần truyền nhỏ hơn (chỉ chèn thêm các header cho bảo mật vào gói ban đầu, không tạo gói mới).
  - Chế độ đường hầm (tunnel mode): Hỗ trợ bảo vệ toàn bộ gói tin ban đầu (gồm cả header + payload);
    - An toàn cao hơn;
    - Chậm hơn do lượng dữ liệu cần truyền lớn hơn (đóng gói toàn bộ gói tin ban đầu vào 1 gói tin mới).

Chế độ vận chuyển vs đường hầm với AH



Chế độ vận chuyển vs đường hầm với ESP



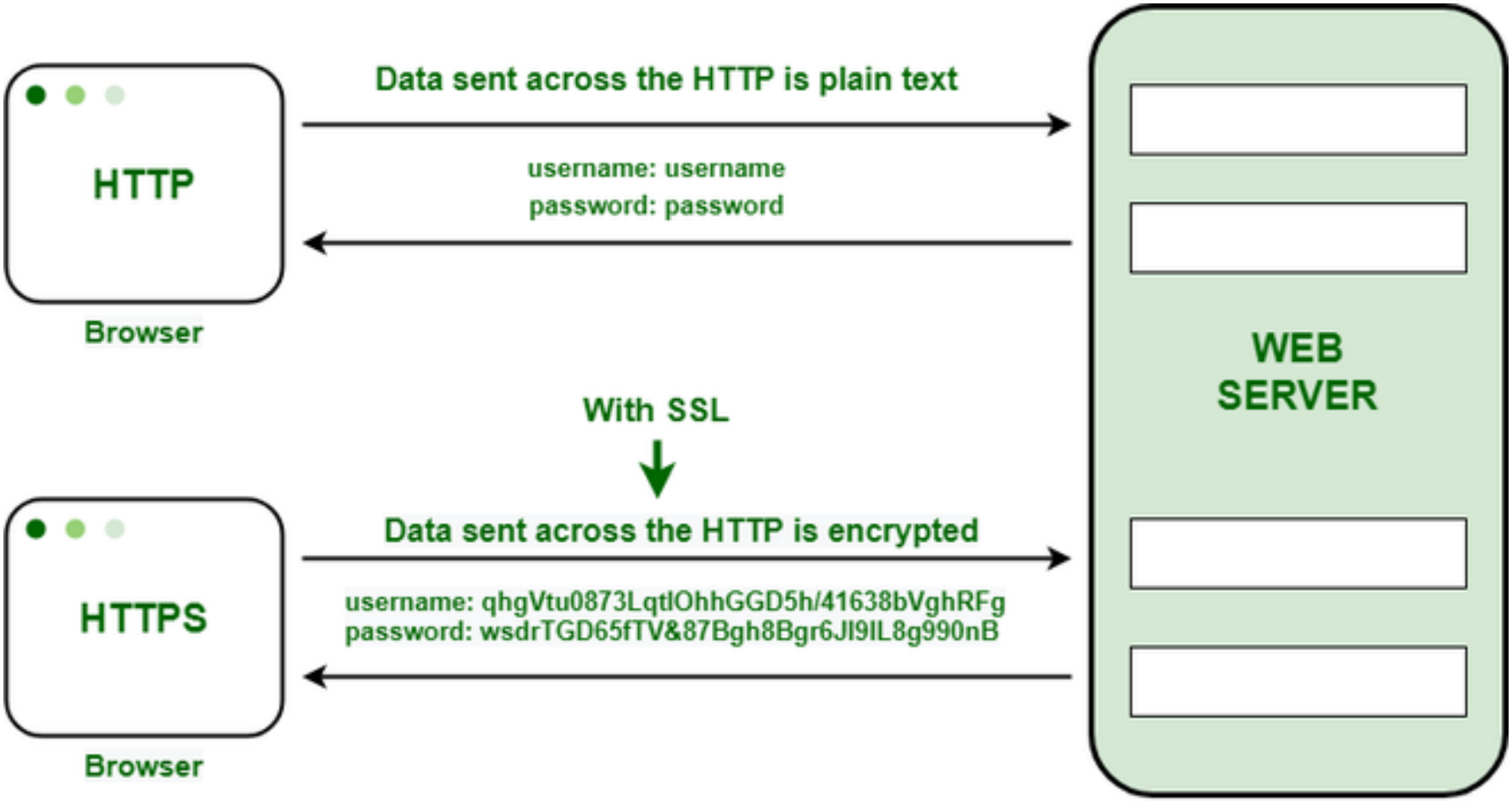
Các thuật toán mật mã sử dụng trong IPSec

- Các thuật toán băm có khóa:
  - HMAC-MD5
  - HMAC-SHA1, HMAC-SHA2
  - AES128_XCBC_96, AES_GMAC_128, AES_GMAC_256
- Các thuật toán mã hóa:
  - DES, 3-DES
  - AES_CBC, AES_GCM_16
- Các thuật toán trao đổi khóa:
  - Diffie–Hellman
  - ISAKMP.

Giao thức HTTPS

- HTTPS là sự kết hợp của các giao thức HTTP và SSL/TLS để bảo mật giao tiếp giữa máy chủ và máy khách web;
- Hầu hết các máy chủ web và trình duyệt web hỗ trợ HTTPS;
- Các thành phần sau được mã hóa với HTTPS:
  - URL của tài liệu được yêu cầu
  - Nội dung tài liệu
  - Nội dung các form gửi từ trình duyệt lên máy chủ web
  - Cookie gửi từ trình duyệt lên máy chủ web và ngược lại
  - Nội dung của HTTP header.
- Các request/response của HTTPS được đóng gói trong gói SSL/TLS nhằm đảm bảo tính bí mật, toàn vẹn và xác thực chủ thể.

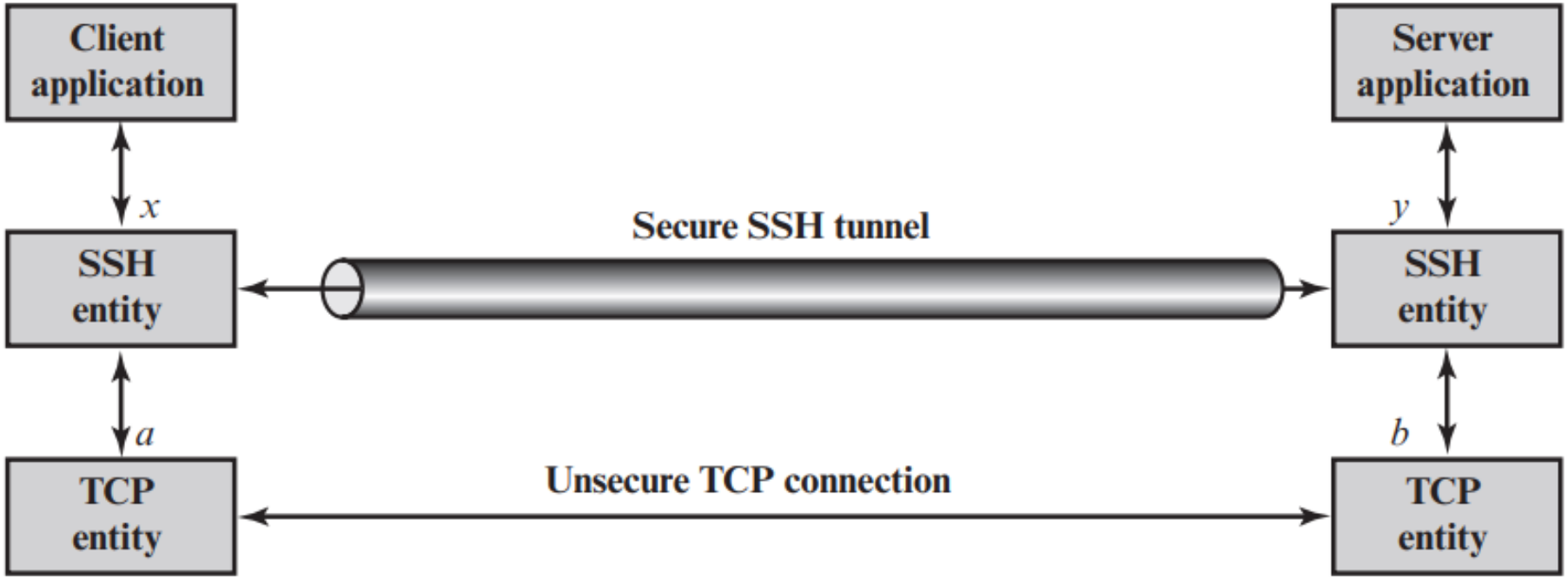
Giao thức HTTPS



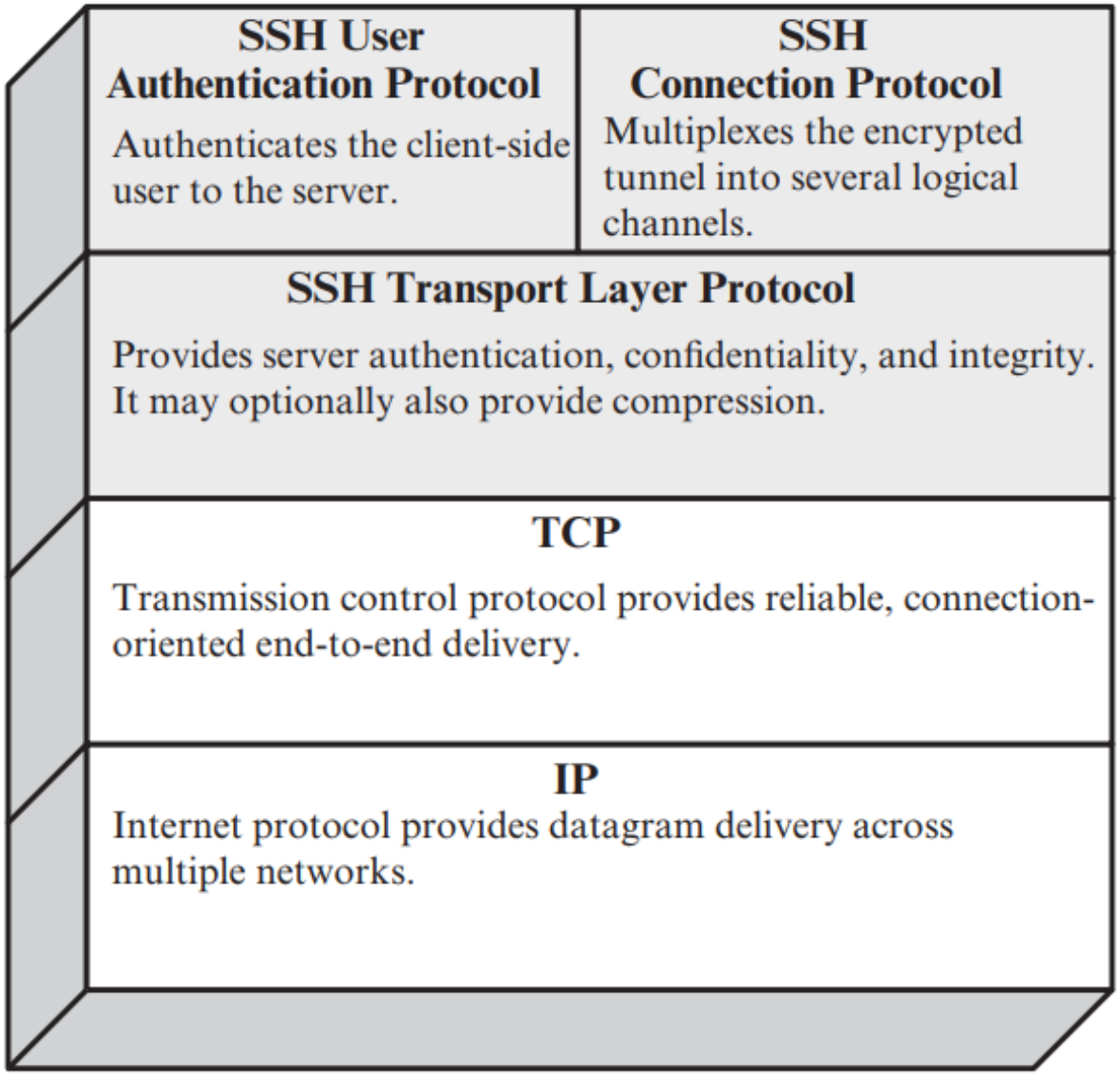
Giao thức SSH

- SSH (Secure Shell) là giao thức bảo mật thông tin truyền với thiết kế đơn giản, chi phí thấp và dễ thực hiện;
  - Bản đầu tiên SSH1 tập trung cung cấp tiện ích bảo mật cho đăng nhập từ xa cho giao thức Telnet hoặc các giao thức không bảo mật.
  - SSH2 sửa nhiều lỗi của SSH1 và được IETF trong các RFC 4250-4256.
- SSH gồm các thành phần:
  - Transport Layer Protocol: Hỗ trợ xác thực máy chủ và tính bí mật, toàn vẹn dữ liệu truyền;
  - User Authentication Protocol: Xác thực người dùng với máy chủ;
  - Connection Protocol: Hỗ trợ nhiều kênh giao tiếp đồng thời trên 1 kết nối SSH.

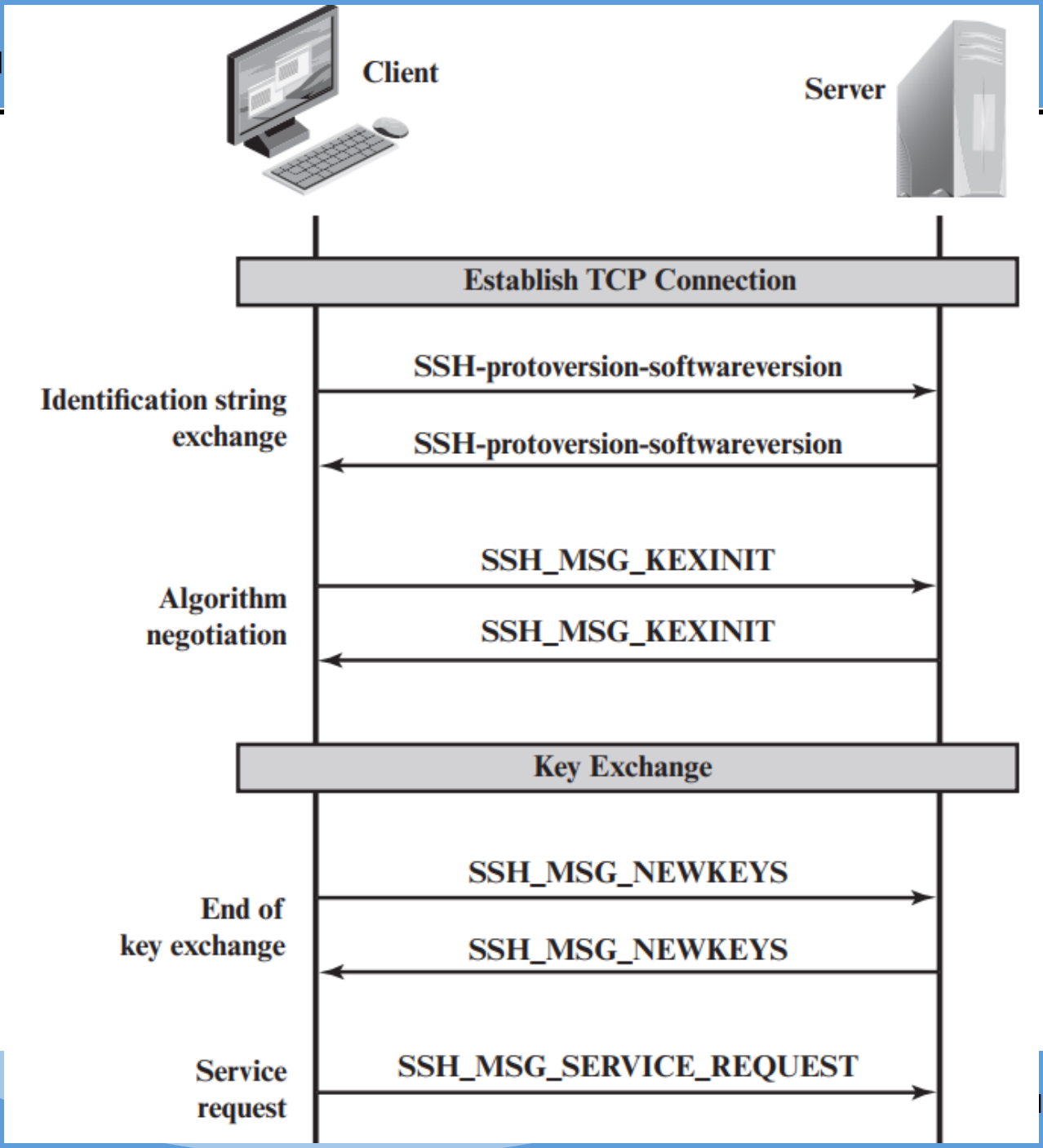
Giao thức SSH



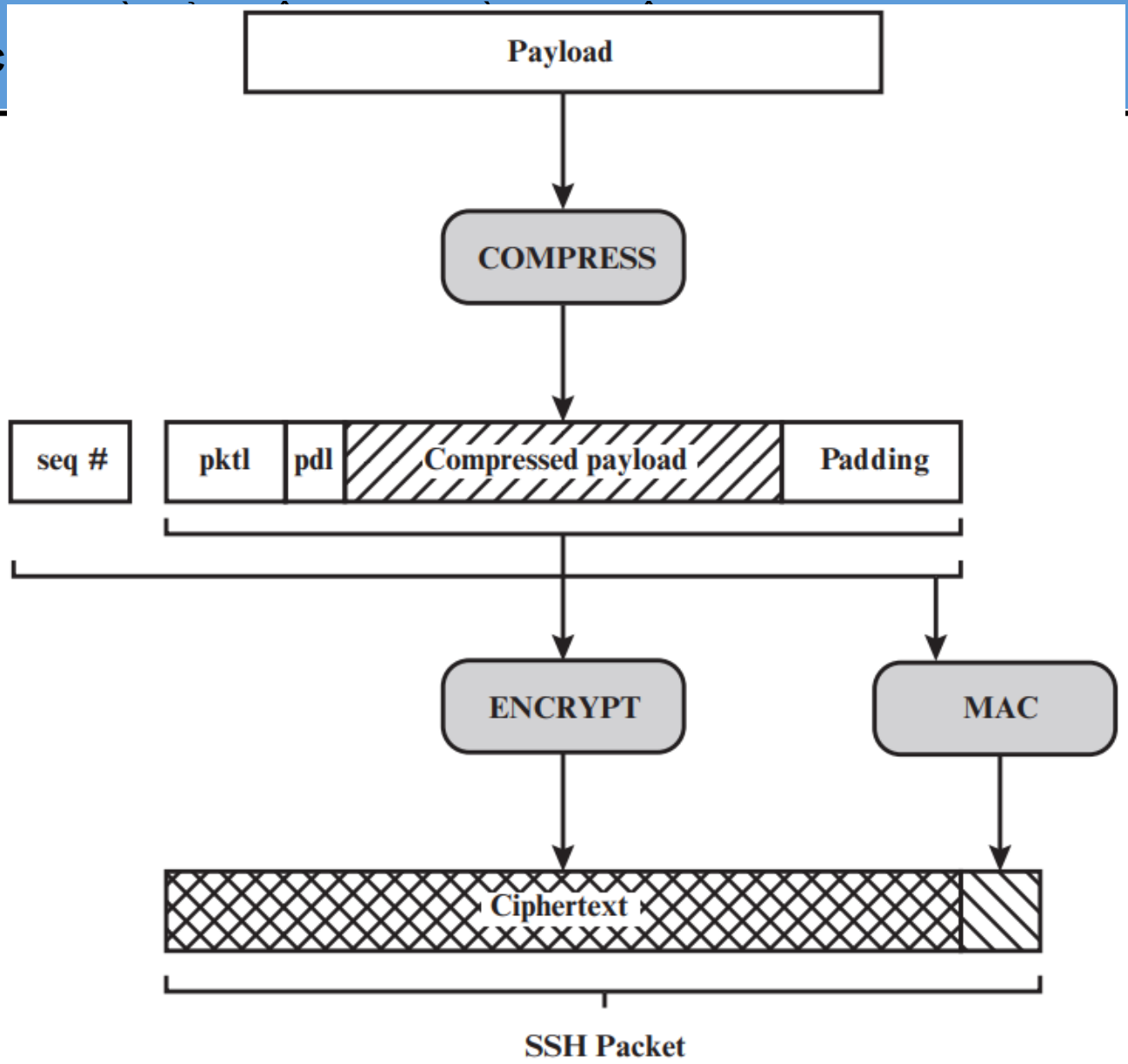
Giao thức SSH: Các thành phần



Giao thức SSH: Khởi tạo kết nối và trao đổi khóa sử dụng thuật toán Diffie-Hellman



Giao thức SSH: Tạo gói tin trong SSH Transport Layer Protocol



Giao thức SSH: Các thuật toán mật mã hỗ trợ

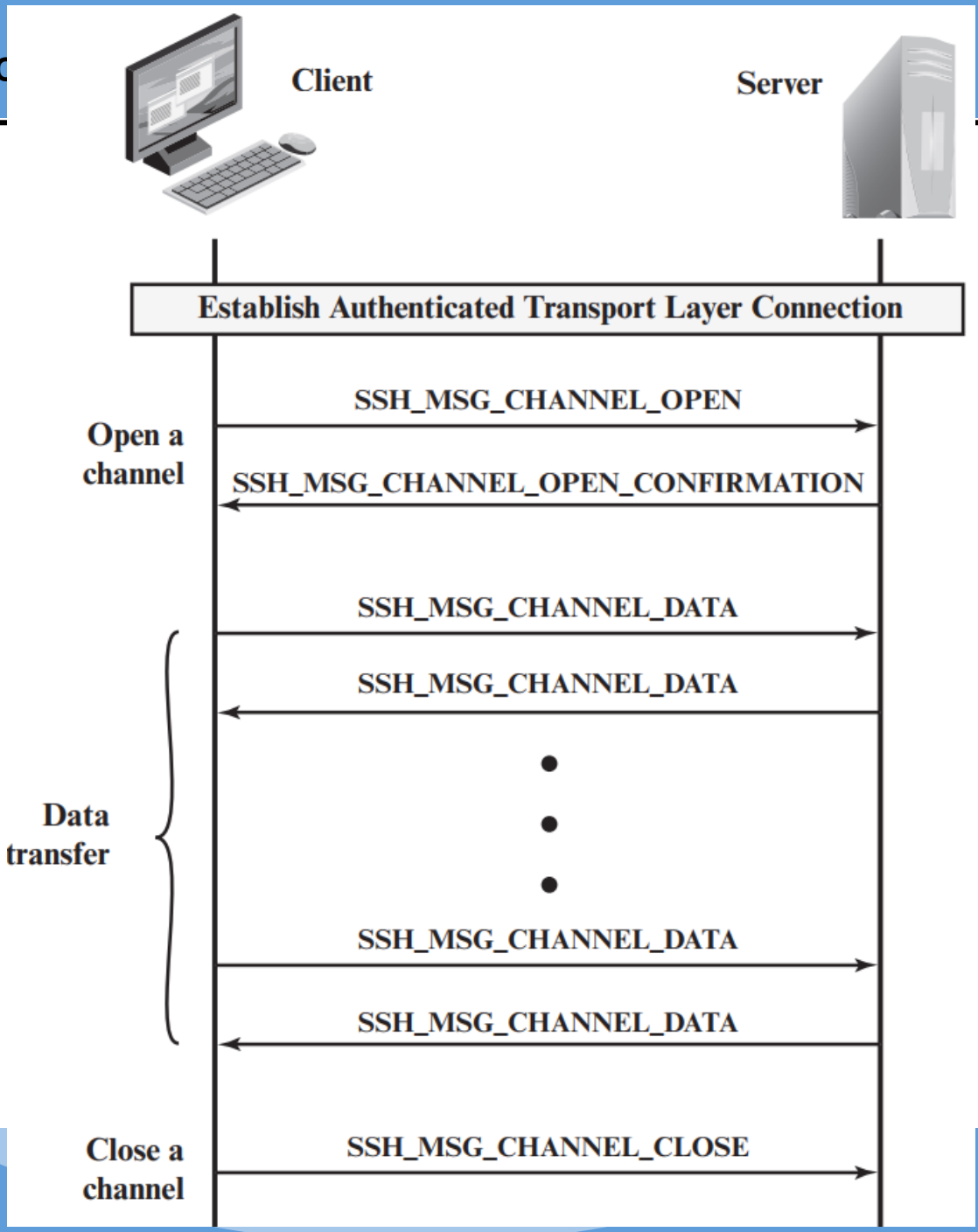
Cipher	
3des-cbc*	Three-key 3DES in CBC mode
blowfish-cbc	Blowfish in CBC mode
twofish256-cbc	Twofish in CBC mode with a 256-bit key
twofish192-cbc	Twofish with a 192-bit key
twofish128-cbc	Twofish with a 128-bit key
aes256-cbc	AES in CBC mode with a 256-bit key
aes192-cbc	AES with a 192-bit key
aes128-cbc**	AES with a 128-bit key
Serpent256-cbc	Serpent in CBC mode with a 256-bit key
Serpent192-cbc	Serpent with a 192-bit key
Serpent128-cbc	Serpent with a 128-bit key
arcfour	RC4 with a 128-bit key
cast128-cbc	CAST-128 in CBC mode

MAC algorithm	
hmac-sha1*	HMAC-SHA1; digest length = key length = 20
hmac-sha1-96**	First 96 bits of HMAC-SHA1; digest length = 12; key length = 20
hmac-md5	HMAC-MD5; digest length = key length = 16
hmac-md5-96	First 96 bits of HMAC-MD5; digest length = 12; key length = 16

Compression algorithm	
none*	No compression
zlib	Defined in RFC 1950 and RFC 1951

* = Required
** = Recommended

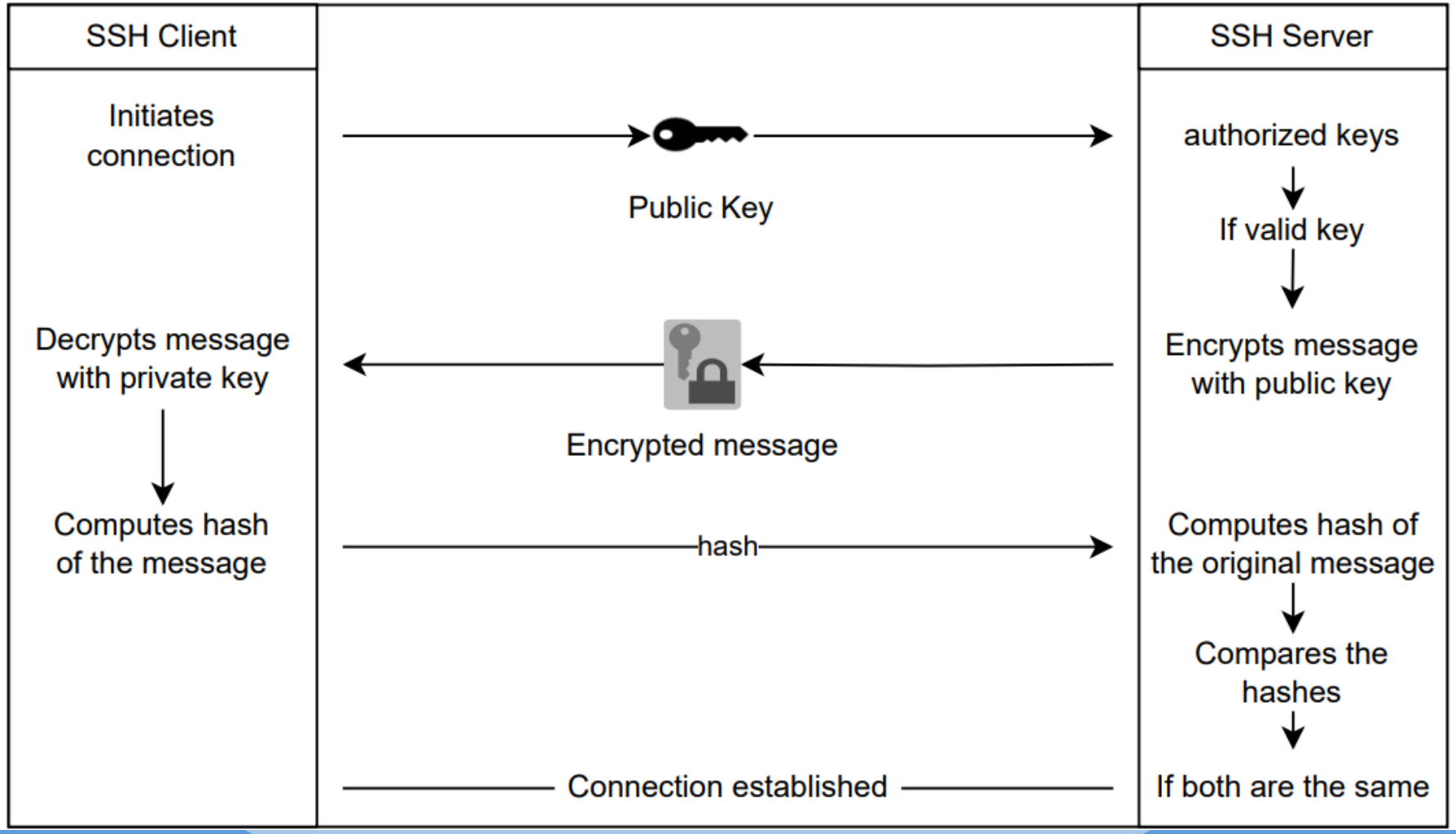
Giao thức SSH: Hỗ trợ đa kênh giao tiếp trên 1 kết nối SSH



Giao thức SSH: Các phương pháp xác thực người dùng

- SSH hỗ trợ 3 phương pháp xác thực người dùng:
  - publickey: Sử dụng khóa công khai và chữ ký số của máy khách để xác thực;
  - password: Máy khách gửi 1 mật khẩu ở dạng rõ để xác thực tài khoản. Mật khẩu được bảo mật nhờ Transport Layer Protocol;
  - hostbased: Xác thực theo host (máy) mà không xác thực từng client. Khi host được xác thực thì tất cả các client chạy trên máy đều được xác thực. Xác thực hostbased được thực hiện tương tự publickey.

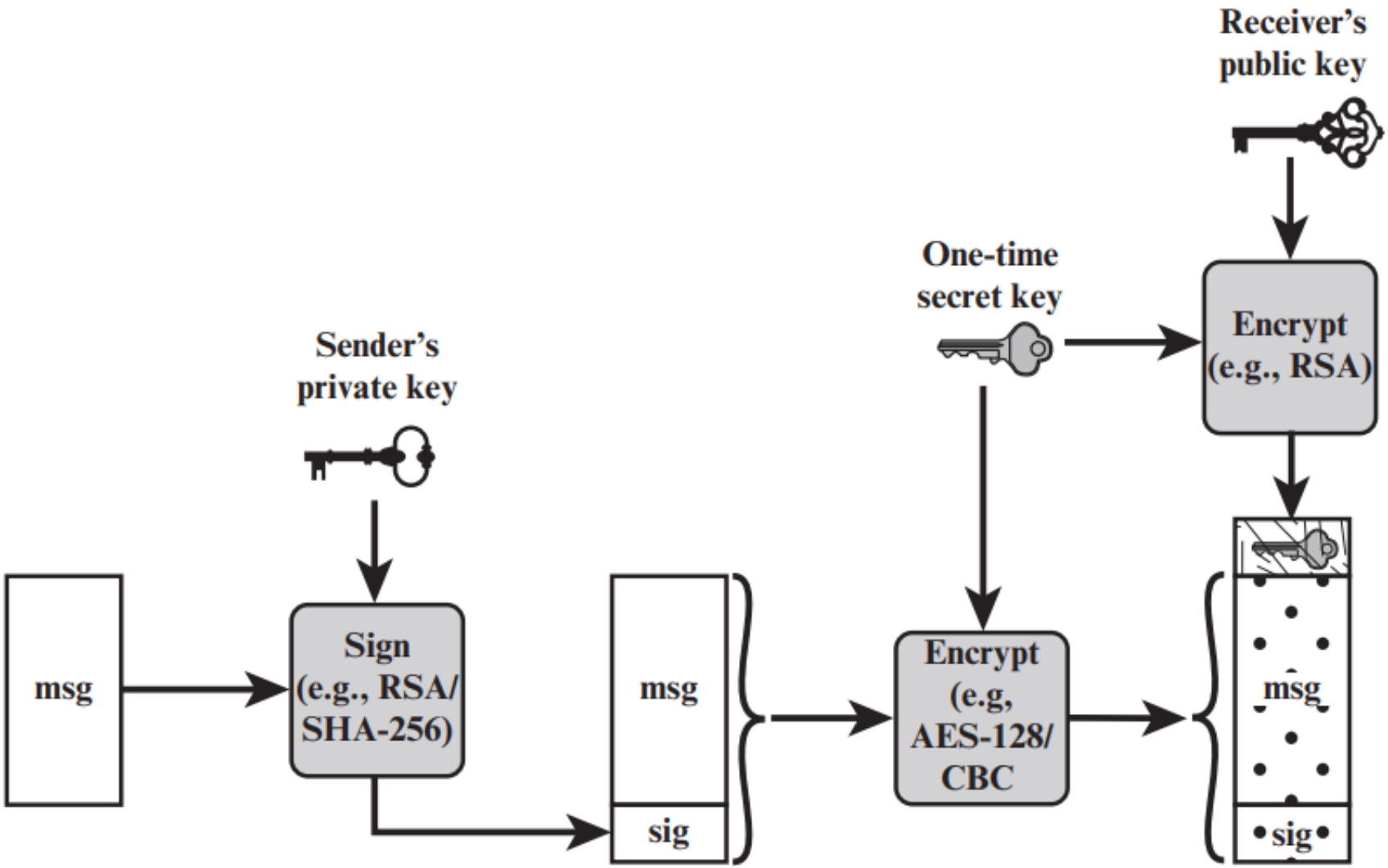
Giao thức SSH: Xác thực sử dụng publickey



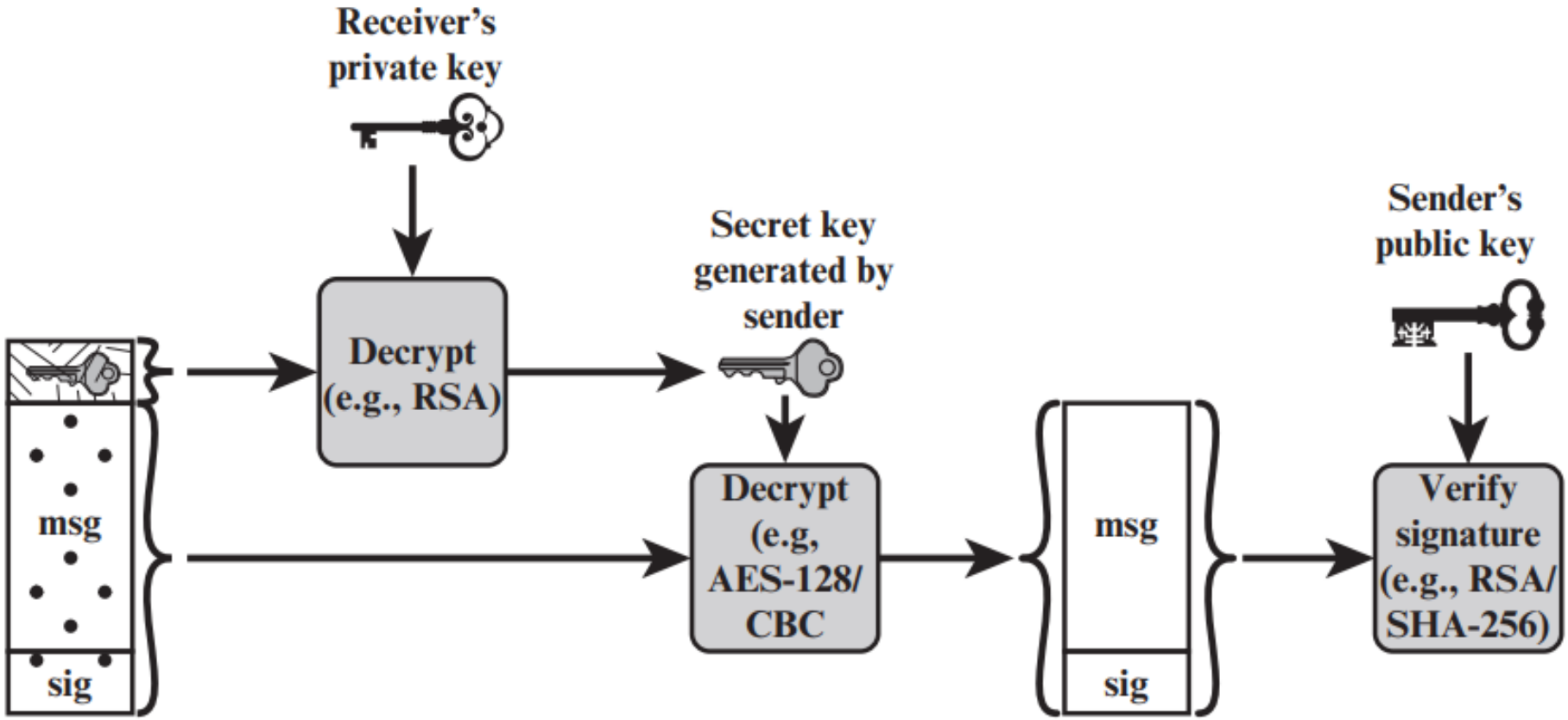
Giao thức S/MIME

- S/MIME (Secure/Multipurpose Internet Mail Extension) là một giải pháp bảo mật tăng cường an toàn cho giao thức vận chuyển email MIME do RSA Data Security đề xuất.
- S/MIME cung cấp:
  - Tính bí mật dữ liệu sử dụng kết hợp mã khóa khóa công khai và mã hóa khóa bí mật;
  - Xác thực tính toàn vẹn sử dụng chữ ký số
  - Nén dữ liệu.

Giao thức S/MIME: Ký và mã hóa ở bên gửi



Giao thức S/MIME: Giải mã và xác thực chữ ký ở bên nhận



Giao thức S/MIME: Các giải thuật mật mã hỗ trợ

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-256 SHOULD support SHA-1 Receiver SHOULD support MD5 for backward compatibility
Use message digest to form a digital signature.	MUST support RSA with SHA-256 SHOULD support —DSA with SHA-256 —RSASSA-PSS with SHA-256 —RSA with SHA-1 —DSA with SHA-1 —RSA with MD5
Encrypt session key for transmission with a message.	MUST support RSA encryption SHOULD support —RSAES-OAEP —Diffie–Hellman ephemeral-static mode
Encrypt message for transmission with a one-time session key.	MUST support AES-128 with CBC SHOULD support —AES-192 CBC and AES-256 CBC —Triple DES CBC