

CHƯƠNG 3

CÁC GIAO THỨC BẢO MẬT

12/1/2021

ThS. Nguyễn Duy
duyn@uit.edu.vn

Nội dung

2

duyn@uit.edu.vn

- IP Security
- Secure Socket Layer /Transport Layer Security
- Pretty Good Privacy
- Secure Shell

Nội dung

3

duyn@uit.edu.vn

- **IP Security**
- Secure Socket Layer /Transport Layer Security
- Pretty Good Privacy
- Secure Shell

IP Security

Tổng quan

4

duyn@uit.edu.vn

- 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 gửi và người nhận.

IP Security – tt

Tổng quan

5

duyn@uit.edu.vn

- 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.

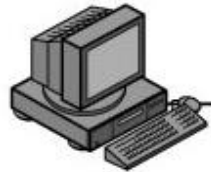
IP Security – tt

Tổng quan

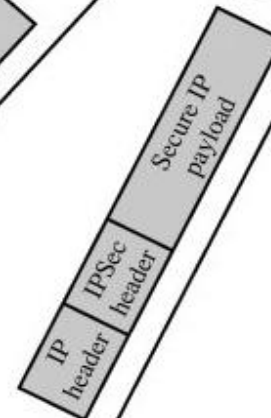
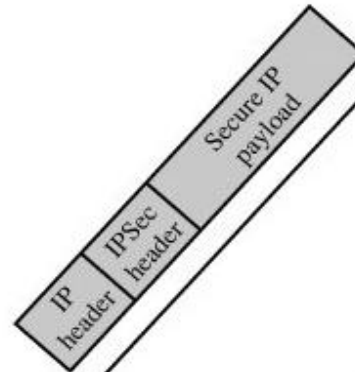
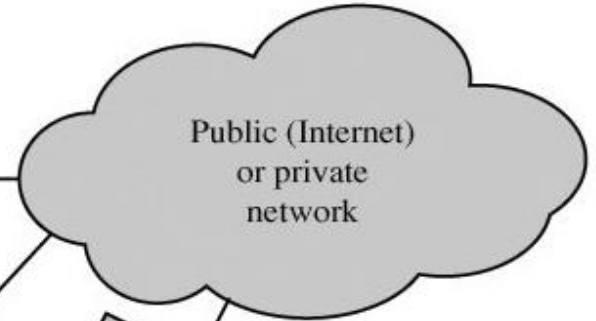
6

duyn@uit.edu.vn

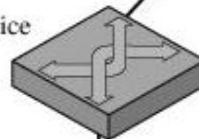
User system
with IPSec



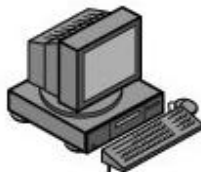
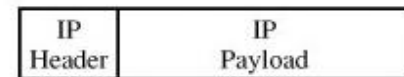
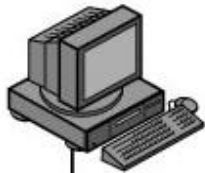
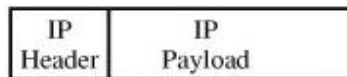
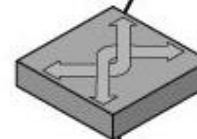
Public (Internet)
or private
network



Networking device
with IPSec



Networking device
with IPSec



IP Security – tt

Tổng quan

7

duyn@uit.edu.vn

- Ví dụ minh họa:
 - 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.

IP Security – tt

Tại sao cần sử dụng IP Security

8

duyn@uit.edu.vn

- IPv4 không được thiết kế với tính bảo mật
- Những cuộc tấn công có thể xảy ra với IPv4
 - Eavesdropping
 - Data modification
 - Identity spoofing (IP address spoofing)
 - Denial-of-service attack
 - Man-in-the-middle attack

IP Security – tt

Tại sao cần sử dụng IP Security

9

duyn@uit.edu.vn

- Eavesdropping
 - Mã hóa dữ liệu.
- Data modification
 - IP sử dụng thuật toán hàm băm
- Identity spoofing (IP address spoofing)
 - Sử dụng cơ chế xác thực lẫn nhau
- Denial-of-service attack
 - Cho phép block traffic
- Man-in-the-middle attack
 - Sử dụng cơ chế xác thực lẫn nhau + Shared Key

IP Security – tt

Security Association (SA)

10

duyn@uit.edu.vn

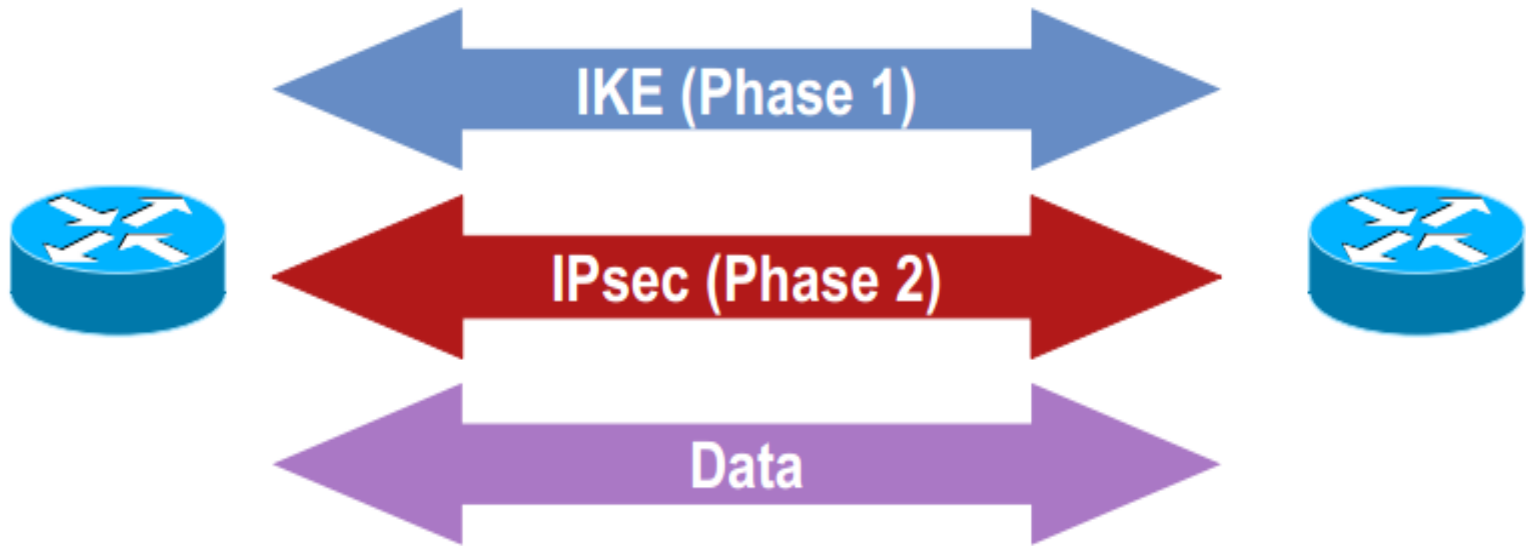
- Một SA cung cấp các thông tin sau:
 - Chỉ mục các thông số bảo mật (SPI - Security parameters index): là một chuỗi nhị phân 32 bit được sử dụng để xác định một tập cụ thể của các giải thuật và thông số dùng trong phiên truyền thông. SPI được bao gồm trong cả AH và ESP để chắc chắn rằng cả hai đều sử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

IP Security

Cơ chế hoạt động

11

duyn@uit.edu.vn



IP Security - tt

Cơ chế hoạt động - tt

12

duyn@uit.edu.vn

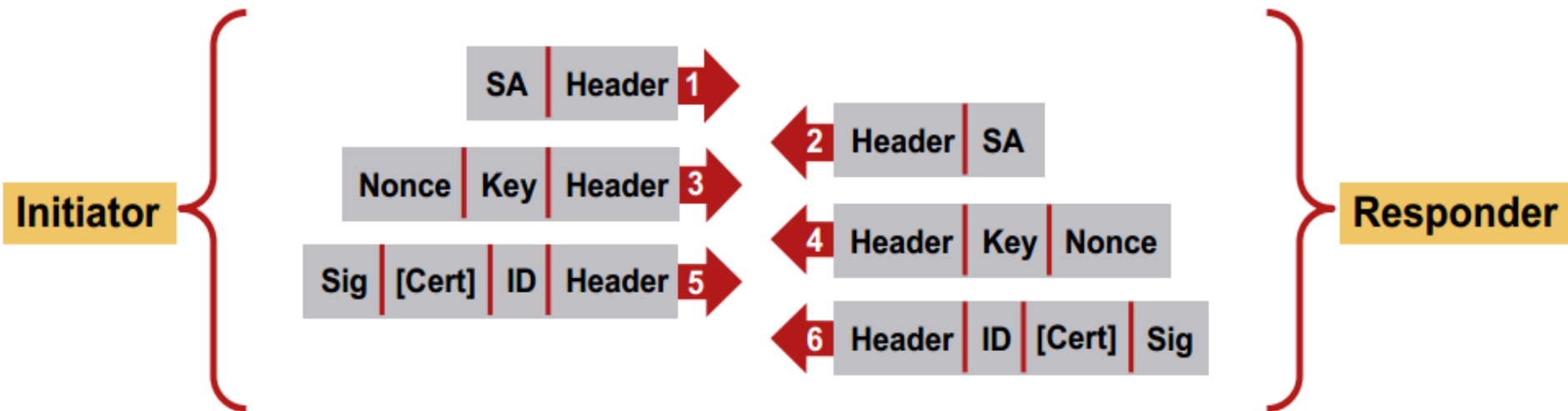
- IKE là cơ chế trao đổi key
- Được sử dụng để thiết lập phiên làm việc của IPSec
- Có 5 giá trị được thỏa thuận:
 - 2 modes (main mode và aggressive mode)
 - 3 phương thức xác thực (Preshared-Key, Kerberos và Certification)

IP Security - tt

IKE – Main Mode

13

duyn@uit.edu.vn



- MSG 1: Initiator offers acceptable encryption and authentication algorithms (3DES, MD5, or RSA)—i.e., the transform-set.
- MSG 2: Responder presents acceptance of the proposal (or not).
- MSG 3: Initiator Diffie-Hellman key and nonce (key value is usually a number of 1024-bit length).
- MSG 4: Responder Diffie-Hellman key and nonce.
- MSG 5: Initiator signature, ID, and keys (maybe cert), i.e., authentication data.
- MSG 6: Responder signature, ID, and keys (maybe cert).

IP Security - tt

IKE – Main Mode

duyn@uit.edu.vn

Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000210	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) request id=0x0200,
4	0.002699	192.168.1.1	192.168.1.2	ISAKMP	318	Identity Protection (Main Mode)
5	0.106273	192.168.1.2	192.168.1.1	ISAKMP	190	Identity Protection (Main Mode)
6	0.153392	192.168.1.1	192.168.1.2	ISAKMP	274	Identity Protection (Main Mode)
7	0.187149	192.168.1.2	192.168.1.1	ISAKMP	274	Identity Protection (Main Mode)
8	0.195156	192.168.1.1	192.168.1.2	ISAKMP	110	Identity Protection (Main Mode)
9	0.196965	192.168.1.2	192.168.1.1	ISAKMP	110	Identity Protection (Main Mode)
10	0.198273	192.168.1.1	192.168.1.2	ISAKMP	326	Quick Mode
11	0.199263	192.168.1.2	192.168.1.1	ISAKMP	206	Quick Mode
12	0.199610	192.168.1.1	192.168.1.2	ISAKMP	94	Quick Mode

⊕ Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

⊕ Ethernet II, Src: vmware_29:f6:39 (00:0c:29:29:f6:39), Dst: vmware_04:e1:b6 (00:0c:29:04:e1:b6)

⊕ Internet Protocol Version 4, Src: 192.168.1.2 (192.168.1.2), Dst: 192.168.1.1 (192.168.1.1)

Internet Control Message Protocol

Filter:		Expression... Clear Apply				
No.	Time	Source	Destination	Protocol	Length	Info
3	0.000210	192.168.1.2	192.168.1.1	ICMP	74	Echo (ping) request id=0x0200,
4	0.002699	192.168.1.1	192.168.1.2	ISAKMP	318	Identity Protection (Main Mode)
5	0.106273	192.168.1.2	192.168.1.1	ISAKMP	190	Identity Protection (Main Mode)
6	0.153392	192.168.1.1	192.168.1.2	ISAKMP	274	Identity Protection (Main Mode)
7	0.187149	192.168.1.2	192.168.1.1	ISAKMP	274	Identity Protection (Main Mode)
8	0.195156	192.168.1.1	192.168.1.2	ISAKMP	110	Identity Protection (Main Mode)
9	0.196965	192.168.1.2	192.168.1.1	ISAKMP	110	Identity Protection (Main Mode)
10	0.198273	192.168.1.1	192.168.1.2	ISAKMP	326	Quick Mode
11	0.199263	192.168.1.2	192.168.1.1	ISAKMP	206	Quick Mode
12	0.199610	192.168.1.1	192.168.1.2	ISAKMP	94	Quick Mode

SPI Size: 0

Proposal transforms: 4

[-] Type Payload: Transform (3) # 1

Next payload: Transform (3)

Payload length: 36

Transform number: 1

Transform ID: KEY IKE (1)

⊕ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC

⊕ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA

⊕ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group

⊕ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK

⊕ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds

⊕ Transform IKE Attribute Type (t=12,l=4) Life-Duration : 0

⊕ Type Payload: Transform (3) # 2

⊕ Type Payload: Transform (3) # 3

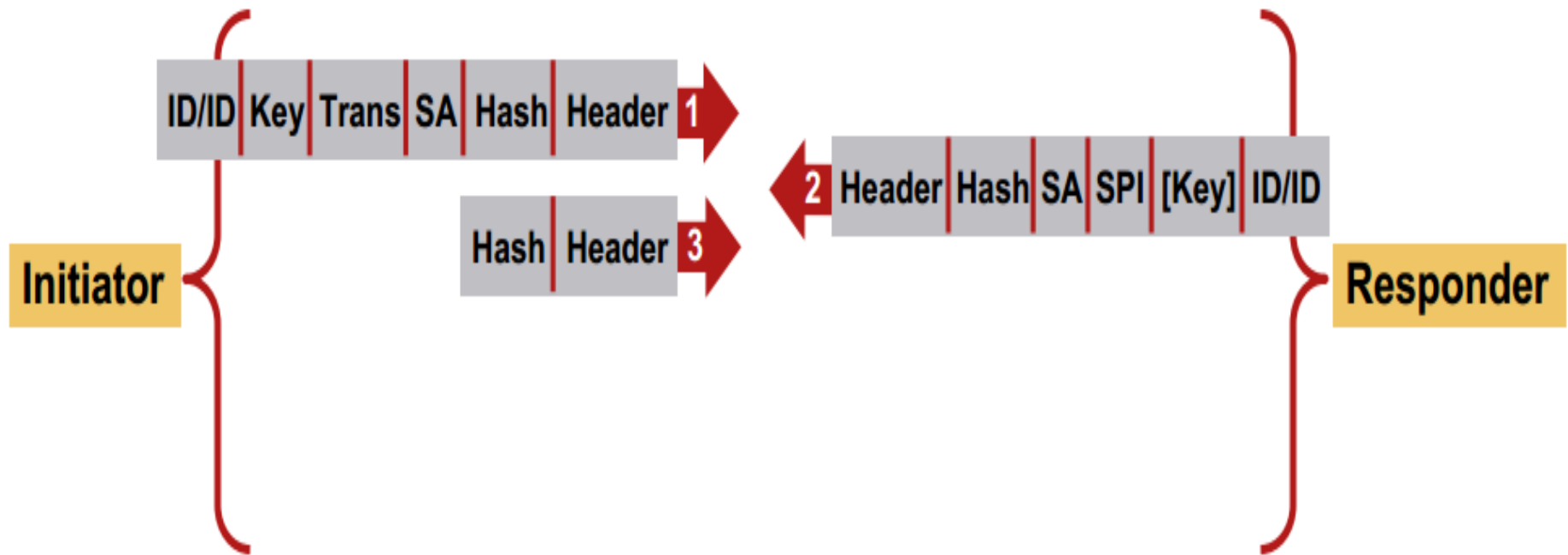
⊕ Type Payload: Transform (3) # 4

IP Security

IPSecurity: Quick mode

17

duyn@uit.edu.vn



- MSG 1: Hash, SA proposal, IPsec transform, keying material, and ID (proxy identities, source, and destination)
- MSG 2: Responder hash, agreed to SA proposal, Responder SPI, and key
- MSG 3: Hash to verify current and live peer

IP Security – tt

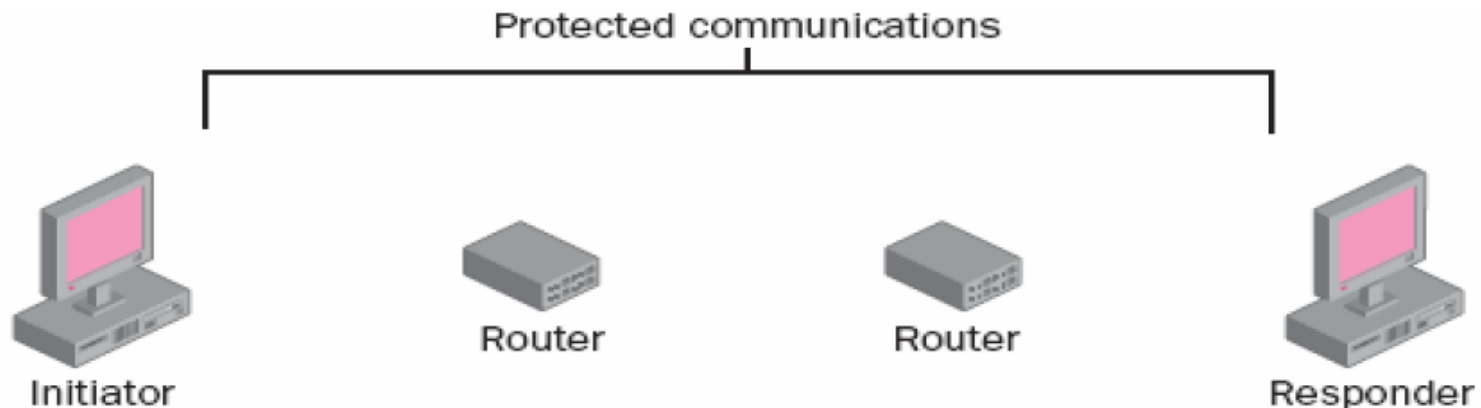
Các phương thức hoạt động của IPsec

18

duyn@uit.edu.vn

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)



IP Security – tt

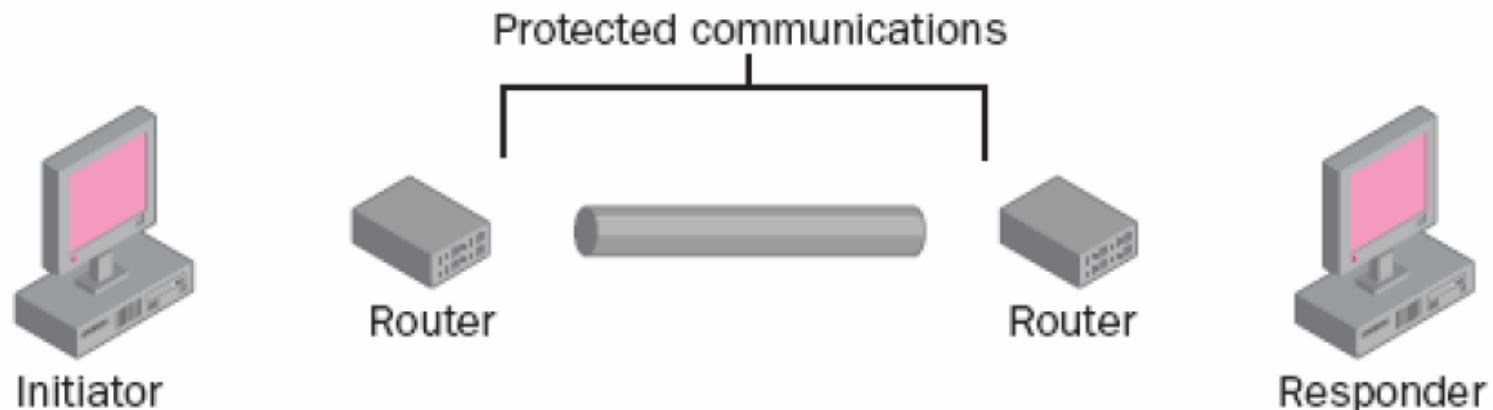
Các phương thức hoạt động của IPsec

19

duyn@uit.edu.vn

IPsec bao gồm 2 phương thức:

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

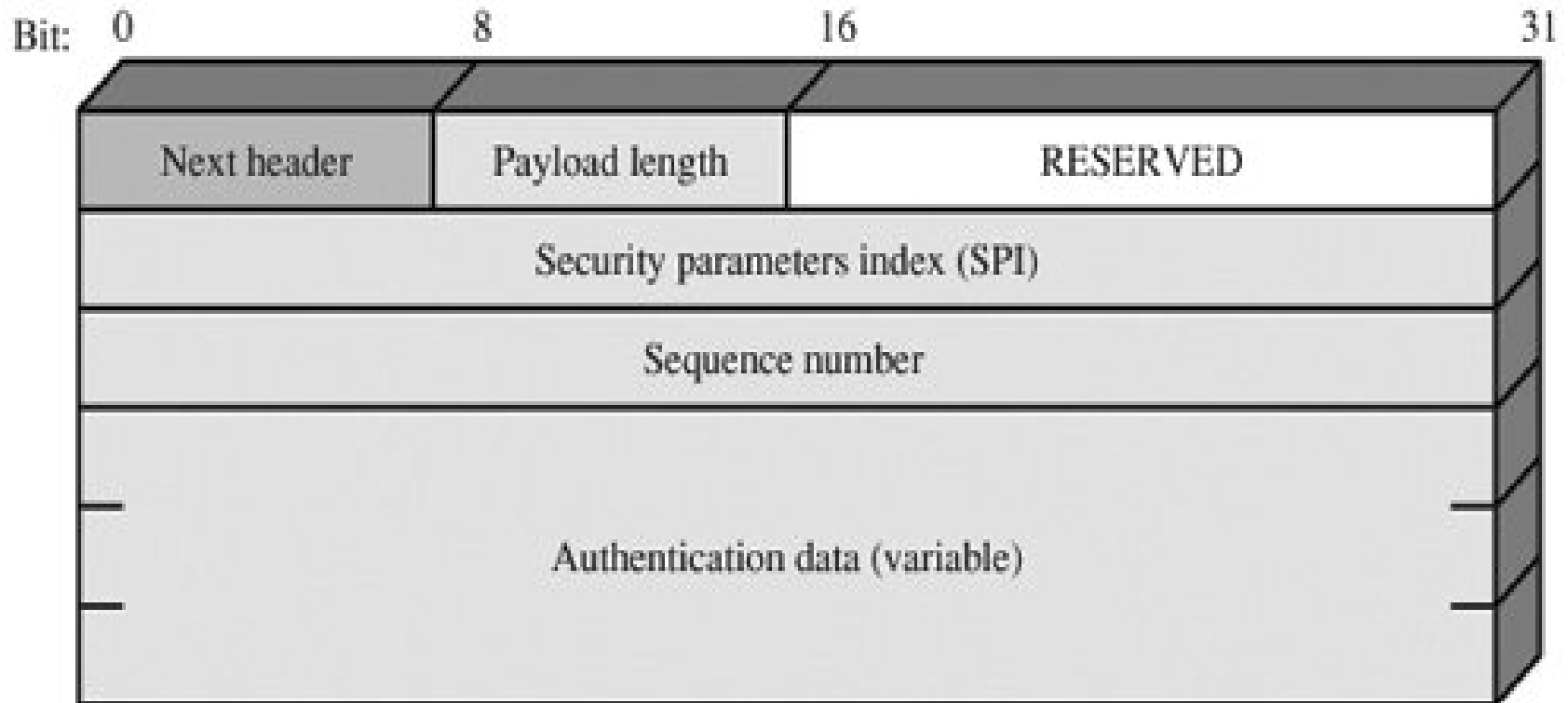


IP Security – tt

Định dạng AH

20

duyn@uit.edu.vn



IPSec Authentication Header

IP Security – tt

Định dạng AH

21

duyn@uit.edu.vn

- 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.

IP Security – tt

Định dạng AH

22

duyn@uit.edu.vn

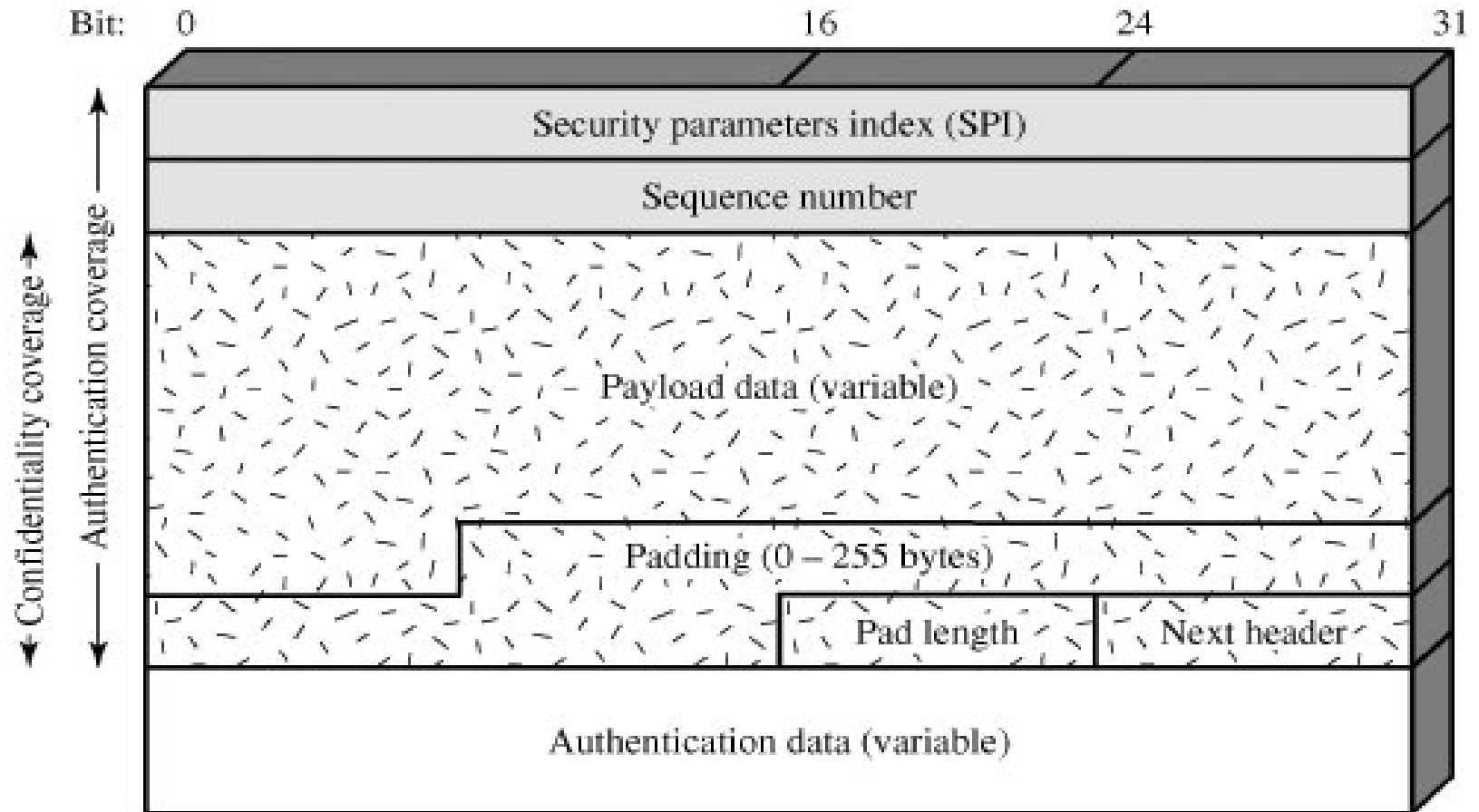
- Authentication Header
 - Xác thực
 - Toàn vẹn
 - Tránh tấn công Replay-Attack

IP Security – tt

Định dạng ESP

23

duyn@uit.edu.vn



IPSec ESP format

IP Security – tt

Định dạng ESP

24

duyn@uit.edu.vn

- 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 (0-255 bytes)
 - Pad Length (8 bits): chỉ ra số byte vùng đứng ngay trước vùng này.

IP Security – tt

Định dạng ESP

25

duyn@uit.edu.vn

- Một gói ESP chứa các vùng sau:
 - 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.

IP Security – tt

Định dạng ESP

26

duyn@uit.edu.vn

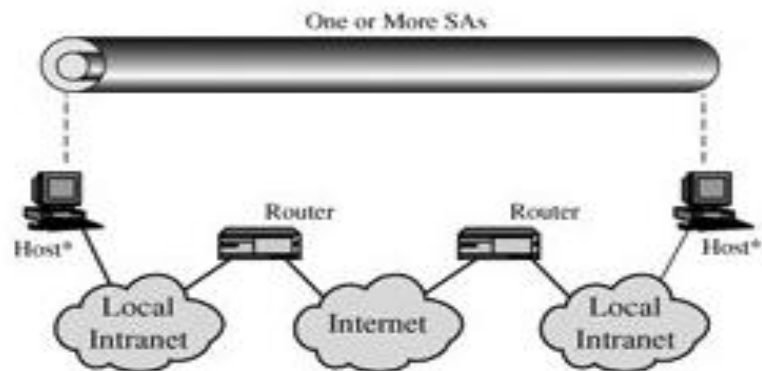
- Encapsulating Security Payload (ESP)
 - Xác thực
 - Toàn vẹn
 - Bảo mật
 - Tránh tấn công Replay-Attack

IP Security – tt

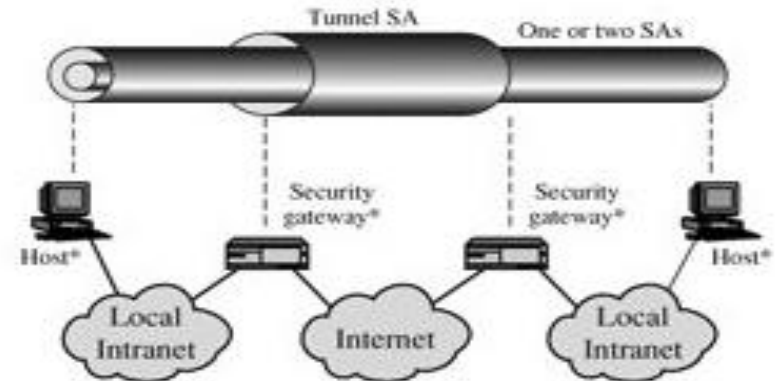
Sự kết hợp của các SA

27

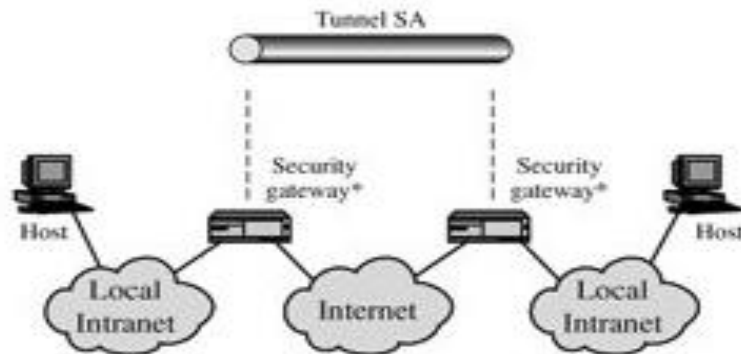
duyn@uit.edu.vn



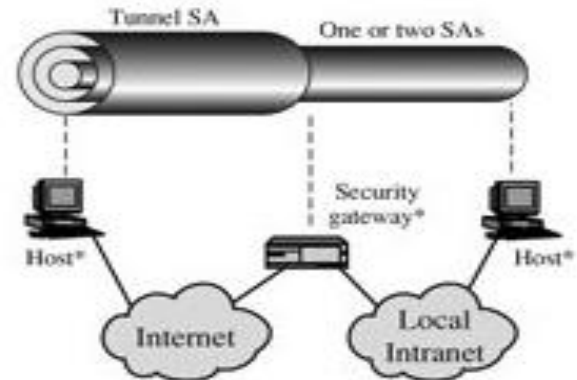
AH in transport mode



ESP followed by AH in transport mode



ESP in transport mode



Any one of a, b, or c inside an AH or ESP in tunnel mode

Basic Combinations of Security Associations

IP Security – tt

Các giải thuật mã hoá và chứng thực

28

duyn@uit.edu.vn

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

Nội dung

29

duyn@uit.edu.vn

- IP Security
- **Secure Socket Layer /Transport Layer Security**
- Pretty Good Privacy
- Secure Shell

SSL/TLS

Tổng quan

30

duyn@uit.edu.vn

- 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.

SSL/TLS

Các thành phần của SSL

31

duyn@uit.edu.vn

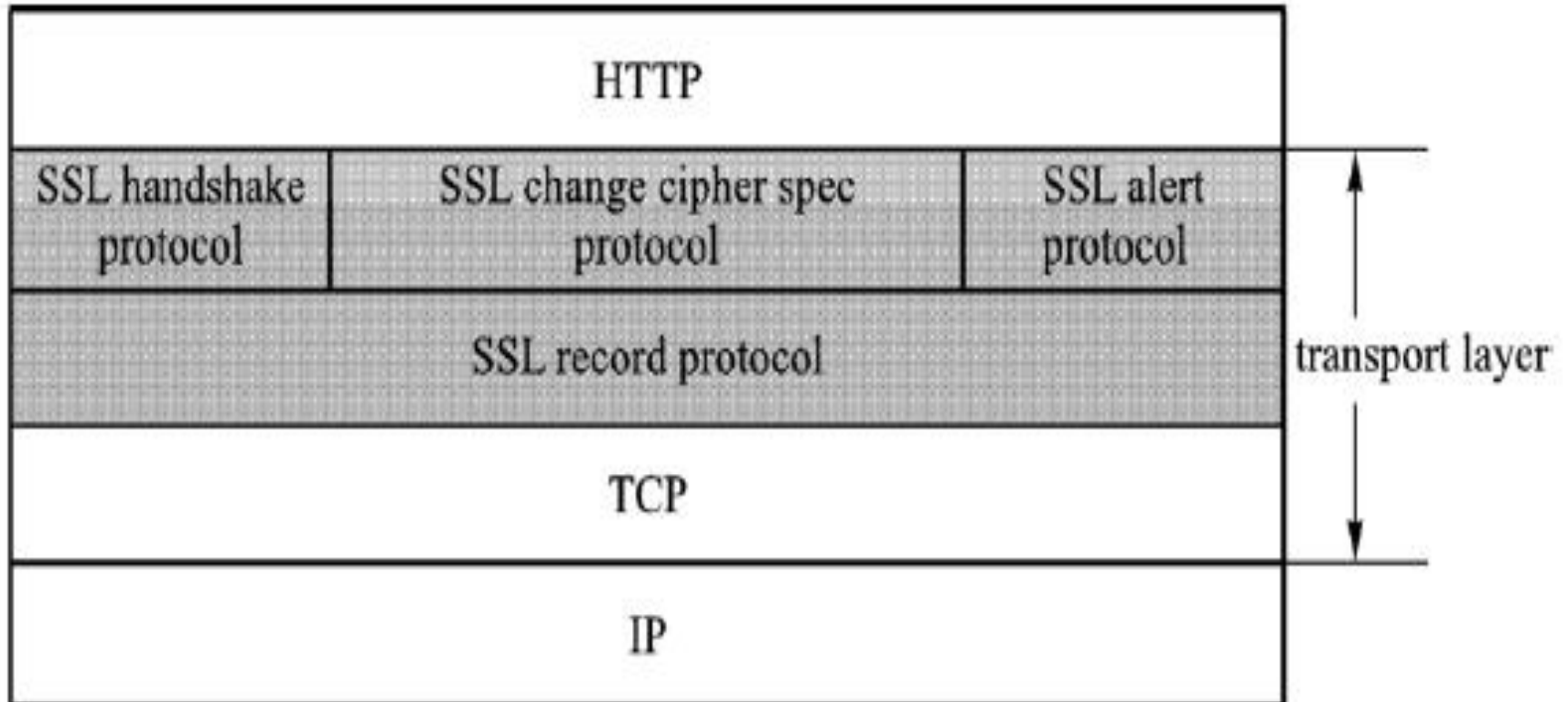
- Giao thức SSL bao gồm 2 thành phần:
 - Thành phần thứ nhất được gọi là record protocol, được đặt trên đỉnh của các giao thức lớp vận chuyển.
 - Thành phần thứ hai được đặt giữa các giao thức tầng ứng dụng (như HTTP) và record protocol , bao gồm các giao thức:
 - Handshake protocol
 - Change-cipher-spec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

SSL/TLS

Cấu trúc của SSL

32

duyn@uit.edu.vn



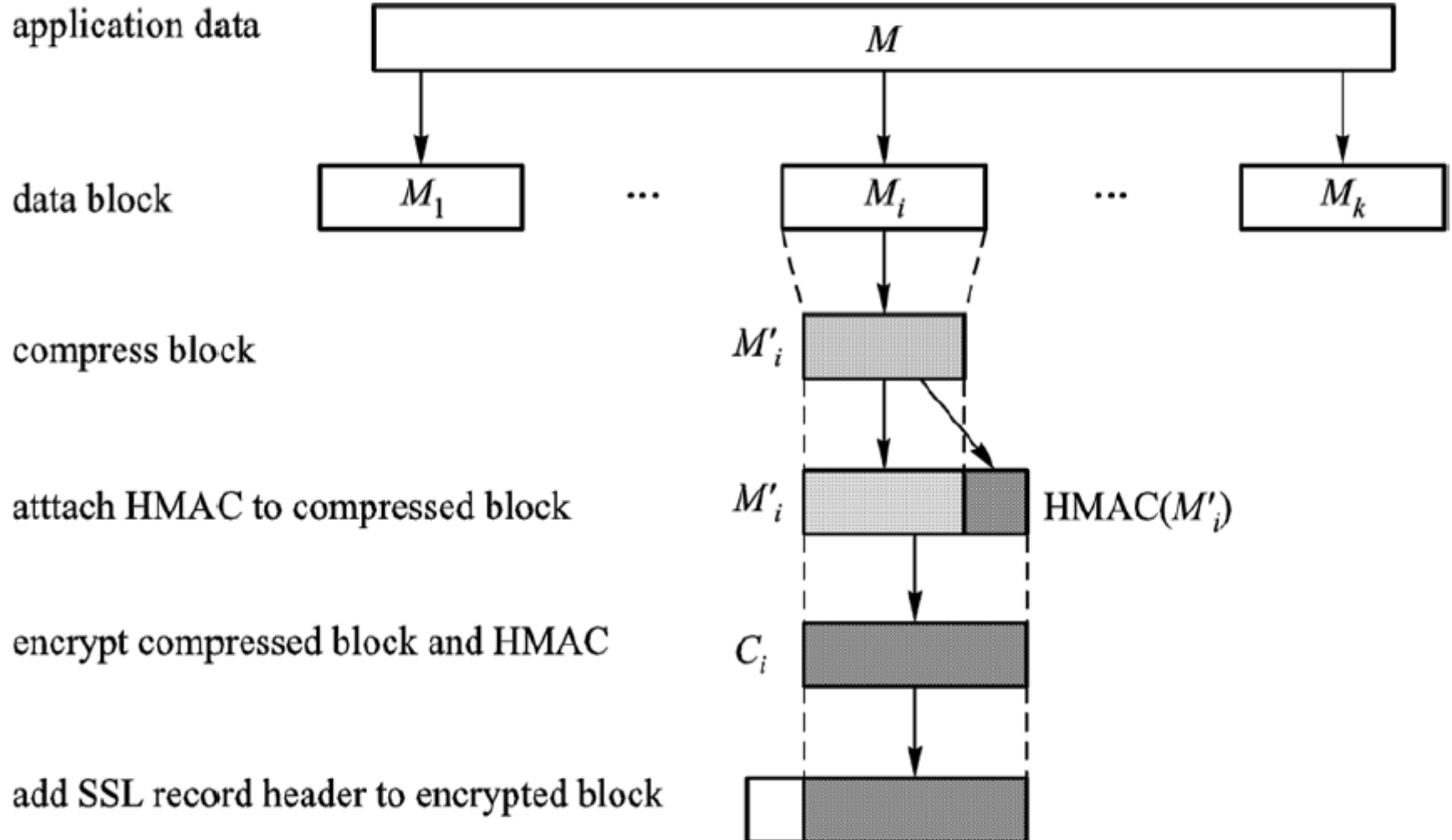
SSL structure

SSL/TLS

Giao thức bản ghi (record protocol) của SSL

33

duyn@uit.edu.vn



SSL/TLS

Các giao thức của SSL

34

duyn@uit.edu.vn

- **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.

SSL/TLS

Giao thức bắt tay của SSL

35

duyn@uit.edu.vn

- **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 gửi 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 gửi cho nhau thông điệp finish.

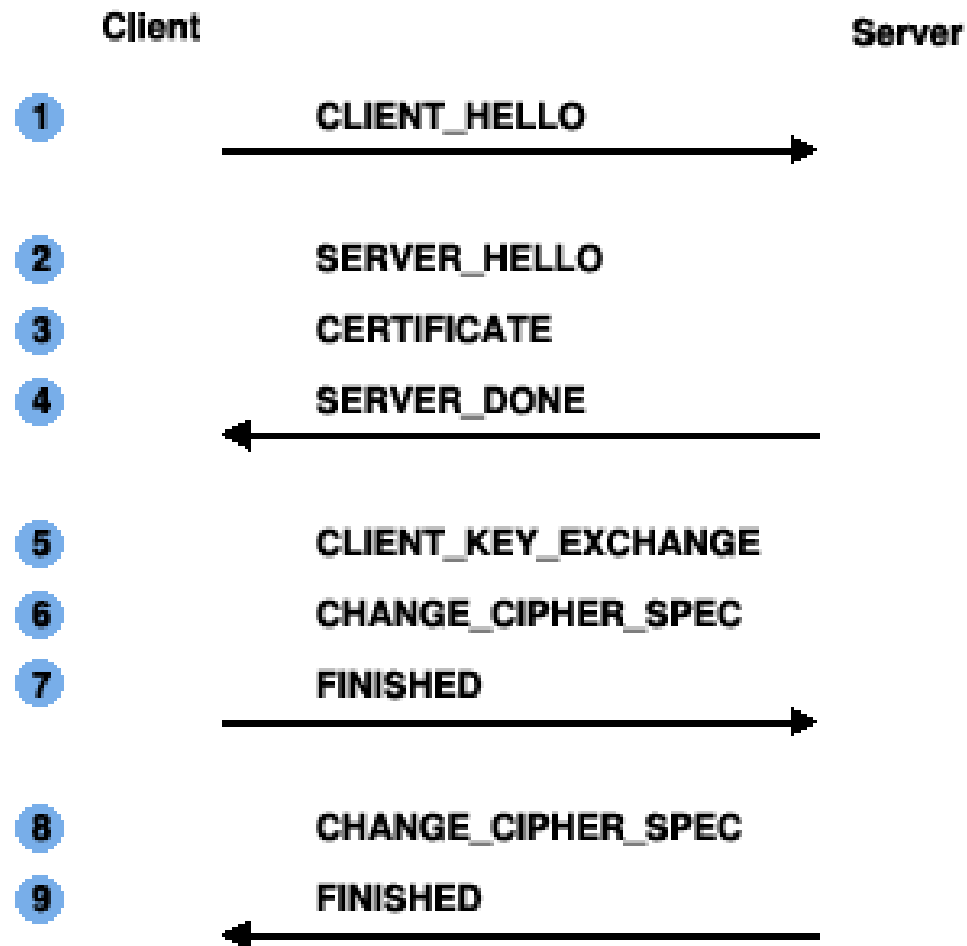
SSL/TLS

Quá trình thiết lập kết nối SSL

36

duyn@uit.edu.vn

Handshake Flow for a New Session





SSL Client



SSL Server

Client Hello

I want to establish secure connection. I support
<this> version of SSL and <these> ciphers

Server Hello

Ok, I initially accept request. I have chosen <this>
version of SSL and <this> cipher suite

Server's Certificate (optional)

Server Key Exchange (optional)

Here is my public key (if I don't have certificate)

Client Certificate Request (optional)

I want to authenticate you. Send me
your certificate signed by <this> CA

Server Hello Done

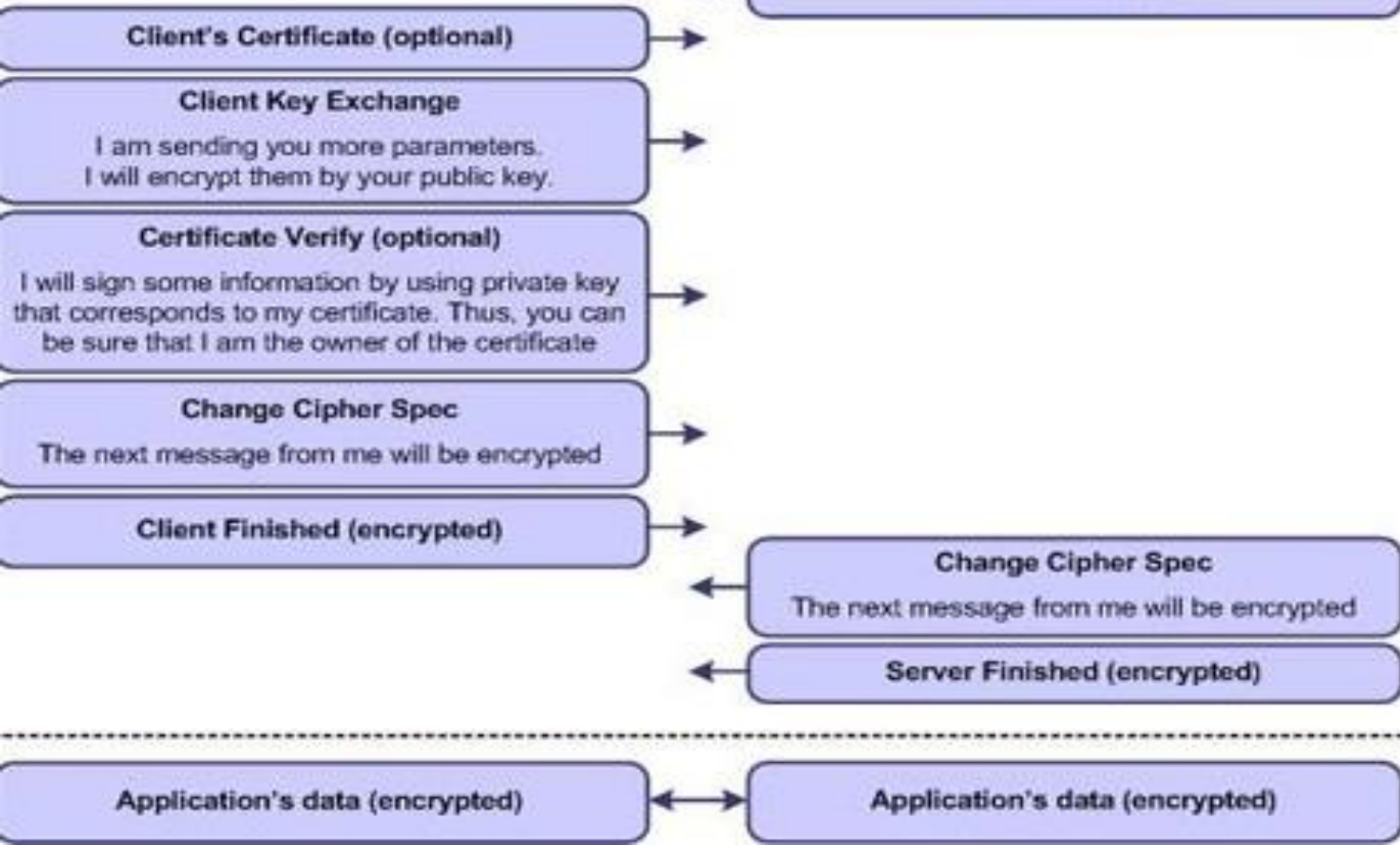
Time



SSL Client



SSL Server



1. Client sends *ClientHello* message.

2. Server acknowledges with *ServerHello* message.

3. Server sends its certificate.

(4. Server requests client's certificate.)

(5. Client sends its certificate.)

6. Client sends *ClientKeyExchange* message.

(7. Client sends a *Certificate Verify* message.)

8. Both send *ChangeCipherSpec* messages.

9. Both send *Finished* messages.

Client
(browser)

Server

Session
key

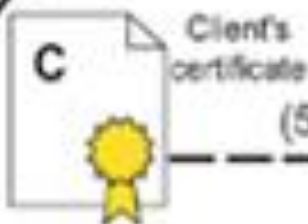
Server's
public key

Server's
private key

Session
key

Digital envelope

Digital signature



Nội dung

40

duyn@uit.edu.vn

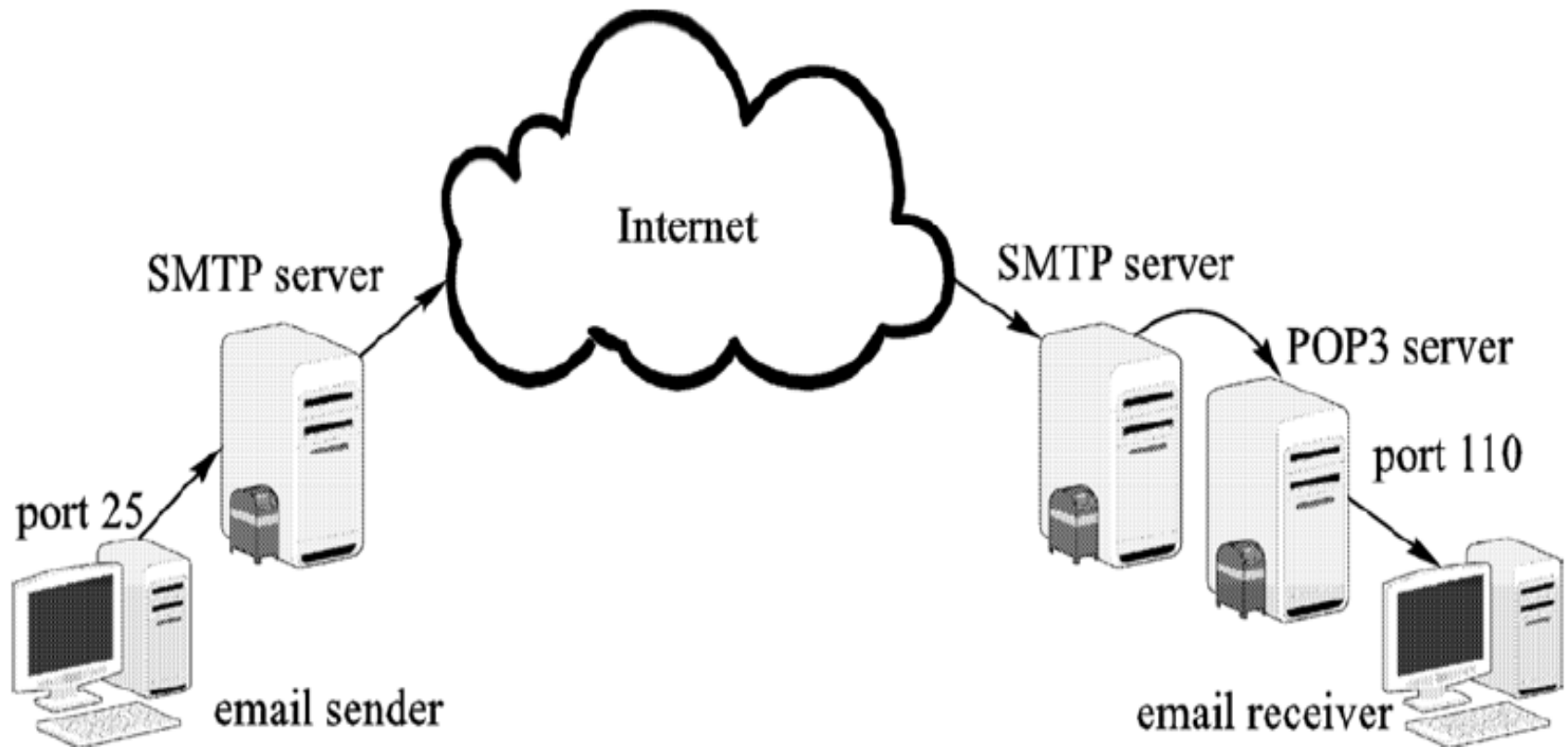
- IP Security
- Secure Socket Layer /Transport Layer Security
- **Pretty Good Privacy**
- Secure Shell

Pretty Good Privacy (PGP)

Tổng quan

41

duyn@uit.edu.vn



SMTP and POP3 flow diagram

Pretty Good Privacy (PGP)

Tổng quan

42

duyn@uit.edu.vn

- Mục đích sử dụng để bảo vệ (encrypt and/or sign) tập tin
- Có thể được sử dụng để bảo vệ e-mail messages
- Có thể sử dụng cho Doanh Nghiệp hay Cá Nhân
- Cryptographic algorithms (IDEA, RSA, SHA-1)
- At <http://www.pgpi.org>
- Phiên bản đầu tiên được phát triển bởi Phil Zimmermann
- RFC 3156

Pretty Good Privacy (PGP)

Tính năng PGP

43

duyn@uit.edu.vn

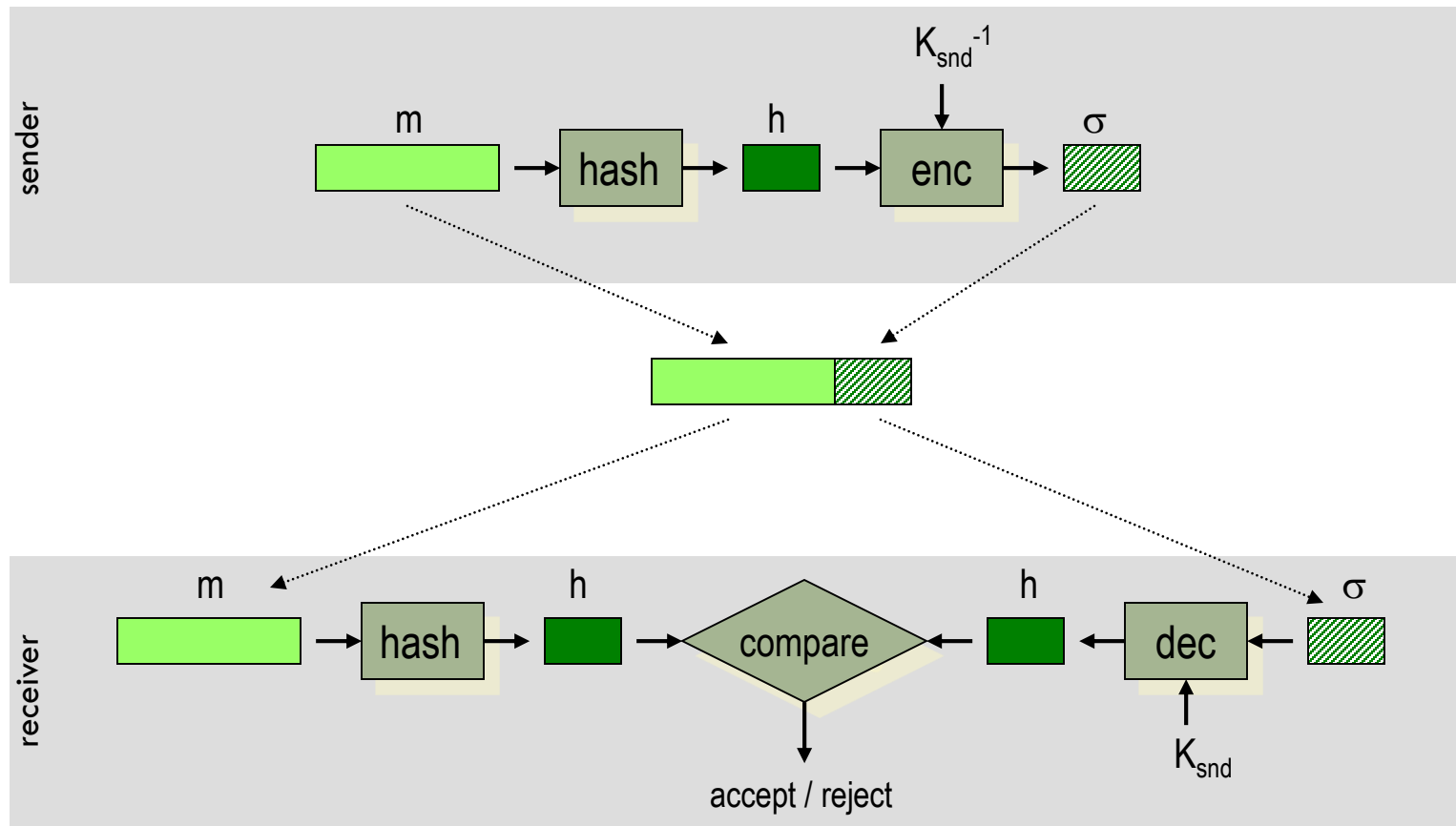
- messages
 - authentication
 - confidentiality
 - compression
 - e-mail compatibility
 - segmentation and reassembly

- key management
 - generation, distribution, and revocation of public/private keys
 - generation and transport of session keys and IVs

Message authentication

44

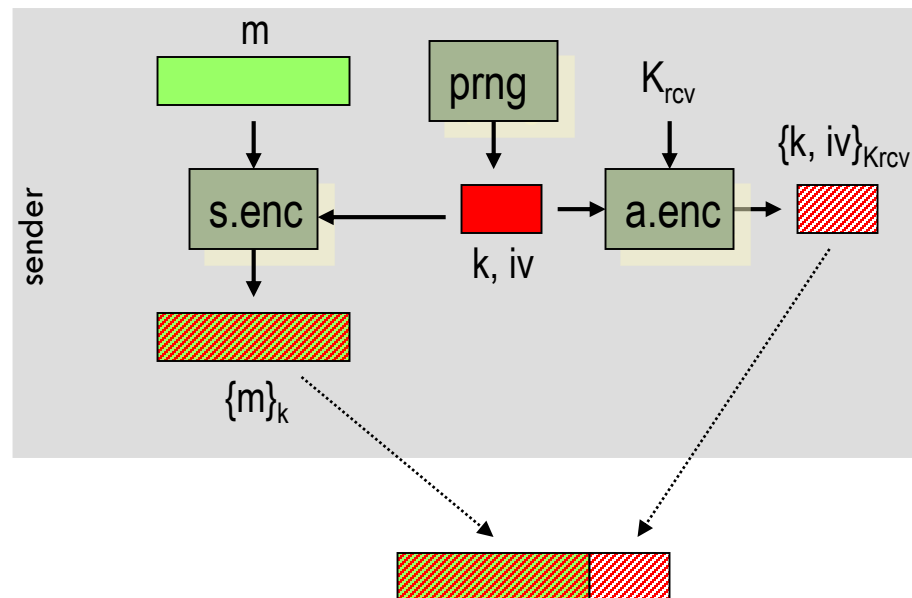
- based on digital signatures
- supported algorithms: RSA/SHA and DSS/SHA



Message confidentiality

45

- supported algorithms:
 - symmetric: CAST, IDEA, 3DES
 - asymmetric: RSA, ElGamal



Compression

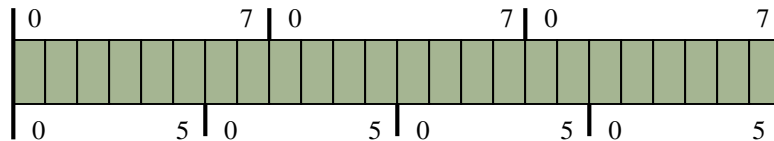
46

- applied after the signature
 - enough to store clear message and signature for later verification
 - it would be possible to dynamically compress messages before signature verification, but ...
 - then all PGP implementations should use the same compression algorithm
 - however, different PGP versions use slightly different compression algorithms
- applied before encryption
 - compression reduces redundancy → makes cryptanalysis harder
- supported algorithm: ZIP

E-mail compatibility

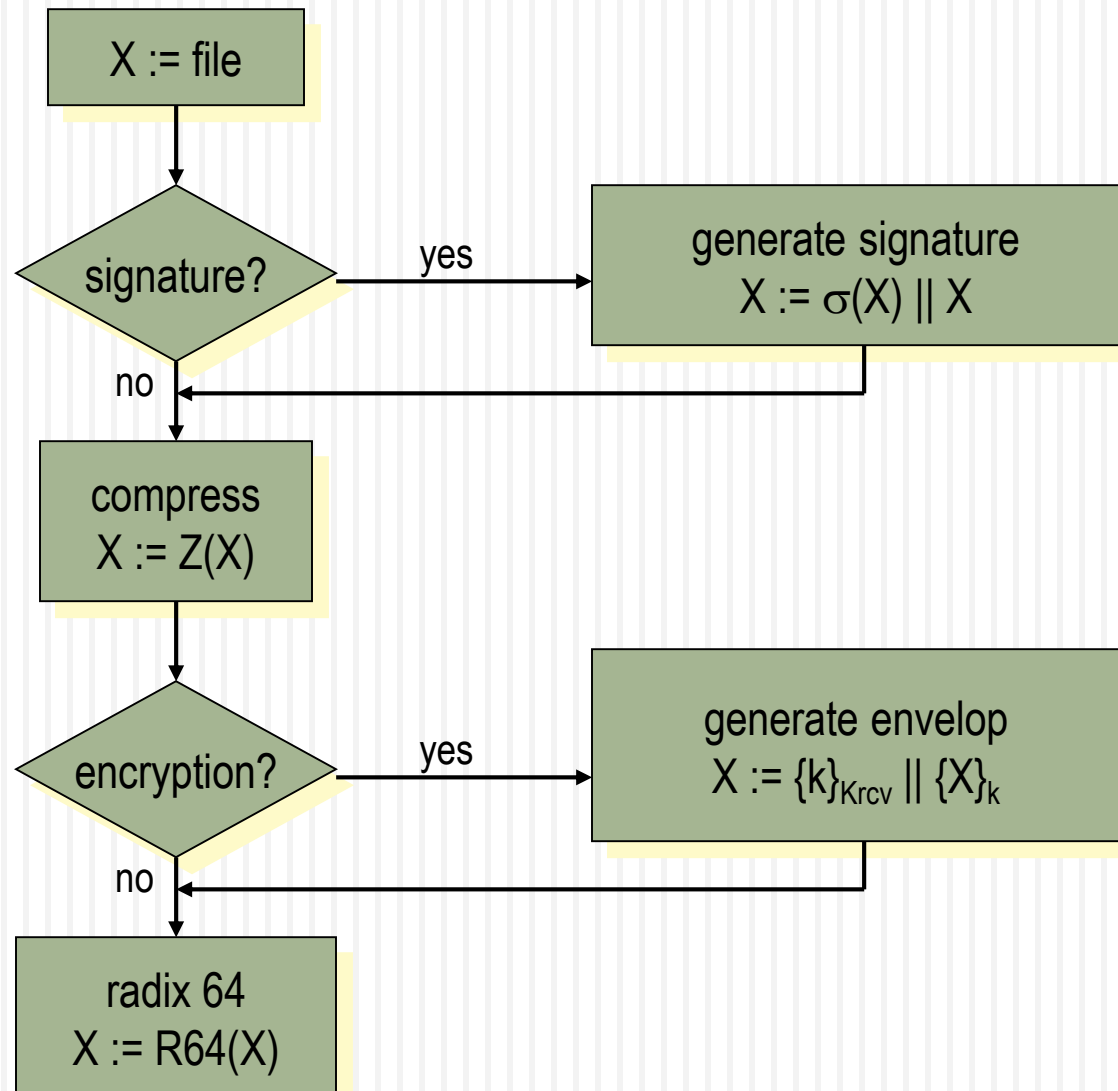
47

- encrypted messages and signatures may contain arbitrary octets
- most e-mail systems support only ASCII characters
- PGP converts an arbitrary binary stream into a stream of printable ASCII characters
- radix 64 conversion: 3 8-bit blocks → 4 6-bit blocks

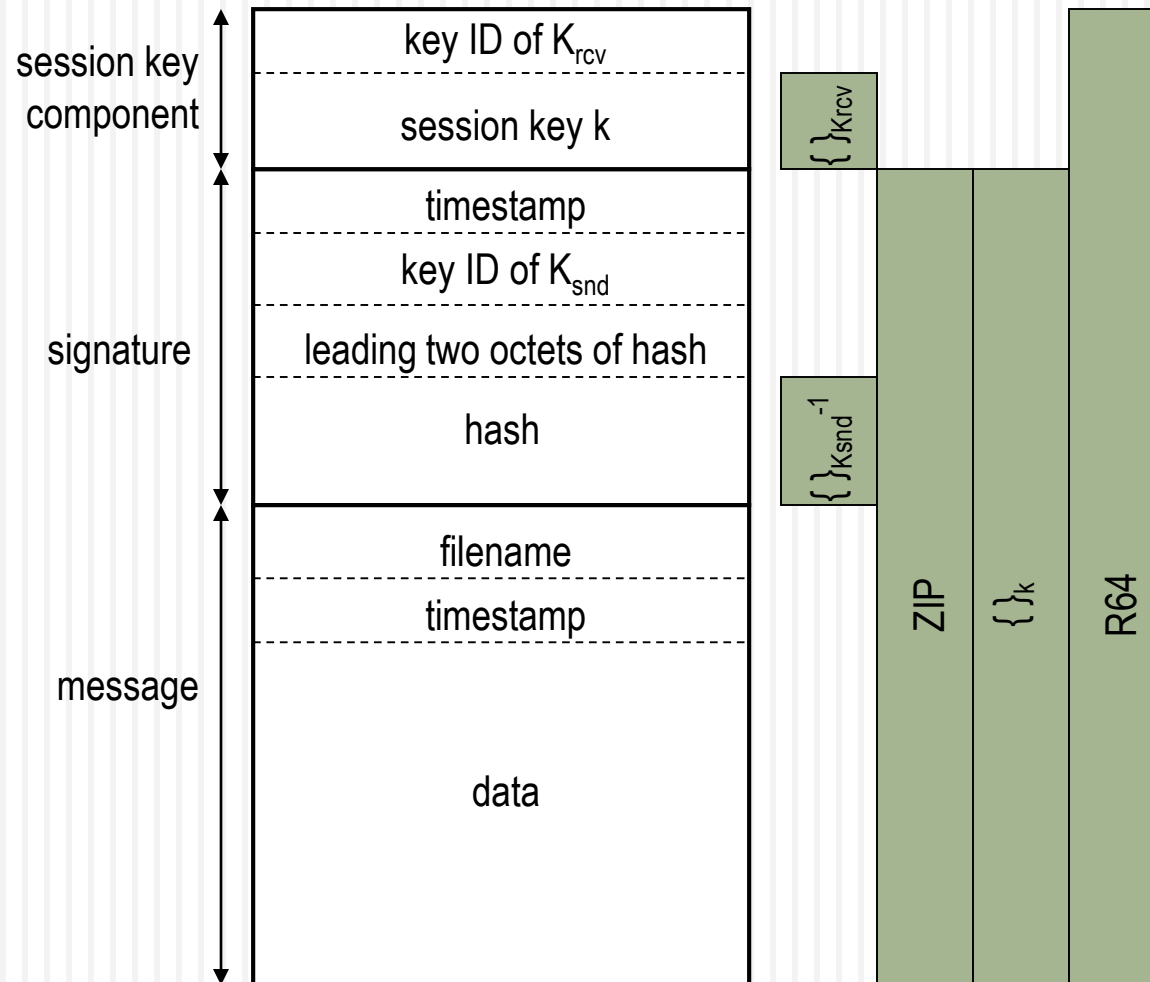


6-bit value	character encoding	6-bit value	character encoding
0	A	52	0
...
25	Z	61	9
26	a	62	+
...	...	63	/
51	z	(pad)	=

Combining services



PGP message format



Key IDs

50

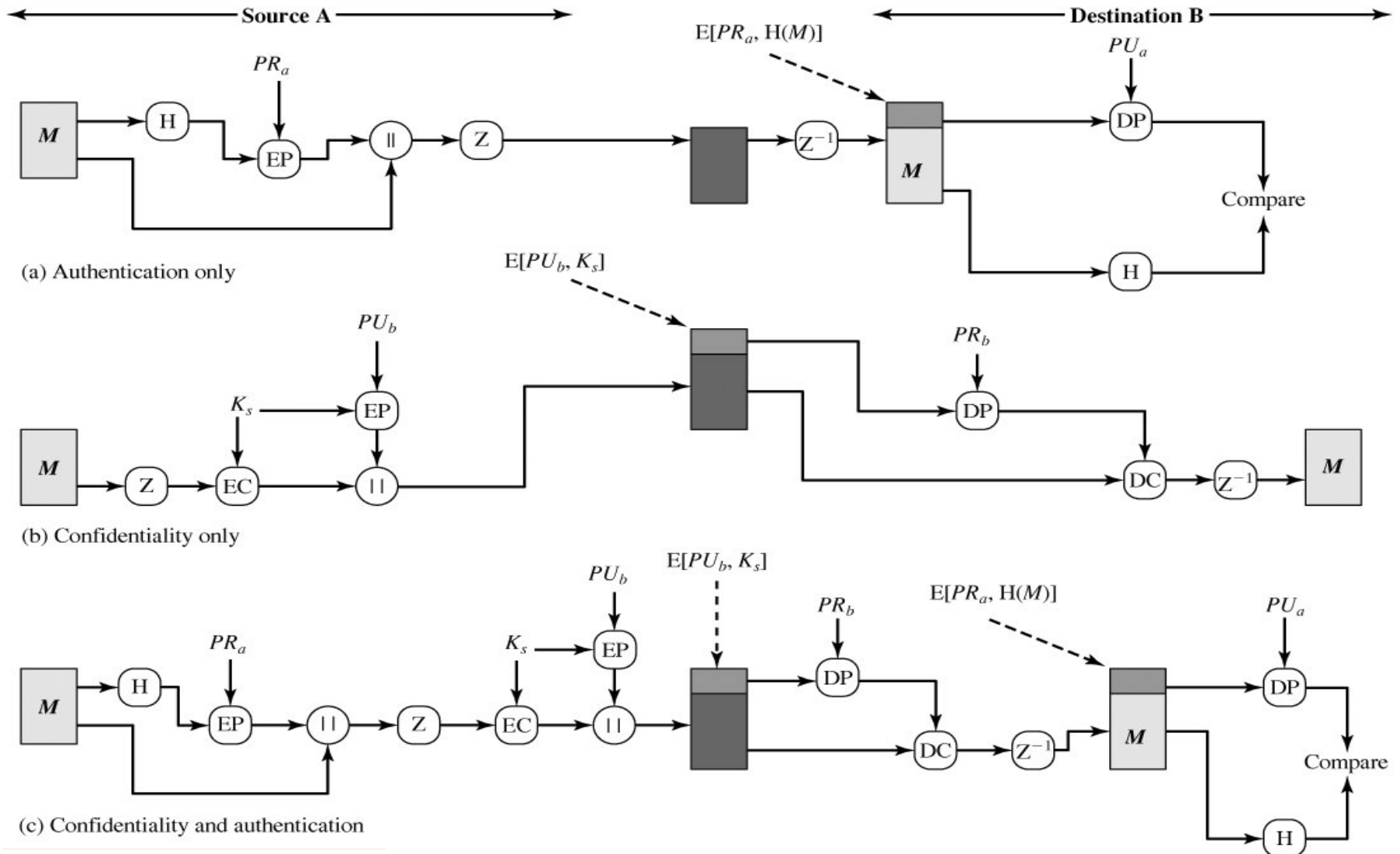
- a user may have several public key – private key pairs
 - which private key to use to decrypt the session key?
 - which public key to use to verify a signature?
- transmitting the whole public key would be wasteful
- associating a random ID to a public key would result in management burden
- PGP key ID: least significant 64 bits of the public key
 - unique within a user with very high probability

Pretty Good Privacy (PGP)

Các chức năng của PGP

51

duyn@uit.edu.vn



Pretty Good Privacy (PGP)

Các chức năng của PGP

52

duyn@uit.edu.vn

➤ Chú thích:

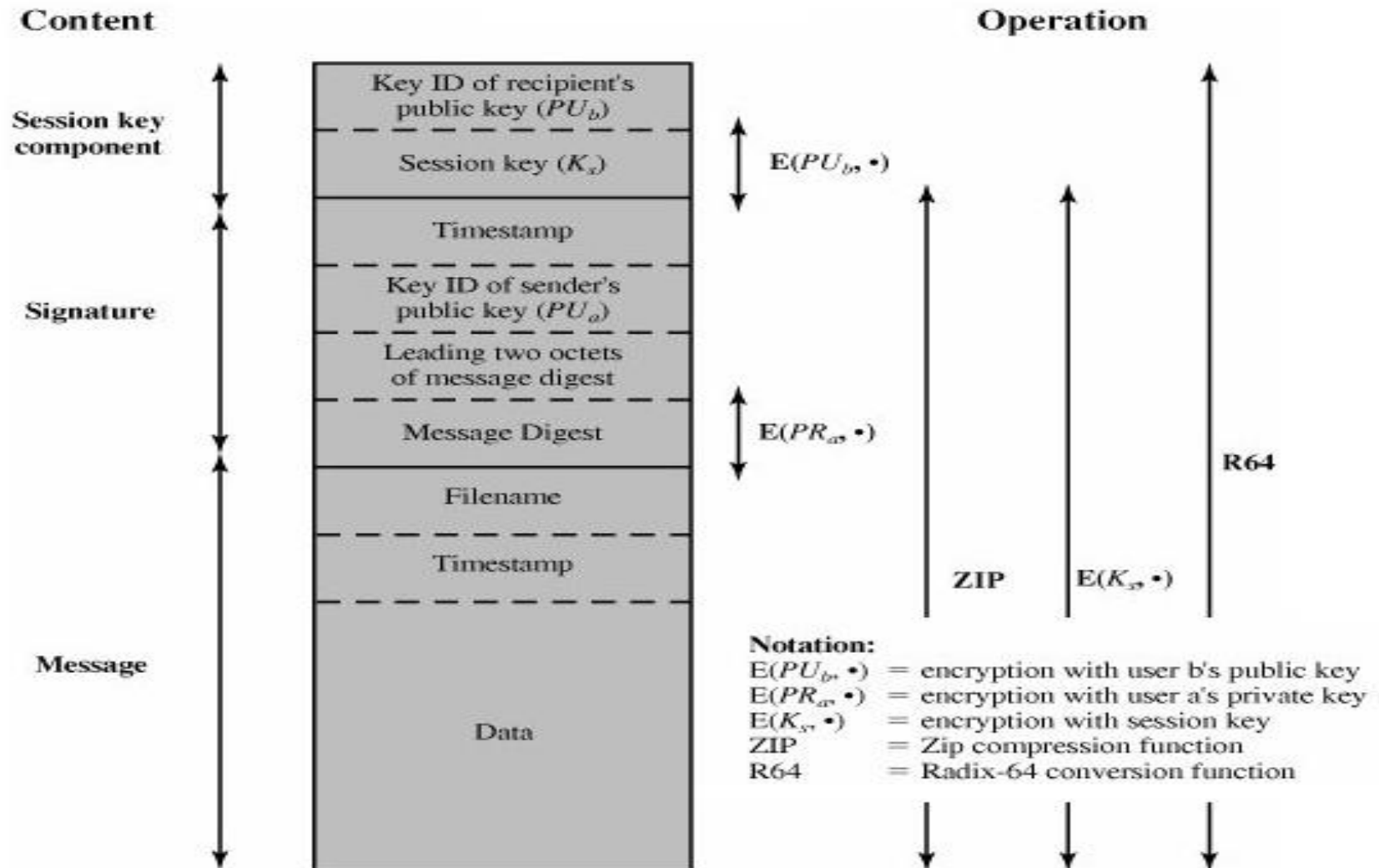
- K_s : session key dùng trong mã hoá symmetric
- Pr_a : private key của user A
- PU_a : public key of user A
- EP: mã hoá public-key (asymmetric)
- DP: giải mã public-key (asymmetric)
- EC: mã hoá symmetric
- DC: giải mã symmetric
- H: hàm băm
- ||: kết nối, ghép chuỗi
- Z: nén sử dụng giải thuật ZIP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

Pretty Good Privacy (PGP)

Định dạng tổng quát của một thông điệp PGP

53

duyn@uit.edu.vn

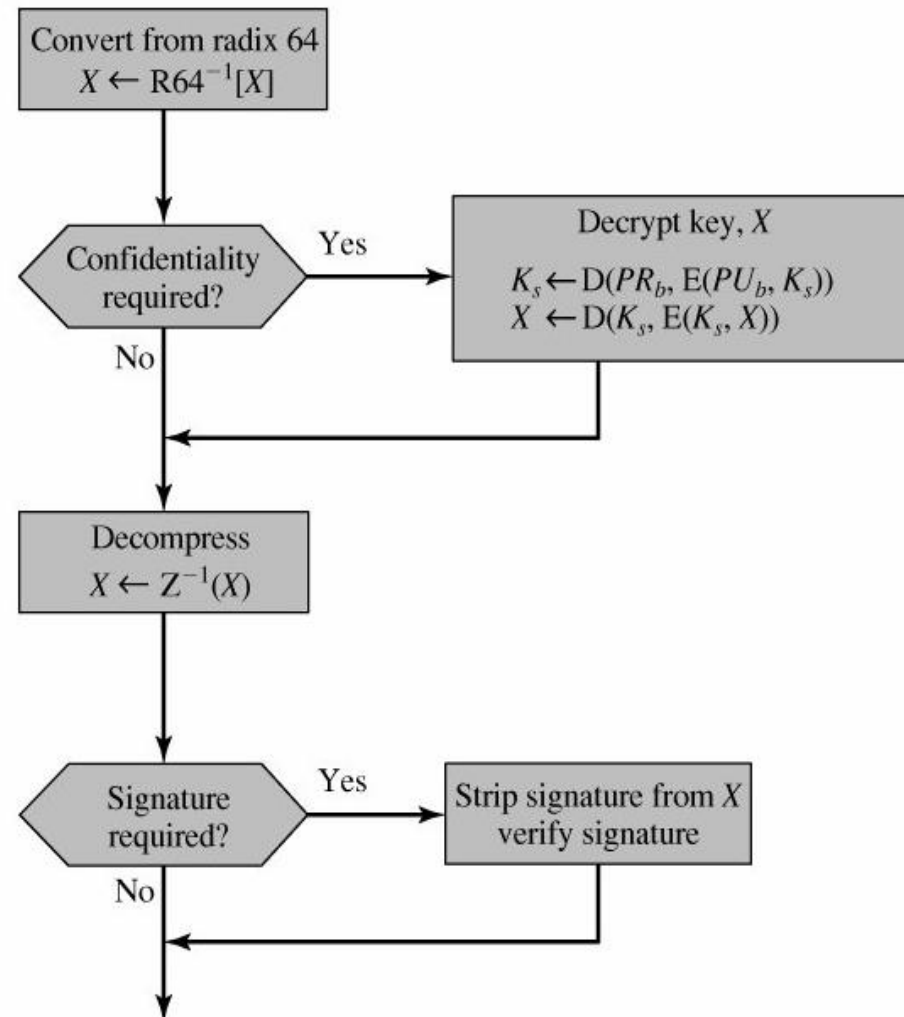
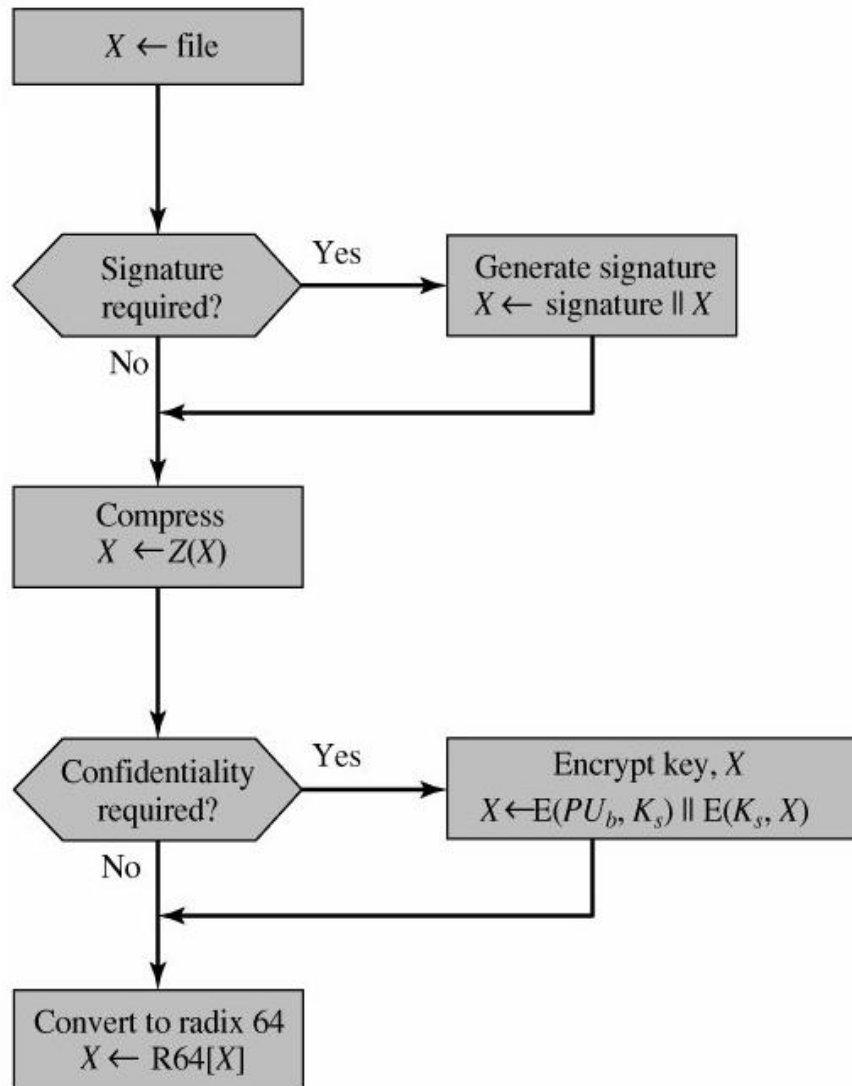


Pretty Good Privacy (PGP)

Truyền và nhận thông điệp PGP

54

duyn@uit.edu.vn



Pretty Good Privacy (PGP)

Một số đặc tính của PGP

55

duyn@uit.edu.vn

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

Secure/Multipurpose Internet Mail Extensions (S/MIME)

56

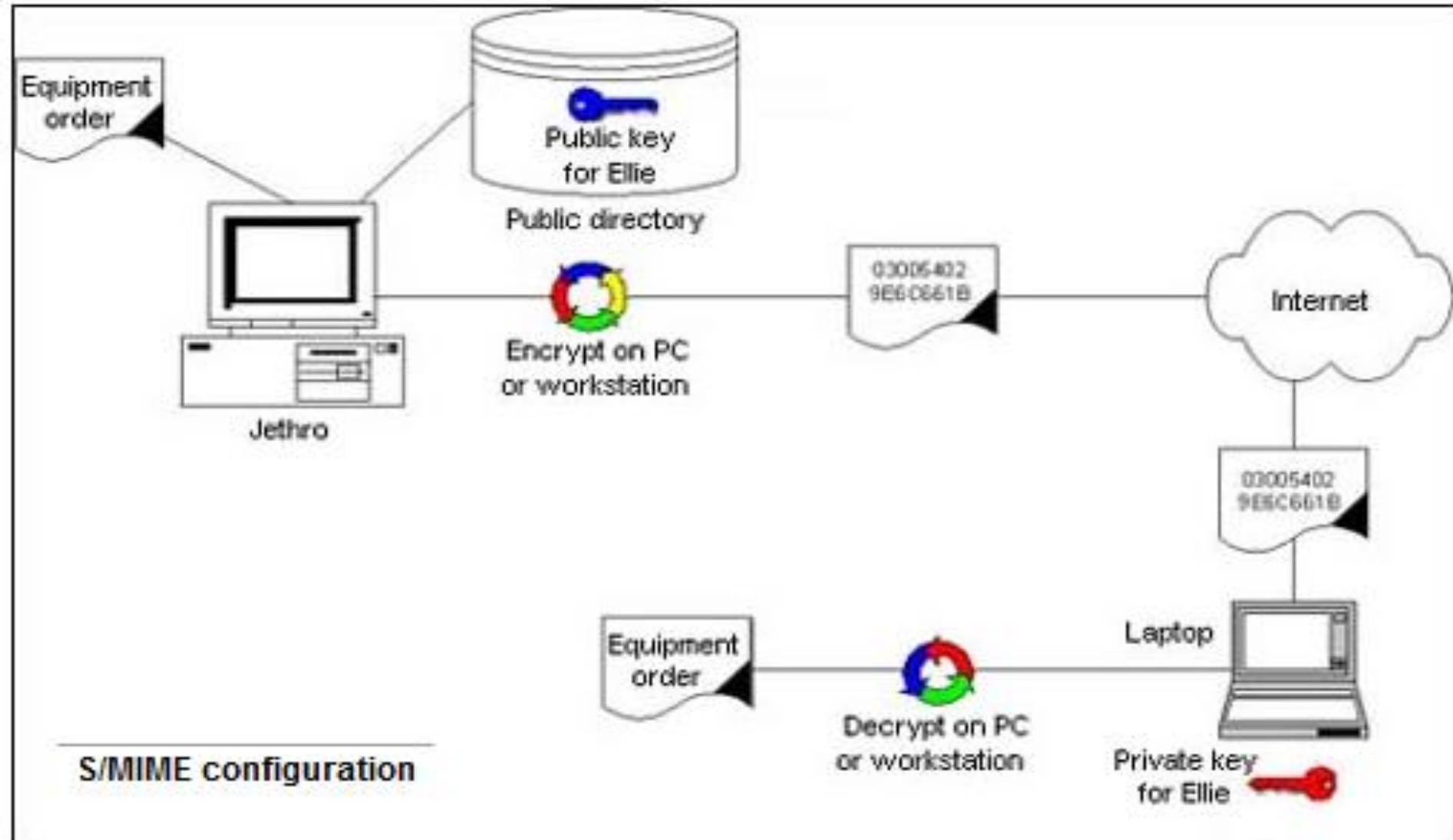
duyn@uit.edu.vn

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

S/MIME

57

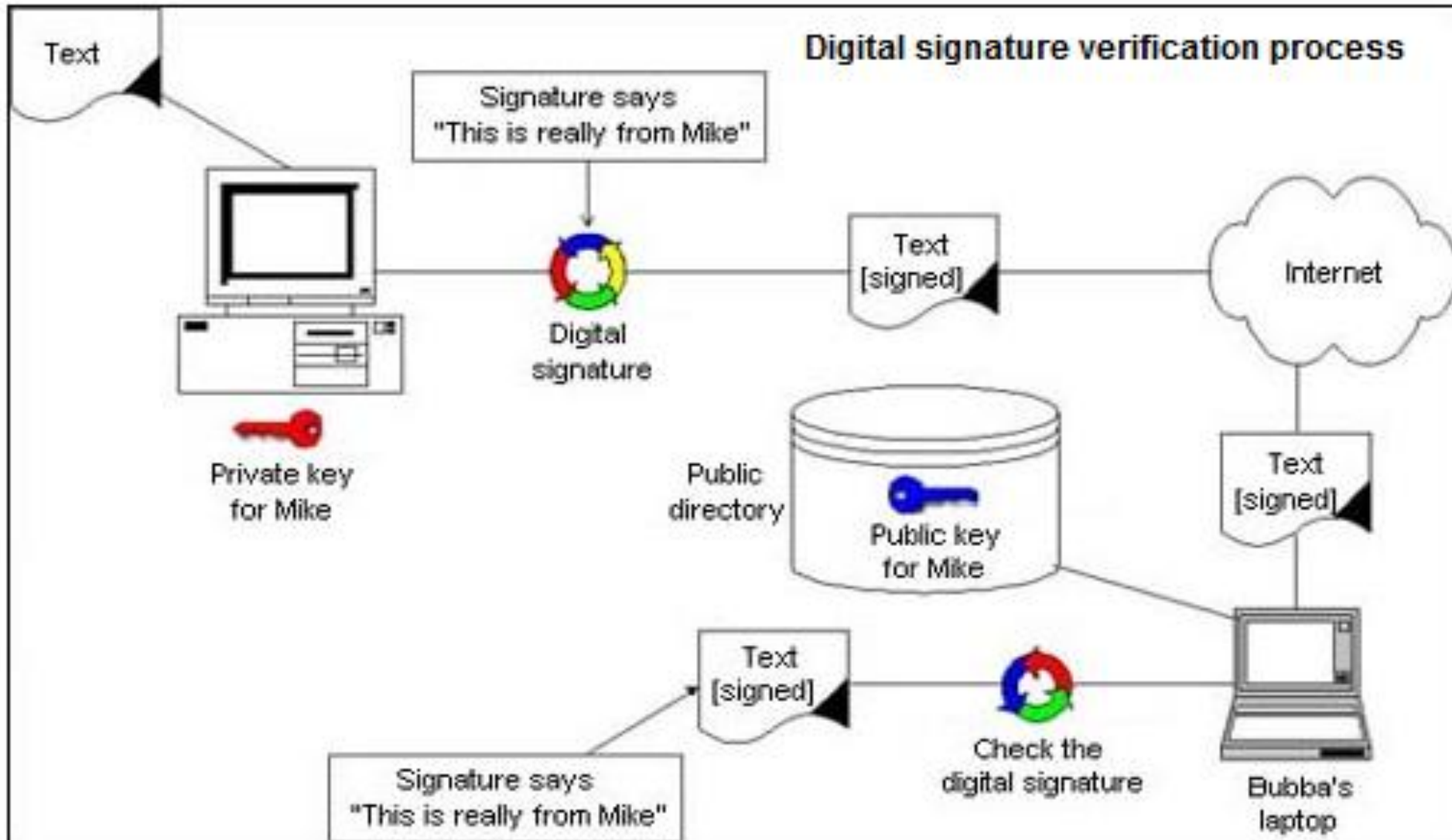
duyn@uit.edu.vn



S/MIME

58

duyn@uit.edu.vn



S/MIME

59

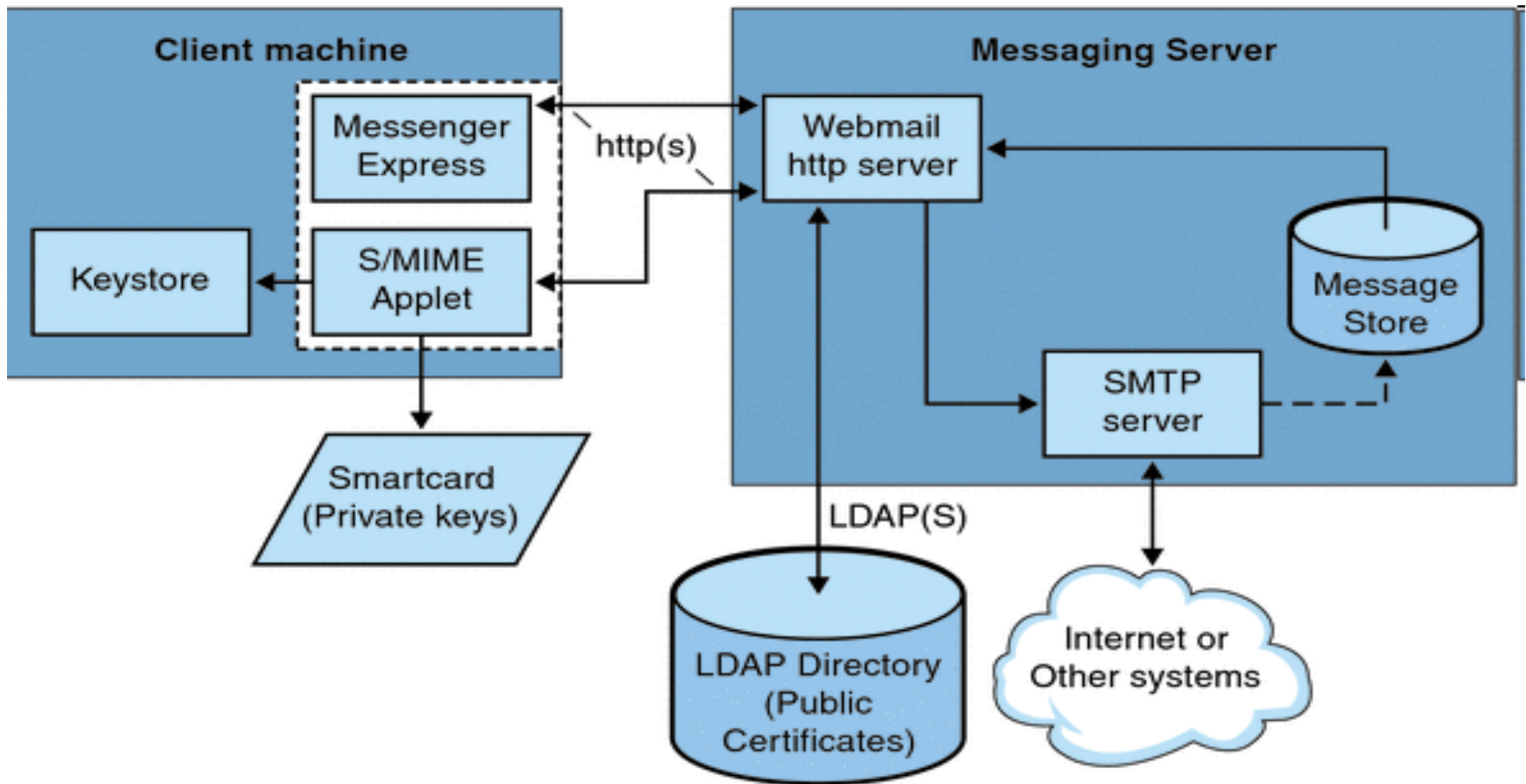
duyn@uit.edu.vn

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

S/MIME

60

duyn@uit.edu.vn













S/MIME

61

duyn@uit.edu.vn

File Edit View Insert Format Tools Actions Help

Send         Options...  

To: Ellie-May@thevendorcompany.xyz

Cc:

Subject: Here is my signed message -

Message Options  

Message settings

 Importance: Normal

 Sensitivity: Normal

Security

 ☐ Encrypt message contents and attachments

 ☒ Add digital signature to outgoing message

Delivery options

 ☐ Have replies sent to: 

☒ Save sent message to: Sent Items 

☐ Do not deliver before: 

☐ Expires after: 

Send message using: NTMain 

S/MIME

62

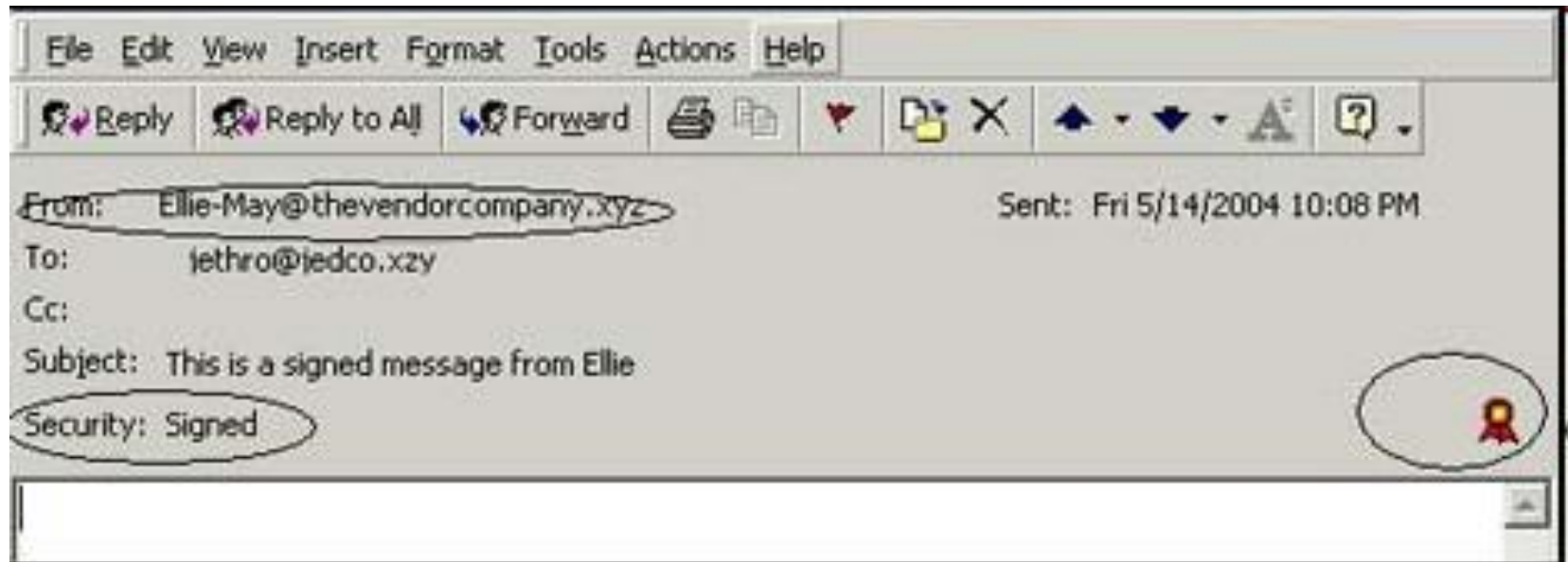
duyn@uit.edu.vn



S/MIME

63

duyn@uit.edu.vn



Nội dung

64

duyn@uit.edu.vn

- IP Security
- Secure Socket Layer /Transport Layer Security
- Pretty Good Privacy
- **Secure Shell**

Secure Shell

Tổng quan

65

duyn@uit.edu.vn

- SSH được định nghĩa trong RFC 4251.
- SSH sử dụng cổng TCP 22.
- SSH có thể hoạt động trên các platform 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.

Secure Shell

Tổng quan

66

duyn@uit.edu.vn

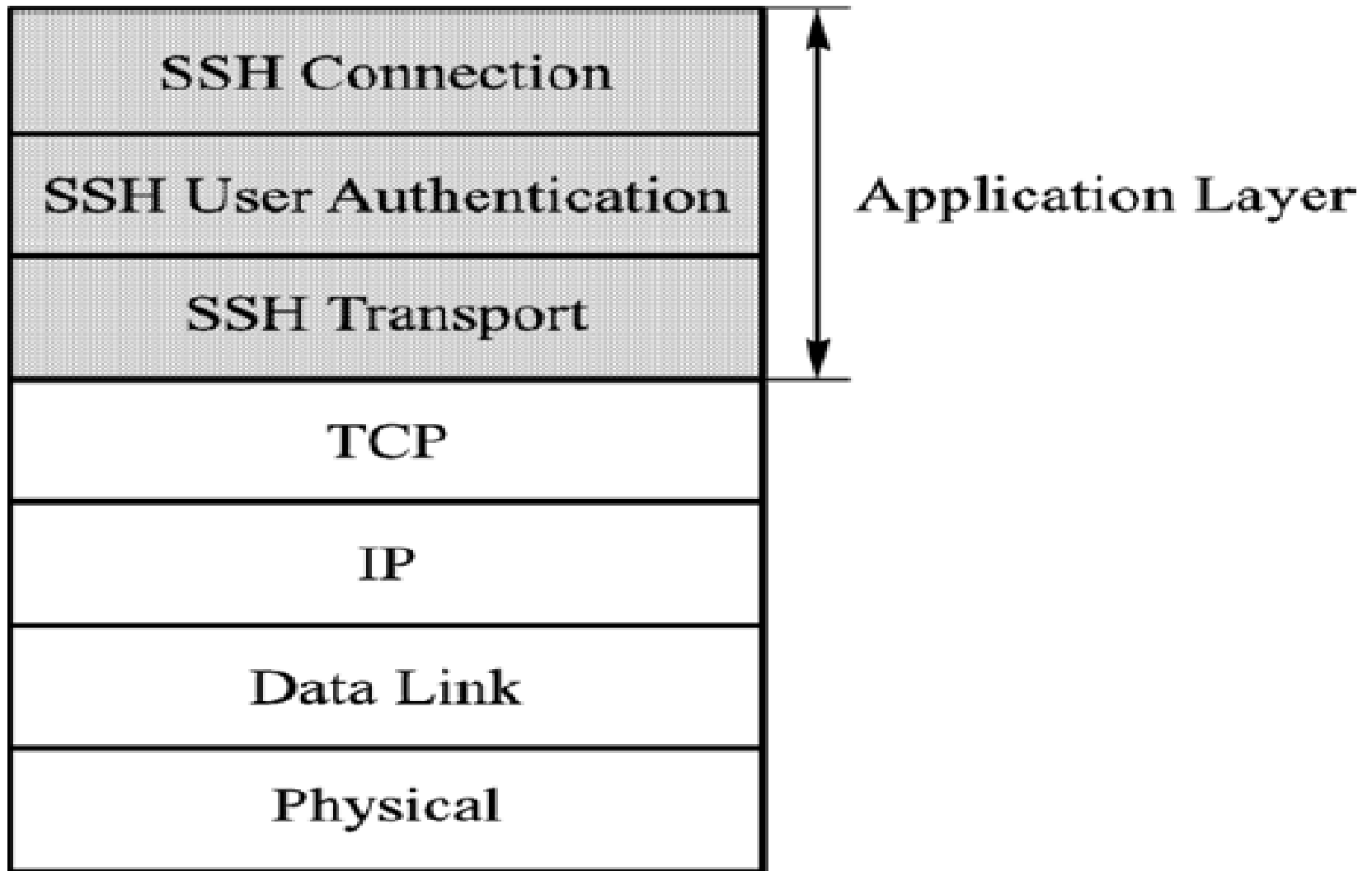
- SSH tạo ra một kết nối bảo mật giữa hai máy tính sử dụng các giải thuật mã hoá và chứng thực.
- Có khả năng nén dữ liệu, bảo mật cho dữ liệu truyền (SFTP) và sao chép file (SCP).
- Là giao thức ứng dụng client-server. SSH được chia thành 3 lớp trong lớp ứng dụng của mô hình mạng TCP/IP:
 - Connection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

Secure Shell

Tổng quan

67

duyn@uit.edu.vn



Secure Shell

Cách thức hoạt động

68

duyn@uit.edu.vn

- SSH được thực hiện qua 3 bước:

1. Định danh host:

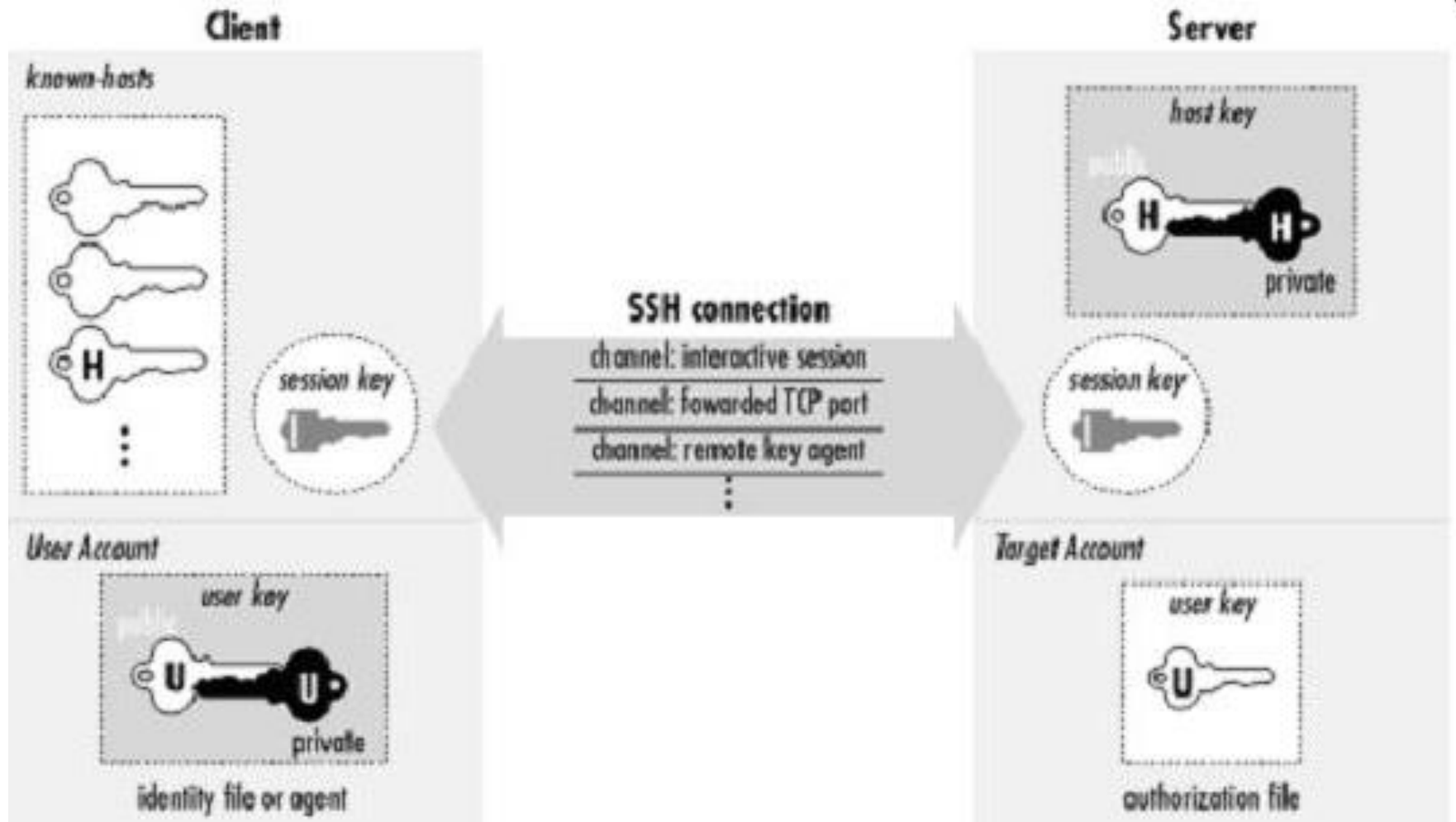
- Việc định danh host được thực hiện qua việc trao đổi khoá. Mỗi máy tính có hỗ trợ kiểu truyền thông SSH có một khoá định danh duy nhất. Khoá này gồm hai thành phần: khoá riêng và khoá công khai. Khoá công khai được sử dụng khi cần trao đổi giữa các máy chủ với nhau trong phiên làm việc SSH, dữ liệu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

Secure Shell

Cách thức hoạt động

69

duyn@uit.edu.vn



Secure Shell

Cách thức hoạt động

70

duyn@uit.edu.vn

2. Mã hoá:

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

Secure Shell

Cách thức hoạt động

71

duyn@uit.edu.vn

3. Chứng thực:

- Mọi 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.

Question ???