Security in Computer Networks

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

Audio/Video recordings of this lecture are available on-line at:

http://www.cse.wustl.edu/~jain/cse473-22/

Student Questions

Overview

1. Secret Key Encryption
2. Public Key Encryption
3. Hash Functions, Digital Signature, Digital Certificates
4. Secure Email

Not Covered:, SSL, IKE, WEP, IPSec, VPN, Firewalls, Intrusion Detection. These topics will not be included in the exam.

Note: This class lecture is based on Chapter 8 of the textbook (Kurose and Ross) and the figures provided by the authors.

Student Questions

Security Requirements

- **Integrity**: Received = sent?
- **Availability**: Legal users should be able to use.
  Ping continuously ⇒ No useful work gets done.
- **Confidentiality and Privacy**:
  No snooping or wiretapping
- **Authentication**: You are who you say you are.
  A student at Dartmouth posing as a professor canceled the exam.
- **Authorization** = Access Control
  Only authorized users get to the data
- **Non-repudiation**: Neither sender nor receiver can deny the existence of a message

Student Questions

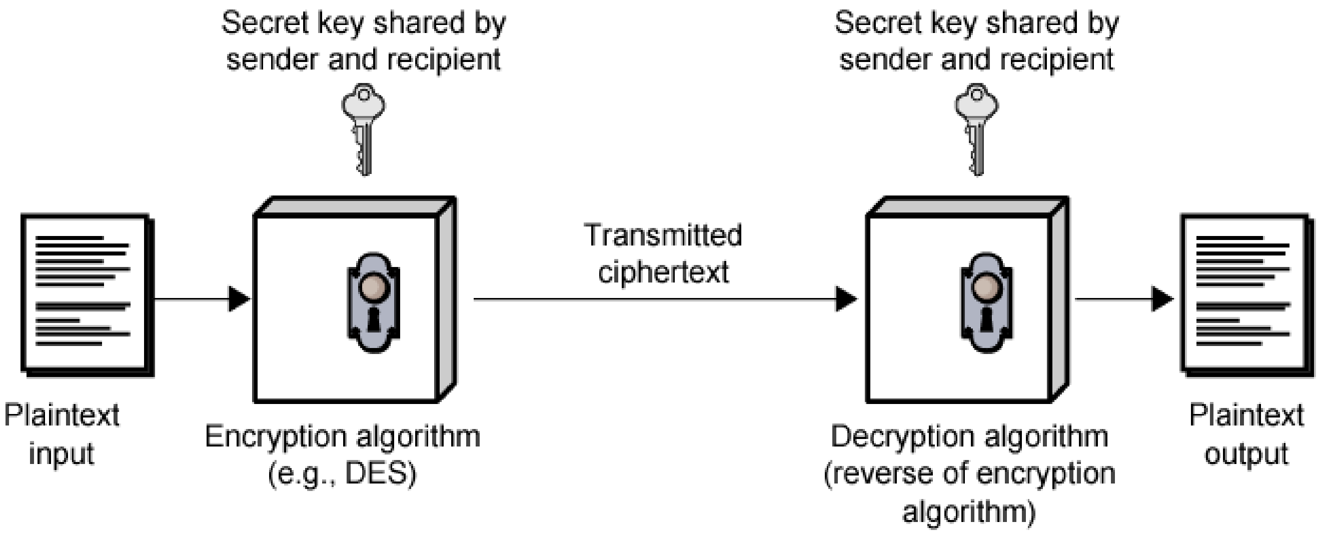
Secret Key Encryption: Overview

1. Concept: Secret Key Encryption
2. Method: Block Encryption
3. Improvement: Cipher Block Chaining (CBC)
4. Standards: DES, 3DES, AES

Student Questions

Secret Key Encryption

- Also known as symmetric key encryption
- Encrypted_Message = Encrypt(Key, Message)
- Message = Decrypt(Key, Encrypted_Message)
- Example: Encrypt = division
- 433 = 48 R 1 (using divisor of 9)


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

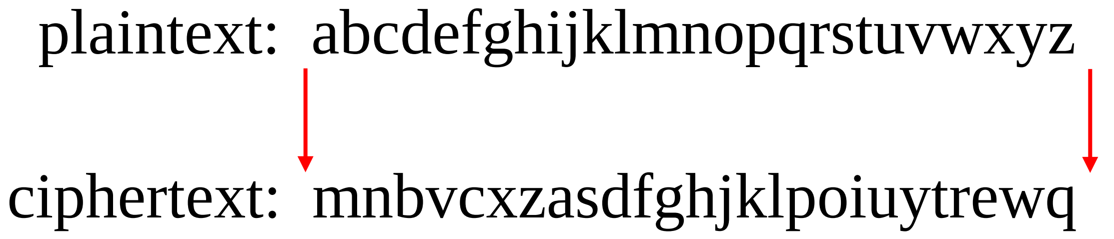
Student Questions

- What are the disadvantages of secret key encryption?

1. *Secret is known to two people. Either person can loose it.*
2. *It needs to be exchanged securely.*

Secret Key: A Simple Example

- ❑ **Substitution**: Substituting one thing for another
- ❑ **Monoalphabetic**: substitute one letter for another



plaintext: abcdefghijklmnopqrstuvwxyz

ciphertext: mnbvcxzasdfghjklpoiuytrewq

E.g.:

Plaintext: bob. i love you. alice

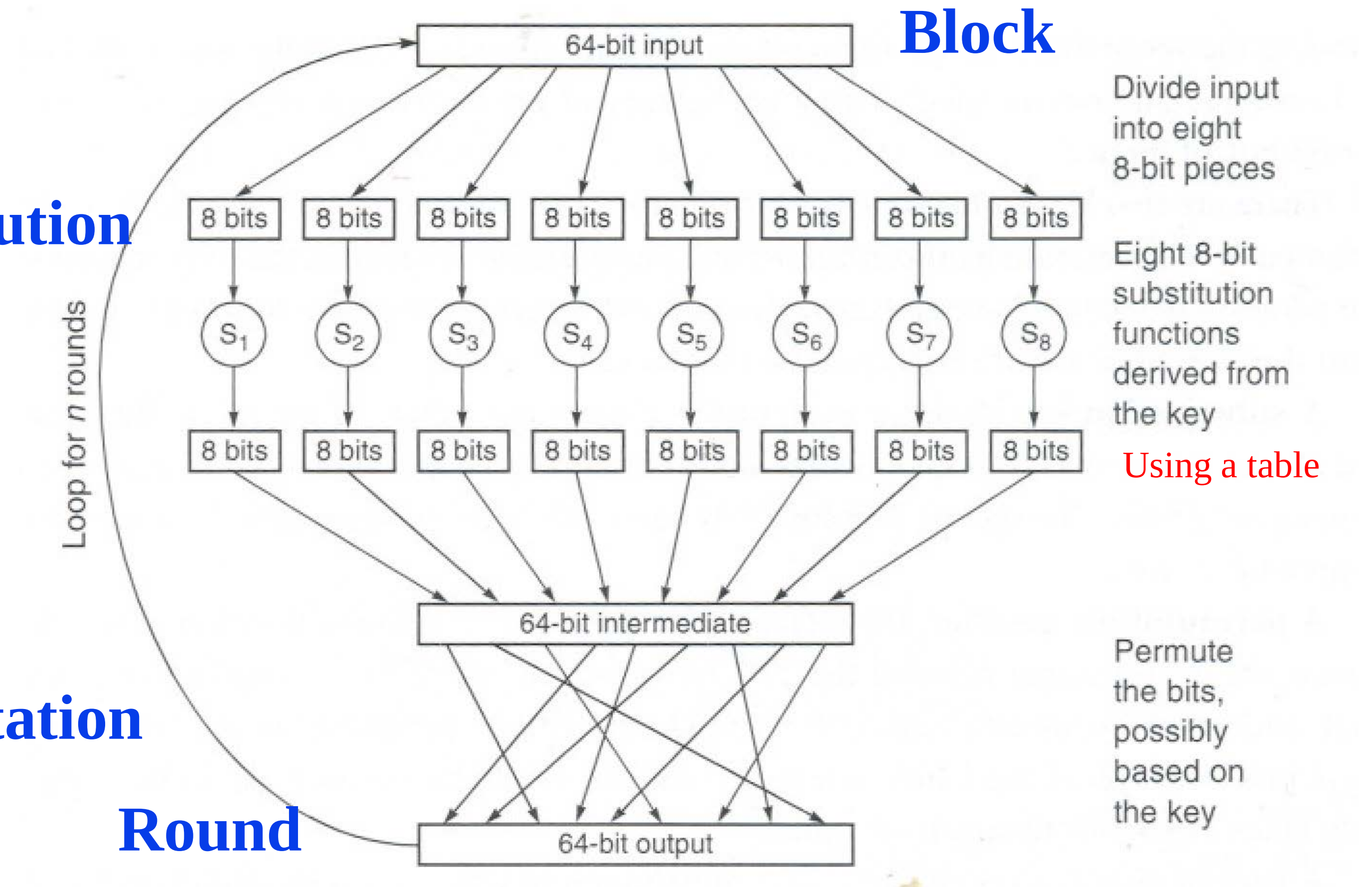
ciphertext: nkn. s gktc wky. mgsbc

- ❑ **Polyalphabetic**: Use multiple substitutions C1, C2, …
  Substitution selected depends upon the position
  ⇒Same letter coded differently in different position

Student Questions

Block Encryption

- Block Encryption



Student Questions

- Does the permutation happen the same way for each iteration? Or does that also change?

Both substitution and permutations for each round are specified by the encryption scheme.

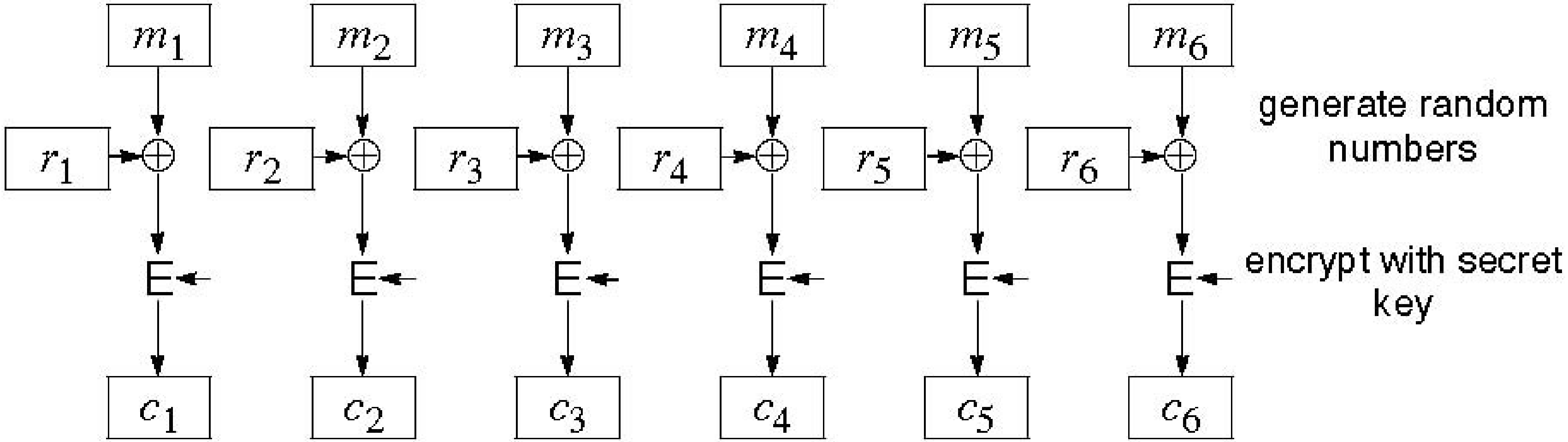
Block Encryption (Cont)

- Short block length ⇒ tabular attack
- 64-bit block
- Transformations:
  - Substitution: replace k-bit input blocks with k-bit output blocks
  - Permutation: move input bits around.
    1 → 13, 2 → 61, etc.
- Round: Substitution round followed by permutation round and so on. Diffusion + Confusion.
  Diffusion ⇒ 1 bit change in input changes many bits in output
  Confusion ⇒ Relationship between input and output is complex

Student Questions

Cipher Block Chaining (CBC)

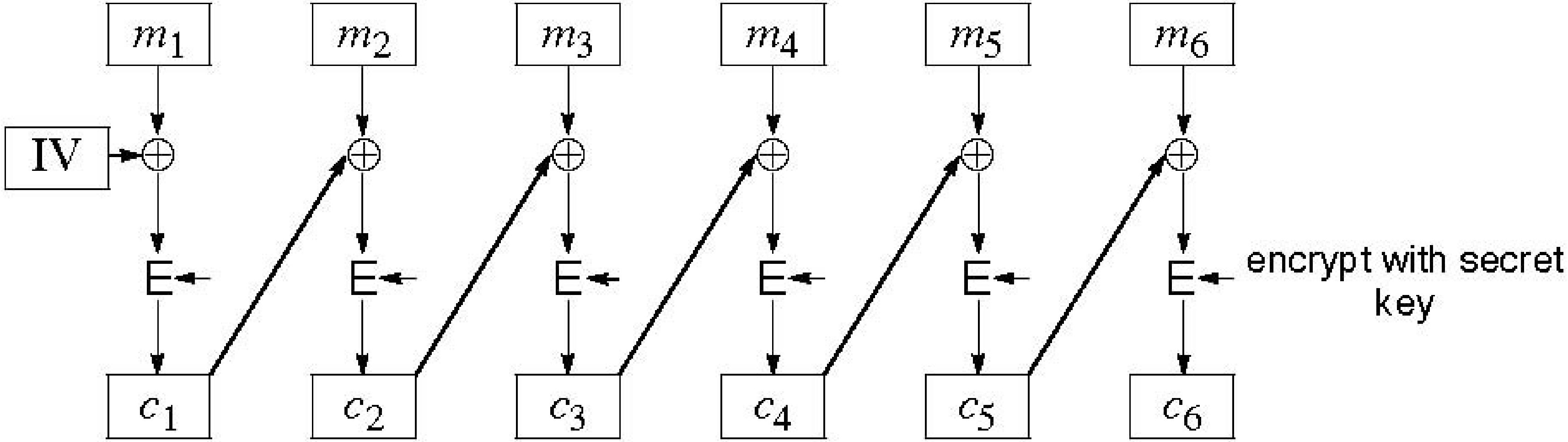
- Goal: Same message encoded differently
- Add a random number before encoding



Student Questions

CBC (Cont)

- Use C_i as random number for i+1



- Need Initial Value (IV)
- no IV ⇒ Same output for same message
  ⇒ one can guess changed blocks
- Example: Continue Holding, Start Bombing

Student Questions

- Does CBC have good diffusion as well?

Yes. CBC distributes one bit change in a block to all blocks.

- Is the IV also shared between the sender and recipient?

IV is sent in clear

Data Encryption Standard (DES)

- Published by NIST in 1977
- For commercial and *unclassified* government applications
- 8 octet (64 bit) key.
  Each octet with 1 odd parity bit ⇒ 56-bit key
- Efficient hardware implementation
- Used in most financial transactions
- Computing power goes up 1 bit every 2 years
- 56-bit was secure in 1977 but is not secure today
- Now we use DES three times ⇒ Triple DES = 3DES
  Cipher Text= DES(key1, DES(key2, DES(key1, Plain Text)))

Student Questions

Advanced Encryption Standard (AES)

- Designed in 1997-2001 by National Institute of Standards and Technology (NIST)
- Federal information processing standard (FIPS 197)
- Symmetric block cipher, Block length 128 bits
- Key lengths 128, 192, and 256 bits.
  Full key is used. No parity bit in the byte.
  Memory may use 9-bits to store a byte.

Student Questions

Secret Key Encryption: Review

1. Secret key encryption requires a shared secret key
2. Block encryption, e.g., DES, 3DES, AES break into fixed size blocks and encrypt
3. CBC is one of many modes are used to ensure that the same plain text results in different cipher text.

Ref: Section 8.1, 8.2.1, Review Questions R1, R2, R6, Problems P1-P6

Student Questions

Homework 8A

- [6 points] Consider 3-bit block cipher in the Table below

Plain	000	001	010	011	100	101	110	111
Cipher	110	111	101	100	011	010	000	001

- Suppose the plaintext is 100101100.

(a) Initially assume that CBC is not used. What is the resulting ciphertext?

(b) Suppose Trudy sniffs the cipher text. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn’t know the specific cipher), what can she surmise?

(c) Now suppose that CBC is used with IV-111. What is the resulting ciphertext?

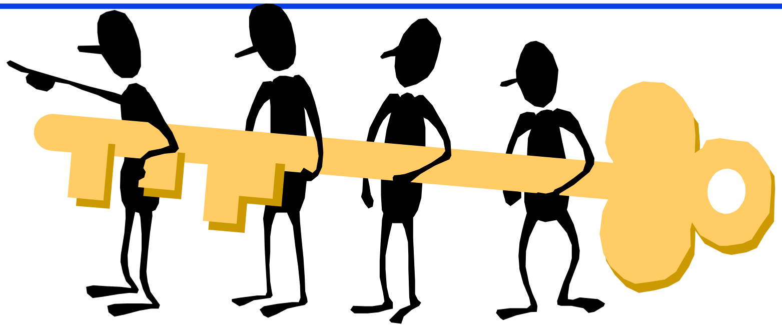
Student Questions

Public Key Encryption

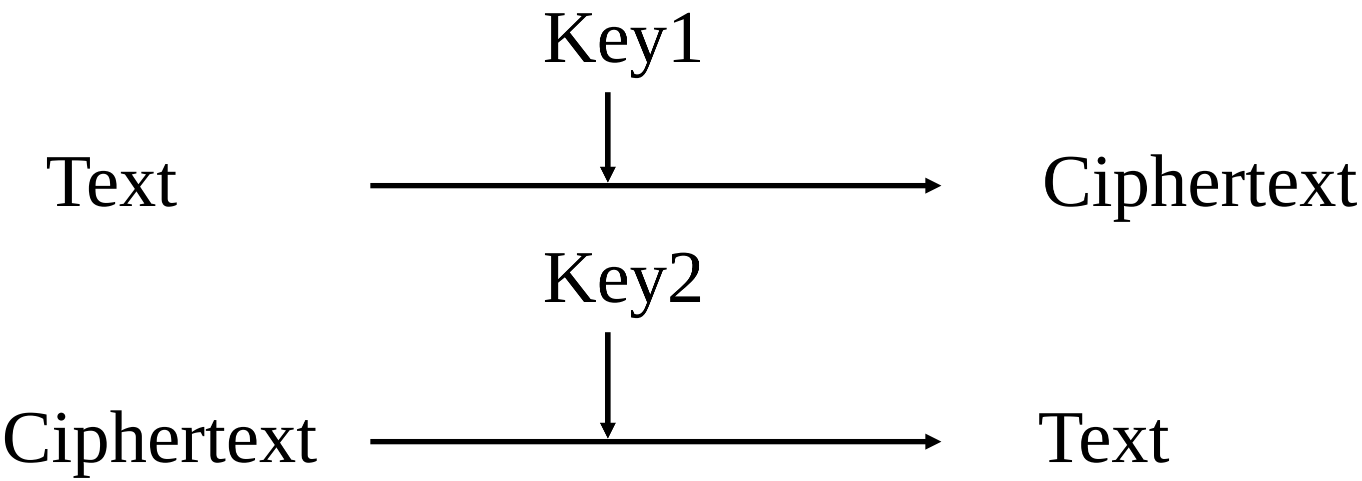
1. Public Key Encryption
2. Modular Arithmetic
3. RSA Public Key Encryption

Student Questions

Public Key Encryption



- ❑ Invented in 1975 by Diffie and Hellman
- ❑ Encrypted_Message = Encrypt(Key1, Message)
- ❑ Message = Decrypt(Key2, Encrypted_Message)



Student Questions

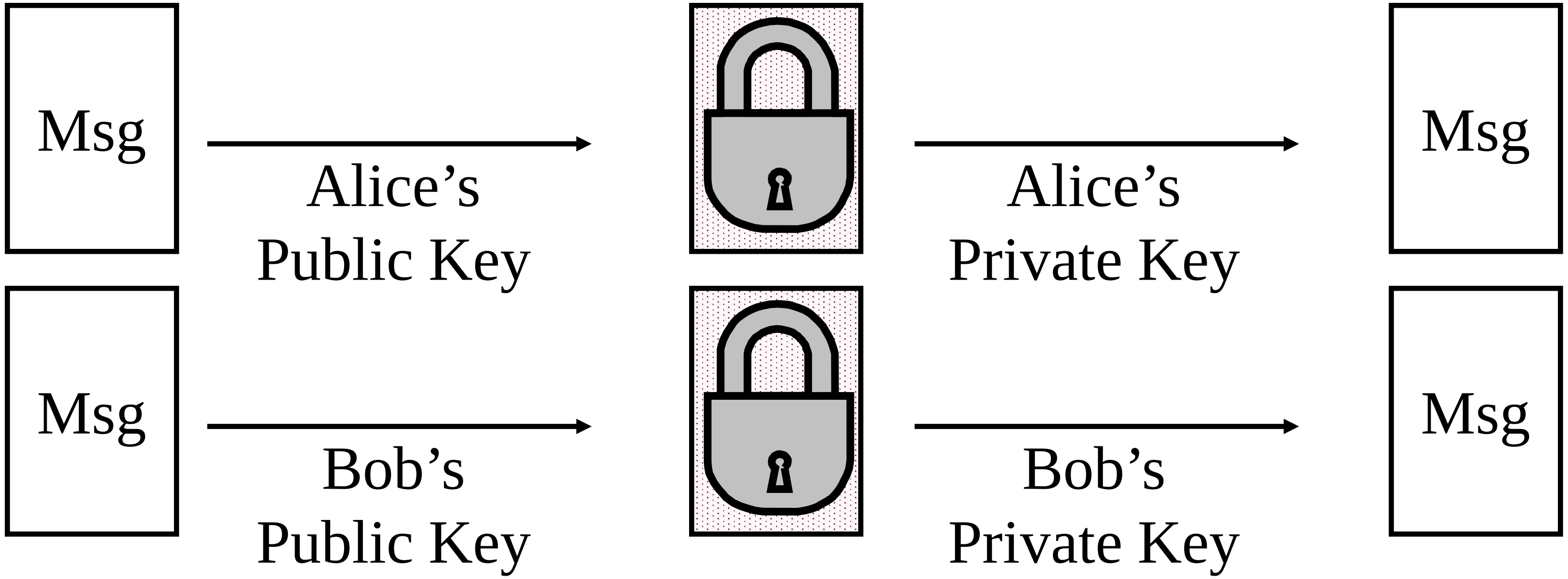
- ❑ Can you define what a semantically secure encryption system is?

You cannot get any more information from ciphertext than from their lengths. Given two plaintexts of equal length and their two respective ciphertexts, cannot determine which ciphertext belongs to which plaintext. Perfect Secrecy: No information at all.

REF: https://en.wikipedia.org/wiki/Semantic_security

Public Key (Cont)

- One key is private and the other is public
- Message=Decrypt(Public_Key, Encrypt(Private_Key, Message))
- Message=Decrypt(Private_Key, Encrypt(Public_Key, Message))
- Encrypted with public key can be decrypted by private key
  Encrypted with private key can be decrypted by public key



Student Questions

- What are the disadvantages of public key encryption?

Lot of computation.

Need very long keys

Public Key Encryption Method

- Rivest, Shamir, and Adelson (RSA) method
- Example: Key1 = <3,187>, Key2 = <107,187>
- Encrypted_Message = m^3 mod 187
- Message = Encrypted_Message^{107} mod 187
- Message = 5
- Encrypted Message = 5^3 = 125 mod 187 = 125
- Message = 125^{107} mod 187 = 5
  = $125^{(64+32+8+2+1)}$ mod 187
  = {(125^{64} mod 187)(125^{32} mod 187)...
  (125^2 mod 187)(125 mod 187)} mod 187

Student Questions

Modular Arithmetic

- $xy \bmod m = (x \bmod m)\,(y \bmod m) \bmod m$
- $x^4 \bmod m = (x^2 \bmod m)(x^2 \bmod m) \bmod m$
- $x^{ij} \bmod m = (x^i \bmod m)^j \bmod m$
- 125 mod 187 = 125
- 125^2 mod 187 = 15625 mod 187 = 104
- 125^4 mod 187 = $(125^2$ mod $187)^2$ mod 187
  = 104^2 mod 187 = 10816 mod 187 = 157
- 125^8 mod 187 = 157^2 mod 187 = 152
- 125^{16} mod 187 = 152^2 mod 187 = 103
- 125^{32} mod 187 = 103^2 mod 187 = 137
- 125^{64} mod 187 = 137^2 mod 187 = 69
- 125^{107}= $125^{64+32+8+2+1}$ mod 187
  = 69×137×152×104×125 mod 187
  = 18679128000 mod 187 = 5
- Need to be able to do additions to convert 107 to 64+32+8+2+1

Notation:
x = y mod z
or
x = y (mod z)
or
x mod z = y

Student Questions

RSA Public Key Encryption

- Ron Rivest, Adi Shamir, and Len Adleman at MIT 1978
- Both plain text M and cipher text C are integers between 0 and n-1.
- Key 1 = {e, n},
  Key 2 = {d, n}
- $C = M^e \bmod n$
  $M = C^d \bmod n$
- How to construct keys:
  - Select two large primes: p, q, $p \neq q$
  - $n = p \times q$
  - Calculate $z = (p-1)(q-1)$
  - Select e, such that $\gcd(z, e) = 1$; $0 < e < z$
  - Calculate d such that $de \bmod z = 1$

Student Questions

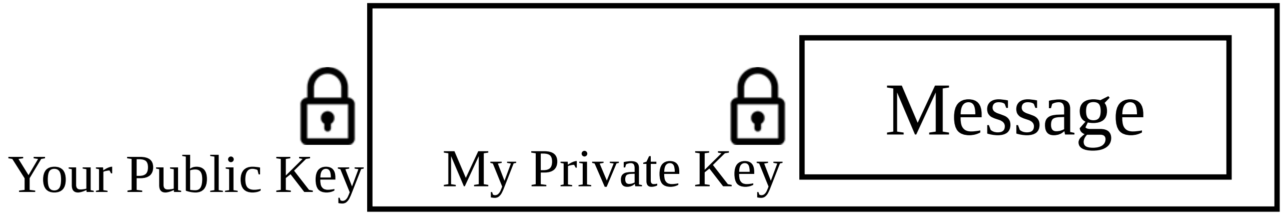
RSA Algorithm: Example

- Select two large primes: p, q, $p \neq q$
  $p = 17, q = 11$
- $n = p \times q = 17 \times 11 = 187$
- Calculate $z = (p-1)(q-1) = 16x10 = 160$
- Select e, such that $\gcd(z, e) = 1$; $0 < e < z$
  say, $e = 7$
- Calculate d such that de mod z = 1
  - $160k+1 = 161, 321, 481, 641$
  - Check which of these is divisible by 7
  - 161 is divisible by 7 giving $d = 161/7 = 23$
- Key 1 = {7, 187}, Key 2 = {23, 187}

Student Questions

Confidentiality and Non-Repudiation

- User 1 to User 2:
- Encrypted_Message
  = Encrypt(Public_Key2,
  Encrypt(Private_Key1, Message))
- Message = Decrypt(Public_Key1, Decrypt(Private_Key2, Encrypted_Message)
  ⇒ Authentic and Private



Student Questions

- Do we encrypt with the destination's public key to provide an indisputable declaration of the intended recipient?

The main purpose is so that no one else can decrypt it. However, this feature can be used to establish that only you could have decrypted it.

Public Key Encryption: Review

1. Public Key Encryption uses two keys: Public and Private
2. Either key can be used to encrypt. Other key will decrypt.
3. RSA public key method is based on difficulty of factorization

Ref: Section 8.2.2, Review exercises:R3, R7, Problems: P7, P9, P10

Student Questions

Homework 8B

Consider RSA with p=11, q=13

A. what are n and z

B. let e be 7. Why is this an acceptable choice for e?

C. Find d such that de=1(mod z)

D. Encrypt the message m=15 using the public key (n, e). Let c be the corresponding cipher text.

E. What is the private key. Verify that we can get the original message using the private key. Show all work.

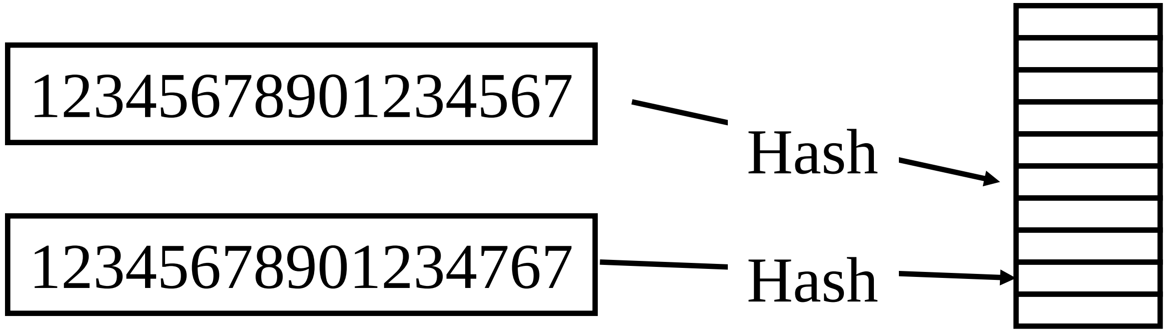
Student Questions

Hash, Signatures, Certificates

1. Hash Functions
2. MD5 Hash
3. SHA-1 Algorithm
4. Message Authentication Code (MAC)
5. Digital Signature
6. Digital Certificates
7. End Point Authentication

Student Questions

Hash Functions



Example: CRC can be used as a hash (not recommended for security applications)

Requirements:

1. Applicable to any size message
2. Fixed length output
3. Easy to compute
4. Difficult to Invert ⇒ Can't find *x* given H(*x*) ⇒ One-way
5. Difficult to find y, such that H(*x*) = H(*y*) ⇒ Can't change msg
6. Difficult to find *any* pair (*x*, *y*) such that H(*x*) = H(*y*) ⇒ Strong hash

Student Questions

- What is the difference between points 5 and 6?

5. Given H(x) and x, find y.

6. Nothing is given, Can you find x and y.?

MD5 Hash

- 128-bit hash using 512 bit blocks using 32-bit operations
- Invented by Ron Rivest in 1991
- Described in RFC 1321
- Commonly used to check the integrity of files (easy to fudge message and the checksum)
- Also used to store passwords

Student Questions

SHA-1 Algorithm

- 160 bit hash using 512 bit blocks and 32 bit operations
- Five passes (compared to 4 in MD5 and 3 in MD4)
- Maximum message size is 2^{64} bit

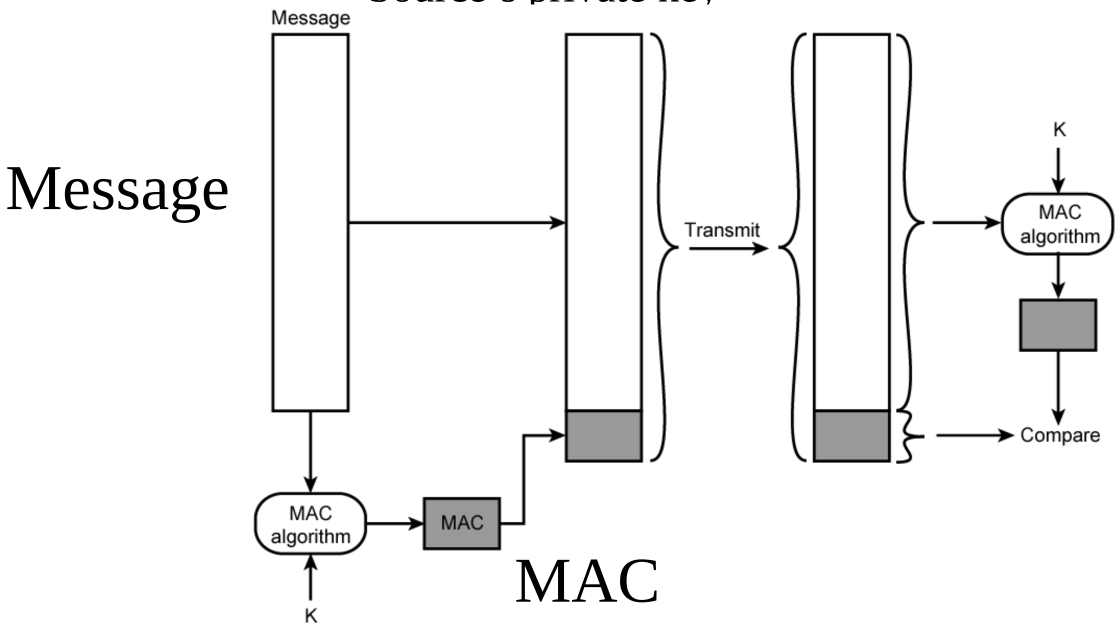
Student Questions

- What do you mean by "five passes" if the parentheses then list 4 + 3 passes in MD5/4?

SHA-1 is not a combination of MD5 and MD4. It is stronger then them.

Message Authentication Code (MAC)

- Authentic Message = Contents unchanged + Source Verified
- May also want to ensure that the time of the message is correct
- Encrypt$_{\text{secret key}}${Message, CRC, Time Stamp}
- Message + Encrypt$_{\text{secret key}}$(Hash)
  Or, Message + Encrypt$_{\text{Source's private key}}$(Hash)



Student Questions

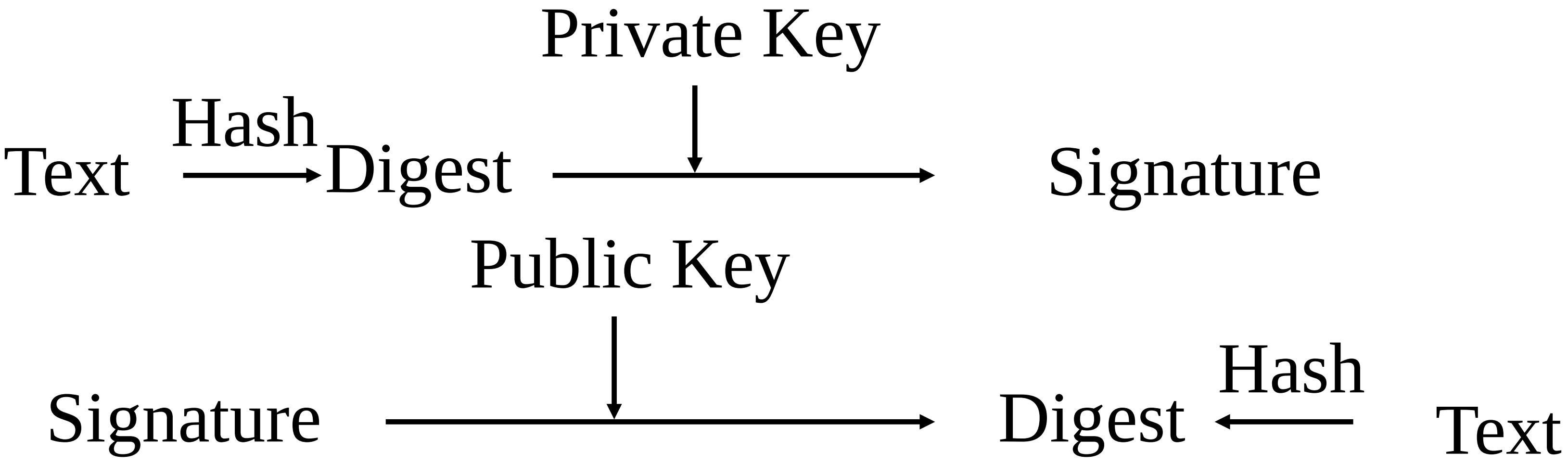
HMAC Overview

- Keyed Hash ⇒ includes a key along with message
- HMAC is a general design. Can use any hash function
  ⇒ HMAC-MD5, HMAC-AES
- Uses hash functions without modifications
- Has well understood cryptographic analysis of authentication mechanism strength

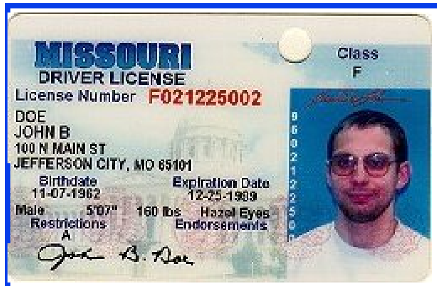
Student Questions

Digital Signature

- ❑ Message Digest = Hash(Message)
- ❑ Signature = Encrypt(Private_Key, Hash)
- ❑ Hash(Message) = Decrypt(Public_Key, Signature)
  ⇒ Authentic
- ❑ Also known as Message *authentication* code (MAC)



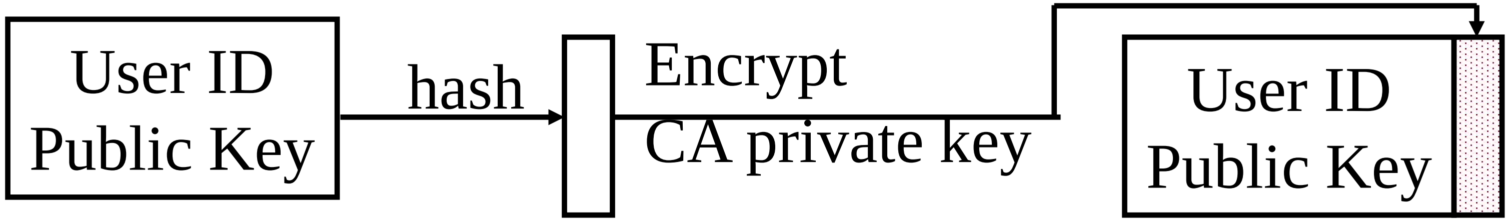
Student Questions



MISSOURI
DRIVER LICENSE
License Number F021225002
Class F
DOE
JOHN B
100 N MAIN ST
JEFFERSON CITY, MO 65101
Birthdate 11-07-1962
Expiration Date 12-25-1989
Male 5'07" 160 lbs Hazel Eyes
Restrictions A
Endorsements
John B. Doe

Digital Certificates

- ❑ Like driver license or passport
- ❑ Digitally signed by Certificate authority (CA) - a trusted organization
- ❑ Public keys are distributed with certificates
- ❑ CA uses its private key to sign the certificate
  ⇒ Hierarchy of trusted authorities
- ❑ X.509 Certificate includes: Name, organization, effective date, expiration date, public key, issuer's CA name, Issuer's CA signature

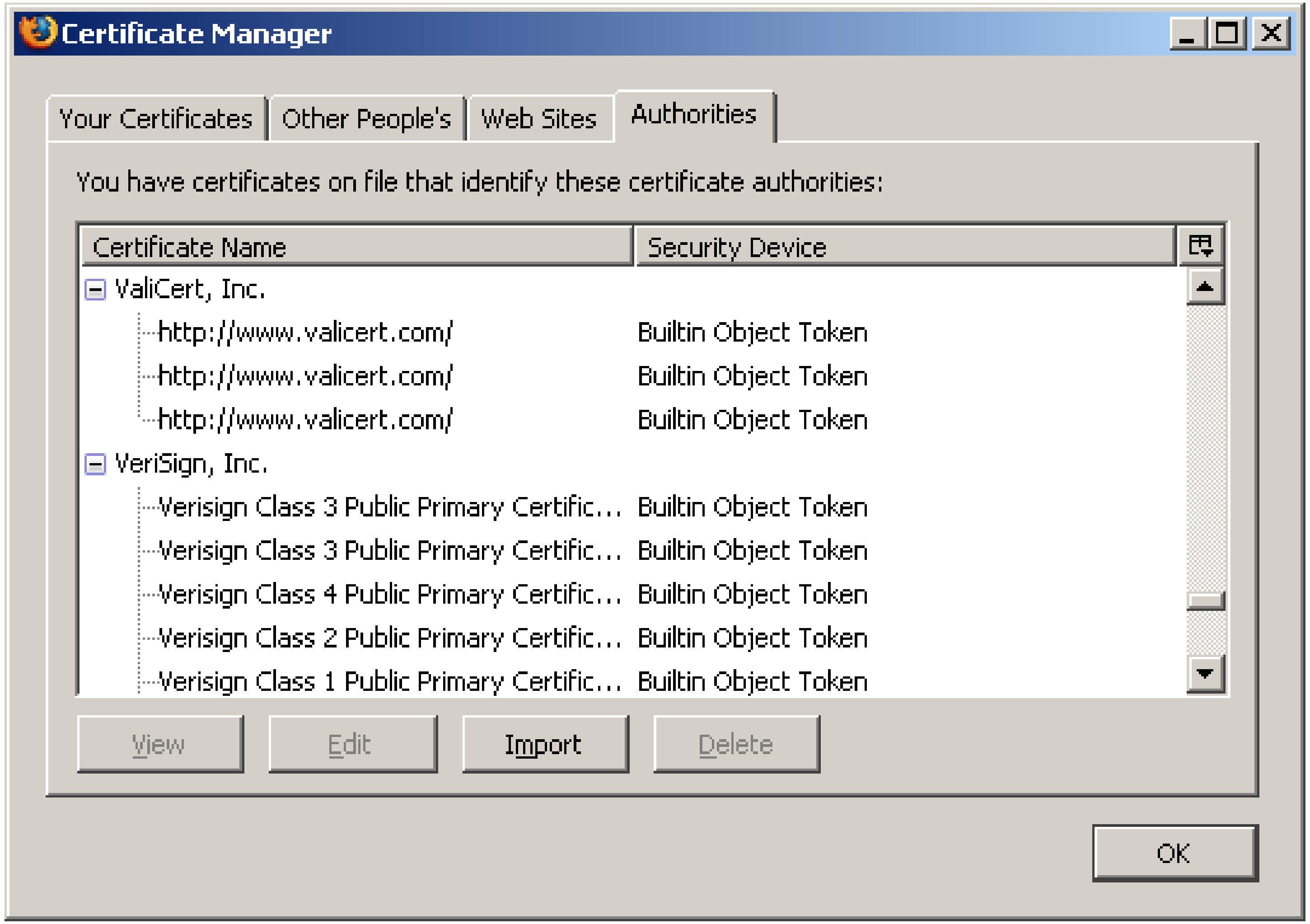


Student Questions

- ❑ What is a root CA and how many different root CA's are there?

There is no limit on number of Root CAs. You can become a root CA if other people trust your certificate. Many companies use internal Root CAs.

Oligarchy Example



You have certificates on file that identify these certificate authorities:

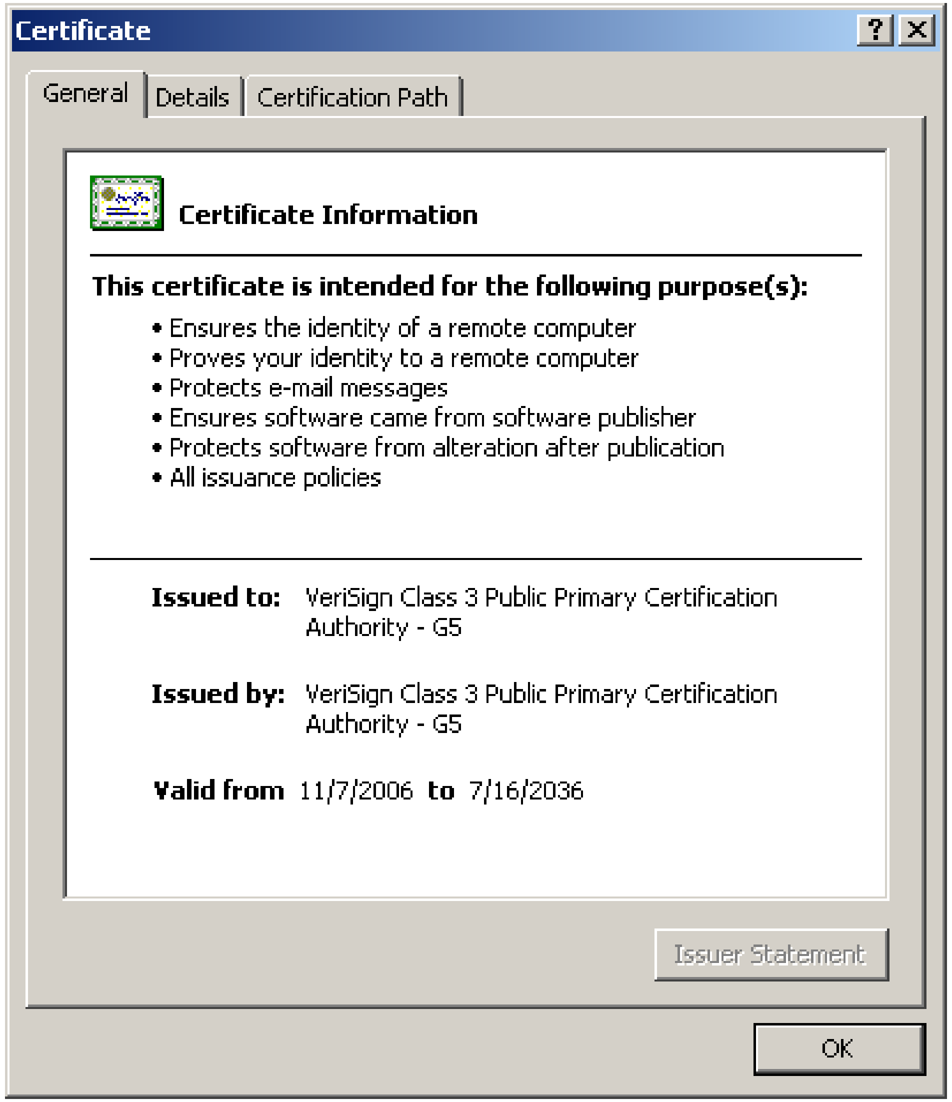
Certificate Name	Security Device
⊟ ValiCert, Inc.	
http://www.valicert.com/	Builtin Object Token
http://www.valicert.com/	Builtin Object Token
http://www.valicert.com/	Builtin Object Token
⊟ VeriSign, Inc.	
Verisign Class 3 Public Primary Certific...	Builtin Object Token
Verisign Class 3 Public Primary Certific...	Builtin Object Token
Verisign Class 4 Public Primary Certific...	Builtin Object Token
Verisign Class 2 Public Primary Certific...	Builtin Object Token
Verisign Class 1 Public Primary Certific...	Builtin Object Token

Ref: Windows: http://smallbusiness.chron.com/see-security-certificates-stored-computer-54732.html
MAC: https://superuser.com/questions/992167/where-are-digital-certificates-physically-stored-on-a-mac-os-x-machine

Student Questions

Sample X.509 Certificate

- Certmgr.msc in Windows



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- All issuance policies

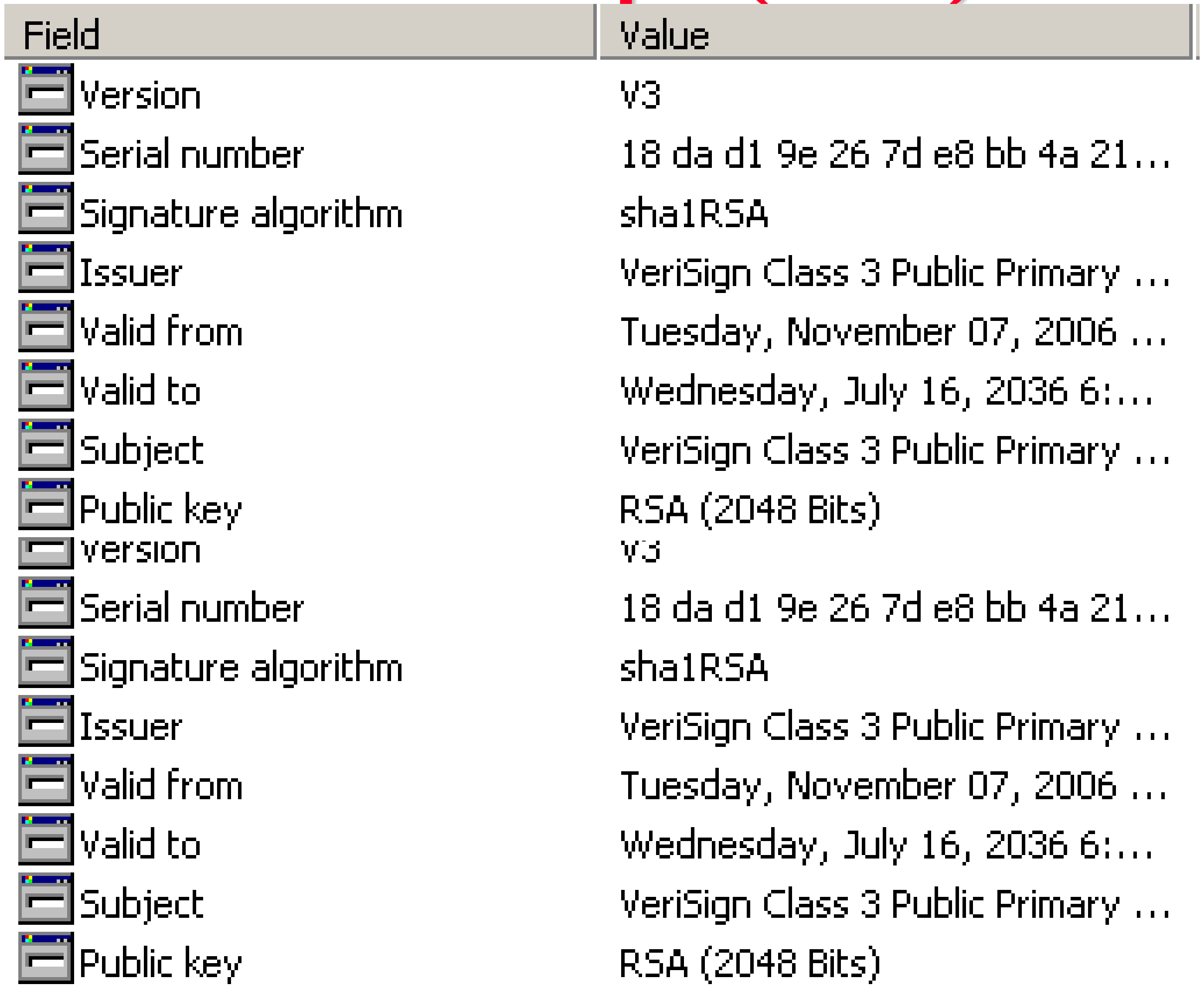
Issued to: VeriSign Class 3 Public Primary Certification Authority - G5

Issued by: VeriSign Class 3 Public Primary Certification Authority - G5

Valid from 11/7/2006 **to** 7/16/2036

Student Questions

X.509 Sample (Cont)



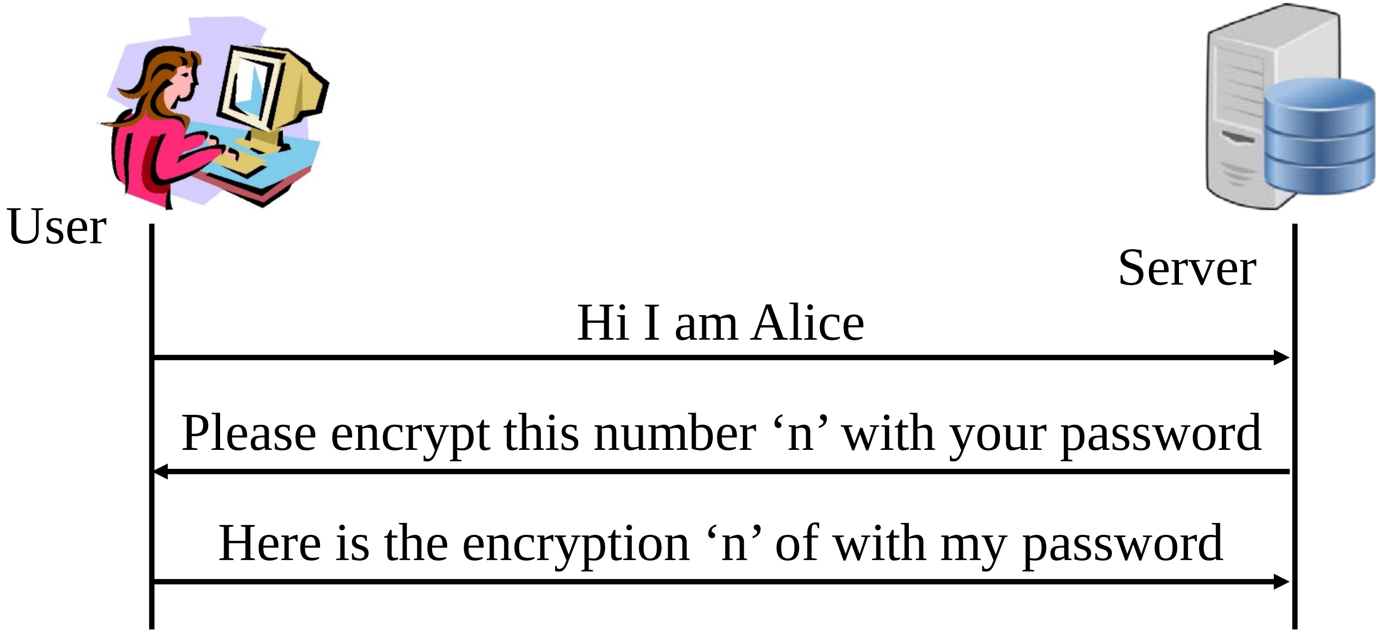
Field	Value
Version	V3
Serial number	18 da d1 9e 26 7d e8 bb 4a 21…
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary …
Valid from	Tuesday, November 07, 2006 …
Valid to	Wednesday, July 16, 2036 6:…
Subject	VeriSign Class 3 Public Primary …
Public key	RSA (2048 Bits)

Field	Value
Version	V3
Serial number	18 da d1 9e 26 7d e8 bb 4a 21…
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary …
Valid from	Tuesday, November 07, 2006 …
Valid to	Wednesday, July 16, 2036 6:…
Subject	VeriSign Class 3 Public Primary …
Public key	RSA (2048 Bits)

Student Questions

End Point Authentication

- ❑ Passwords can not be exchanged in clear
  Nonce = random **n**umber used only **once**
- ❑ Also done using certificates



User

Server

Hi I am Alice

Please encrypt this number ‘n’ with your password

Here is the encryption ‘n’ of with my password

Requires the server to store passwords in clear.

Student Questions

- ❑ How do the server and user verify they have the same thing if the server doesn't have the password? The server stores a hash of the password that was sent to it securely?

Yes. This exchange protects against third party threats even if the password is stored in clear.

- ❑ Is it possible for someone to listen in on the initial connection and be able to steal the Nonce value that the user is receiving from the server? Also, could someone pose as the server and send the user a nonce value which they would encrypt their data with so that the hacker could decrypt the encrypted password?

Nonce is sent in clear. Anyone can read it. It is not used again and so it has no value. Yes, someone can pose as the server and so server authentication is required before itself.

- ❑ Is nonce the same as salt?

No. Salt is used in hashing inside the server. Nonce is sent on the network.

- ❑ Does the password need to be stored in cleartext on the server?

No. Never. There are several alternatives.

- ❑ Is the End Point Authentication usage of a nonce related to blockchaining's use of nonces?

No. Please use block chain or CBC. Blockchain (one word) relates to crypto currencies not security.

Hashes, Signatures, Certificates

1. Hashes are one-way functions such that it difficult to find another input with the same hash like MD5, SHA-1
2. Message Authentication Code (MAC) ensures message integrity and source authentication using hash functions
3. Digital Signature consists of encrypting the hash of a message using private key
4. Digital certificates are signed by root certification authorities and contain public keys

Ref: Section 8.3-8.4, Review questions R9-18

Student Questions

- ❑ Can cyber criminals fake a Digital Certificates and pretend that digital signature is his?

No. Root certificates have to be in the list before accepting a certificate issued by that CA.

- ❑ Is MD5 still used in the industry?

Yes, for File integrity checking.

Secure Email

1. Secure E-Mail
2. Signed Secure E-Mail
3. Pretty Good Privacy (PGP)

Student Questions

- If a group of users share encrypted emails, but a single user in the email chain replies in plaintext, is the security of the email lost?

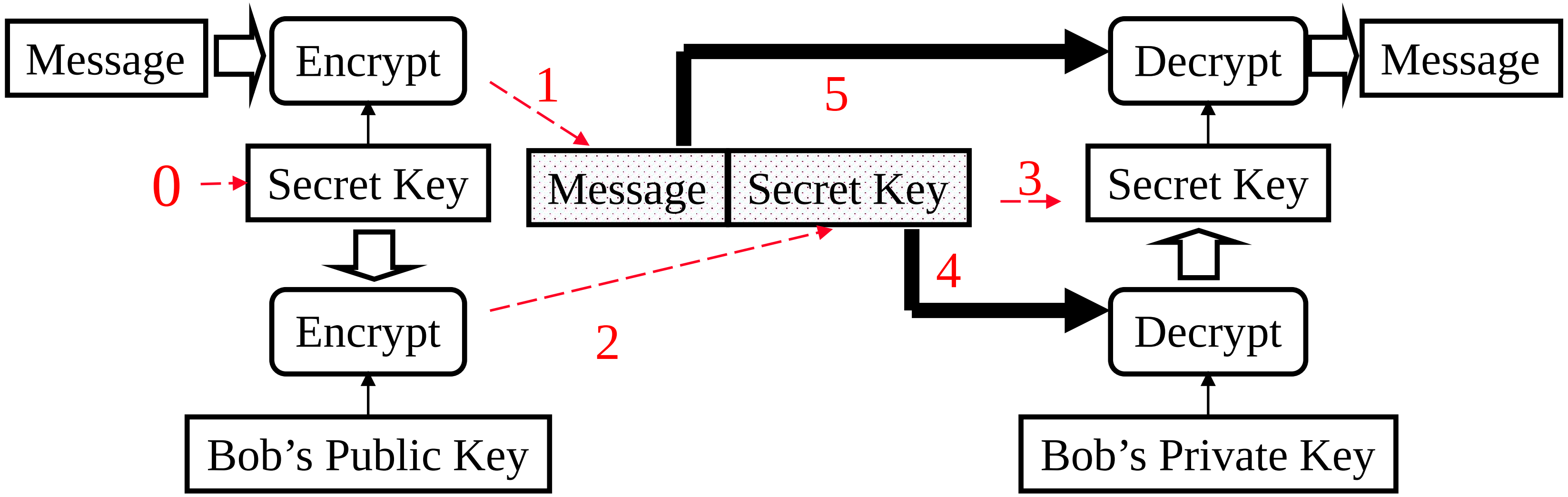
Whatever is in the cleartext is public knowledge.

- The email envelope consisting of sender, receiver, and timestamps appears to be unencrypted. Why is this information not encrypted along with the message?

Message forwarding requires clear headers. However, more secure mail servers could do some key exchanges beforehand to allow encrypted headers.

Secure E-Mail

- Alice wants to send confidential e-mail, m, to Bob.



- **Alice:**

0. Generates random *secret* key, K_S.
1. Encrypts message with K_S (for efficiency)
2. Also encrypts K_S with Bob's public key.
3. Sends both K_S(m) and $K_B(K_S)$ to Bob.

- **Bob:**

4. Bob uses his private key to recover K_s
5. Bob decrypts message

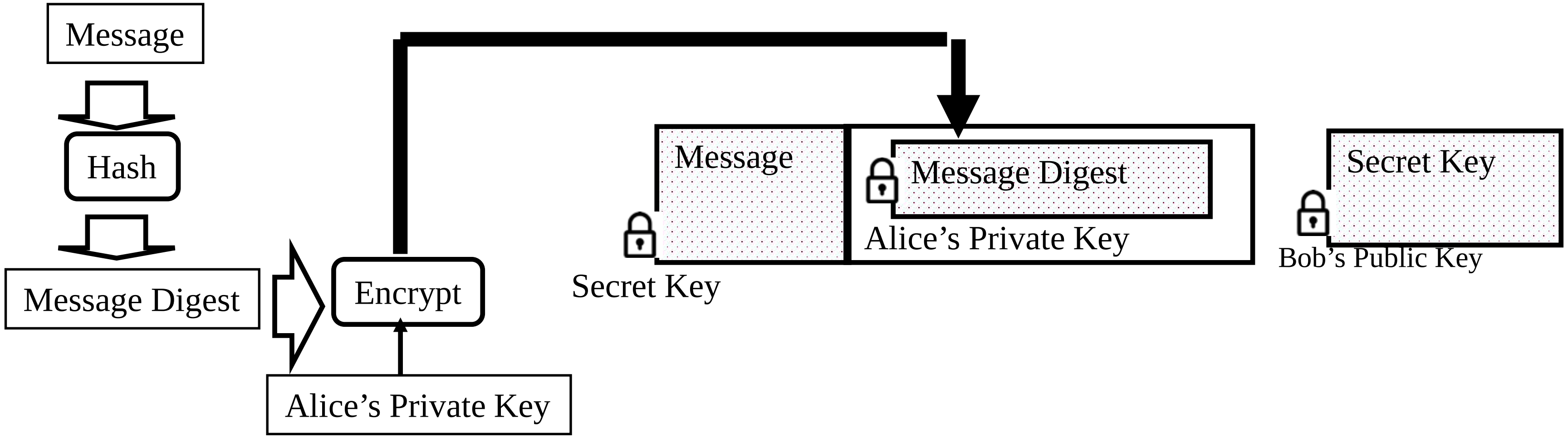
Student Questions

- Is it insecure to reuse the same single-use key for secure email?

New secret keys are periodically generated in all applications that require long exchanges, such as large file transfers.

Signed Secure E-Mail

- Alice wants to provide secrecy, sender authentication, message integrity.



- Alice uses three keys: her private key, Bob's public key, newly created secret key
- Bob uses his private key to recover the secret key
- Bob uses Alice's public key to verify that the message came from Alice and was not changed.

Student Questions

- Does Bob also need to hash the message and verify the message digest matches because the digest is used as a MAC right?

Yes.

- What is the message digest in the picture?

Message Authentication Code to verify integrity of the message.

- Is Alice's secret key newly created by encrypting Message Digest with Alice's Private key?

No. Please see the previous slide about how the secret key is generated and sent.

Pretty Good Privacy (PGP)

- Used RSA and IDEA (RSA patent in US until 2000)
- V2.6.2 became legal for use within US and can be downloaded from MIT
- A patent-free version using public algorithm has also been developed
- Code published as an OCRable book
- Initially used web of trust- certificates issued by people
- Certificates can be registered on public sites, e.g., MIT
- hushmail.com is an example of PGP mail service
- OpenPGP standard [RFC 4880]
- MIME=Multipurpose Internet Mail Extenstion. Allows non-ascii characters to be encoded in ASCII

Ref: http://en.wikipedia.org/wiki/Pretty_Good_Privacy , https://en.wikipedia.org/wiki/MIME

Student Questions

- What features of PGP gave it an advantage over other software implementations for signing?

It was mainly designed when RSA was restricted for export.

- Is a person utilizing MIME when they attach something to an email, or when something is embedded in the message itself?

Yes.

Lab 8: Secure Email

[20 points] You will receive a "signed" email from the TA. Reply to this email with a "encrypted and signed" email to TA.

If outlook says "*There is a problem with the signature on the TA's message*" then click on the signature icon on the top right of the message and accept TA's certificate. The warning will go away.

- You can reply to the TA's email with a signed encrypted message. Content of the reply should be the contents of the "**Enhanced key usage**" field in your new certificate.
- Before sending the reply, on the outlook message window, Select View → Options → (More Options →) Security Settings
  Select encryption and signature. Now send the message.
- **Outlook is required** for both Windows and Mac

Student Questions

Lab 8 (Cont)

- To sign your email with a private key you need your digital certificate. To send an encrypted email you need TA's public key.
- TA's public key is attached with his/her email.
- The steps to obtain a free certificate and use it for email depend upon your email software and your operating system. Registered students of this class will receive a certificate by email.
- Instructions for Outlook on Windows 10 are as included next. If you do not have windows, you can do it using remote desktop to a Wash U windows computer.
- Instructions for Mac are similar. Further details for Mac are in the references cited below.

Ref: https://support.apple.com/guide/mail/use-personal-certificates-mlhlp1179/mac
https://knowledge.digicert.com/solution/SO6722.html

Student Questions

Lab 8 (Cont)

1. Getting your Certificate:

- By this time, you should have received an email from cert-manager.com. Please follow the instructions in that email.
- After completing the steps in the email, click ‘Download’ to collect your certificate. You should save this file to a safe place on your hard drive.
- Import your new certificate in to your email client and/or Internet browser.

Student Questions

- Just to clarify, we are to use Actalis to create a certificate?

No. As indicated in the class, this year WUSTL gave you a free certificate. Please use that only. Actalis will not work since TA does not have Actalis in the list of his/her known root certificates.

Lab 8 (Cont)

2. Installing your Certificate in Outlook:

- Now open the Outlook App (not the website and follow the following click sequence:
- File → Options → Trust Center→ Trust Center Settings → Email Security → Digital IDs import/export
- Import the certificate file and enter the password that was given by certificate issuer. Click OK.
- Now, you can digitally sign an email by selecting the "Options" tab in the composing a message window, and clicking the "Sign" button.

Ref: https://www.thesslstore.com/knowledgebase/email-signing-support/install-e-mail-signing-certificates-outlook/

Student Questions

Lab 8 Hints (Cont)

3. Importing Other's Certificates in Outlook:

- ❑ Outlook automatically saves the certificate, if you get a signed message from your contacts.
- ❑ However, if the sender of the signed message is not in your contact database, you need to open the signed message received. In the message window, right click on the name in the "From field" and select "save as outlook contact"
- ❑ This will open a new contact window. In that window, click on the "certificates" tab.
- ❑ You will see the certificate listed there.
- ❑ Save this contact in your contacts list.
- ❑ When you reply or send email to this contact, you can enable the security options for encryption and signatures.
- ❑ Alternate Procedure:
  - ➢ Open the signed email and click the Certificate icon (blue box).
  - ➢ In the produced window, select Details... → View Certificate → Copy to File → DER encoded binary X.509 (.CER). → File Destination.
  - ➢ Add Outlook Contact → Certificates → Import, and add this certificate.

Student Questions

Lab 8 (Cont)

4. Sending Encrypted Emails:

- The recipient may see "There is a problem with the signature" when they receive the signed message for the first time. This is because they may not have included your certificate issuer as a trusted Certificate Authority. To fix this they need to click on the signature icon on the right-top of the message and accept the issuer's certificate. After this the problem message will go away.
- The recipient can also get a certificate and send a signed message to you. When you open that message, the recipient's public key is automatically installed in your outlook.
- After both of you have each other's public key, you can send encrypted emails to each other. You can send such messages by by selecting the dropdown menu on the "Encrypt" button (right next to the "Sign" button), and selecting "Encrypt with S/MIME".

Student Questions

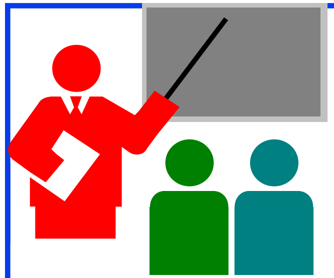
Lab 8 (Cont)

5. Examining your certificate: From the references below.

- In Windows, use Run → Certmgr.msc
- In the window that opens, look for Personal → Certificates
- Double-click on the new certificate. Go to details tab. Scroll down to find "Enhanced Key Usage". Click on it to see the results in the bottom pane. Copy and paste it to your email reply to the TA email.
- Before clicking send, remember to click options and select encryption.
- The process on MAC is in the 2nd reference below but has not been verified.

Ref: https://www.top-password.com/blog/view-installed-certificates-in-windows-10-8-7/
https://www.digicert.com/kb/code-signing/mac-verifying-code-signing-certificate.htm

Student Questions



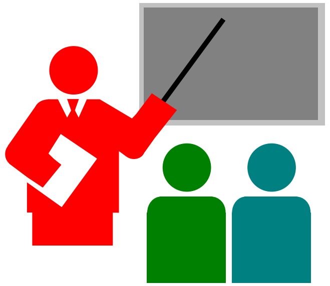
Secure Email: Review

1. Email provide confidentiality using a secret key
2. Public key and Certificates are used to:
    1. Sign the message
    2. To send the secret key

Ref: Section 8.5, Review question R19

Student Questions

Summary: So Far



1. Network security requires confidentiality, integrity, availability, authentication, and non-repudiation
2. Encryption can use one secret key or two keys (public and private)
3. The public key is very compute-intensive and is generally used to send the secret key
4. A digital certificate system is used to certify the public key
5. Secure e-mail uses confidentiality using a secret key, uses certificates and public keys to sign the e-mail and send the secret key

Ref: Sections 8.1 through 8.5

Student Questions

- Unsure what to select for the last question ("Did you watch the video completely?")

No = 0 points

Yes = 4 points

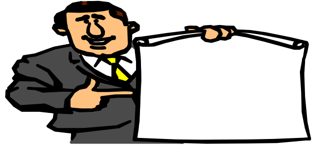
Be honest. If you are not sure, answer No.

- Is there a graph for regraded exam 2 rankings?
- *Not too many changes.*

- How do we secure the digital certificate system itself from attacks?

Digital certificates are public. You can post yours and others on your website. No security is required. It would help if you kept the private key in a safe. The private key is not there in the certificate.

End of Part 2

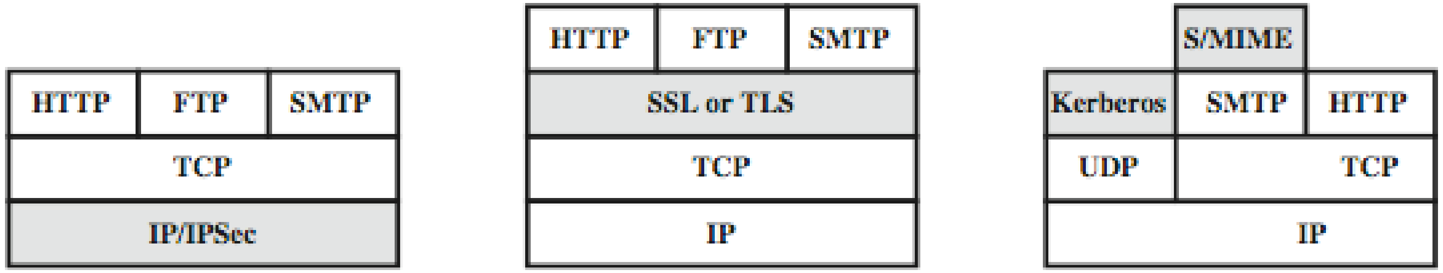


Transport Layer Security (TLS)

- Web Traffic Security Approaches
- History
- SSL/TLS Architecture
- SSL/TLS Protocol Components
- Secure HTTP (HTTPS)

Student Questions

Web Traffic Security Approaches



HTTP | FTP | SMTP
TCP
IP/IPSec

(a) Network Level

HTTP | FTP | SMTP
SSL or TLS
TCP
IP

(b) Transport Level

S/MIME
Kerberos | SMTP | HTTP
UDP | TCP
IP

(c) Application Level
(Not covered in this course)

- SSL/TLS provides the following services **over the TCP** layer:
  1. **Crypto Negotiation**: Negotiate encryption and hash methods
  2. **Key Exchange**: Secret key exchange using public key certificates
  3. **Privacy**: Encryption using a secret key
  4. **Integrity**: Message authentication using a keyed hash

Student Questions

History

- Netscape (Founded by Marc Andreesen/UIUC 1994) developed SSL. V1 was never deployed. V2 had major issues.
- SSL v3 is the most commonly deployed protocol
- TLS V1: IETF standardized SSL V3 with some upgrades as Transport Layer Security (TLS) V1 [RFC 2246 1999]
  TLS is encoded as SSL V3.1
  The differences are small, but the protocols do not interoperate.
- TLS v1.1 (SSL V3.2) added protection against CBC attacks [RFC 4346 2006]
- TLS V1.2: SHA-256 instead of MD5, Specify which hashes and signatures are acceptable [RFC 5246, 2008]
- TLS V1.3: Many enhancements. Implemented in Windows 11 [RFC 8446, 2018]

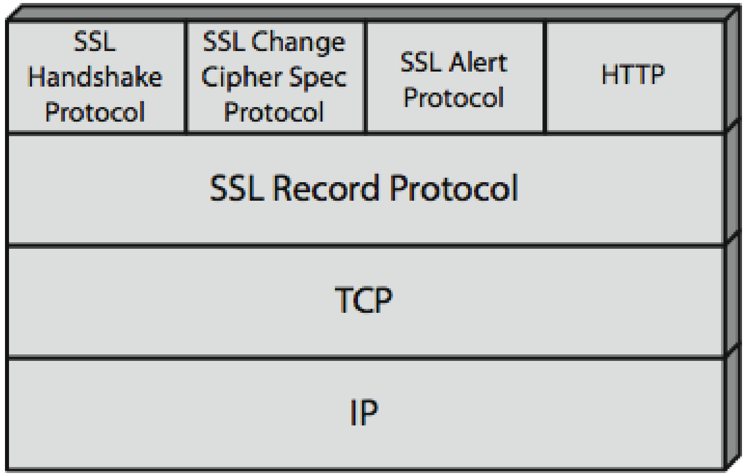
Ref: http://en.wikipedia.org/wiki/Transport_Layer_Security

Student Questions

SSL/TLS Architecture

- SSL has four components in two layers

1. **Handshake protocol**: Negotiates crypto parameters for an “SSL session” that can be used for many “SSL/TCP connections.”
2. **Record Protocol**: Provides encryption and MAC
3. **Alert protocol**: To convey problems
4. **Change Cipher Spec Protocol**: Implement negotiated crypto parameters



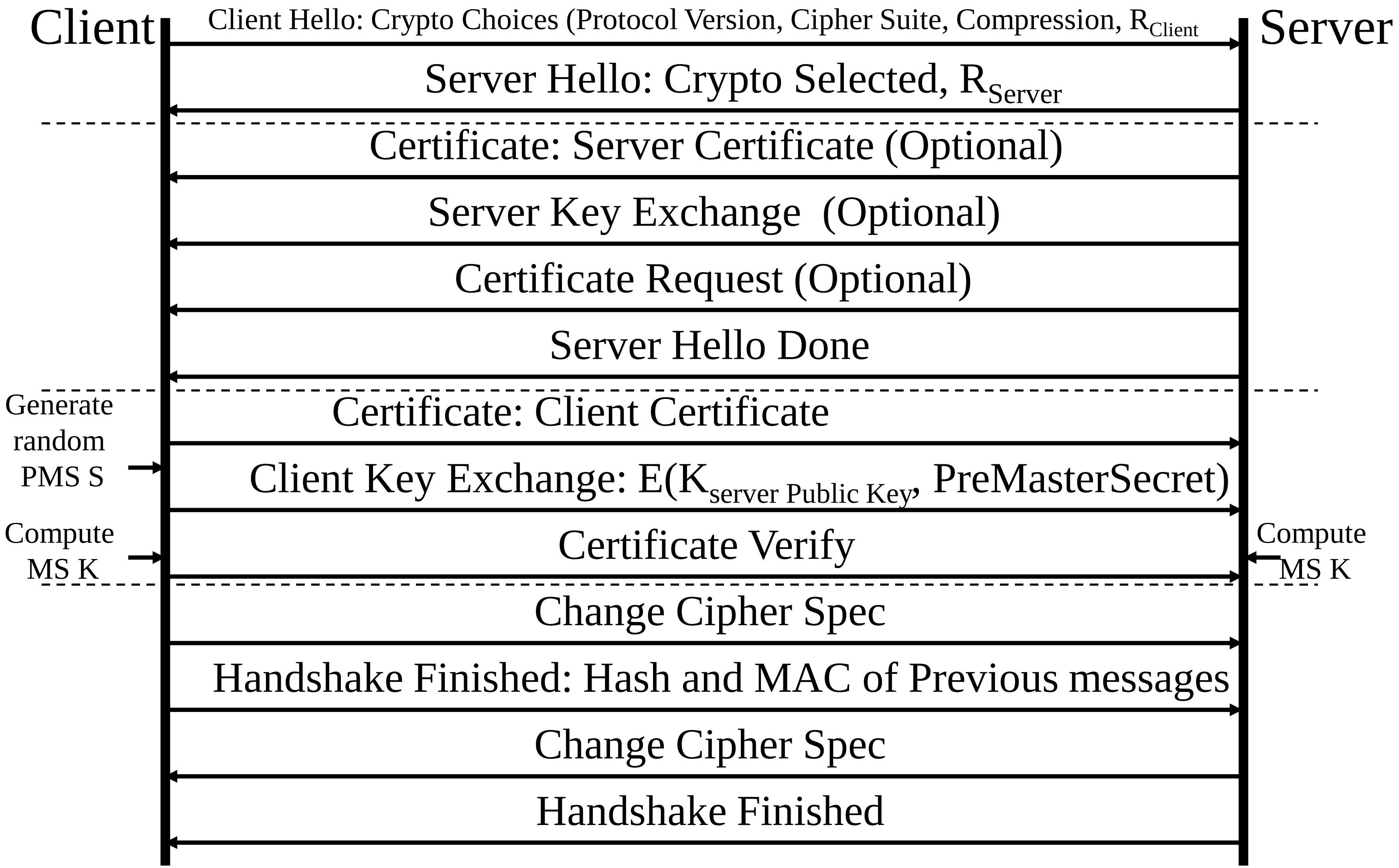
Student Questions

SSL/TLS Handshake Protocol

- ❑ Allows server and client to:
  - ➢ Authenticate each other
  - ➢ To negotiate encryption & MAC algorithms
  - ➢ To negotiate cryptographic keys to be used
- ❑ Comprises a series of messages in phases
  1. Establish Security Capabilities
  2. Server Authentication
  3. Client Authentication and Key Exchange
  4. Finish

Student Questions

SSL/TLS Handshake Protocol Actions



Client

Server

Client Hello: Crypto Choices (Protocol Version, Cipher Suite, Compression, R_{Client}

Server Hello: Crypto Selected, R_{Server}

Certificate: Server Certificate (Optional)

Server Key Exchange (Optional)

Certificate Request (Optional)

Server Hello Done

Certificate: Client Certificate

Generate random PMS S

Client Key Exchange: E($K_{server\ Public\ Key}$, PreMasterSecret)

Compute MS K

Certificate Verify

Compute MS K

Change Cipher Spec

Handshake Finished: Hash and MAC of Previous messages

Change Cipher Spec

Handshake Finished

Student Questions

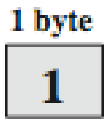
Cryptographic Computations

- Master secret creation
  - A one-time 48-byte value based on nonces
  - A 48-byte pre-master secret is exchanged/generated using secure key exchange (RSA / Diffie-Hellman) and then hashing:
  - *Master_Secret = MD5(Pre_master_Secret || SHA('A' || pre_master_secret || clientHello.random || ServerHello.random)) || MD5(Pre_master_Secret || SHA('BBB' || pre_master_secret || clientHello.random || ServerHello.random)) || MD5(Pre_master_Secret || SHA('CCC' || pre_master_secret || clientHello.random || ServerHello.random))*
- Generation of cryptographic parameters
  - A "client write MAC secret," "a server write MAC secret," "a client write key," "a server write key," "a client write IV," and "a server write IV"
  - Generated by hashing the master secret

Student Questions

SSL/TLS Change Cipher Spec Protocol

- A single 1-byte message
- Causes negotiated parameters to become current
- Hence updating the cipher suite in use



(a) Change Cipher Spec Protocol

Student Questions

SSL/TLS Alert Protocol

Conveys SSL-related alerts to the peer entity

Two-byte message: Level-Alert, level = warning or fatal, fatal ⇒ Immediate termination

0 Close notify (warning or fatal)

10 Unexpected message (fatal)

20 Bad record MAC (fatal)

21 Decryption failed (fatal, TLS only)

22 Record overflow (fatal, TLS only)

41 No certificate (SSL v3 only) (warning or fatal)

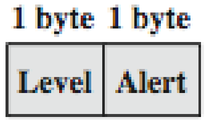
42 Bad certificate (warning or fatal)

43 Unsupported certificate (warning or fatal)

44 Certificate revoked (warning or fatal)

45 Certificate expired (warning or fatal)

….



(b) Alert Protocol

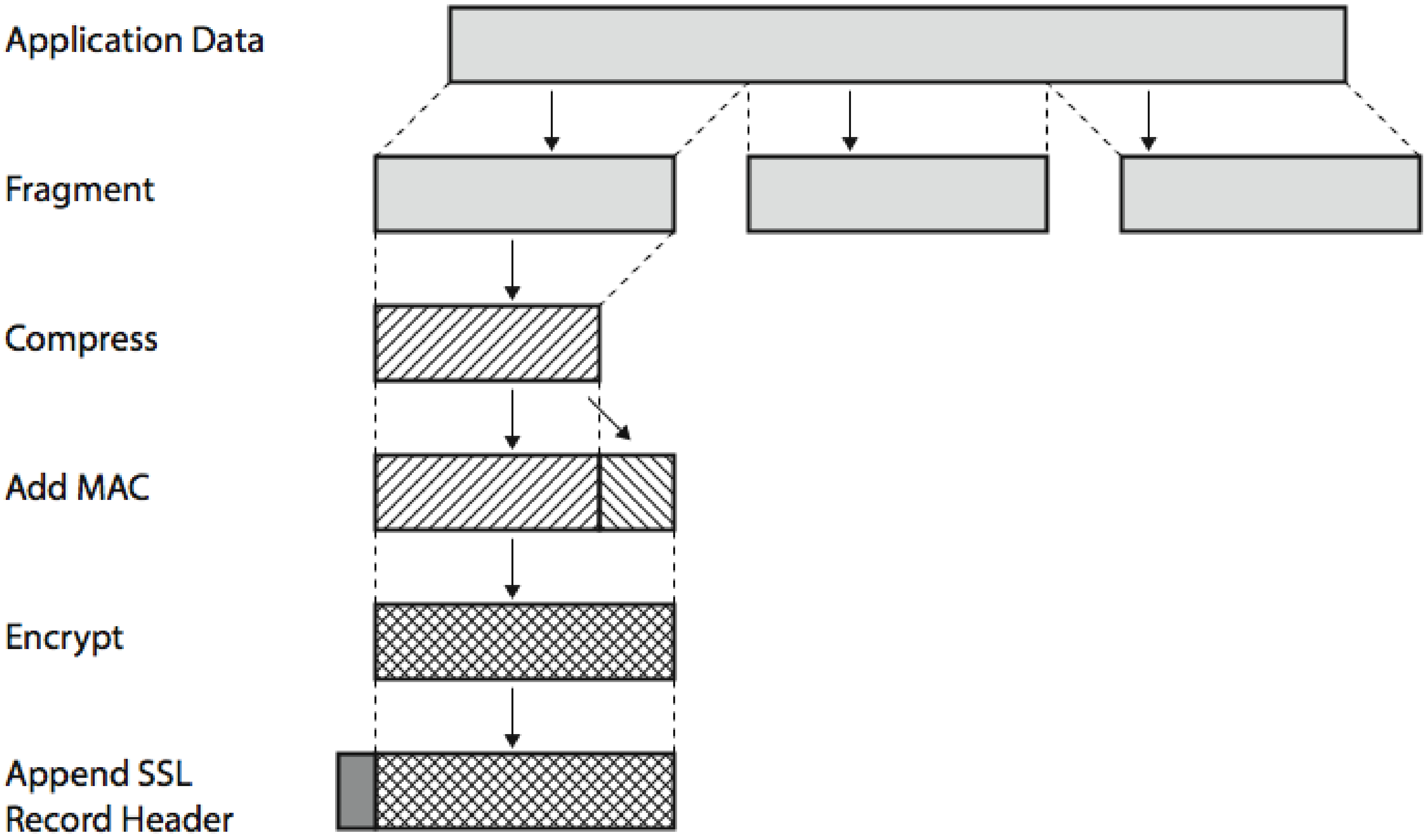
Student Questions

SSL/TLS Record Protocol Services

- **Confidentiality**
  - Using symmetric encryption with a shared secret key defined by Handshake Protocol
  - AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - The message is compressed before encryption
- **Message integrity**
  - Using the MAC with the shared secret key
  - Similar to HMAC but with different padding

Student Questions

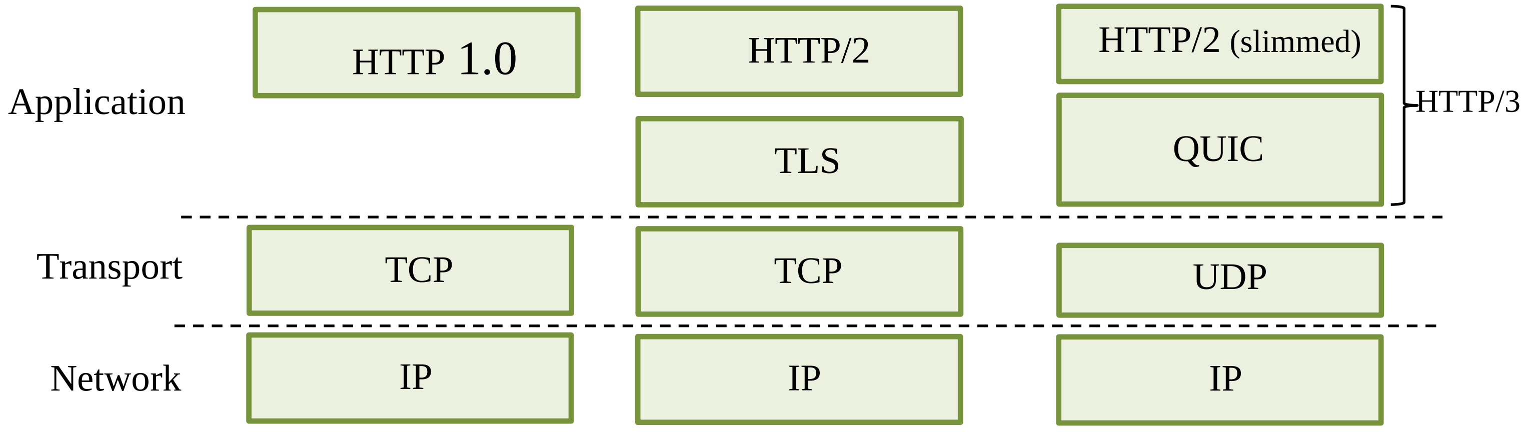
SSL/TLS Record Protocol Operation



Student Questions

Secure HTTP (HTTPS)

- HTTPS (HTTP over SSL)
  - Combination of HTTP & SSL/TLS to secure communications between browser & server [RFC2818]
- Use HTTPS:// URL rather than HTTP://. Use port 443 rather than 80
- Encrypts URL, document contents, form data, cookies, HTTP headers



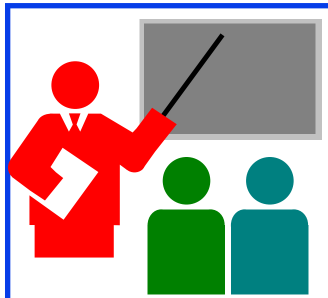
HTTP/2 over TCP

HTTP/2 over TCP

HTTP/2 over QUIC (which incorporates TLS) over UDP

Ref: http://en.wikipedia.org/wiki/HTTP_Secure

Student Questions

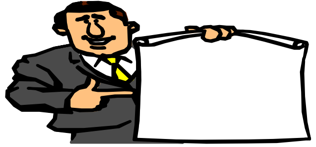


TLS: Summary

1. Netscape invented SSL to secure web transactions
2. TLS is a revised version of SSL V3
3. TLS provides
    a. Crypto negotiation,
    b. Secure key exchange,
    c. Privacy via encryption, and
    d. Integrity using a keyed hash.
4. HTTP over TLS is also called HTTPS

Ref: Read Section 8.6 and Exercises R20-R23

Student Questions



IP Security (IPsec) and VPNs

1. IPsec Applications: VPNs
2. Two ways to secure:
   a. Authentication Header (AH)
   b. Encapsulating Security Payload (ESP)
3. Internet Key Exchange (IKE)

Student Questions

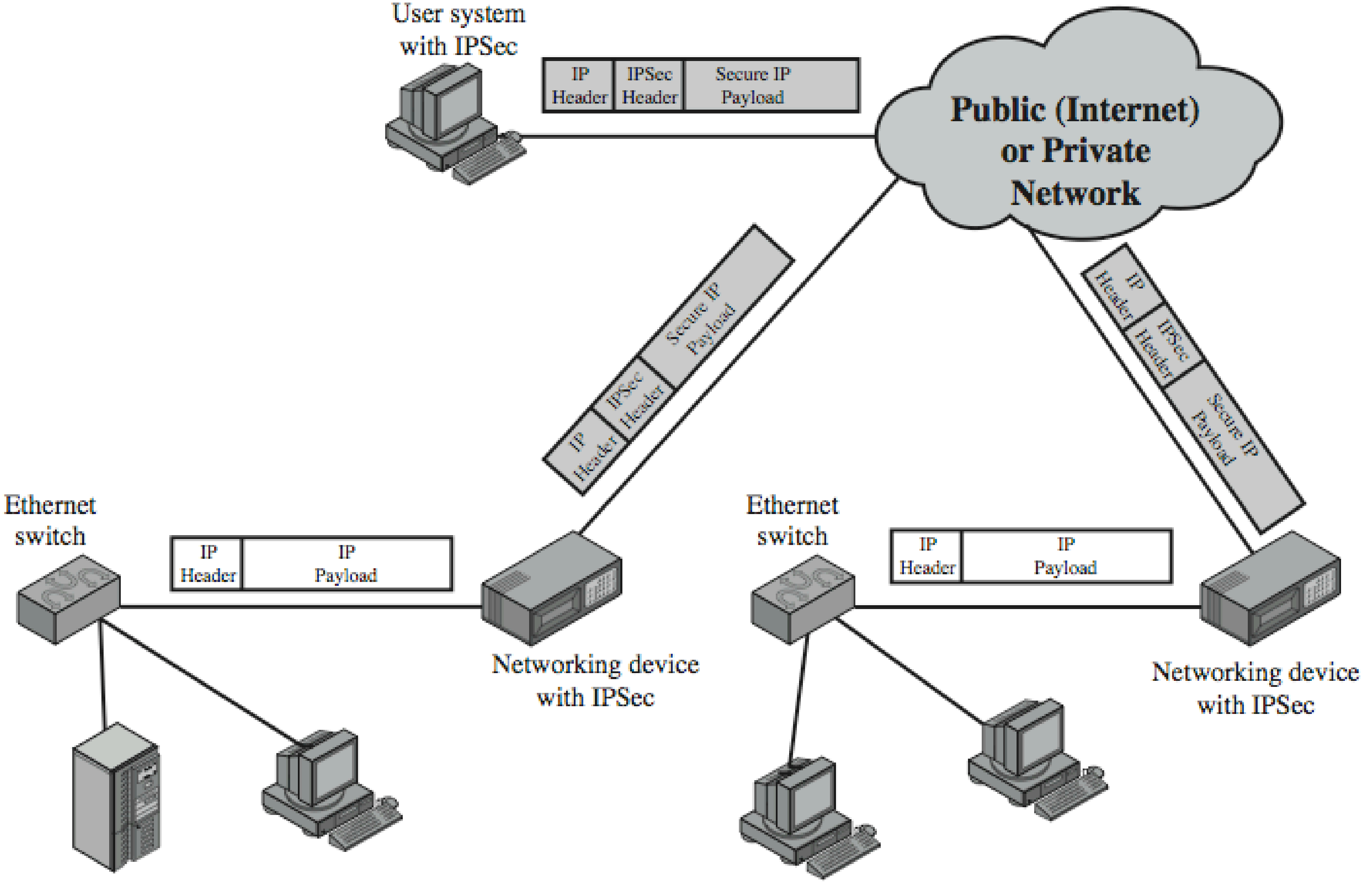
IP Security

- IPsec provides
  - Access control: User authentication
  - Data integrity
  - Data origin authentication
  - Rejection of replayed packets
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality
- Benefits:
  - Security at Layer 3 ⇒ Applies to all transports/applications
  - Can be implemented in Firewall/router
    ⇒ Security to all traffic crossing the perimeter
  - Transparent to applications and can be transparent to end-users
  - Can provide security for individual users
- Applications: VPNs, Branch Offices, Remote Users, Extranets

Ref: http://en.wikipedia.org/wiki/IPsec

Student Questions

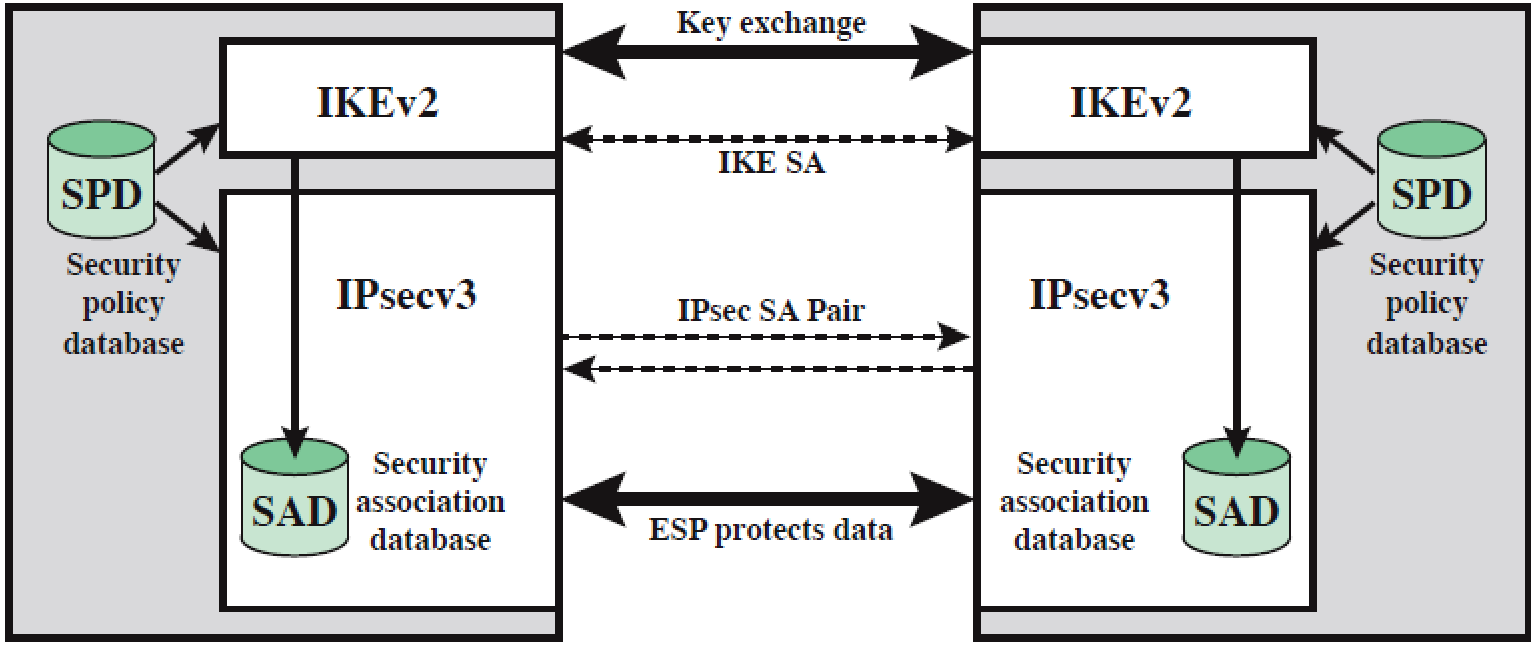
IP Security Applications



Student Questions

IP Security Architecture

- Internet Key Exchange (IKE)
- IPsec
- Security Association Database (SAD)
- Security Policy Database (SPD)



Student Questions

Security Association Database (SAD)

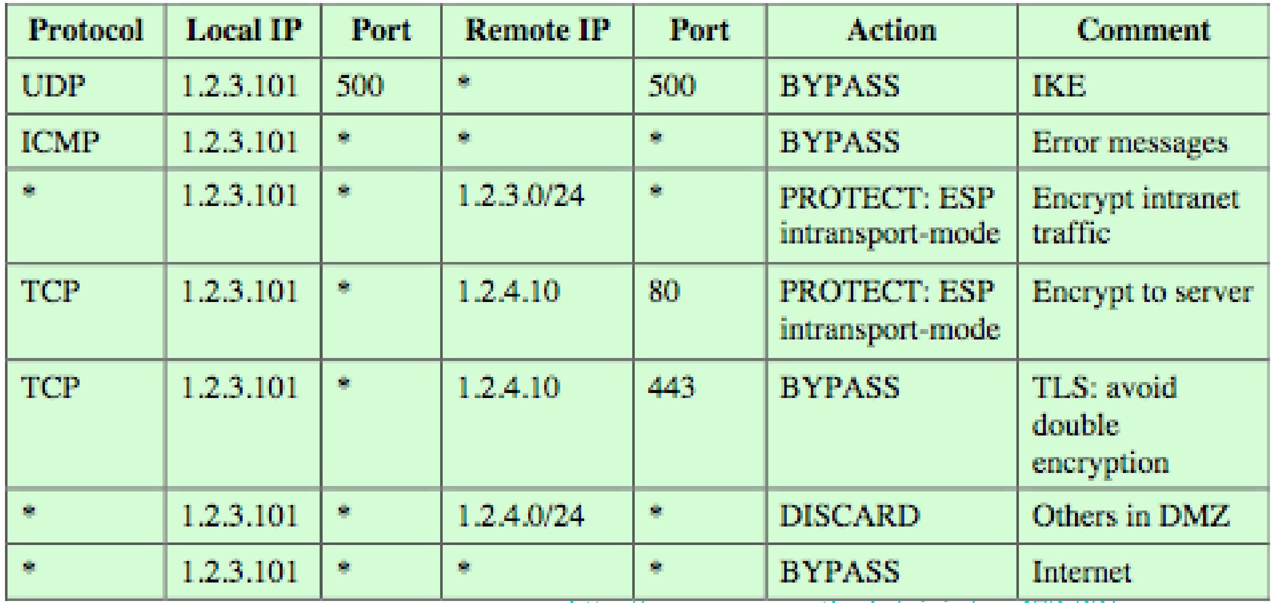
- Each host has a database of Security Associations (SAs)
- SA = One-way security relationship between sender & receiver
  Two-way may use different security ⇒Two SA's required
- Defined by three parameters:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier: AH or ESP
- For each SA, the database contains:
  - SPI
  - Sequence number counter and counter overflow flag
  - Anti-replay window (Acceptable sequence #s)
  - AH Information and ESP information
  - Lifetime of the SA
  - Mode: Transport or tunnel or wildcard
  - Path MTU

Ref: http://en.wikipedia.org/wiki/Security_association

Student Questions

Security Policy Database (SPD)

- Relates IP traffic to specific SAs
  - Match subset of IP traffic to relevant SA
  - Use selectors to filter outgoing traffic to map
  - Based on: local & remote IP addresses, next layer protocol, name, local & remote ports

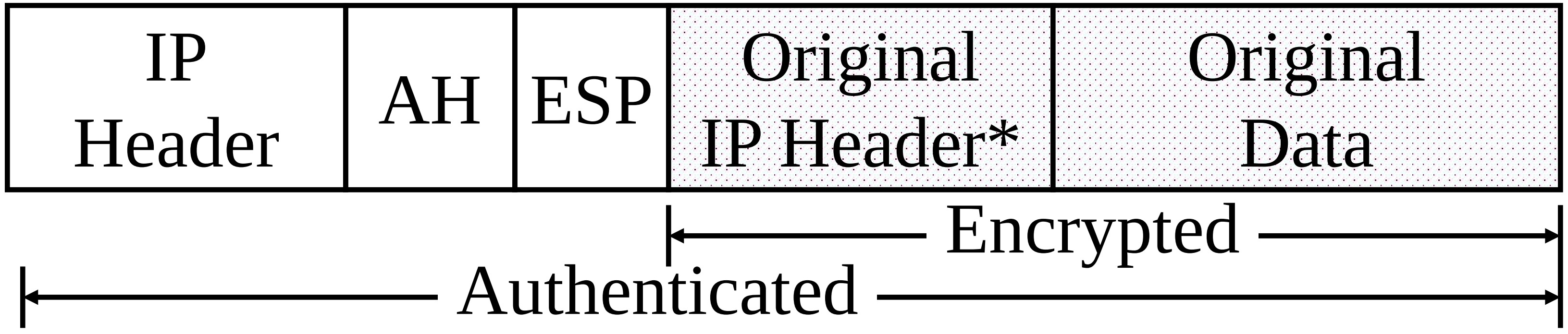


Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

Student Questions

IPsec

- Secure IP: A series of proposals from IETF
- Separate authentication and privacy
- Authentication Header (AH) ensures data *integrity* and *data origin authentication*
- Encapsulating Security Protocol (ESP) ensures *confidentiality*, *data origin authentication, connectionless integrity, and an anti-replay service*

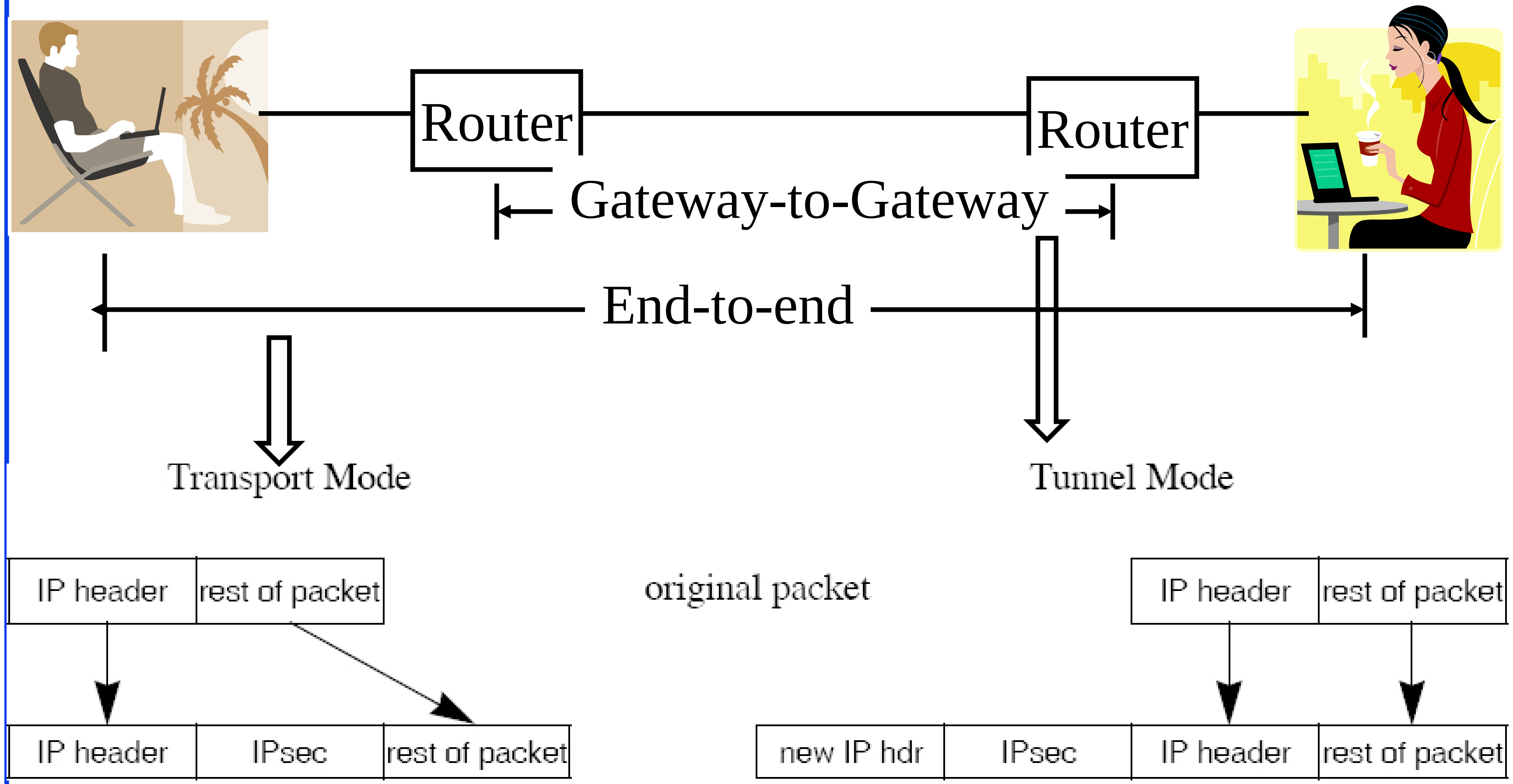


* Optional

Student Questions

Tunnel vs. Transport Mode

- Gateway-to-gateway vs. end-to-end



Student Questions

Authentication Header (AH)

- Provides connectionless integrity using a hash function and a shared secret key
- Integrity Check Value (ICV) covers most of the fields in the datagram
- Guarantees data origin (using MAC)
- Optionally adds sequence numbers to protect against replay attacks

Student Questions

Encapsulating Security Payload (ESP)

Provides:

- Message content confidentiality,
- Data origin authentication,
- Connectionless integrity,
- Anti-replay service,
- Limited traffic flow confidentiality (TFC)
- Services depend on options selected when establishing Security Association (SA), net location
- Can use a variety of encryption & authentication algorithms

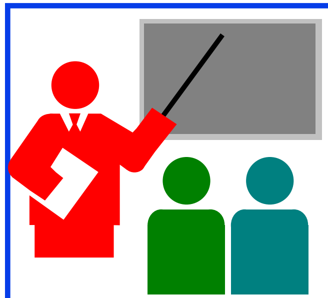
Student Questions

IPsec Key Management (IKE)

- Handles key generation & distribution
- Typically need two pairs of keys
  - Two per direction for integrity and confidentiality
- Manual key management
  - System administrator manually configures every system
- Automated key management
  - Automated system for on-demand creation of keys for SA's in large systems

Ref: http://en.wikipedia.org/wiki/Internet_Key_Exchange

Student Questions

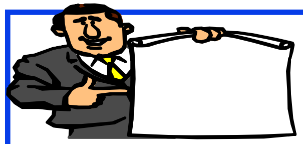


Summary: IPsec

1. IPsec provides authentication, confidentiality, and key management at Layer 3. Applies to all traffic.
2. Security associations are one-way and can be bundled together.
3. Authentication header for message authentication
4. Encapsulating security protocol (ESP) for confidentiality and/or integrity
5. Both can be used end-to-end with the original IP header inside (Tunnel) or without the original IP header (Transport) mode

Ref: Read Section 8.7 and Exercises R24-R26

Student Questions



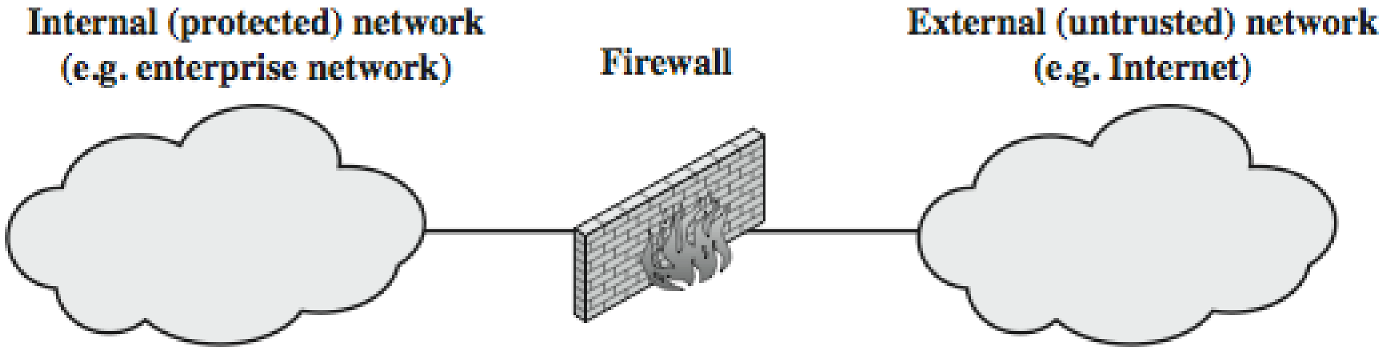
Firewalls and IDS

1. What is a Firewall?
2. Types of Firewalls
3. Intrusion Detection Systems
4. Honeypots

Student Questions

What is a Firewall?

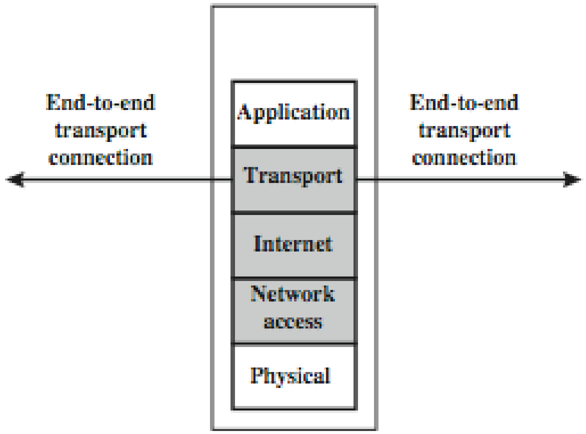
- Interconnects networks with differing trust
  - Only authorized traffic is allowed
- Auditing and controlling access
  - Can implement alarms for abnormal behavior
- Provides network address translation (NAT) and usage monitoring
- Implements VPNs

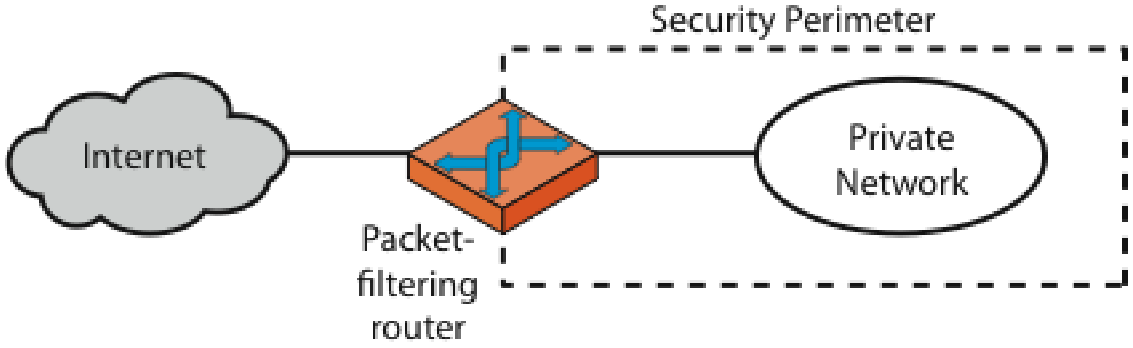

Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)

Student Questions

Firewalls – Packet Filters

- Examine each IP packet (no context) and permit or deny according to the rules


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection



(a) Packet-filtering router

Student Questions

Firewalls – Packet Filters

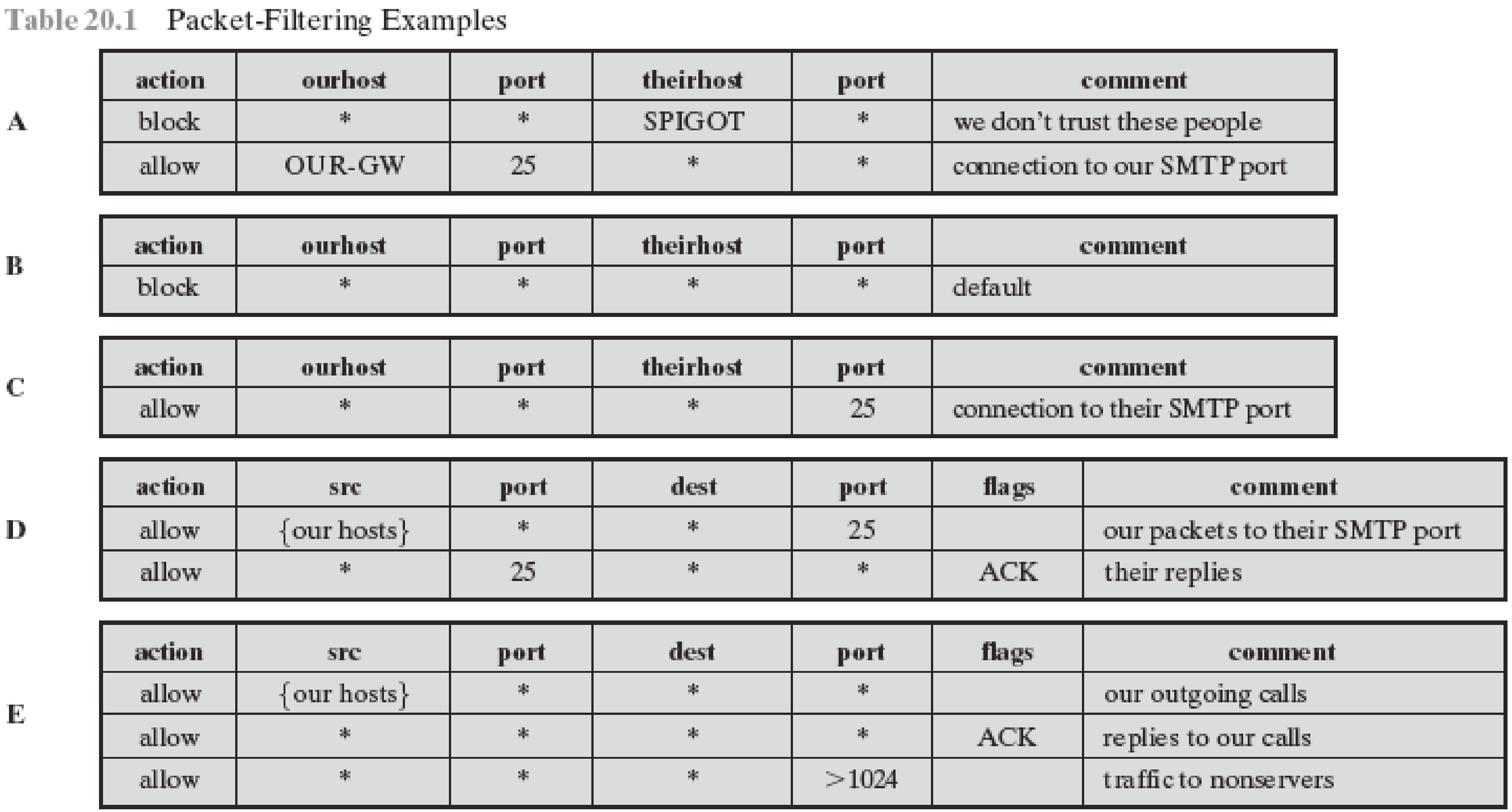


Table 20.1 Packet-Filtering Examples

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

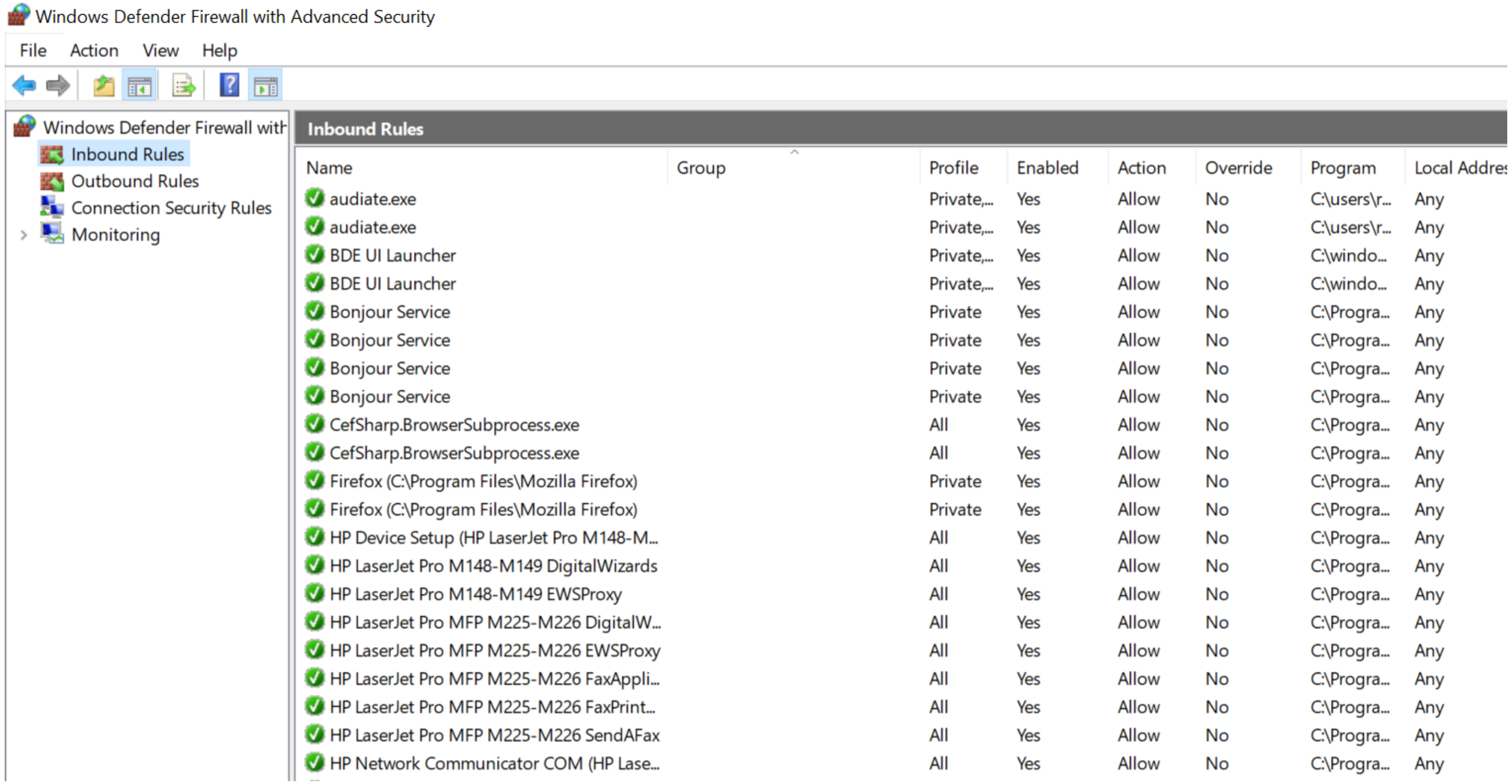
E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Student Questions

Packet Filter Example: Windows Firewall

- Windows Defender Firewall with Advanced Security → Inbound Rules


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Addres
audiate.exe		Private,...	Yes	Allow	No	C:\users\r...	Any
audiate.exe		Private,...	Yes	Allow	No	C:\users\r...	Any
BDE UI Launcher		Private,...	Yes	Allow	No	C:\windo...	Any
BDE UI Launcher		Private,...	Yes	Allow	No	C:\windo...	Any
Bonjour Service		Private	Yes	Allow	No	C:\Progra...	Any
Bonjour Service		Private	Yes	Allow	No	C:\Progra...	Any
Bonjour Service		Private	Yes	Allow	No	C:\Progra...	Any
Bonjour Service		Private	Yes	Allow	No	C:\Progra...	Any
CefSharp.BrowserSubprocess.exe		All	Yes	Allow	No	C:\Progra...	Any
CefSharp.BrowserSubprocess.exe		All	Yes	Allow	No	C:\Progra...	Any
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow	No	C:\Progra...	Any
HP Device Setup (HP LaserJet Pro M148-M...		All	Yes	Allow	No	C:\Progra...	Any
HP LaserJet Pro M148-M149 DigitalWizards		All	Yes	Allow	No	C:\Progra...	Any
HP LaserJet Pro M148-M149 EWSProxy		All	Yes	Allow	No	C:\Progra...	Any
HP LaserJet Pro MFP M225-M226 DigitalW...		All	Yes	Allow	No	C:\Progra...	Any
HP LaserJet Pro MFP M225-M226 EWSProxy		All	Yes	Allow	No	C:\Progra...	Any
HP LaserJet Pro MFP M225-M226 FaxAppli...		All	Yes	Allow	No	C:\Progra...	Any
HP LaserJet Pro MFP M225-M226 FaxPrint...		All	Yes	Allow	No	C:\Progra...	Any
HP LaserJet Pro MFP M225-M226 SendAFax		All	Yes	Allow	No	C:\Progra...	Any
HP Network Communicator COM (HP Lase...		All	Yes	Allow	No	C:\Progra...	Any

Student Questions

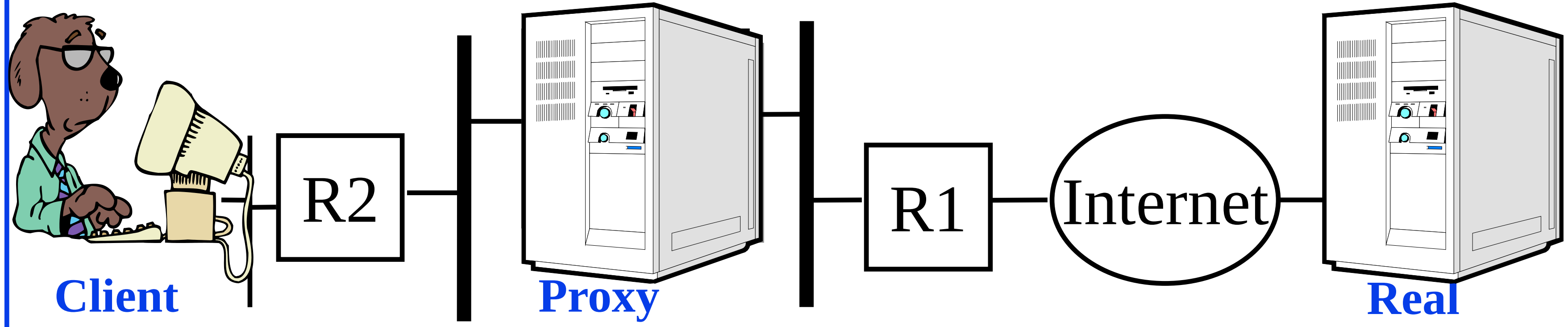
Firewalls – Stateful Packet Filters

- Examine each IP packet in its context
  - Keep track of client-server sessions
- May even inspect limited application data

Student Questions

Proxy Servers

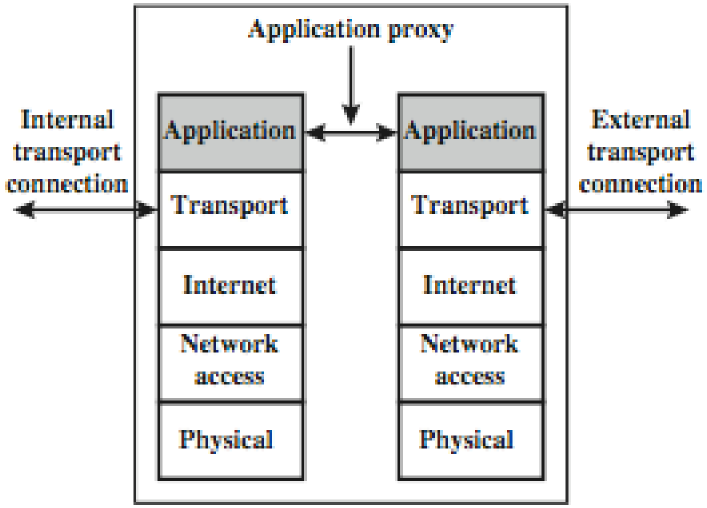
- ❑ Specialized server programs
- ❑ Take user's requests and forward them to real servers
- ❑ Take server's responses and forward them to users
- ❑ Enforce site security policy ⇒ Refuse some requests.
- ❑ Also known as application-level gateways
- ❑ With special "Proxy client" programs, proxy servers are almost transparent

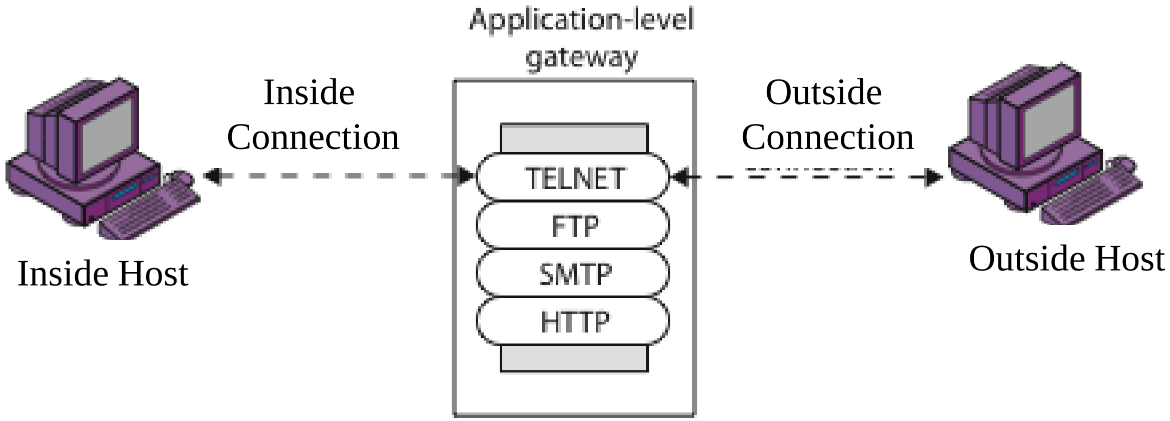


http://www.cse.wustl.edu/~jain/cse473-22/

Student Questions

Application Level Gateway (Cont)



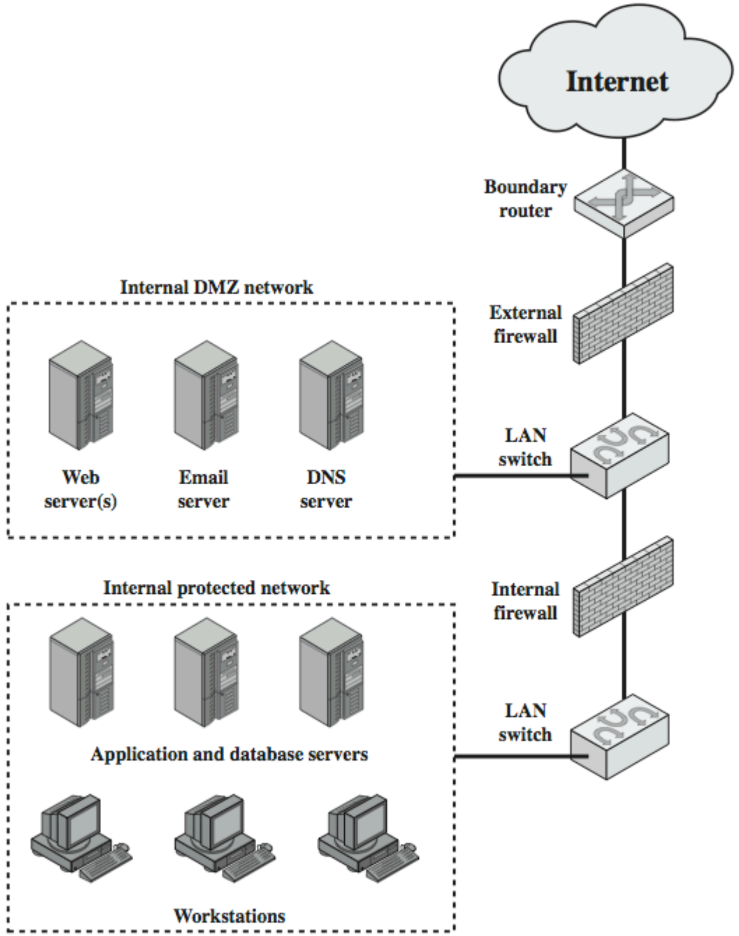


(b) Application-level gateway

Student Questions

DMZ Networks

- Demilitarized Zone



Student Questions

Firewall Limitations

- It cannot protect from attacks bypassing it
  - E.g., sneakernet, utility modems, trusted organizations, trusted services (e.g., SSL/SSH)
- It cannot protect against internal threats
  - E.g., disgruntled or colluding employees
- It cannot protect against access via Wireless LAN
  - If improperly secured against external use, e.g., personal hot spots
- It cannot protect against malware imported via laptops, PDAs, and storage infected outside

Student Questions

Intrusion vs. Extrusion Detection

- **Intrusion Detection**: Detecting unauthorized activity by inspecting inbound traffic
- **Extrusion Detection**: Detecting unauthorized activity by inspecting outbound traffic
- **Extrusion**: Insider visiting a malicious website or a Trojan contacting a remote internet relay chat channel

Student Questions

Types of IDS

- **Signature Based IDS**: Search for known attack patterns using pattern matching, heuristics, protocol decode
- **Rule-Based IDS**: Violation of security policy
- **Anomaly-Based IDS**
- **Statistical or non-statistical** detection. Now **AI-based**.
- Response:
  - **Passive**: Alert the console
  - **Reactive**: Stop the intrusion ⇒ Intrusion Prevention System ⇒ Blocking
- **Snort**: A wide-used open-source IDS

Ref: http://en.wikipedia.org/wiki/Intrusion_detection_system, http://en.wikipedia.org/wiki/Intrusion_detection https://en.wikipedia.org/wiki/Snort_(software)

Student Questions

Honeypots

- Decoy systems to lure attackers
  - Away from accessing critical systems
  - To collect information about their activities
  - To encourage the attacker to stay on the system so the administrator can respond
- Are filled with fabricated information
- Instrumented to collect detailed information on attackers' activities
- Single or multiple networked systems

Ref: http://en.wikipedia.org/wiki/Honeypot_(computing)

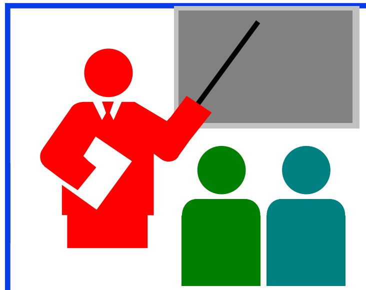
Student Questions

Firewalls and IDS: Summary

1. Firewalls separate networks of different trust levels
2. Some traffic, such as laptops, smartphones, and wireless can bypass the firewall
3. A firewall can be a simple packet filter or an application-level proxy
4. Intruders can be both internal, external or organized
5. IDS can be signature based, anomaly based, or statistical
6. Honeypots can be used to detect intruders

Ref: Section 8.9 and Exercises R28-R32

Student Questions



Summary

1. Network security requires confidentiality, integrity, availability, authentication, and non-repudiation
2. Encryption can use one secret key or two keys (public and private). The public key is very compute-intensive and is generally used to send the secret key
3. The digital certificate system is used to certify the public key. Secure e-mail uses confidentiality using a secret key, uses certificates and public keys to sign the e-mail and send the secret key
4. The web uses SSL/TLS for transport-level security
5. IPsec/IKE is used for VPN
6. Firewalls and IDS are used for security protection

Ref: Sections 8.1 through 8.7, and 8.9

Student Questions

Acronyms

3DES	Triple DES
AES	Advanced Encryption Standard
AH	Authentication Header
ASCII	American Standard Code for Information Interchange
CA	Certificate authority
CBC	Cipher Block Chaining (CBC)
CER	A filetype for certificates
CRC	Cyclic Redundancy Check
DA	Destination Address
DER	Distinguished Encoding Rules (used in X.509)
DES	Data Encryption Standard (DES)
D-H	Diffie-Hellman
DoS	Denial of Service
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing standard
HMAC	Hash-based Message Authentication Code

Student Questions

Acronyms (Cont)

❑ HTTP	Hypertext Transfer Protocol
❑ HTTPS	Hypertext Transfer Protocol with Security
❑ HW	Hardware
❑ ICV	Integrity Check Value
❑ ID	Identifier
❑ IDEA	International Data Encryption Algorithm
❑ IDS	Intrusion Detection System
❑ IETF	Internet Engineering Task Force
❑ IKE	Internet Key Exchange
❑ IKEv2	Internet Key Exchange version 2
❑ IPsec	Secure IP
❑ IPv4	Internet Protocol version 4
❑ IPv6	Internet Protocol version 6
❑ ISAKMP	Internet Security and Key Management Protocol
❑ IV	Initialization Vector
❑ LAN	Local Area Network

Student Questions

Acronyms (Cont)

MAC	Message Authentication Code
MacOS	Mac Operating System
MD4	Message Digest 4
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
MIT	Massachusetts Institute of Technology
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
OpenPGP	Open PGP
PGP	Pretty Good Privacy
RC2	Ron’s Code 2
RC4	Ron’s Code 4
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman

Student Questions

Acronyms (Cont)

SA	Security Association
SHA	Secure Hash
SPI	Security Parameter Index
SSH	Secure Shell
SSL	Secure Socket Layer
SW	Software
TA	Teaching Assistant
TCP	Transmission Control Protocol
TFC	Traffic Flow Confidentiality
TLS	Transport Level Security
TLV	Type-Length-Value
UDP	Universal Datagram Protocol
US	United States
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
XOR	Exclusive OR
WUSTL	Washington University in St. Louis

Student Questions

Scan This to Download These Slides

Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse473-22/i_8sec.htm

Student Questions

Related Modules

CSE 567: The Art of Computer Systems Performance Analysis
https://www.youtube.com/playlist?list=PLjGG94etKypJEKjNAa1n_1X0bWWNyZcof

CSE473S: Introduction to Computer Networks (Fall 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypJWOSPMh8Azcgy5e_10TiDw

CSE 570: Recent Advances in Networking (Spring 2013)

https://www.youtube.com/playlist?list=PLjGG94etKypLHyBN8mOgwJLHD2FFIMGq5

CSE571S: Network Security (Spring 2011),
https://www.youtube.com/playlist?list=PLjGG94etKypKvzfVtutHcPFJXumyyg93u

Video Podcasts of Prof. Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw

Student Questions