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 online at:

http://www.cse.wustl.edu/~jain/cse4703-26/

Student Questions

©2026 Raj Jain



Overview

1. Secret Key Encryption
2. Public Key Encryption
3. Hash Functions, Digital Signature, Digital Certificates
4. Secure e-mail
5. Transport Level Security (TLS)
6. IP Security (IPsec)
7. Firewalls and Intrusion detection systems (IDS)

Note 1: Section 8.8 on Wi-Fi and 4G/5G security are not covered. These topics will not be included in the exam.

Note 2: This class lecture is based on Chapter 8 of the textbook (Kurose and Ross) and the figures provided by the authors. Several figures are also from Lawrie Brown's slides supplied with William Stalling's book "Cryptography and Network Security: Principles and Practice," 7th Ed, 2017.

Student Questions

©2026 Raj Jain



Security Requirements

- **Integrity**: Received = sent?
- **Availability**: Legal users should be able to use it.
  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 the sender nor the receiver can deny the existence of a message.

Student Questions

©2026 Raj Jain

Secret Key Encryption: Overview

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

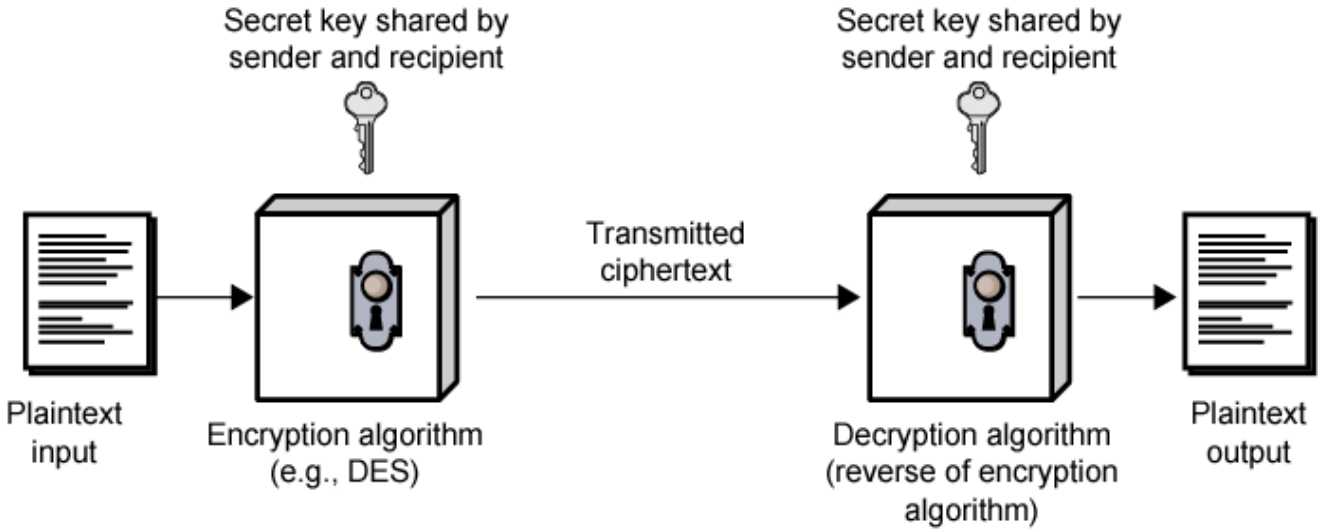
Student Questions

©2026 Raj Jain



Secret Key Encryption

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



Student Questions

©2026 Raj Jain

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

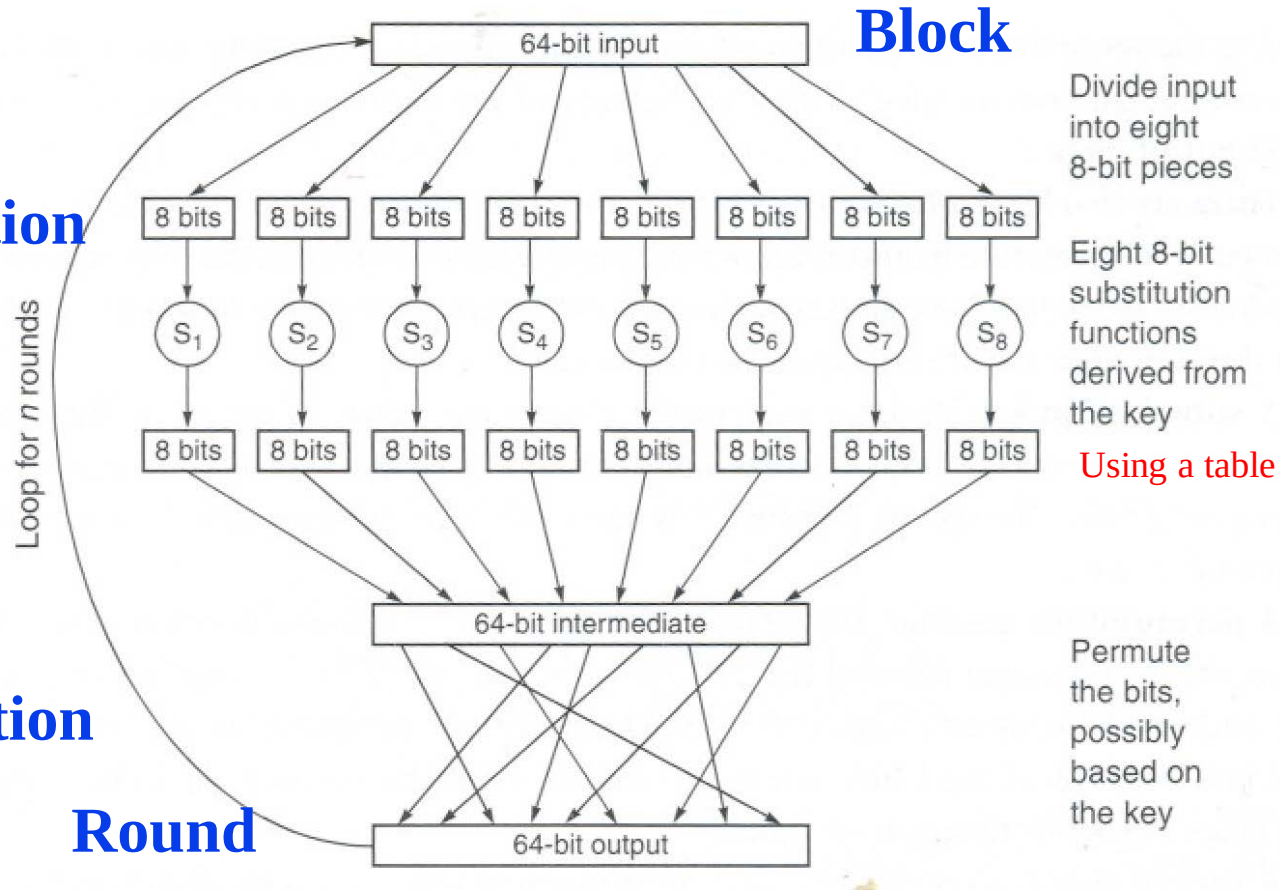
- **Polyalphabetic**: Use multiple substitutions C1, C2, …
  The substitution selected depends upon the position.
  ⇒ The same letter coded differently in a different position.

Student Questions

©2026 Raj Jain

Block Encryption

- Block Encryption



Student Questions

©2026 Raj Jain

Block Encryption (Cont)

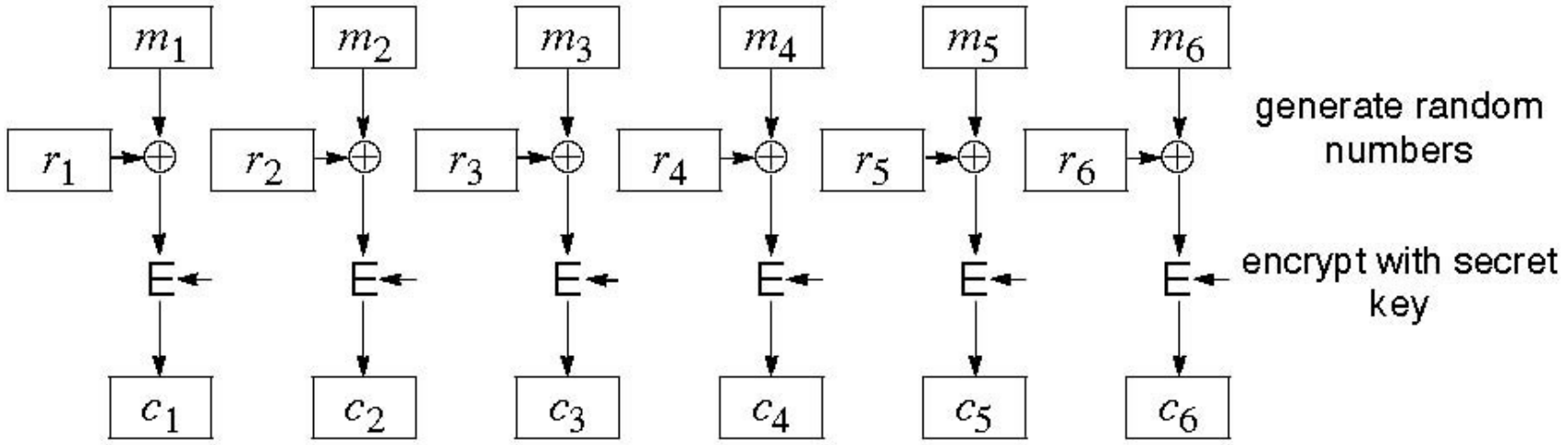
- Short block length ⇒ tabular attack
- 64-bit block
- Transformations:
  - Substitution: replace k-bit input blocks with k-bit output blocks
  - Permutation: move input bits around.
    $1 \rightarrow 13$, $2 \rightarrow 61$, etc.
- Round: Substitution round followed by permutation round and so on.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

Student Questions

©2026 Raj Jain

Cipher Block Chaining (CBC)

- Goal: The same message is encoded differently
- Add a random number before encoding

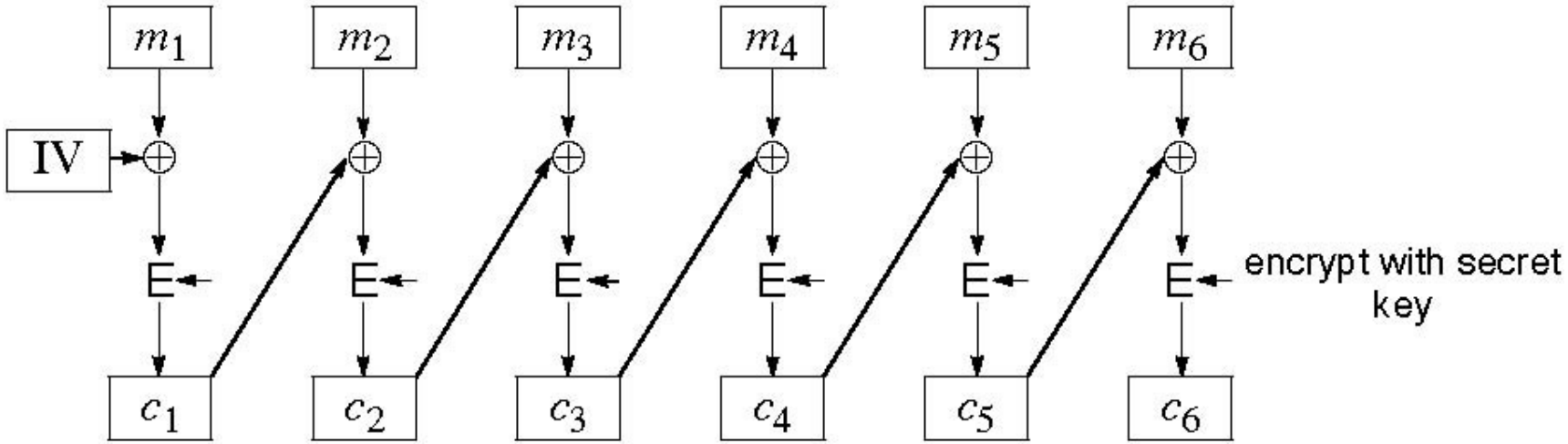


Student Questions

©2026 Raj Jain

CBC (Cont)

- Use C_i as a random number for i+1



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

Student Questions

©2026 Raj Jain

Data Encryption Standard (DES)

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

Student Questions

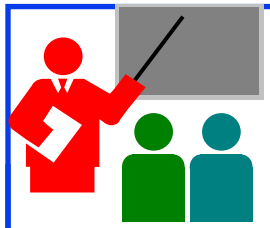
©2026 Raj Jain

Advanced Encryption Standard (AES)

- Designed in 1997-2001 by the National Institute of Standards and Technology (NIST)
- Federal information processing standard (FIPS 197)
- A symmetric block cipher with a block length of 128 bits
- Key lengths 128, 192, and 256 bits.
  The entire key is used-no parity bit in the byte.
  The memory may use 9 bits to store a byte.

Student Questions

©2026 Raj Jain



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 to ensure that the same plain text results in different ciphertexts.

Student Questions

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

©2026 Raj Jain

Homework 8A

- [6 points] Consider the 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 ciphertext. 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

©2026 Raj Jain



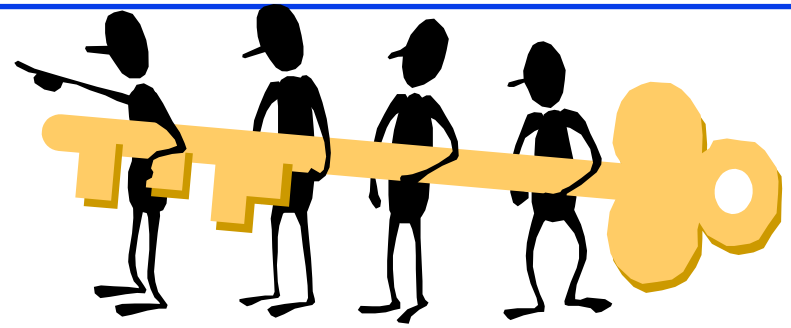
Public Key Encryption

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

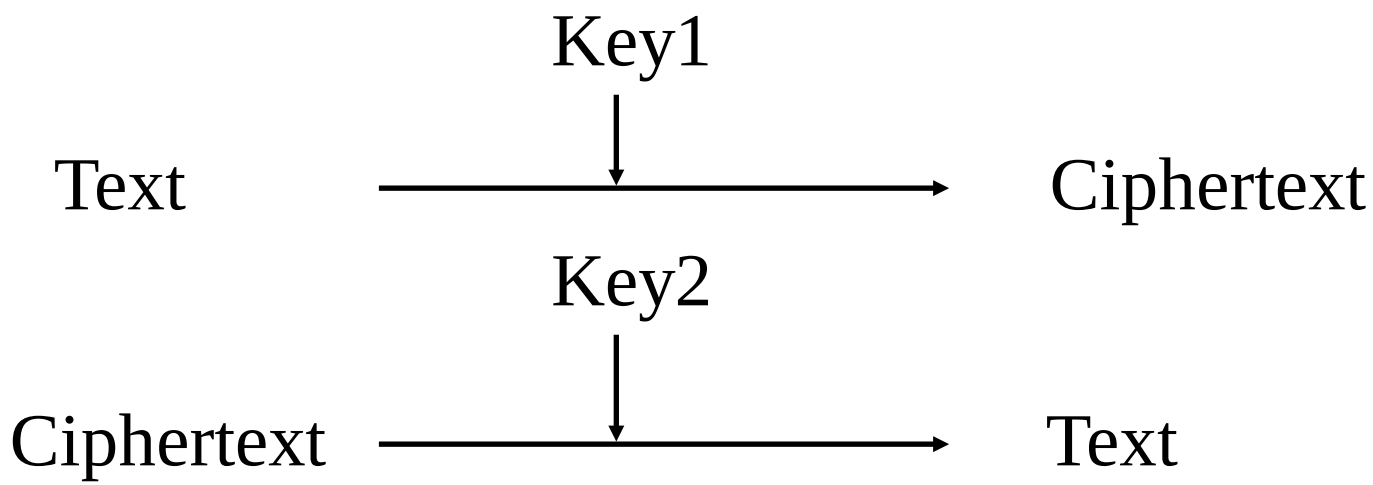
Student Questions

©2026 Raj Jain

Public Key Encryption



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

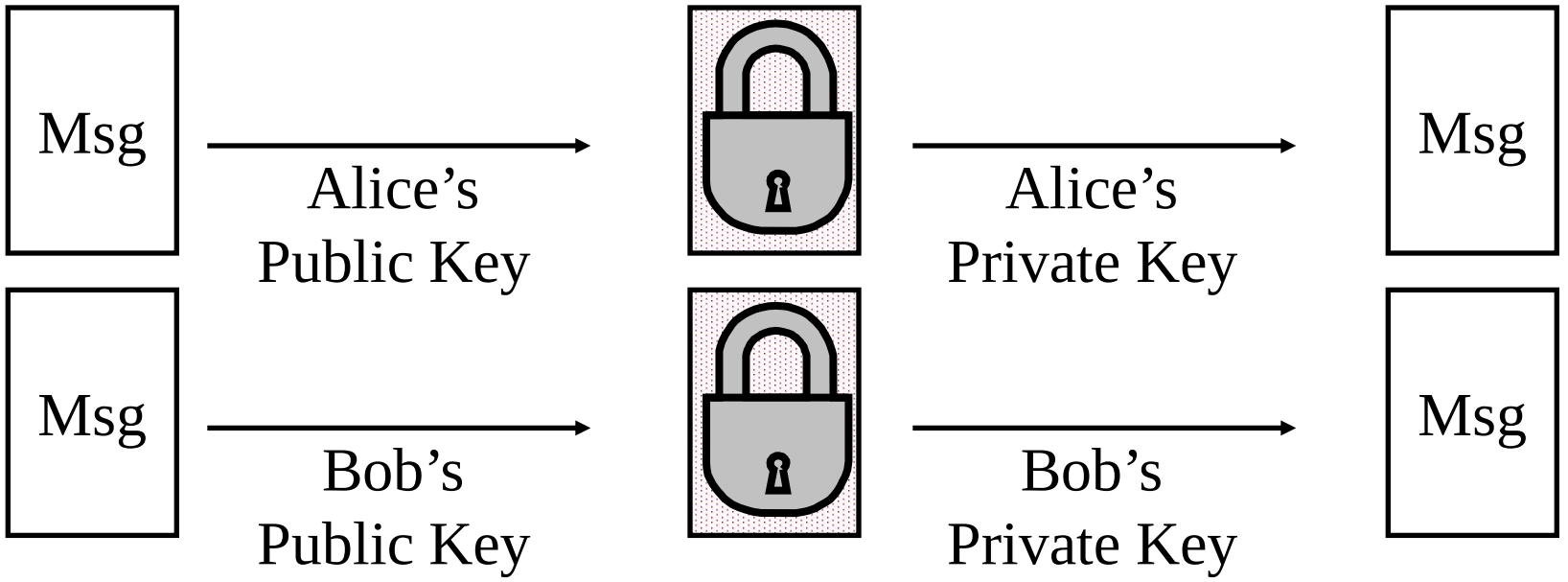


Student Questions

©2026 Raj Jain

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 the public key can be decrypted by the private key
  Encrypted with the private key can be decrypted by the public key



Student Questions

©2026 Raj Jain

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

©2026 Raj Jain

Modular Arithmetic

- $xy \bmod m = (x \bmod m)\,(y \bmod m) \bmod m$
- $x^4 \bmod m = (x^2 \bmod m)(x^2 \bmod m) \bmod m$
- $x^{ij} \bmod m = (x^i \bmod m)^j \bmod m$
- $125 \bmod 187 = 125$
- $125^2 \bmod 187 = 15625 \bmod 187 = 104$
- $125^4 \bmod 187 = (125^2 \bmod 187)^2 \bmod 187$
  $= 104^2 \bmod 187 = 10816 \bmod 187 = 157$
- $125^8 \bmod 187 = 157^2 \bmod 187 = 152$
- $125^{16} \bmod 187 = 152^2 \bmod 187 = 103$
- $125^{32} \bmod 187 = 103^2 \bmod 187 = 137$
- $125^{64} \bmod 187 = 137^2 \bmod 187 = 69$
- $125^{107} = 125^{64+32+8+2+1} \bmod 187$
  $= 69 \times 137 \times 152 \times 104 \times 125 \bmod 187$
  $= 18679128000 \bmod 187 = 5$
- You 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

End Part 1

©2026 Raj Jain

RSA Public Key Encryption

- Ron Rivest, Adi Shamir, and Len Adleman at MIT 1978
- Both plain text M and ciphertext 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

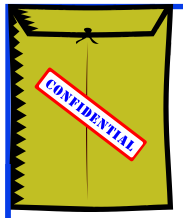
©2026 Raj Jain

RSA Algorithm: Example

- Select two large primes: p, q, p ≠ q
  p = 17, q = 11
- n = p×q = 17×11 = 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}

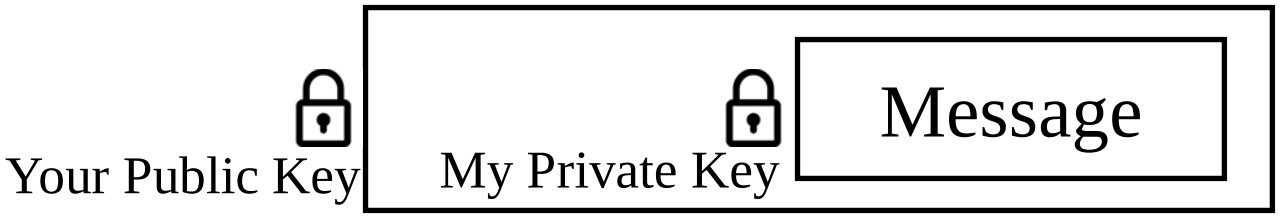
Student Questions

©2026 Raj Jain



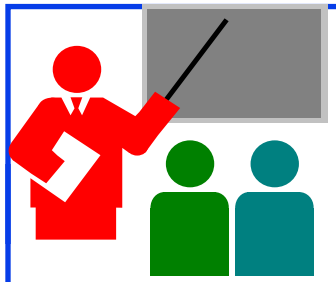
Confidentiality and Non-Repudiation

- 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

©2026 Raj Jain



Public Key Encryption: Review

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

Student Questions

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

©2026 Raj Jain

Homework 8B

Consider RSA with p=7, q=17

A. what are n and z

B. let e be 5. Why is this an acceptable choice for e?

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

D. Encrypt the message m=25 using the public key (n, e). Let c be the corresponding ciphertext.

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

Student Questions

©2026 Raj Jain



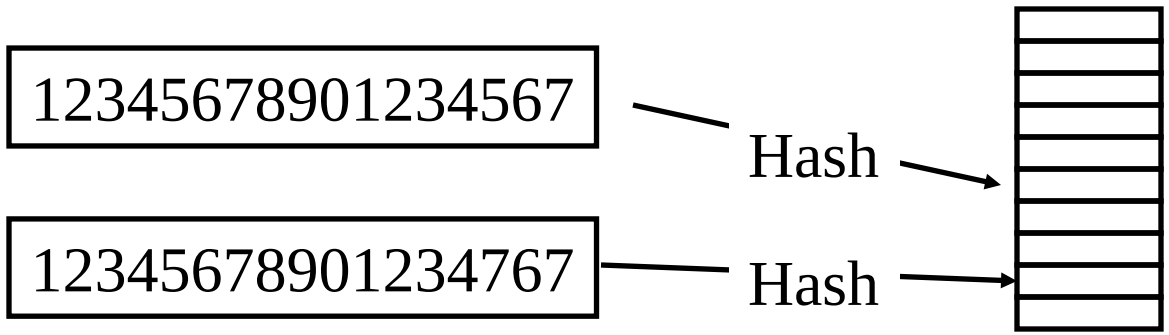
Hash, Signatures, Certificates

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

©2026 Raj Jain

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

©2026 Raj Jain

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

©2026 Raj Jain

SHA-1 Algorithm

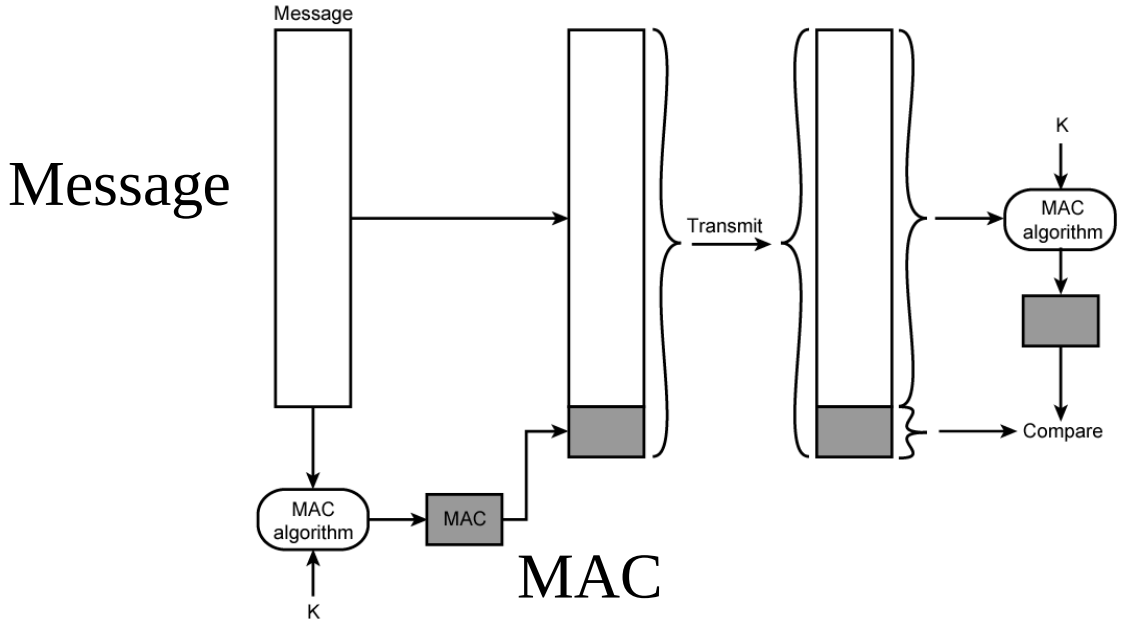
- 160-bit hash using 512-bit blocks and 32-bit operations
- Five passes (compared to 4 in MD5 and 3 in MD4)
- The maximum message size is 2^{64} bit

Student Questions

©2026 Raj Jain

Message Authentication Code (MAC)

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



Student Questions

©2026 Raj Jain

HMAC Overview

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

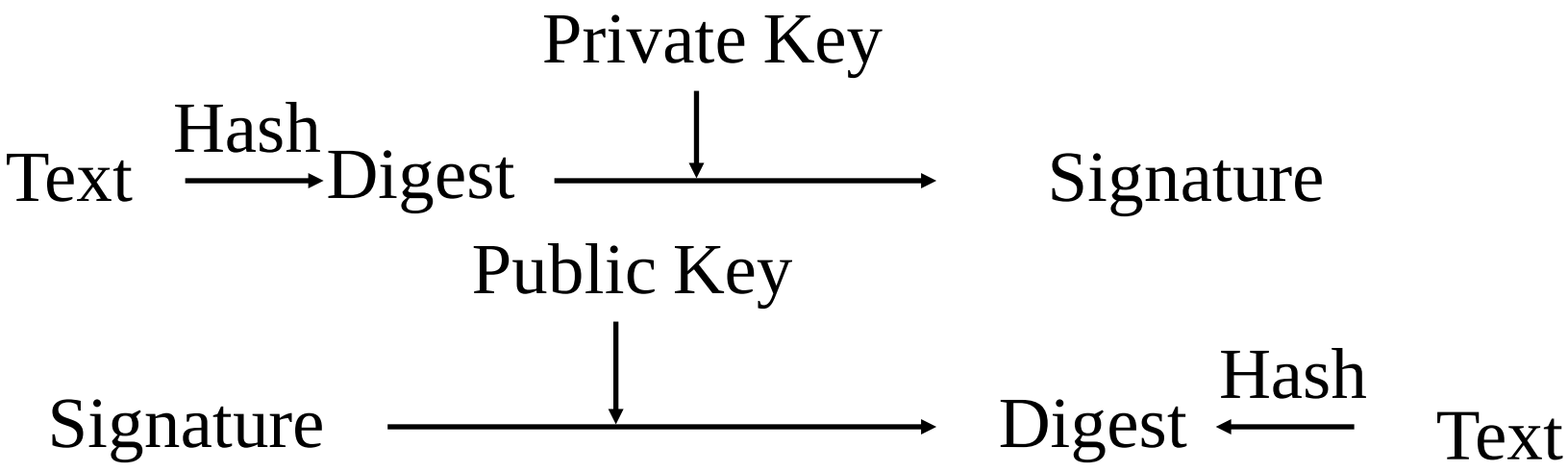
Student Questions

©2026 Raj Jain



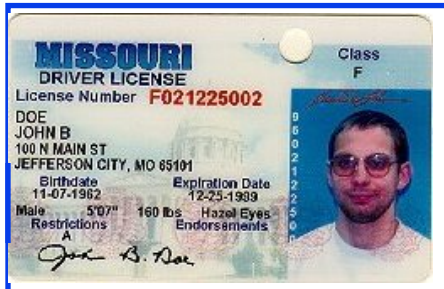
Digital Signature

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



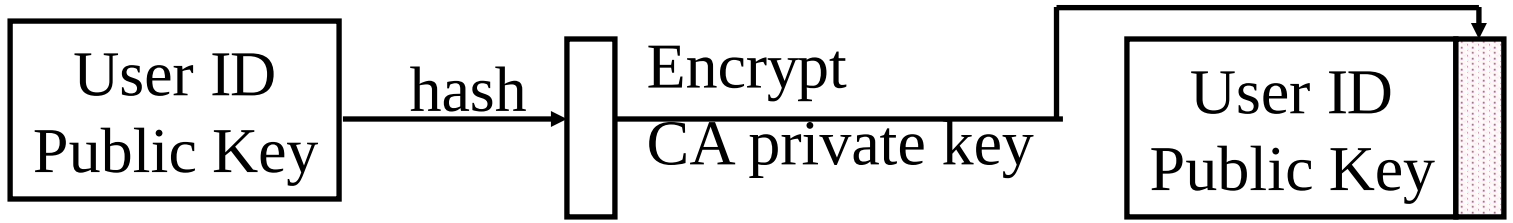
Student Questions

©2026 Raj Jain



Digital Certificates

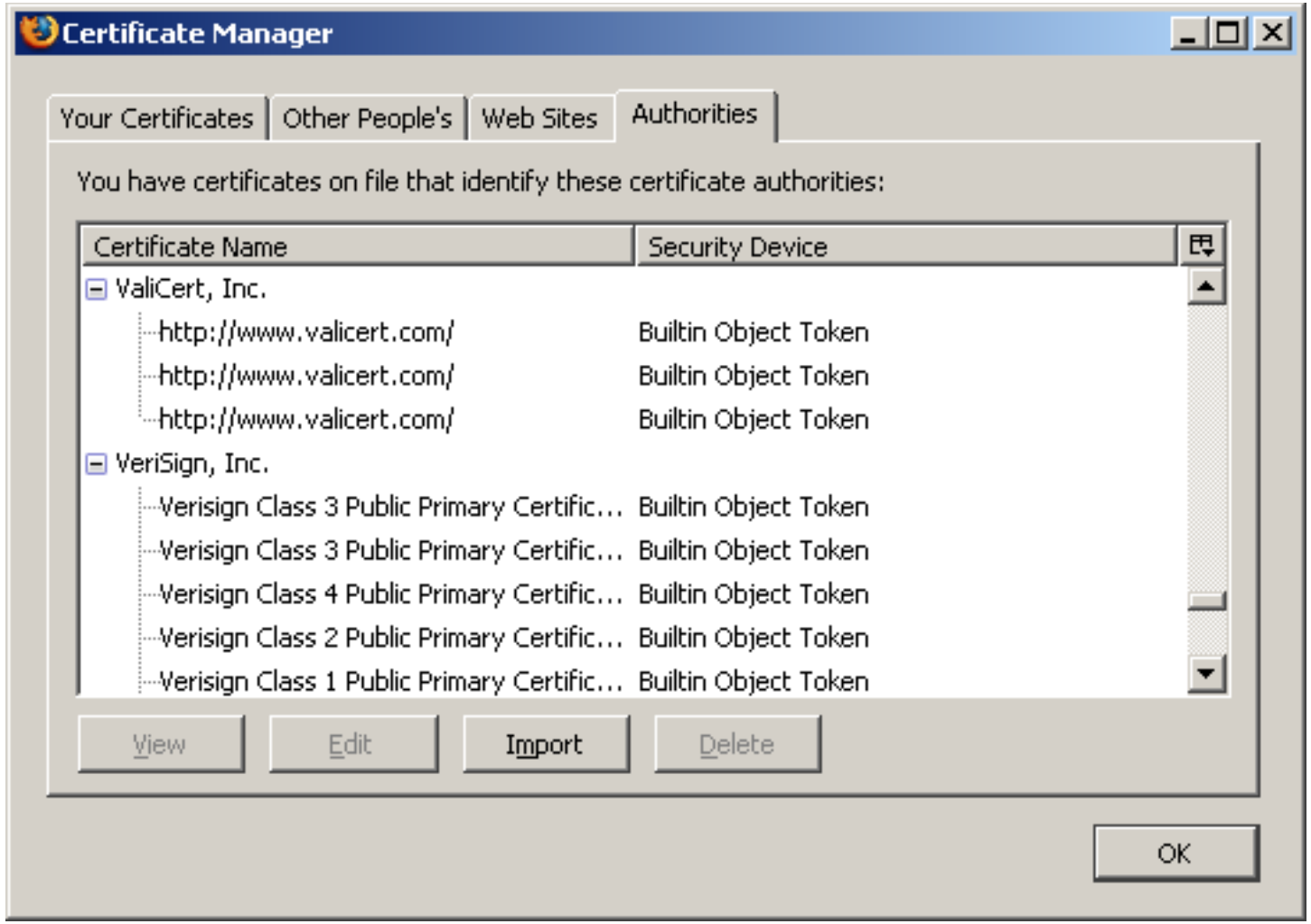
- Like a driver's license or passport
- Digitally signed by a Certificate Authority (CA) - a trusted organization
- Public keys are distributed with certificates
- CA uses its private key to sign the certificate
  ⇒ Hierarchy of trusted authorities
- X.509 Certificate includes: Name, organization, effective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



Student Questions

©2026 Raj Jain

Oligarchy Example



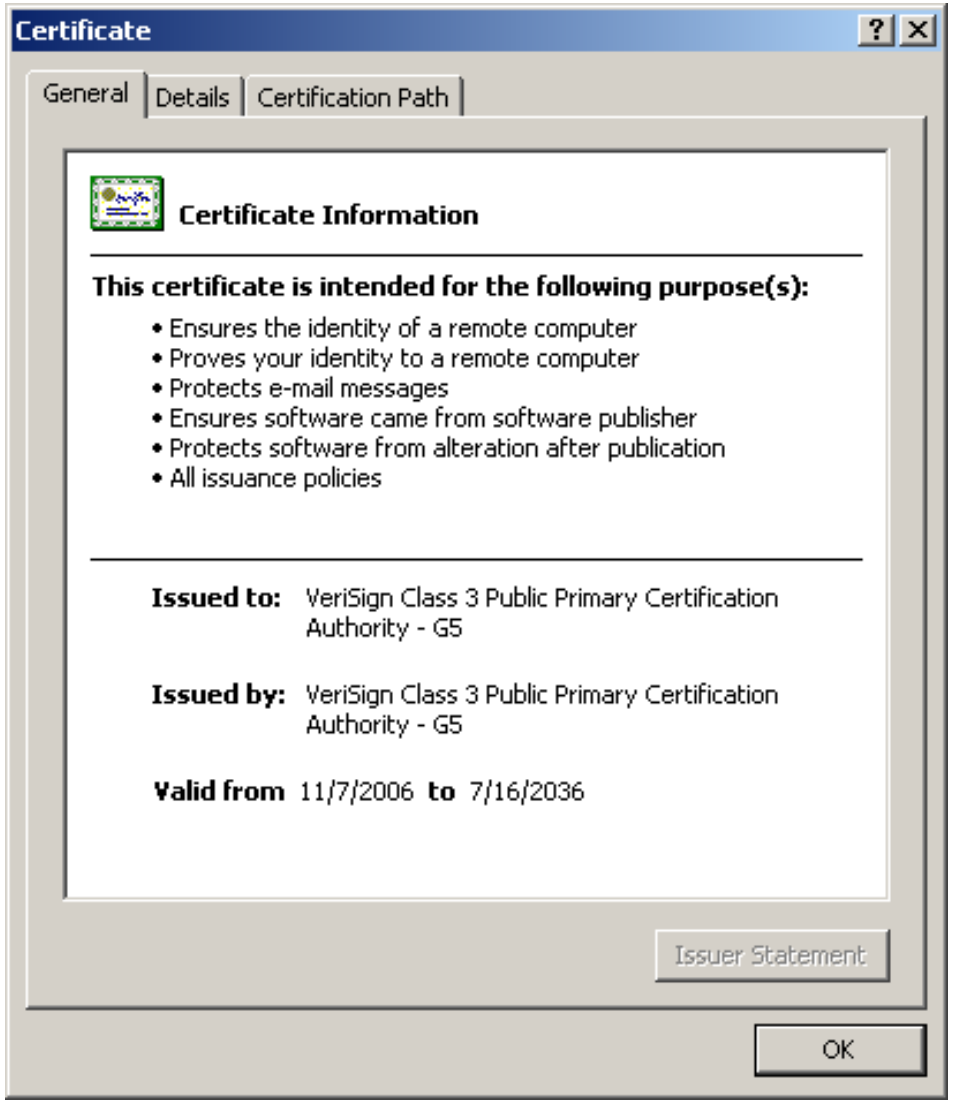
Ref: Windows: http://smallbusiness.chron.com/see-security-certificates-stored-computer-54732.html
MAC: https://superuser.com/questions/992167/where-are-digital-certificates-physically-stored-on-a-mac-os-x-machine

Student Questions

©2026 Raj Jain

Sample X.509 Certificate

- Certmgr.msc in Windows



Student Questions

©2026 Raj Jain

X.509 Sample (Cont)

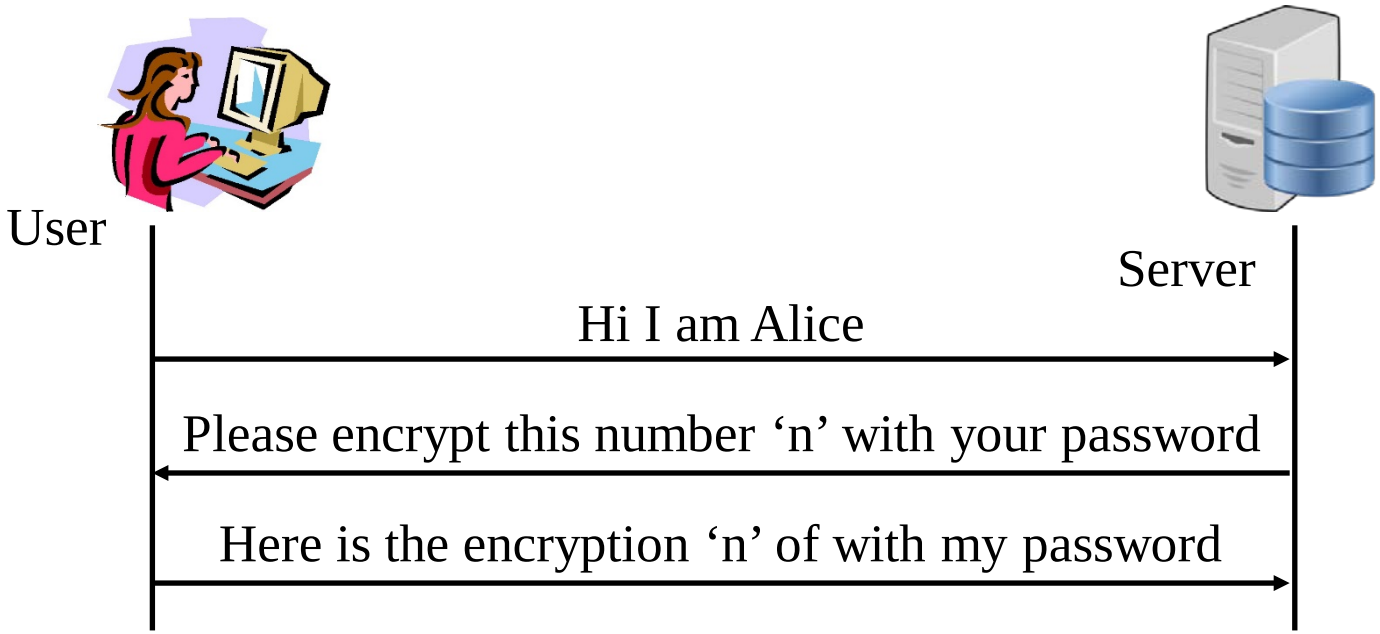
Field	Value
Version	V3
Serial number	18 da d1 9e 26 7d e8 bb 4a 21...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Public Primary ...
Valid from	Tuesday, November 07, 2006 ...
Valid to	Wednesday, July 16, 2036 6:...
Subject	VeriSign Class 3 Public Primary ...
Public key	RSA (2048 Bits)
version	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 of Part 1

End Point Authentication

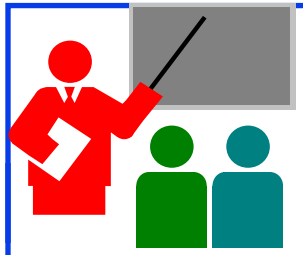
- Passwords can not be exchanged in clear
  Nonce = random **n**umber used only **once**
- Also done using certificates



Requires the server to store passwords in clear.

Student Questions

©2026 Raj Jain



Hashes, Signatures, Certificates

1. Hashes are one-way functions such that it is difficult to find another input with the same hash, like MD5 and 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 the private key.
4. Digital certificates are signed by root certification authorities and contain public keys.

Student Questions

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

©2026 Raj Jain



Secure E-mail

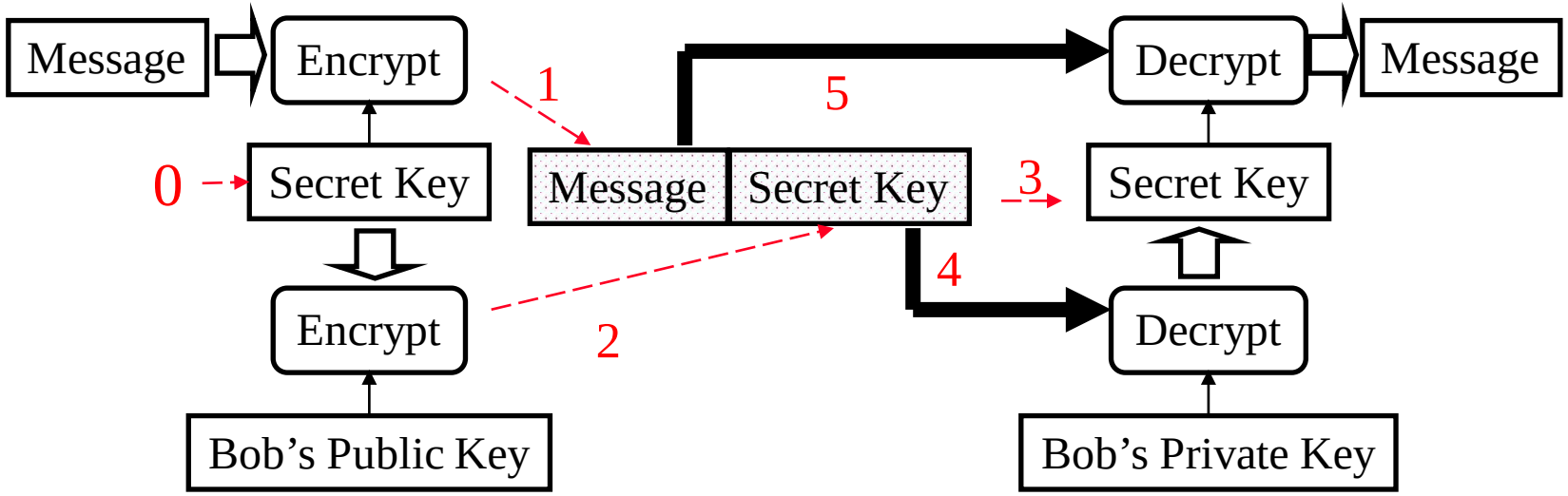
1. Secure E-Mail
2. Signed a Secure E-Mail
3. Pretty Good Privacy (PGP)

Student Questions

©2026 Raj Jain

Secure E-Mail

- Alice wants to send a 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.

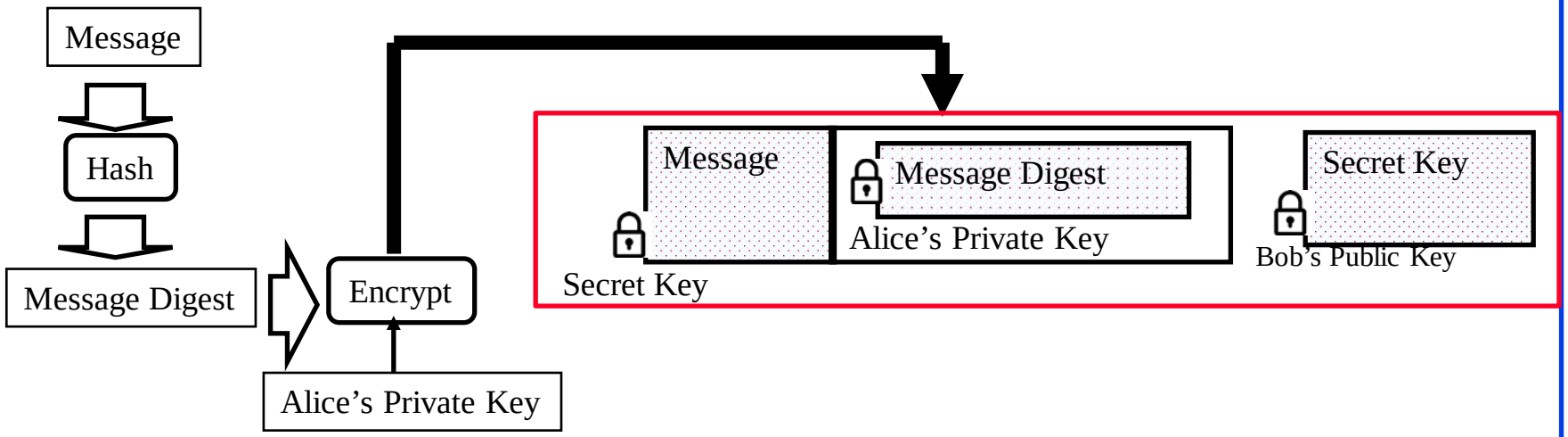
- **Bob:**
  4. Bob uses his private key to recover K_s
  5. Bob decrypts the message

Student Questions

©2026 Raj Jain

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

©2026 Raj Jain

Pretty Good Privacy (PGP)

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

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

©2026 Raj Jain

Student Questions



Lab 8: Secure e-mail

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

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

- You can reply to the TA's e-mail with a signed, encrypted message. The reply content should be the contents of the "**Enhanced key usage**" field in your new certificate.
- Before sending the reply, on the Outlook message window, Set the security options as required.
  Select encryption and signature. Now send the message.
  Take a screenshot and submit it on Canvas.
- **Outlook is required** for both Windows and Mac.
- **Common Mistakes**: 1. Not signing. 2. Not encrypting. 3. Not looking at your certificate to find the correct field to send the message. Please avoid all three.

Student Questions

©2026 Raj Jain

Lab 8 (Cont)

- To sign your e-mail with a private key, you need your digital certificate.
- To send an encrypted e-mail to TA, you need TA's public key.
- TA's public key is attached with their e-mail in his certificate.
- The steps to obtain a free certificate and use it for e-mail depend on your e-mail software and operating system. Instructions for Outlook on Windows 10 are included next.
- Instructions for Mac are similar. Further details for Mac are in the reference cited below.

Ref: https://support.apple.com/guide/mail/use-personal-certificates-mlhlp1179/mac

Student Questions

©2026 Raj Jain

1. Getting Your Certificate

- In any browser, go to https://extrassl.actalis.it/portal/uapub/freemail?lang=en
- Enter your wustl.edu e-mail address. Leave everything else blank. and click on "Send Verification e-mail." Leave the page open.
- Check your e-mail. You will receive a verification code in an e-mail within a few minutes. Enter the received verification code on the previous page. Enter Captcha, if any. Accept the conditions. Submit request. It will send the certificate in an e-mail and present a password on the screen. Copy and paste the password into some text file. Also, print the page to pdf (as a backup) to save the password.
- You will receive a zip file by e-mail. Unzip it to get the .pfx file.

Student Questions

©2026 Raj Jain

2. Installing your Certificate in Outlook (Windows)

- Open the Outlook App (not the website and follow the following click sequence:
- File → Options → Trust Center→ Trust Center Settings → e-mail Security → Digital IDs import/export
- Import the certificate file and enter the password that the certificate issuer gave. Click OK.
- Note: If you select always sign outgoing messages or always encrypt outgoing messages, Outlook will ask your permission to access the private store every time you send an e-mail. If it becomes a nuisance, clear those options. You can still sign and encrypt individual messages using message options.

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

Student Questions

©2026 Raj Jain

2. Installing Certificate in Outlook (Mac)

1. On Mac, open the application "Keychain Access.app"
2. On the left sidebar, there should be a category called "System Keychains.“ Within that category, click on the “System” keychain.
3. File>Import Items. Select the certificate file you downloaded.
4. You will be prompted to enter at least the certificate password and your macOS user password.
5. You should see the new certificate added to the "System" keychain. Restart Microsoft Outlook.
6. Open Outlook Preferences>Account>Select your WUSTL account>Security. Under the two certificate drop-down menus, select your newly added certificate. Set your preferences.

Ref: How to Install Certificates on OS X Apple Mail & Outlook, https://sectigo.com/resource-library/install-certificates-os-x-apple-mail-outlook

Student Questions

©2026 Raj Jain

3. Sending Secure e-mail Using Outlook

Microsoft has done its best to hide the security options four levels down. Here is your cheat sheet to get there.

- While composing a message, if you are in a part of the screen, pop out to a full window (see pop-out on the top right of the message panel)
- Click-Options (4th menu item on the top)
- Click "…" (3 dots on the right. You would never know what this is for.) A new panel will open.
- Select the bottom option – Message options
- In the panel that opens up, select security settings (right top 2nd line)
- There are four checkboxes. Select them as you like.
- You may want to clear the check box for "Send this message as clear text signed." Microsoft wants you to send it as clear text, so this option is pre-checked for you. Clear it.

Student Questions

©2026 Raj Jain

4. Importing Contacts' 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.
- Right-click on the name in the "From field" in the message window 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 an e-mail to this contact, you can enable the security options for encryption and signatures.
- Alternate Procedure:
  - Open the signed e-mail 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

©2026 Raj Jain

4. Sending Encrypted E-mails

- The recipient may see "There is a problem with the signature" when they receive the signed message for the first time. 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. The recipient's public key is automatically installed in your Outlook when you open that message.
- After both of you have each other's public keys, you can send encrypted e-mails to each other. You can send such messages by selecting the drop-down menu on the "Encrypt" button (right next to the "Sign" button) and selecting "Encrypt with S/MIME."

Student Questions

©2026 Raj Jain

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 the Details tab. Scroll down to find "Enhanced Key Usage." Click on it to see the results in the bottom pane. Please copy and paste it to your e-mail reply to the TA e-mail.
- 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

©2026 Raj Jain

Lab 8 Hints (Cont)

- If you get the error:

"I didn't receive a valid Certificate Request, please try a different browser."

- To work around this, please follow the steps below using **CAcert's manual CSR submission method**:

1. Go to the following website to generate a CSR:

   https://community.cacert.org/clientcert/
2. Fill in your details and generate the certificate signing request (CSR).
3. You will receive a block of text like this:
   -----BEGIN CERTIFICATE REQUEST-----
   (some encoded lines)
   -----END CERTIFICATE REQUEST-----
4. Copy and paste the entire CSR (**including the "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE REQUEST-----" lines)** into the certificate request field on the CAcert.org website.
5. Then, click to proceed, and on the next screen, click "install the certificate into your browser".
6. Continue with the remaining steps to complete the process.

Student Questions

©2026 Raj Jain

Lab 8 Hints iPad (Cont)

- On iPad (10th Generation or higher) with IOS 18.3.2 or higher, go to Actalis website and download the S/MIME certificate (.p12 file). A pop-up will say "Profile Downloaded - Review the profile in the Settings app if you want to install it". Close the popup and go to Settings where under the Profile Name and above Airplane Mode (the first setting), you will see "Profile Downloaded". Click it, and install the Profile. It will ask for device password. After putting in your password, you will need to also put in the password Actalis sent you in the email. Then it should direct you to the certificate, located in General -> VPN & Device Management -> and you should see your email under the Configuration Protocol. Here you can find data and information about the certificate.
- For the next step, however, still in Settings go to Apps ->Mail ->Mail Accounts -> Exchange (For Wustl) -> Account Settings -> Advanced Settings -> and under S/MIME make sure Sign and Encrypt are Yes by clicking and toggling the setting. Your certificate should be under this setting and when you click on it it should be Trusted.
  Then, in your IOS Mail app, you will be able to email the TA and when you do, it should say "Encrypted" at the top. The TA's contact has a lock icon next to it as well. Then send the Enhanced Key information in the email.

Student Questions

©2026 Raj Jain

Lab 8 Hints (Cont)

- Even if you use iPad, one way to see Enhanced Key Usage is to download the Certificate from Actalis onto a Windows PC, following the steps from the slides (Run->certmgr.msc->Personal->Certificates->Double Click certificate->Details->Enhanced Key Usage).
- **Lab 8 on Mac:** Install Microsoft outlook as an app on a Mac and then followed slides instructions.
- Error:f you receive a pop-up saying you have a "missing or invalid certificate" when trying to send the TA an encrypted email, it's because **TA's public certificate is not stored on your computer yet**.
- You have **two options** to resolve this:
  Option 1: Reply Directly to TA's Signed Email. Simply reply to TA's digitally signed email — Outlook will automatically extract and use TA's certificate, allowing you to encrypt your reply.
  Option 2: Manually Install TA's Certificate and Send a New Email. If you prefer to send a new encrypted email (instead of replying), you need to **i**nstall TA's certificate manually:

Student Questions

©2026 Raj Jain

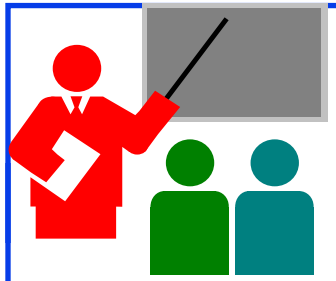
Lab 8 Hints (Cont)

- Option 2 Steps **(for Windows users):**

1. Open the email TA sent you.
2. Click the **certificate icon** (ribbon icon) next to TA's name.
3. Click **"Details…"** in the Digital Signature popup.
4. Select **"Signer: …@wustl.edu"**, then click **"View Details…"**
5. Click **"View Certificate"**.
6. In the new window, go to the **"Details"** tab and click **"Copy to File…"**
7. Choose **"DER encoded binary X.509 (.CER)"** format.
8. Save the file to your computer.
9. Double-click the saved .cer file and follow the prompts to **install the certificate**.
10. After installation, you can **compose a new email** and send it **encrypted**.

Student Questions

©2026 Raj Jain



Secure e-mail: Review

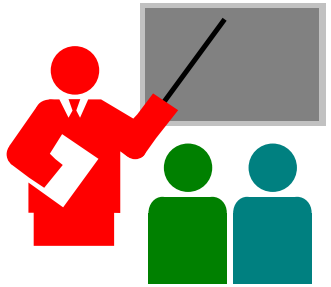
1. e-mail provides confidentiality using a secret key
2. Public keys and certificates are used to:
    1. Sign the message
    2. To send the secret key

Student Questions

Ref: Section 8.5, Review question R19

©2026 Raj Jain

Summary: So Far



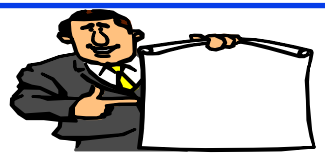
1. Network security requires confidentiality, integrity, availability, authentication, and non-repudiation.
2. Encryption can use one secret key or two keys (public and private)
3. The public key is very compute-intensive and is generally used to send the secret key
4. A digital certificate system is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

©2026 Raj Jain

End of Part 2



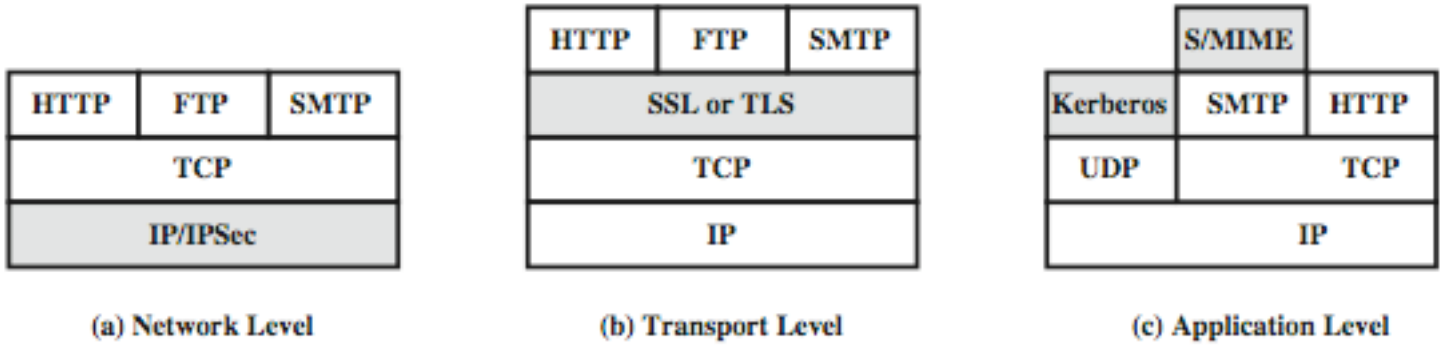
Transport Layer Security (TLS)

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

Student Questions

©2026 Raj Jain

Web Traffic Security Approaches



(a) Network Level (b) Transport Level (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

©2026 Raj Jain

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

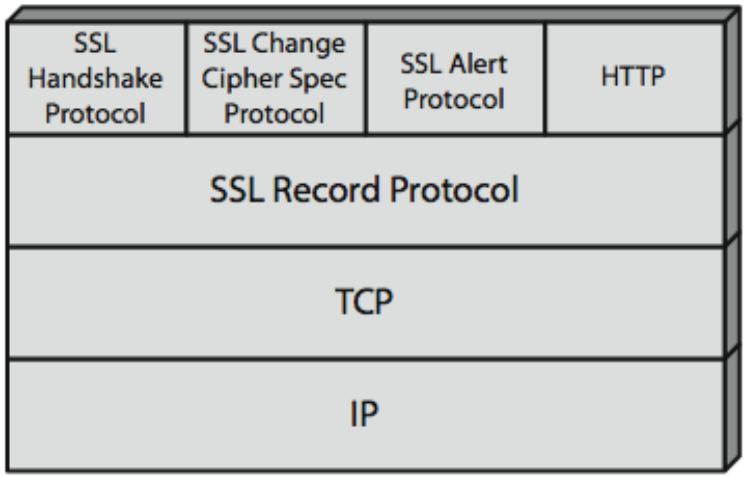
Student Questions

©2026 Raj Jain

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

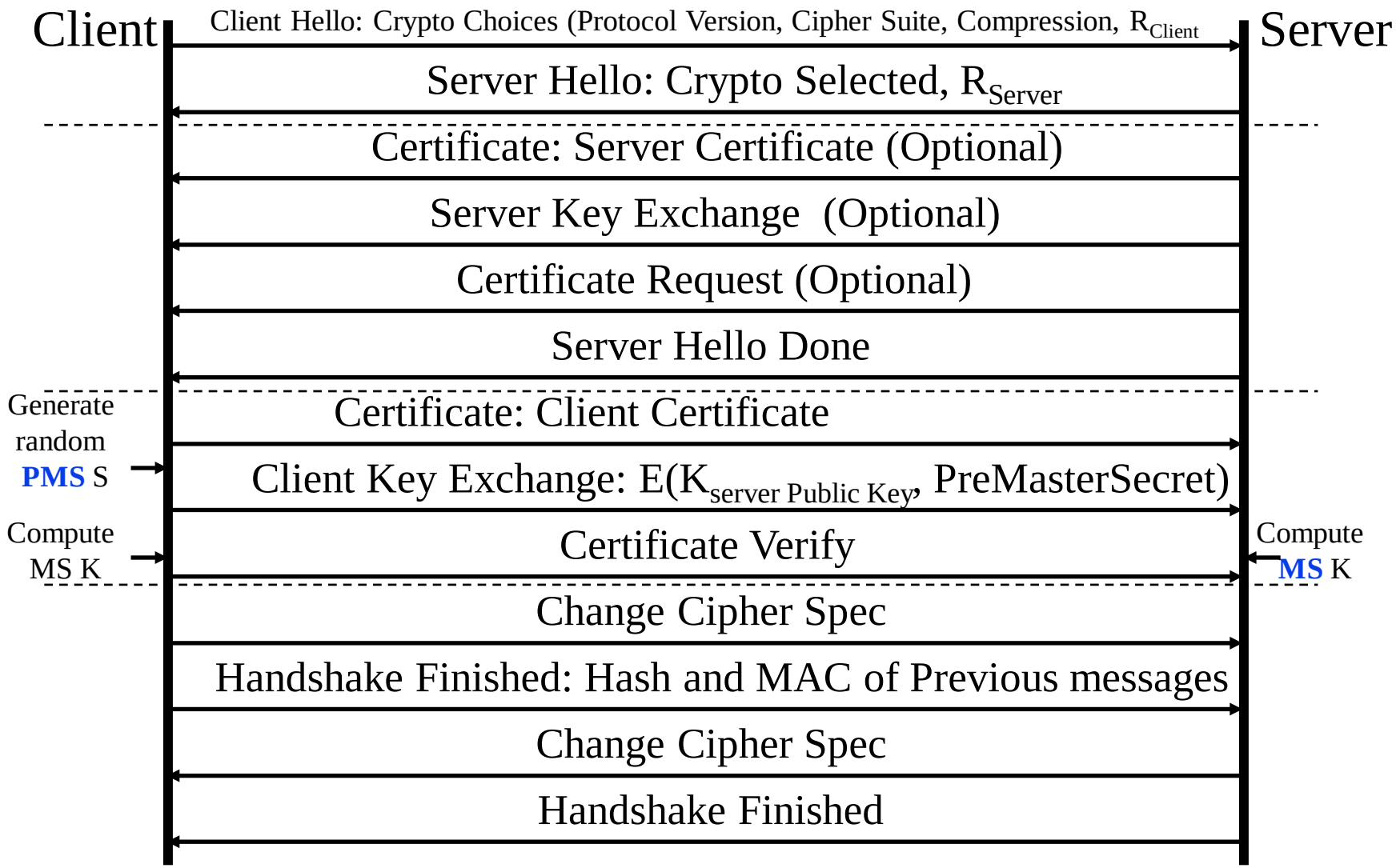
SSL/TLS Handshake Protocol

- 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

©2026 Raj Jain

SSL/TLS Handshake Protocol Actions



Student Questions

©2026 Raj Jain

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

©2026 Raj Jain

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

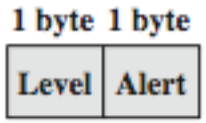
©2026 Raj Jain

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

©2026 Raj Jain

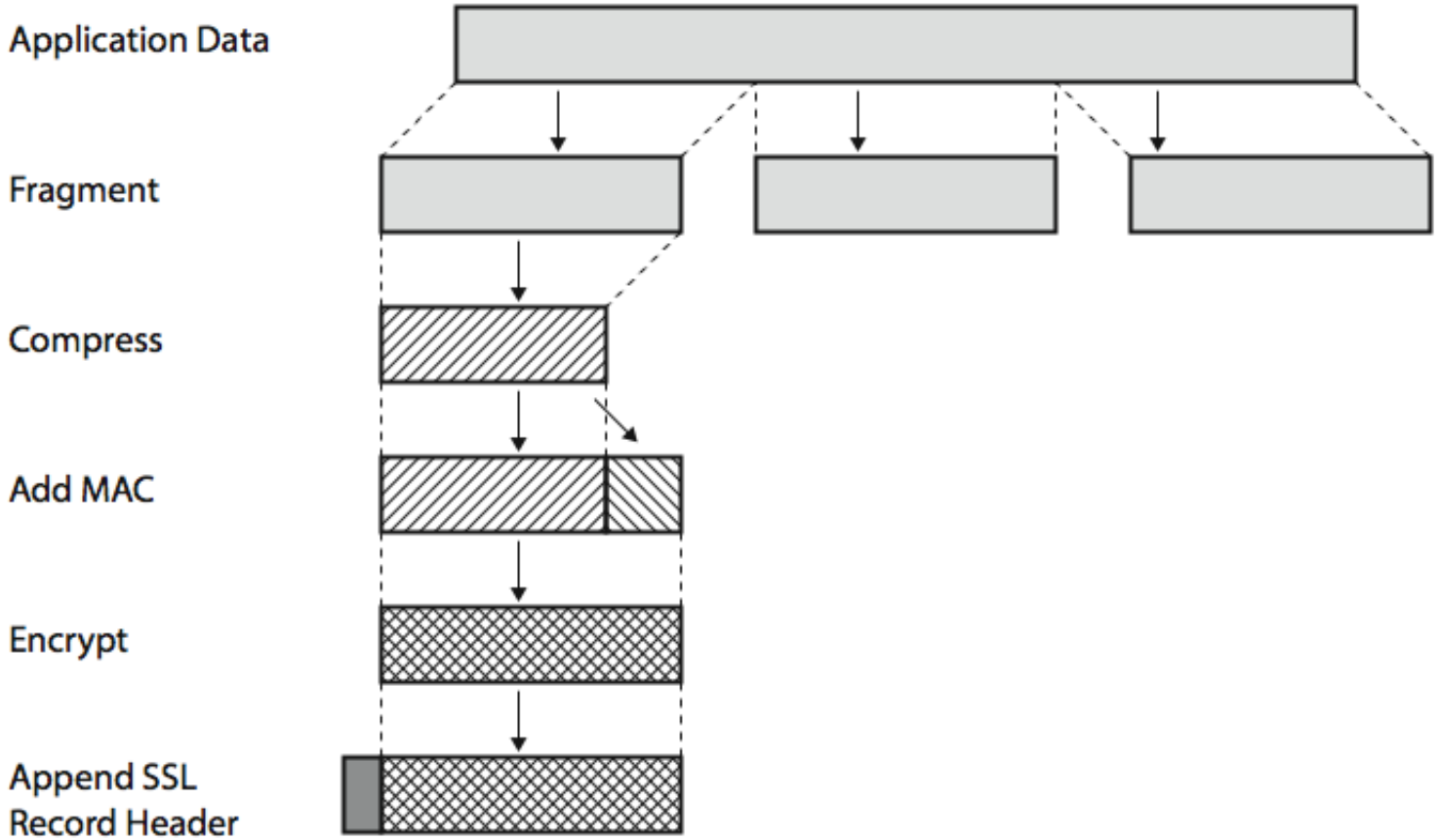
SSL/TLS Record Protocol Services

- **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

©2026 Raj Jain

SSL/TLS Record Protocol Operation

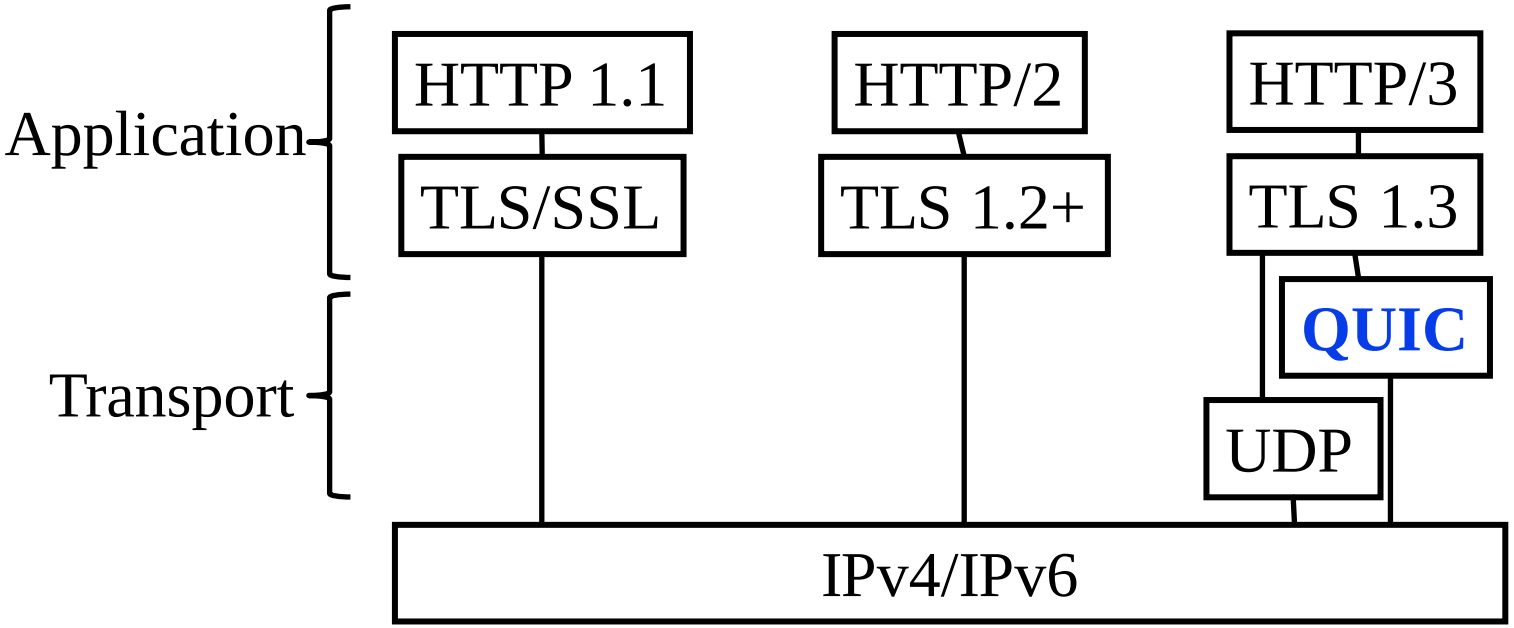


Student Questions

©2026 Raj Jain

Secure HTTP (HTTPS)

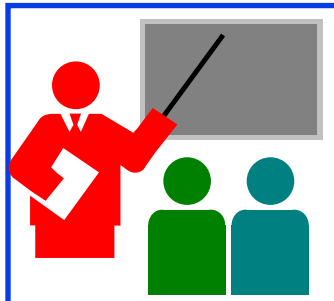
- HTTPS (HTTP over SSL)
  - Combination of HTTP & SSL/TLS to secure communications between browser & server [RFC2818]
- Use HTTPS:// URL rather than HTTP://. Use port 443 rather than 80
- Encrypts URL, document contents, form data, cookies, HTTP headers



Ref https://en.wikipedia.org/wiki/HTTP/3

Student Questions

©2026 Raj Jain



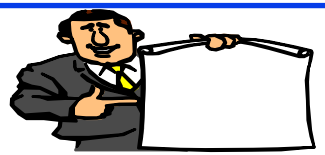
TLS: Summary

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

Student Questions

Ref: Read Section 8.6 and Exercises R20-R23

©2026 Raj Jain



IP Security (IPsec) and VPNs

1. IPsec Applications: Virtual Private Networks (**VPN**s)
2. Two ways to secure:
   a. Authentication Header (**AH**)
   b. Encapsulating Security Payload (**ESP**)
3. Internet Key Exchange (**IKE**)

Student Questions

©2026 Raj Jain

IP Security

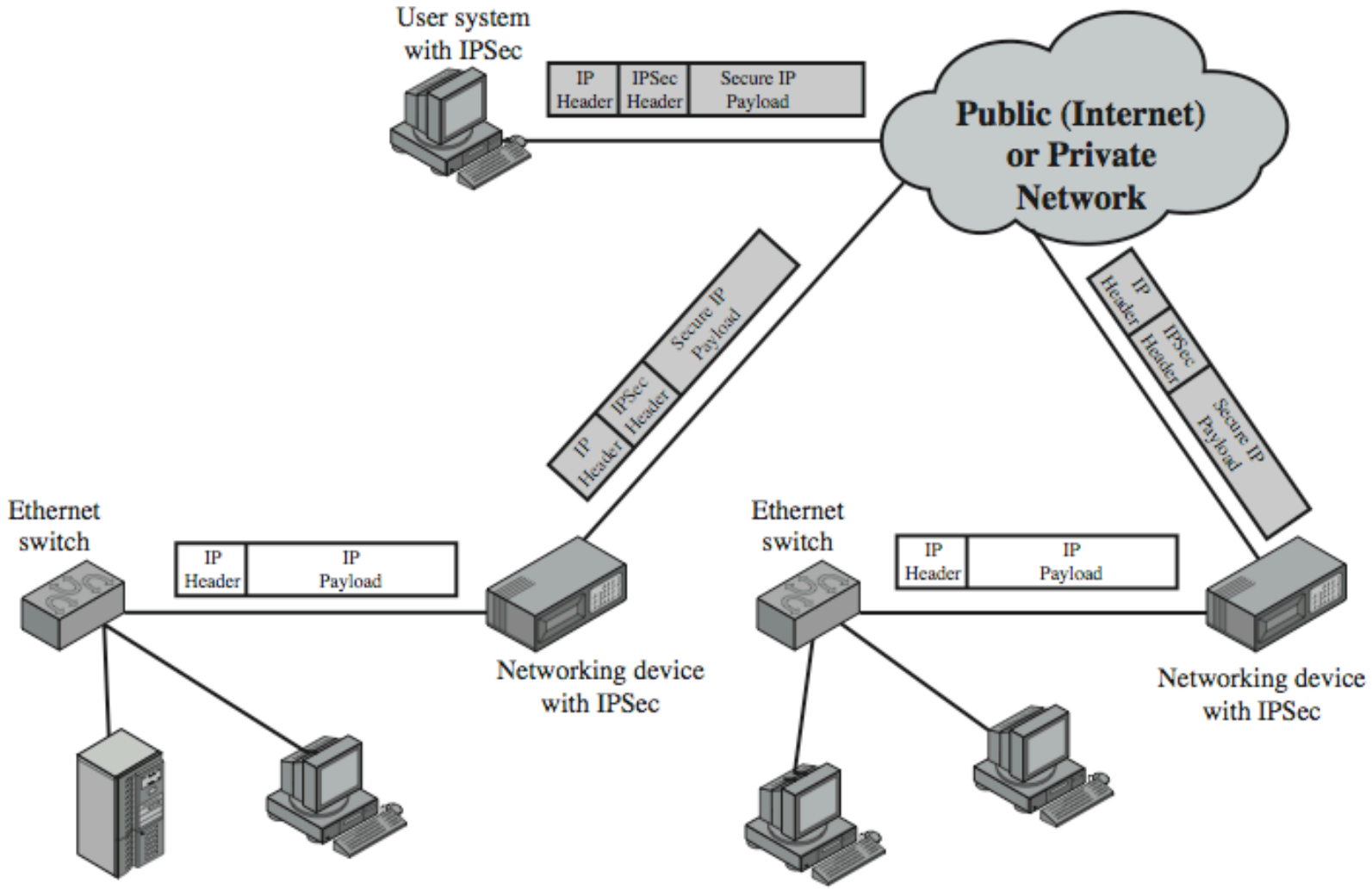
- IPsec provides
  - Access control: User authentication
  - Data integrity
  - Data origin authentication
  - Rejection of replayed packets
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality
- Benefits:
  - Security at Layer 3 ⇒ Applies to all transports/applications
  - It can 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

©2026 Raj Jain

IP Security Applications

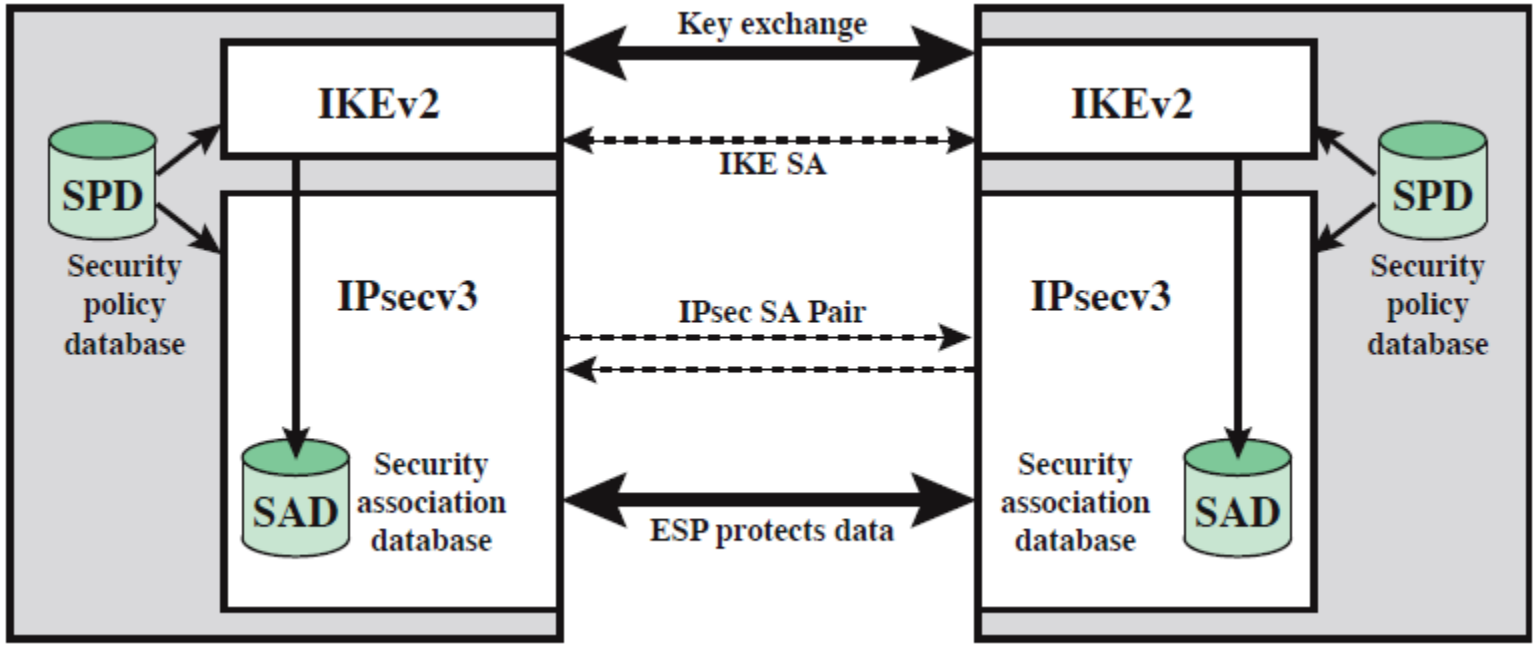


Student Questions

©2026 Raj Jain

IP Security Architecture

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



Student Questions

©2026 Raj Jain

Security Association Database (SAD)

- Each host has a database of Security Associations (**SA**s)
- 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
  - The lifetime of the SA
  - Mode: Transport or tunnel or wildcard
  - Path **MTU**

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

Student Questions

©2026 Raj Jain

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

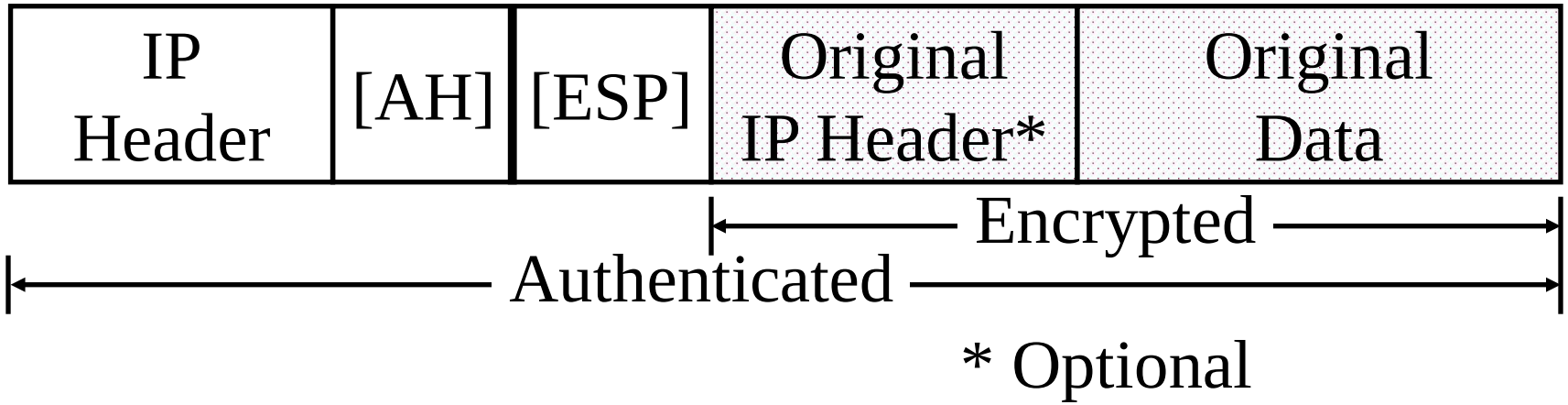
Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	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

©2026 Raj Jain

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.*



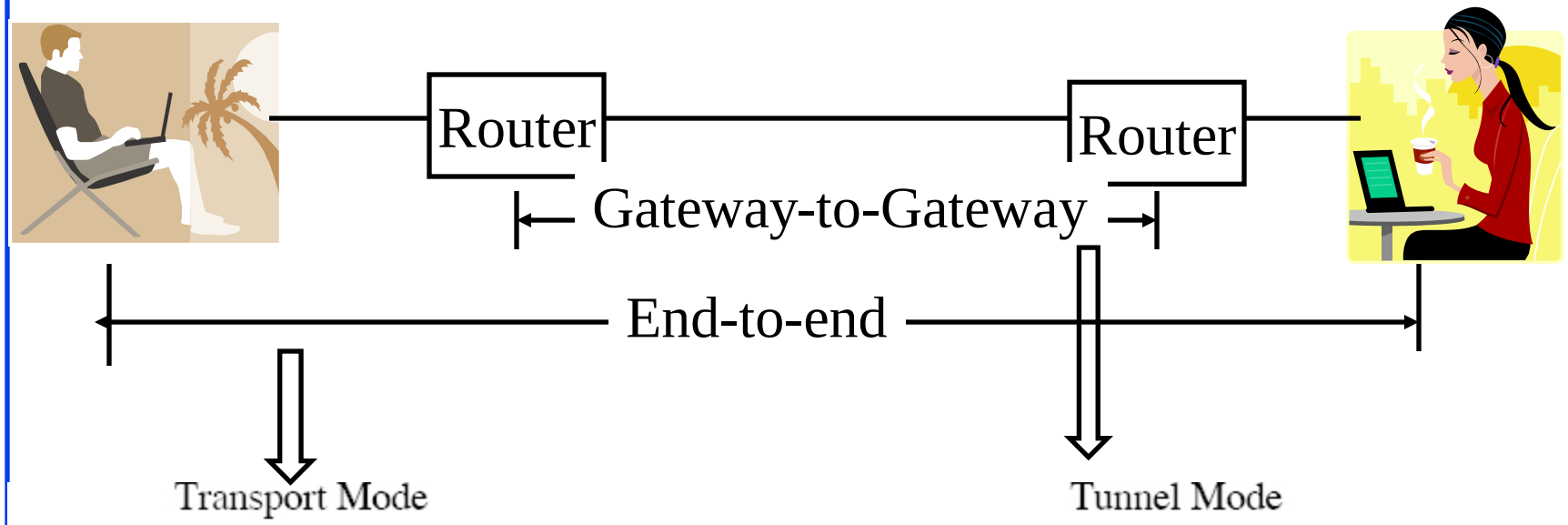
Student Questions

©2026 Raj Jain

End of Part 2

Tunnel vs. Transport Mode

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





Student Questions

©2026 Raj Jain

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

©2026 Raj Jain

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

©2026 Raj Jain

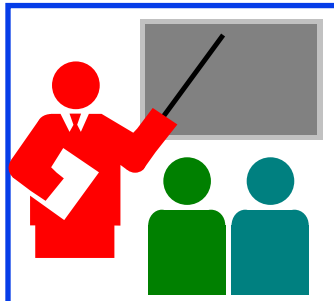
IPsec Key Management (IKE)

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

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

Student Questions

©2026 Raj Jain



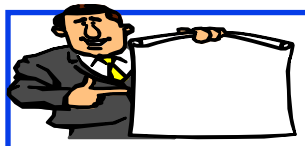
Summary: IPsec

1. IPsec provides authentication, confidentiality, and key management at Layer 3. Applies to all traffic passing through IP.
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 integrity
5. Both can be used end-to-end with the original IP header inside (Tunnel) or without the original IP header (Transport) mode

Student Questions

Ref: Read Section 8.7 and Exercises R24-R26

©2026 Raj Jain



Firewalls and IDS

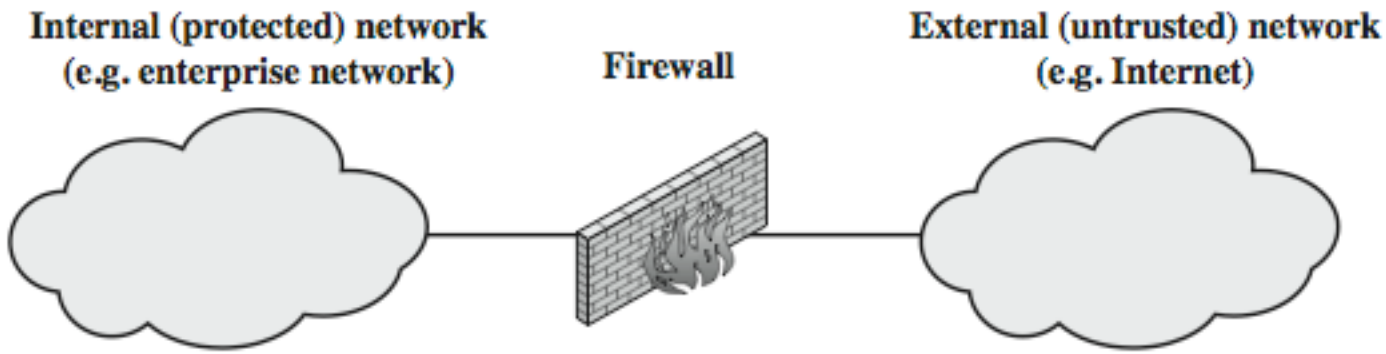
1. What is a Firewall?
2. Types of Firewalls
3. Intrusion Detection Systems
4. Honeypots

Student Questions

©2026 Raj Jain

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

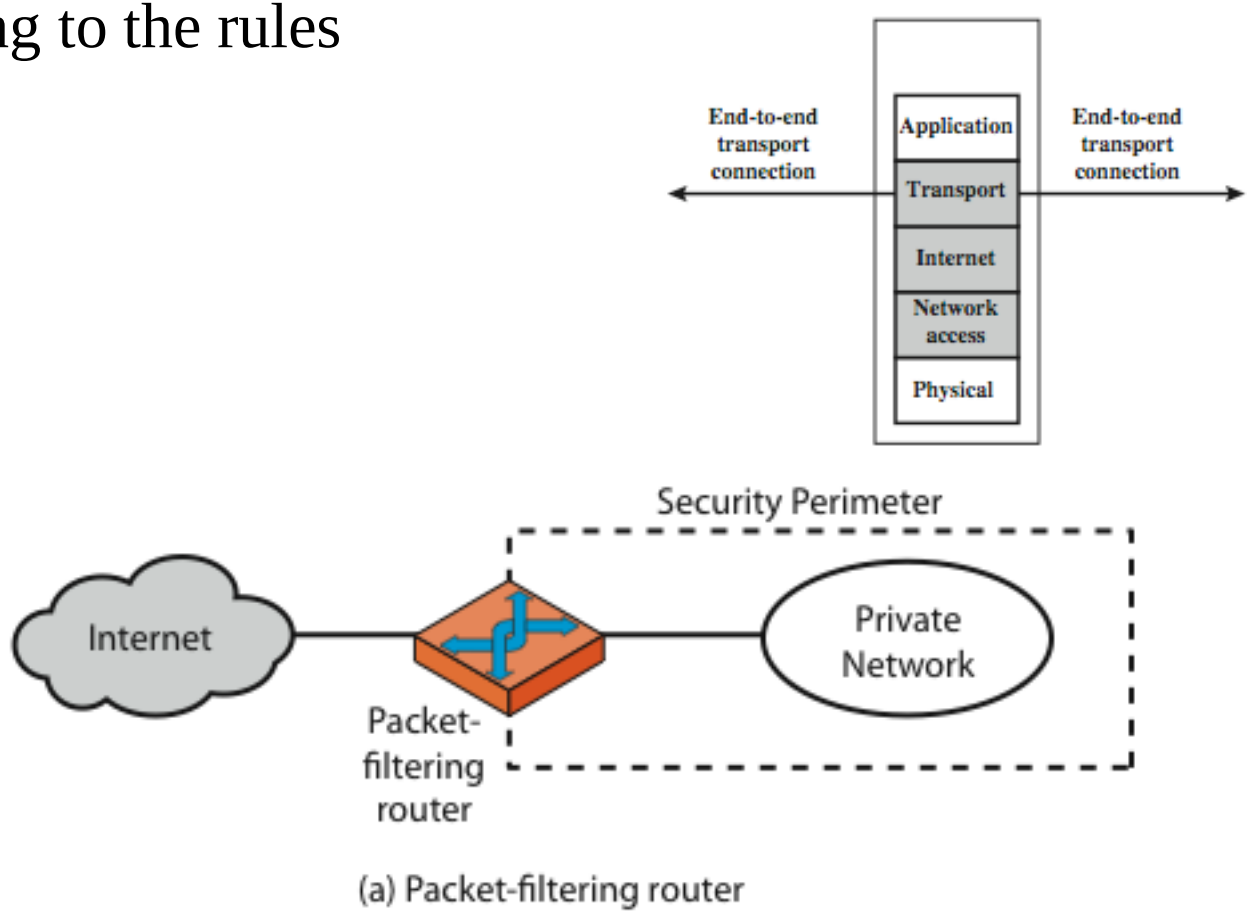


Student Questions

©2026 Raj Jain

Firewalls – Packet Filters

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



(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

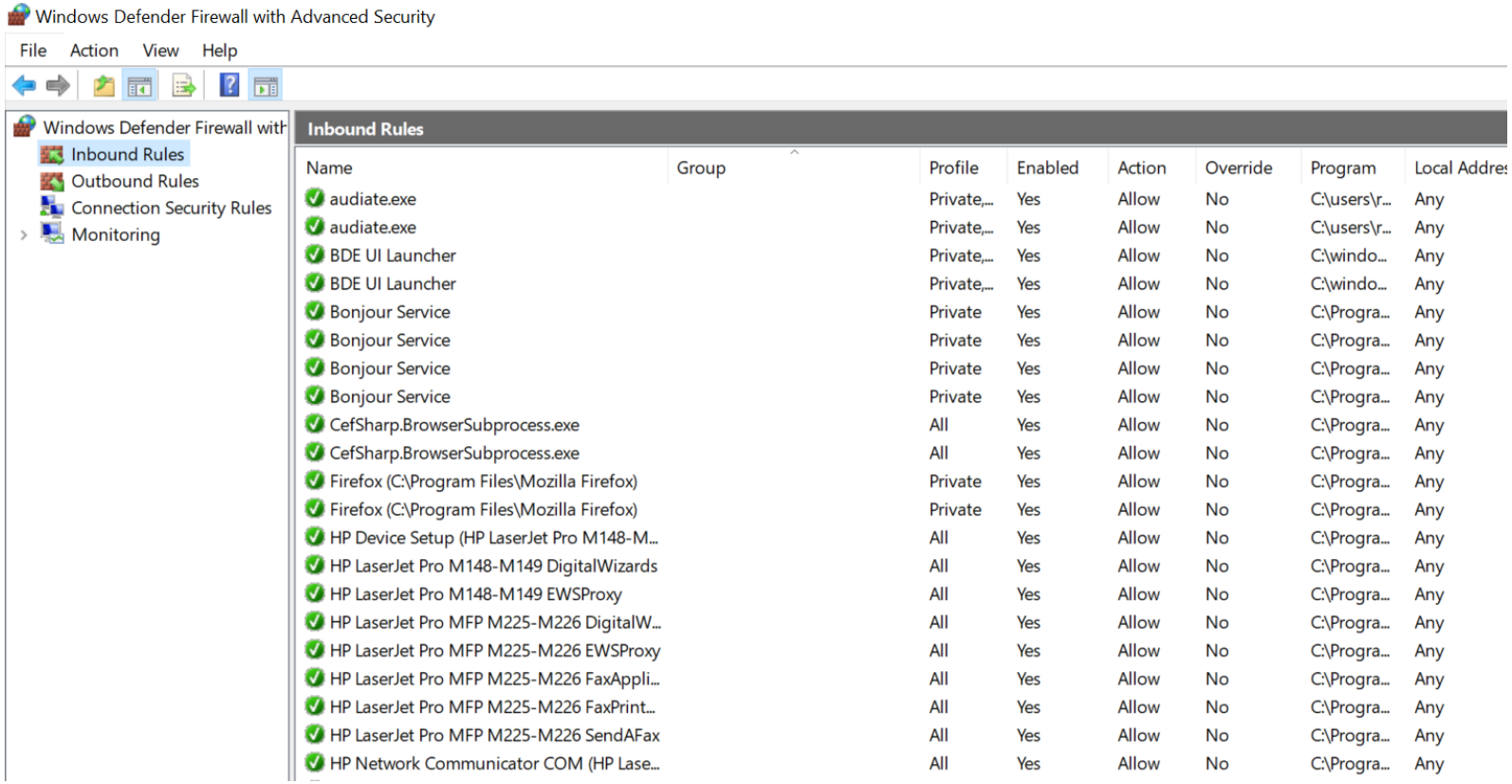
action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Student Questions

©2026 Raj Jain

Packet Filter Example: Windows Firewall

- Windows Defender Firewall with Advanced Security → Inbound Rules



Student Questions

©2026 Raj Jain

Firewalls – Stateful Packet Filters

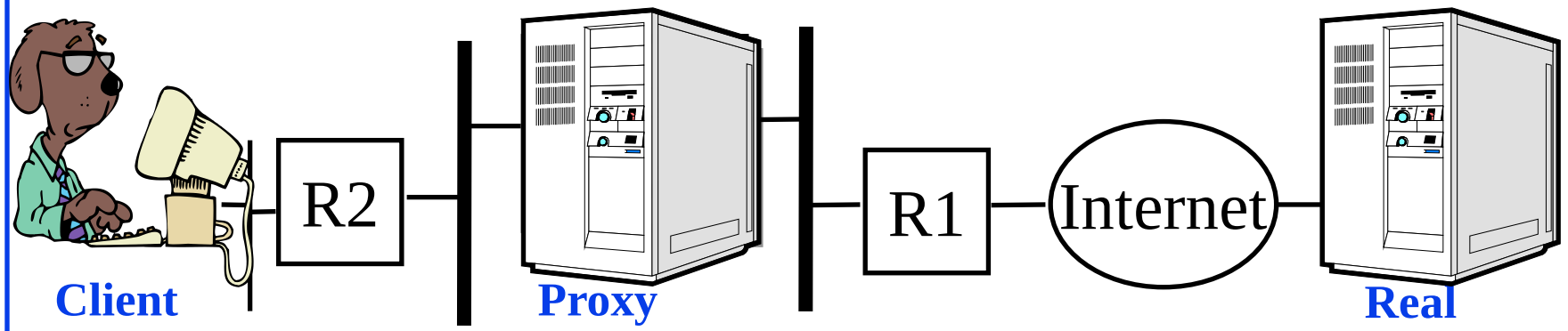
- Examine each IP packet in its context
  - Keep track of client-server sessions
- May even inspect limited application data

Student Questions

©2026 Raj Jain

Proxy Servers

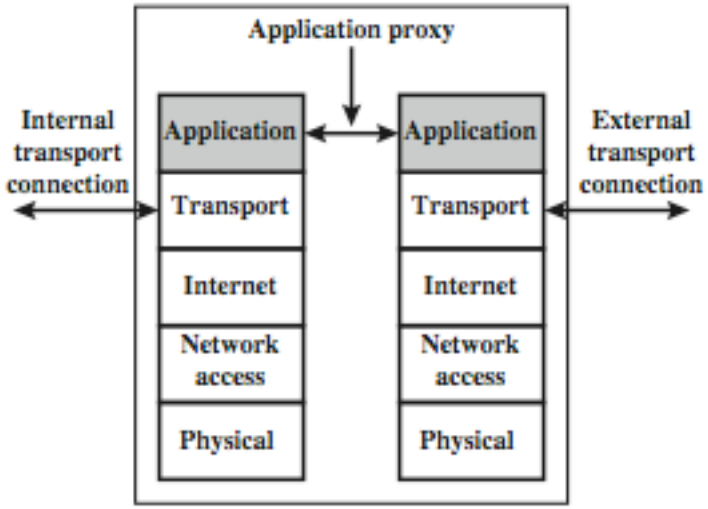
- Specialized server programs
- Take user's requests and forward them to real servers
- Take the server's responses and forward them to users
- Enforce site security policy ⇒ Refuse some requests.
- Also known as application-level gateways
- With special "Proxy client" programs, proxy servers are almost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

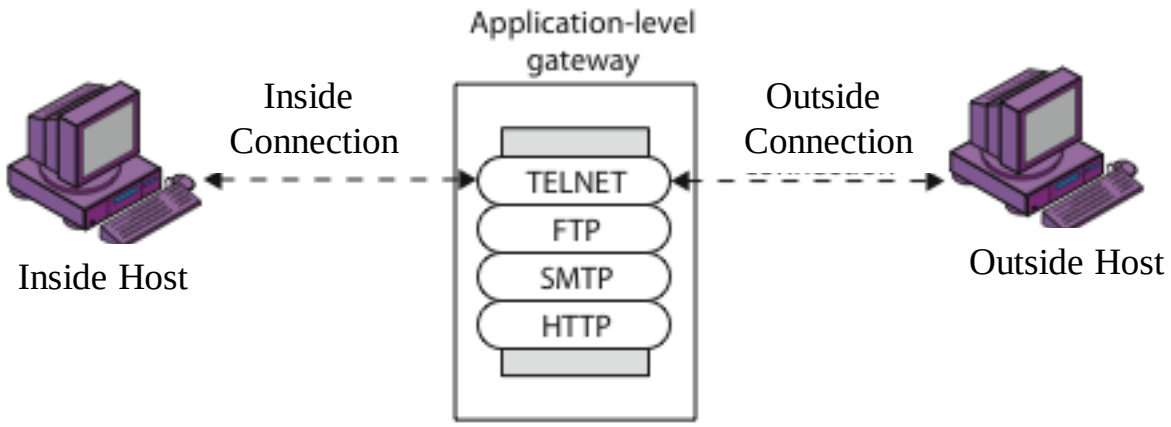


Student Questions

©2026 Raj Jain

Application Level Gateway (Cont)





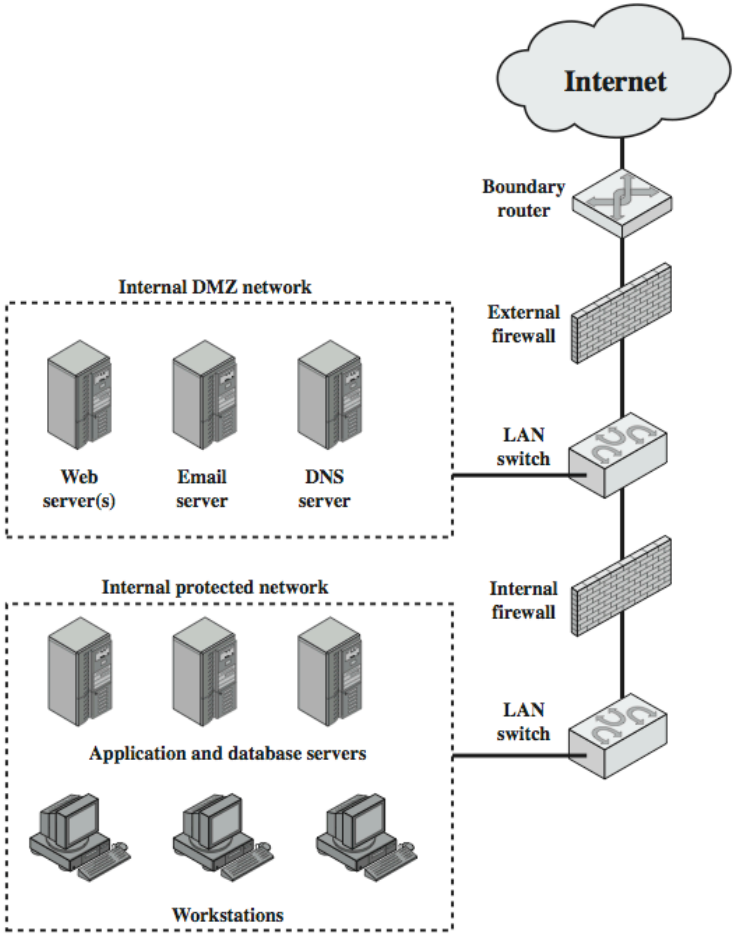
(b) Application-level gateway

Student Questions

©2026 Raj Jain

DMZ Networks

- Demilitarized Zone



Student Questions

©2026 Raj Jain

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, **PDA**s, and storage infected outside

Student Questions

©2026 Raj Jain

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

©2026 Raj Jain

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

©2026 Raj Jain

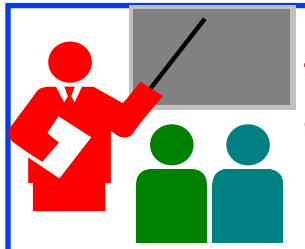
Honeypots

- 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

©2026 Raj Jain



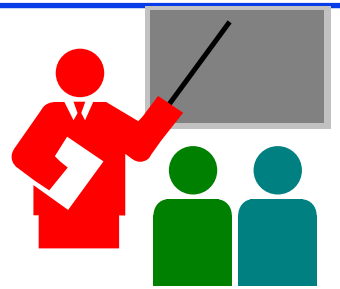
Firewalls and IDS: Summary

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

Student Questions

Ref: Section 8.9 and Exercises R28-R32

©2026 Raj Jain



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.

Student Questions

Ref: Sections 8.1 through 8.7, and 8.9

©2026 Raj Jain

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

©2026 Raj Jain

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

©2026 Raj Jain

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

©2026 Raj Jain

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

©2026 Raj Jain

Scan This to Download These Slides





Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse4703-26/i_8sec.htm

Student Questions

©2026 Raj Jain

Related Modules



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

cse4703S: 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

©2026 Raj Jain