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/cse473-22/

Student Questions

Note: Questions discussed during regular Q&A sessions are marked with ❑. New questions asked during Exam 3 review are marked with ❖

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

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 sender nor receiver can deny the existence of a message

Student Questions

- Is bit-error detection/correction a form of maintaining integrity, or can bit-level errors happen for reasons other than security issues?

Integrity can be violated by natural bit errors or by an attacker. Here, we are concerned about bit changes by the attacker. Simple techniques discussed earlier will not work for attacks.

- Is non-repudiation similar to logging?

No. A common way to ensure non-repudiation is by signatures and by thumbprints.

- Will bit error affect availability?

If an attacker changes every packet, it can cause unavailability. However, most often, it is caused by overload.

Secret Key Encryption: Overview

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

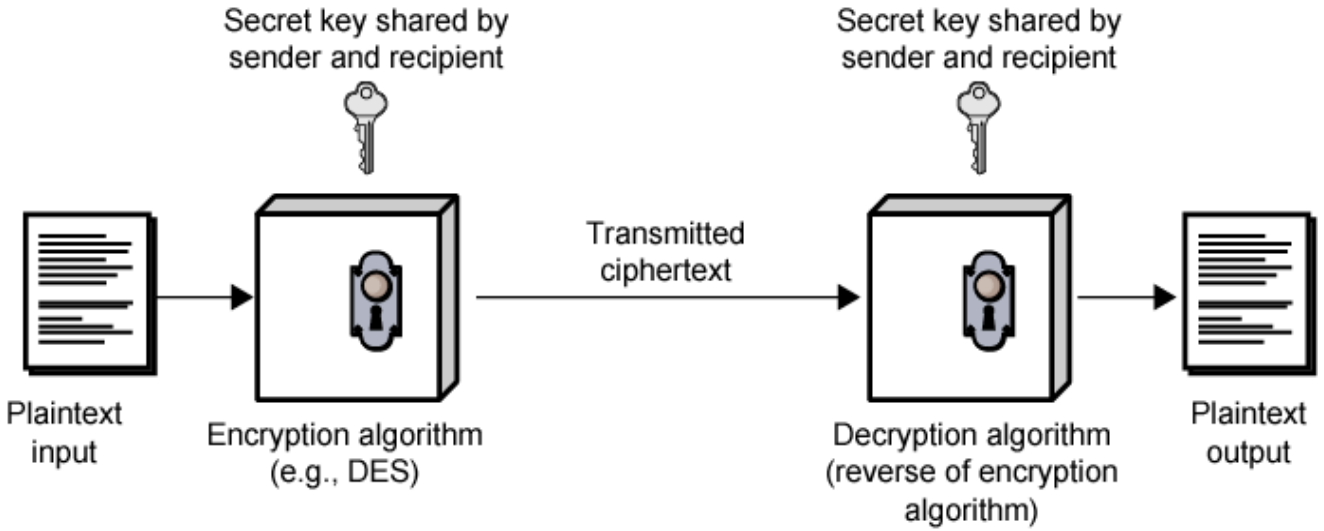
Student Questions

- Question from the book: From a service perspective, what is an important difference between a symmetric-key system and a public-key system?

The main difference is that the key is known to two parties (secret) vs. one party (Private).

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)



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.*

- How do you ensure that the key is passed safely without an intruder before communicating?

There are ways. Mainly by using offline methods or other encryption methods.

- Could you talk about ways to see the encrypted message without the secret key?

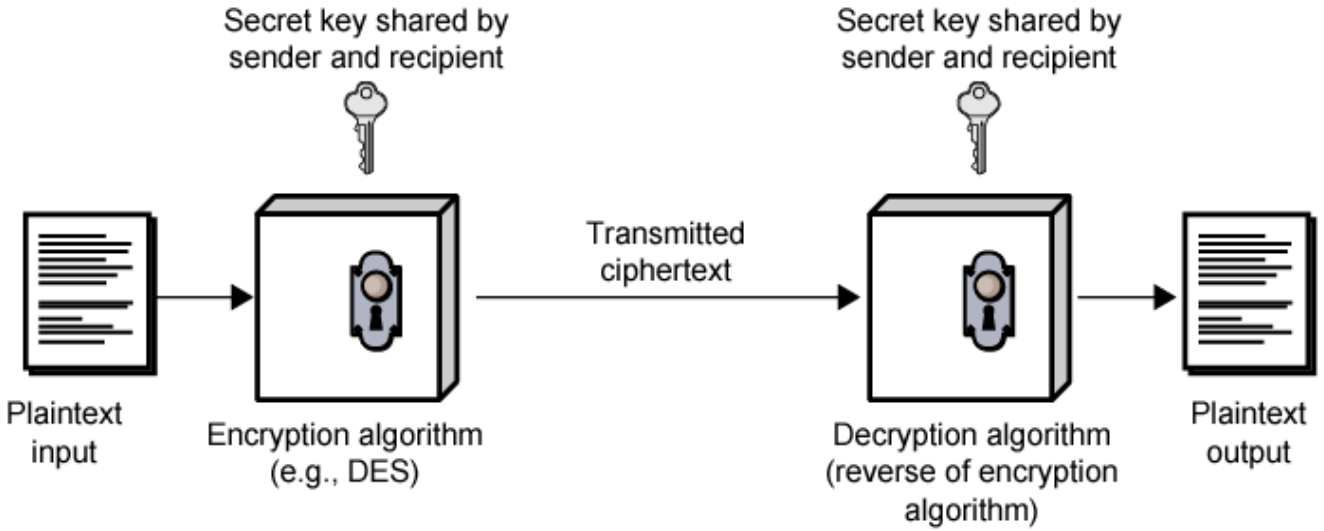
Anyone can see the encrypted message. But no one can see the original message without the key.

- Could we use some sniffers to get the key?

The key is not sent in the clear over the network, so network sniffers will not work. If you infect the sender's computer, you may be able to get the key.

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)



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.*

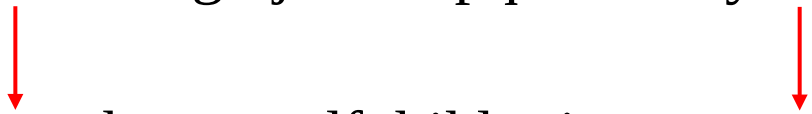
- Even if we know the key, without knowing the encryption algorithm, we still cannot decrypt the message? Why is the key secret, not the encryption algorithm?

The number of algorithms is generally finite. It is easy to try them all.

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

- Can you give an example of Polyalphabetic substitution?

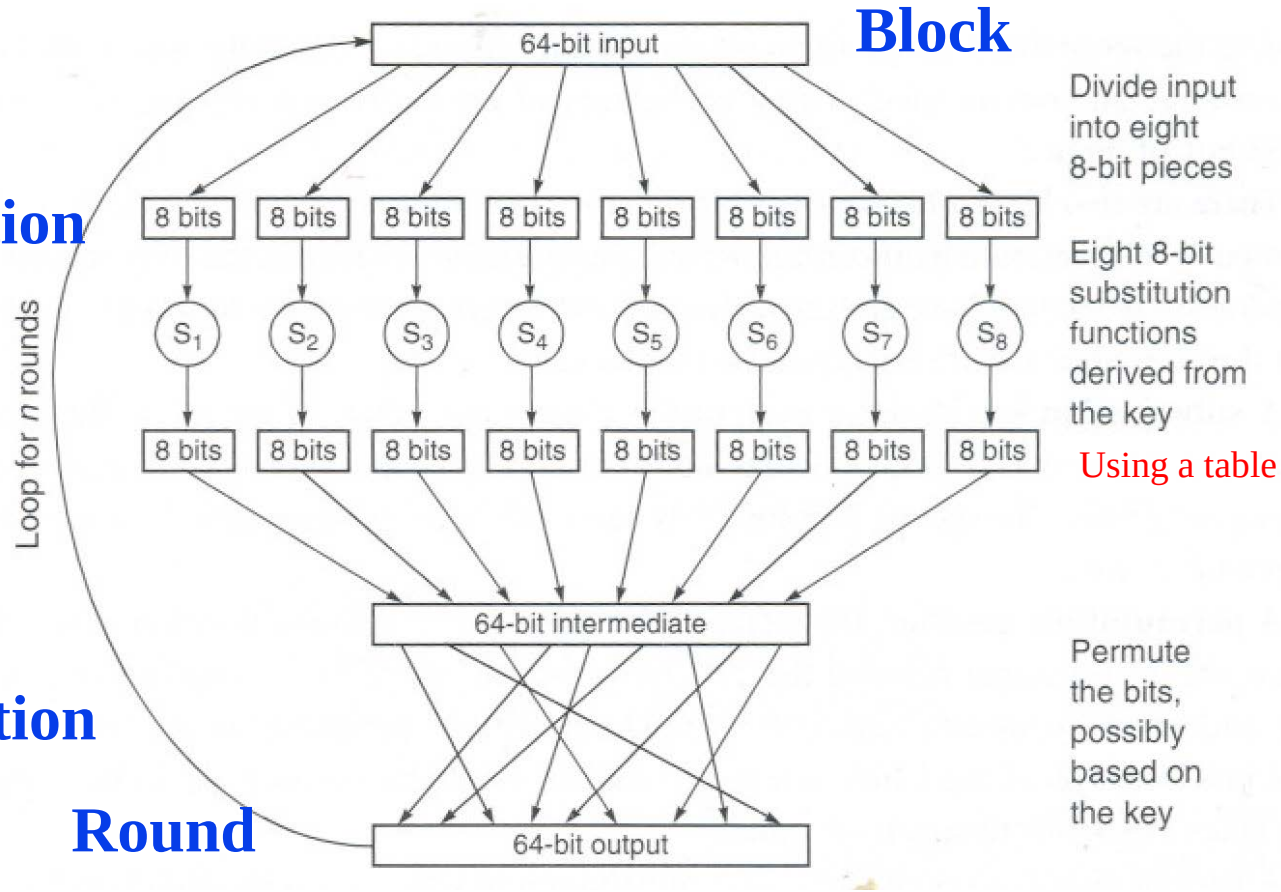
Example: Add position # to the letter
Plaintext: bob
Ciphertext: cqe

- In monoalphabetic, the secret key is the letter to be substituted, and the encryption algorithm is the substitution.

The secret key is the substitution table.

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.

- When decrypting the message, do we use the same steps in the diagram but in the reverse direction (bottom to top, repeat for n rounds)?

Not always. If some steps are not reversible, a decryption algorithm must be specified.

- Is the permutation operated on 8 bits *blocks*, or is it operated on every bit?

Bits in the entire 64-bit block are permuted.

- Does the permutation happen randomly, or are the locations of the bits defined by the type of encryption?

The permutation is pre-specified.

- What is the secret key in Block Encryption? Is the permutation step related to the secret key?

The substitution is based on the key. Permutation can be fixed or based on the key.

- Are a block and a frame the same thing?

No blocks are fixed size—64-bits in the example shown.

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

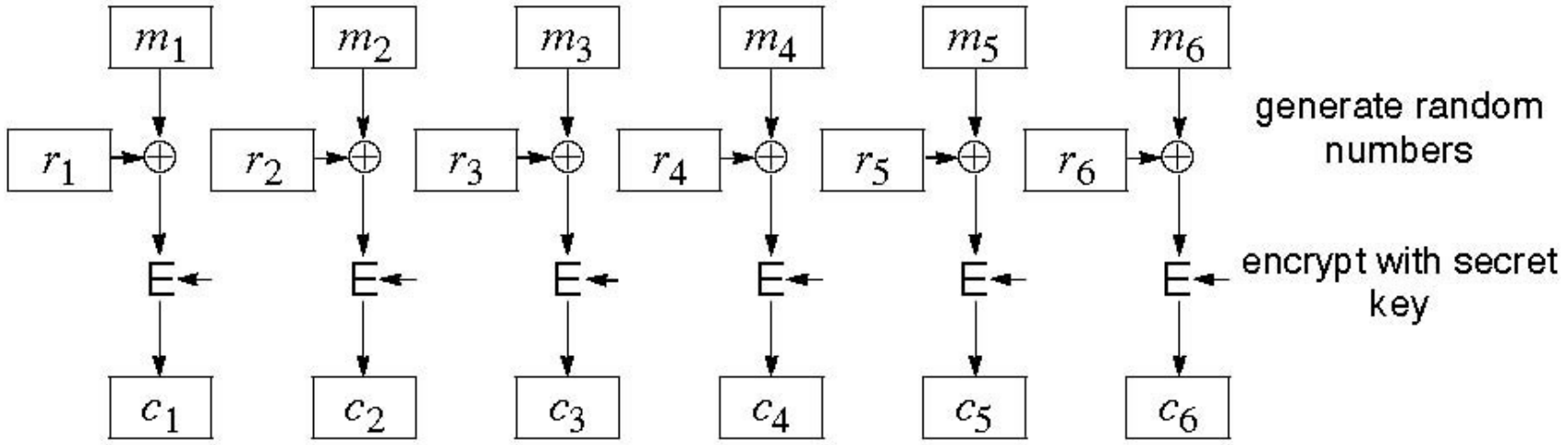
Student Questions

- What is the table?

A tabular attack is one in which all possible answers are stored in a table to make the operation faster.

Cipher Block Chaining (CBC)

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



Student Questions

- If random numbers are added, how do we decode the message?

The random numbers are generated using a pre-specified method discussed in the next slide.

- If the encoding involves a randomly generated number, how for the receiver to decrypt it?

See the previous question.

- Is CBC an improved version of Block Encryption?

It is an additional step in (mode of) block encryption.

- Could you clarify how Chaining is associated with Block Encryption?

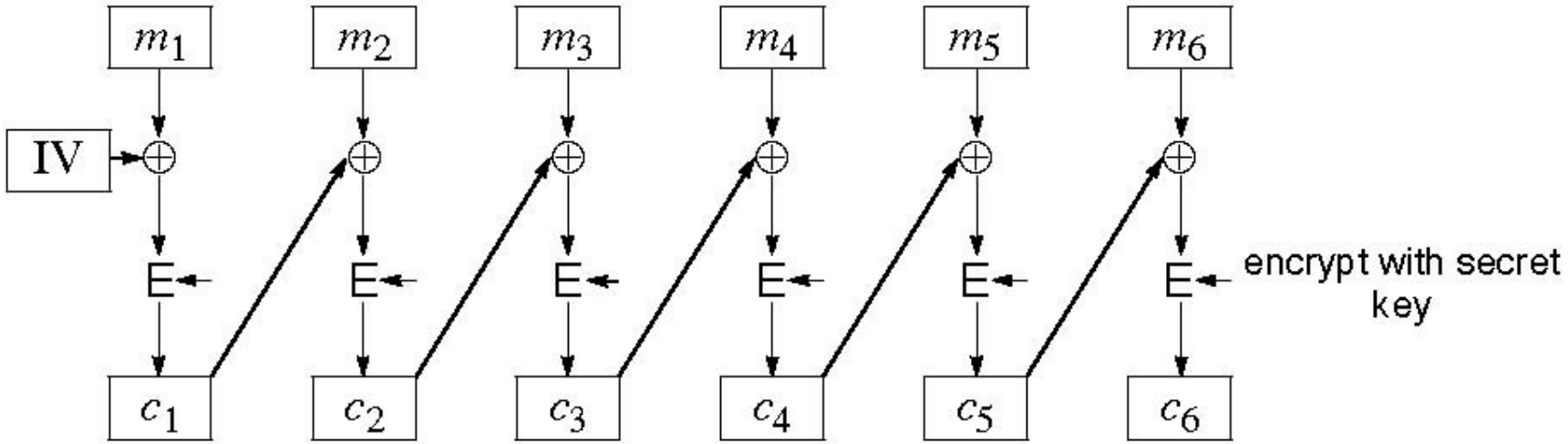
See the previous question.

- Can you give an example of how CRC is used as a hash function?

You compute the CRC and use it as a hash.

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

- 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

- Is the IV helping decryption to generate a corresponding random number to decrypt?

IV is used as the first random number. All subsequent random numbers then change as the IV is changed.
It only prevents statistical decryption. Statistical decryption – the most common letter in English is i.

- Is the initial value random here?

No. It is sent with the message in clear.

- If the value of IV is known, does it mean using CBC is not that helpful for encryption?

It increases confusion a bit more.

- Does each m mean one block?

Yes.

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

- How will security change with the rise of quantum computing? Will that possibly change the computing power needed for encryption?

Quantum computing makes some decryptions easy. Those need to be replaced by quantum-safe encryptions.

- Since there is little difference between even and odd parity in checking for errors, would DES still work if each octet had an even parity bit instead?

No.

- Why does computing power go up by 1 bit every two years?

Moore's Law.
https://en.wikipedia.org/wiki/Moore%27s_law

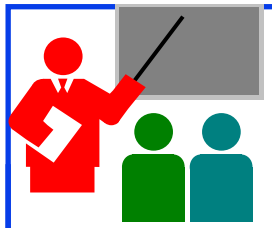
Advanced Encryption Standard (AES)

- Designed in 1997-2001 by the National Institute of Standards and Technology (NIST)
- Federal information processing standard (FIPS 197)
- A symmetric block cipher with 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

- What do you mean by 9-bits to store a byte?

You may use odd/even bit parity to store a byte. But it is not built into the key as in DES.



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 the different ciphertexts.

Student Questions

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

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?

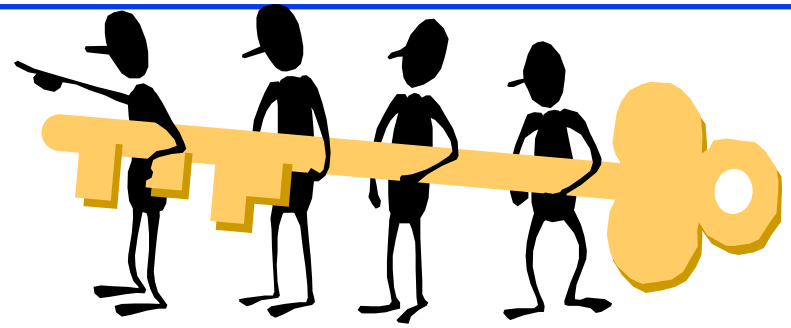
Student Questions

Public Key Encryption

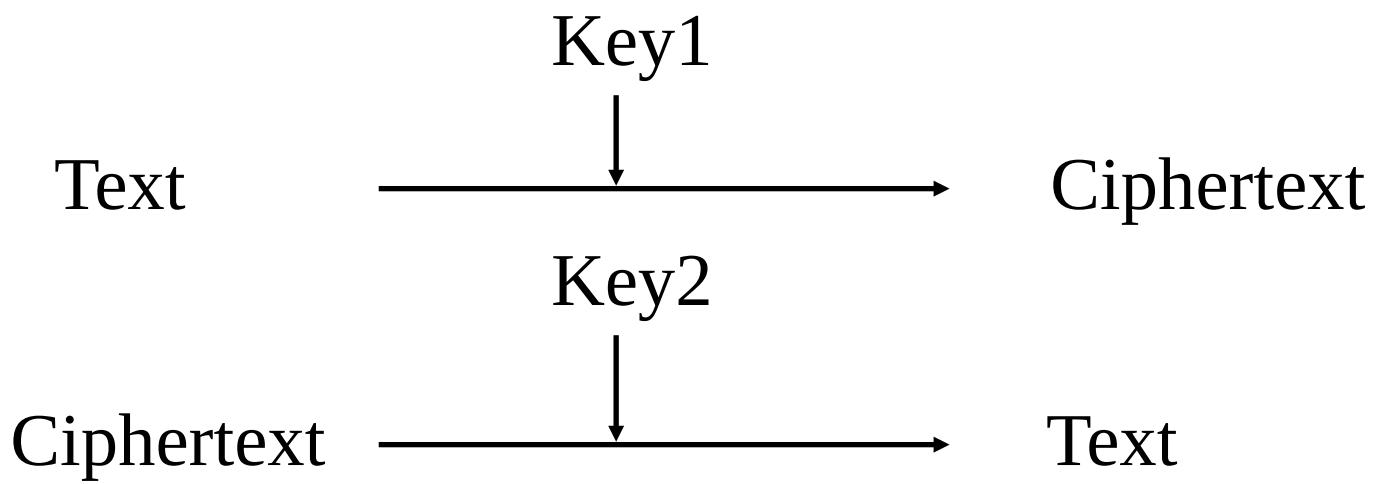
1. Public Key Encryption
2. Modular Arithmetic
3. RSA Public Key Encryption

Student Questions

Public Key Encryption



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



Student Questions

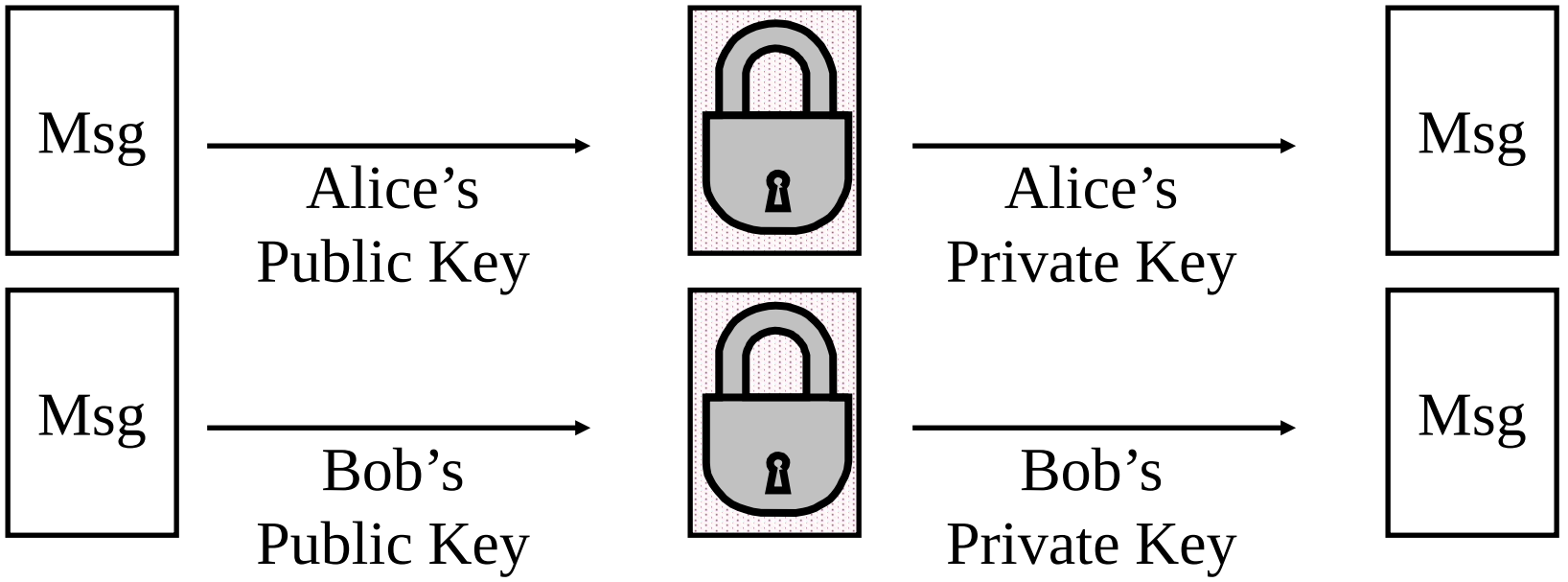
- Can you define what a semantically secure encryption system is?

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



Student Questions

- What are the disadvantages of public key encryption?

Lot of computation.
Need very long keys

- How do you make sure the private key is secure?

Please keep it in a safe so that no one can get it.

- What happens when the public key is corrupted?

Public keys can be kept in many places. They are public.

- Are the public keys only used for sending data, and private keys are used to receive data?

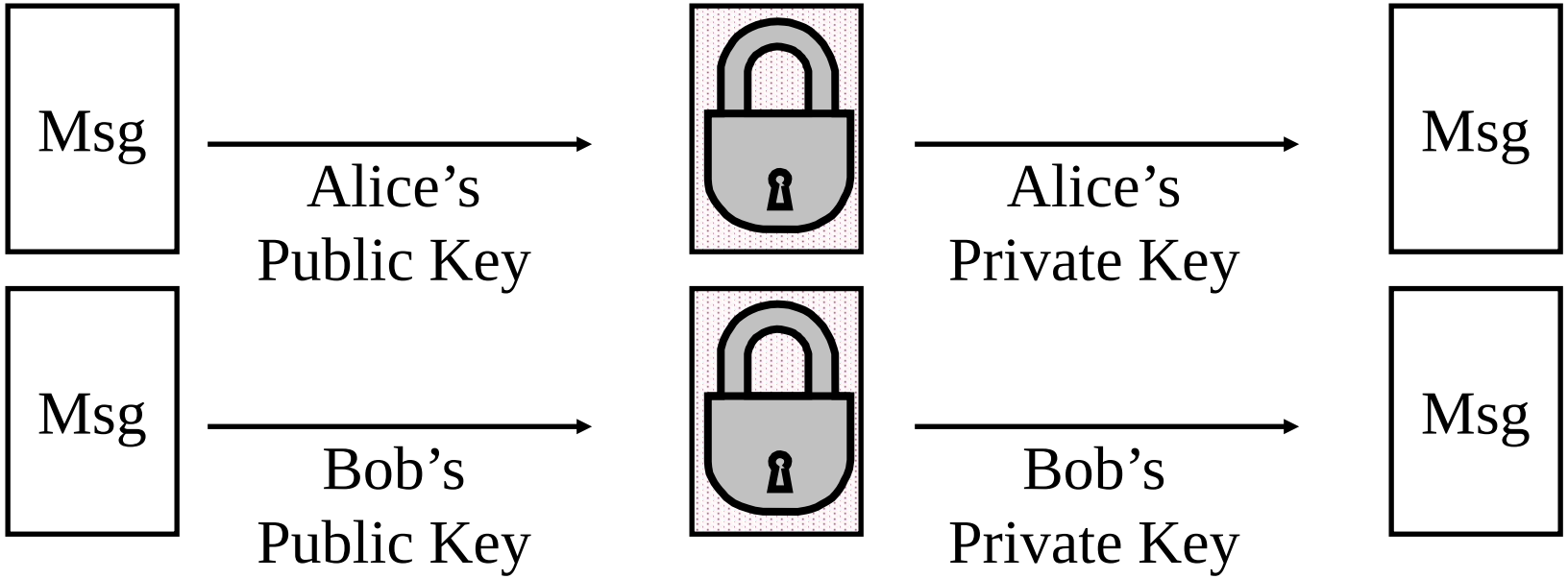
No. Either key can be used to encrypt, and the other key will then be used to decrypt. How to send is discussed in Slide 8-22.

- Does the public key the same for Alice and Bob?

No. Everyone has a different pair of public and private keys.

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

- Can encryption use both symmetric and asymmetric algorithms?

Yes. Both are often used together but for different steps in communication. The public key is computationally expensive and so it is used for certain steps only, e.g., to send the secret key.

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

- Do we need to remember or write down the steps in the exam since the steps look like rules that are hard to remember?

They are not hard to remember. Please practice and see for yourself.

- In this example, which is the public key, which is the private key?

In this example, Key1 is used as the public key. However, if you have the pair, you can decide which key to make public. You cannot change your decision afterward.

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

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

- Is there a way to quickly factor the public value n into prime numbers p and q? So in this way, if RSA is no longer secure?

Factoring prime numbers are simple. The computational power required increases with the magnitude of the number. It takes a lot of computing power to factor in large prime numbers.

- In "Select e," should this e be the largest satisfied number?

No. Any e that is "relatively prime" to z will do.

- What is the method for selecting the two prime numbers, p and q?

They should be large and prime. It isn't easy to find such numbers.

- Is there an algorithm for fast factorization? How to ensure the security of RSA?

RSA is just one way to do asymmetric key encryption. It involves factorization. There are other methods. Quantum computing is expected to make factorization easy. So other methods have been standardized for the future.

RSA Algorithm: Example

- Select two large primes: p, q, $p \neq q$
  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}

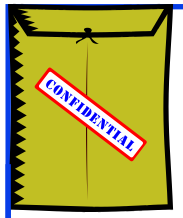
Student Questions

- Can you go over the RSA algorithm example?

Sure.

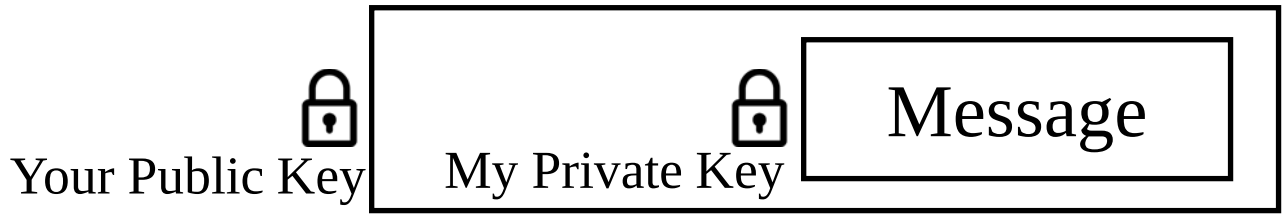
- Can we choose e=9 in this case?

Yes. But that would make a weak key. Better to use a prime e.



Confidentiality and Non-Repudiation

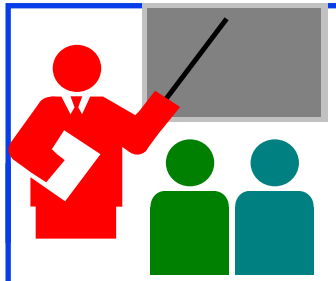
- User 1 to User 2:
- Encrypted_Message
  = Encrypt(Public_Key2,
  Encrypt(Private_Key1, Message))
- Message = Decrypt(Public_Key1, Decrypt(Private_Key2, Encrypted_Message)
  ⇒ Authentic and Private



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. The other key will decrypt.
3. RSA public key method is based on the difficulty of factorization

Student Questions

- Are checksums still used in error detection for an encrypted message? Would these checksums be calculated before or after the encryption?

Yes, checksums are still used. Encryption is optional and is rarely used. For example, you have not sent a secure message so far. Have you?

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

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 (e, n). 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

- Could you please explain why the public key in homework 8B is (n, e) instead of (e, n)?

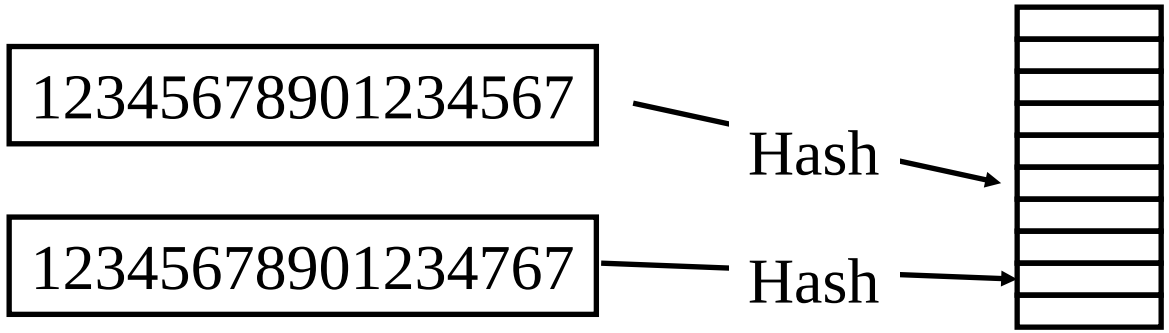
Mistake corrected.

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.?

- Will a different hash function lead to different efficiency for searching?

Yes.

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

- What is a block in a hash algorithm? How will the bits of the blocks affect the hash operation?

The message is divided into fixed-size blocks. Some operations are performed in each block and then combined to get the hash.

- Can you speak on the earlier versions of this hash? Has the IETF supported every version?

Yes, every version was discussed in IETF, and an RFC was written. However, those earlier RFCs were obsoleted by the next version. This is quite common in all standard bodies.

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

- 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.

- In my computer security class, it was mentioned that SHA1 is broken under collision attacks. What are the current hash functions used nowadays?

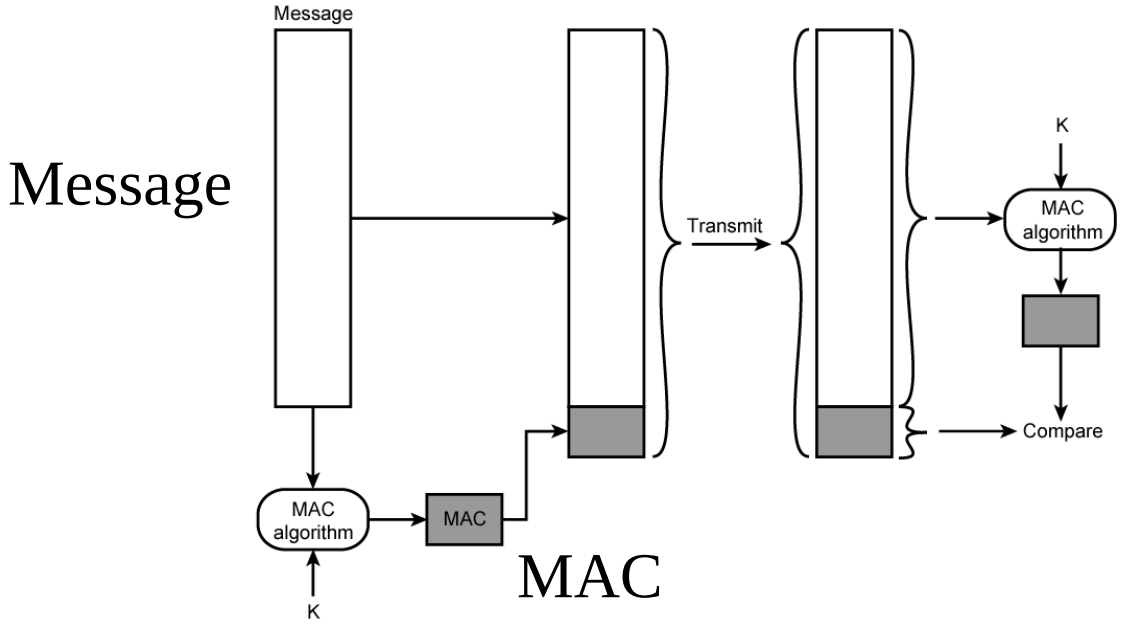
There are SHA-2 and SHA-3.

- What is SHA-256?

SHA-256 is SHA with 256-bit keys. The number after SHA is the version number (if small) or the key size (if large). Similar to Ethernet Type/Length field.

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

- Does CRC here use for checksum?

Here CRC is used as an example of hash.

- So MAC uses both encryption and hashing?

No. Creating a MAC is separate from encrypting the message. You can use both or either. In the last point, the message could be encrypted message or message in clear.

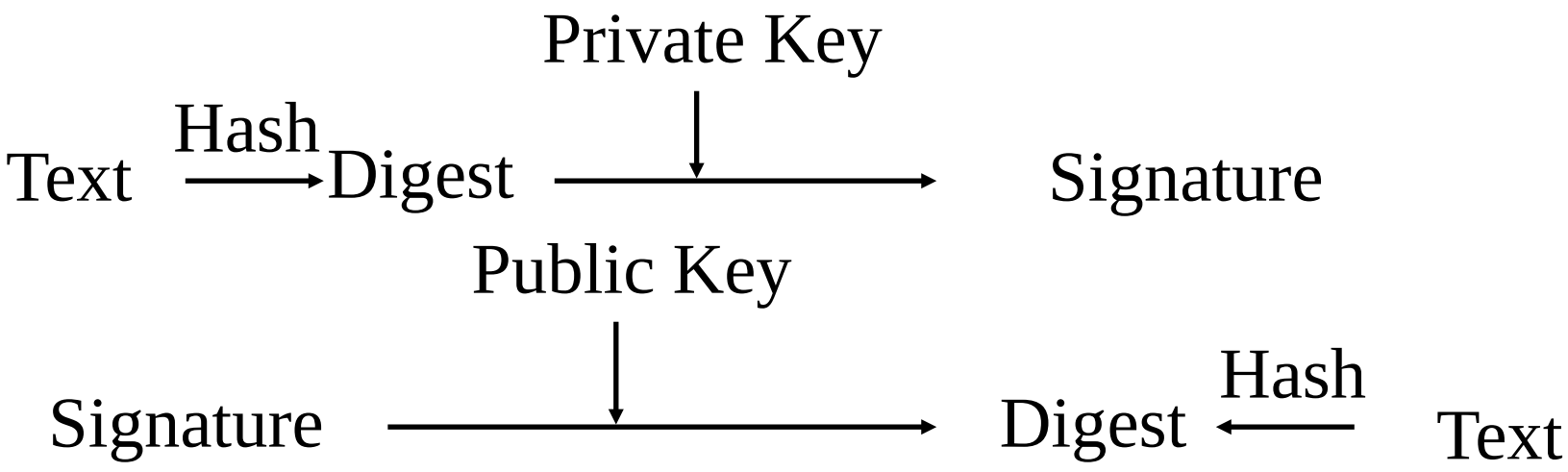
HMAC Overview

- 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 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)



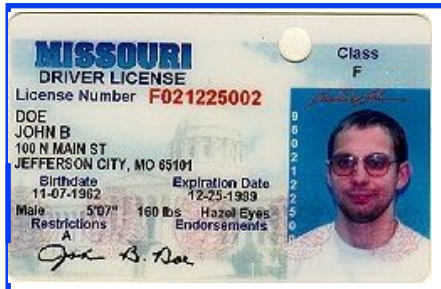
Student Questions

- In the flow chart, what would be the purpose of getting the digest from the signature?

Digests obtained from the signature and the text are compared to prove that the sender is the only one who could send this message since he only knows the private key.

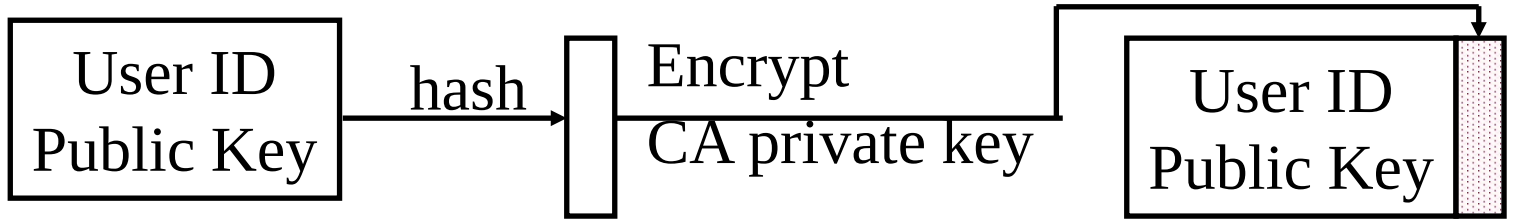
- It says Digital Signature, also known as MAC, while there are differences between them in the book.

Yes, there are differences. In this particular slide, the private key is used for MAC, and so it becomes a signature. If we had used any other key, they would not be equal.



Digital Certificates

- Like 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

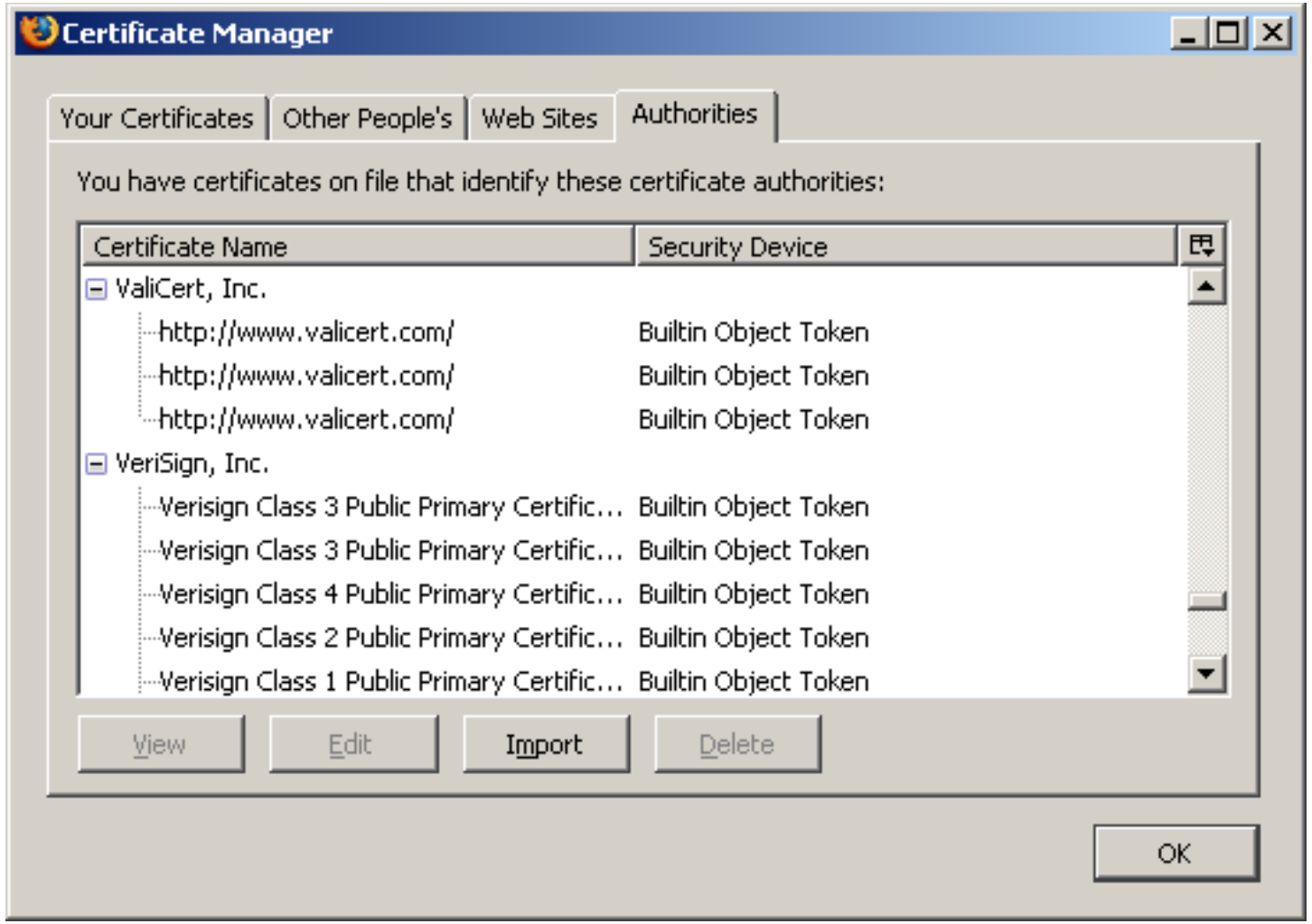


Student Questions

- 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

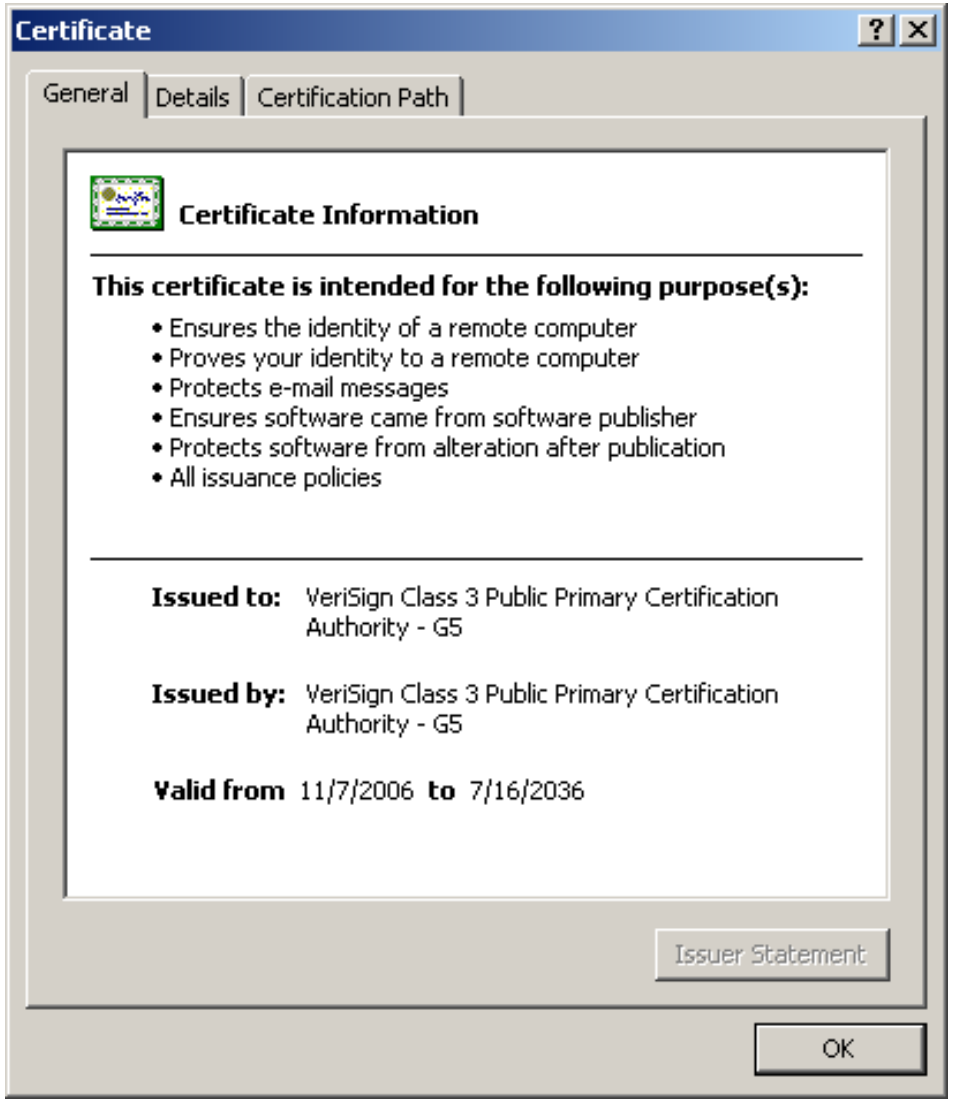


Ref: Windows: http://smallbusiness.chron.com/see-security-certificates-stored-computer-54732.html
MAC: https://superuser.com/questions/992167/where-are-digital-certificates-physically-stored-on-a-mac-os-x-machine

Student Questions

Sample X.509 Certificate

- Certmgr.msc in Windows



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)
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

- If I am in the year 2077 and change the time on my computer to 2033, will this certificate be valid?

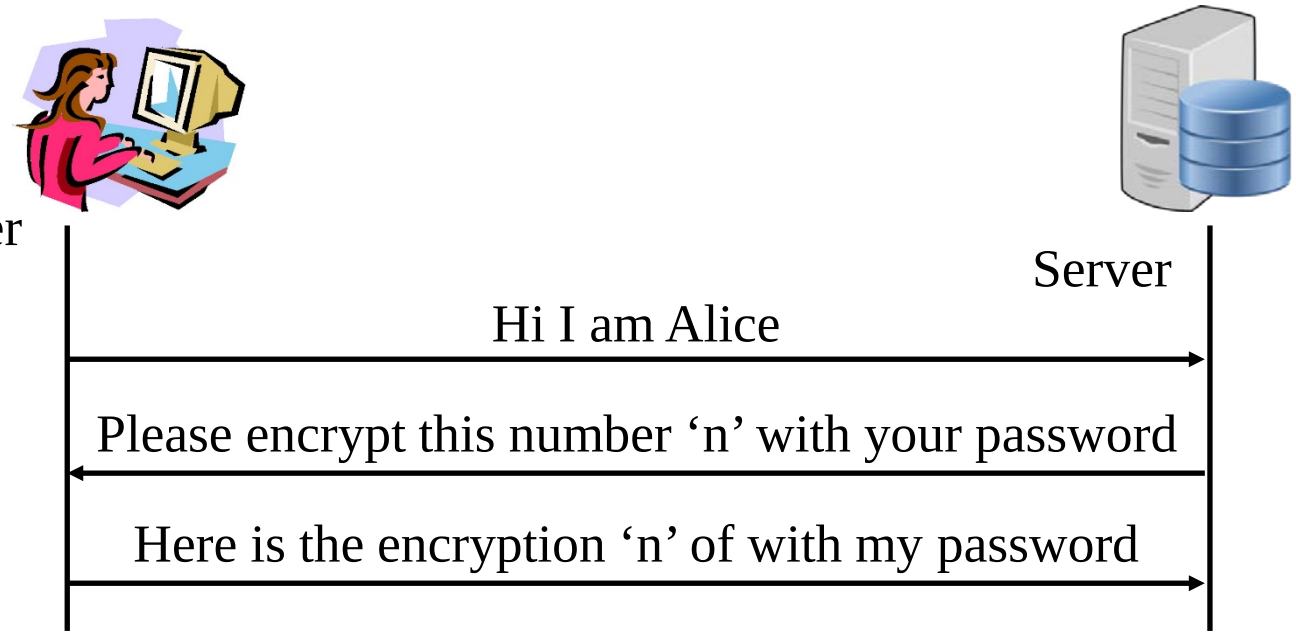
Yes. This is why it is important to synchronize your clock to the world clock.

- Does a server set the nonce on HTTP cookies for further requests? If so, how is this safe?

Cookies are protected with a MAC. It is not possible to create a fake cookie.

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

- 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.

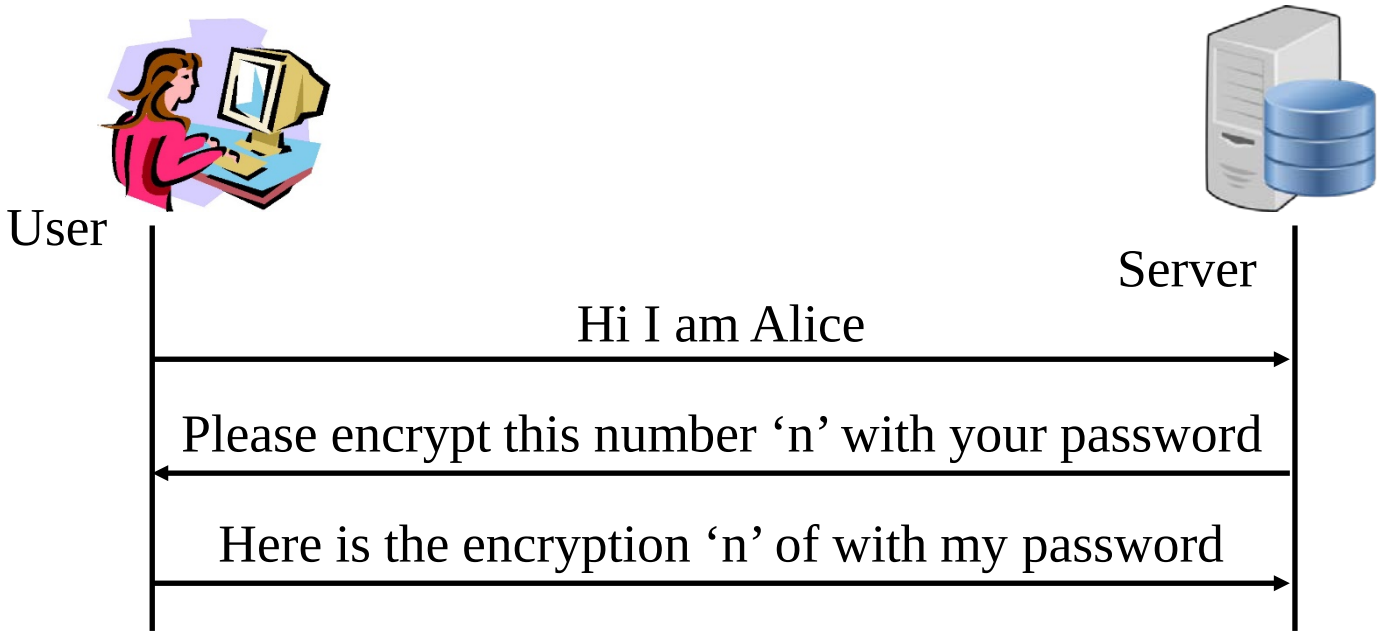
- Is the End Point Authentication usage of a nonce related to blockchaining's use of nonces?

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

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

- Can nonce have any efficient uses in security and passwords?

Nonce are used significantly in security. They may be used in generating new passwords, but the passwords are generally used many times.

- Since the password is always encrypted before sending it to the server, does it mean only the user who encrypts the password can decrypt it?

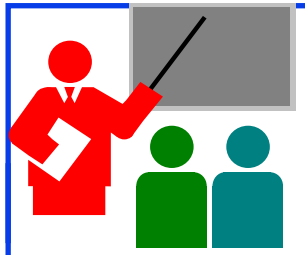
The encryption may be that of the hash of the password. So even the sender can only verify the correctness of the password but not find the password from the info on the net.

- Will it be possible to generate a special sequence of numbers to hack the encryption algorithm and password?

If the encryption is so week that a small number of ciphertext can reveal the secret, it should not be used.

- So what is exactly saved in the server? If it's encryption, isn't each encryption different as a different nonce is used each time?

A hash of the password is saved at the server.



Hashes, Signatures, Certificates

1. Hashes are one-way functions such that it is 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 the private key
4. Digital certificates are signed by root certification authorities and contain public keys

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.

- How do you define a secure hash function?

See Slide 8-28. Requirements 4-6. Difficult to Invert. Difficult to find y, such that H(x) = H(y). Difficult to find any pair (x, y) such that H(x) = H(y)

- Is a root certification authority just an administrator of some sort?

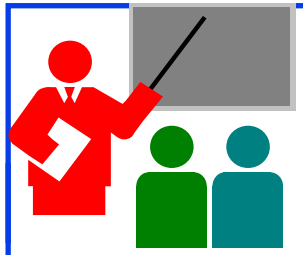
Yes. A trusted administrator.

- What are "root authorities"?

Root Certificate Authorities are trusted administrators whose public keys are known to most computers via their operating system.

- Is checking the "time" of the message. Is done for person-in-the-middle attacks that add time to the transmission?

To avoid replay attacks.



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

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.

- Why can't you fake certificates?

We can quickly check if you have the private key.

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

Secure E-mail

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

Student Questions

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

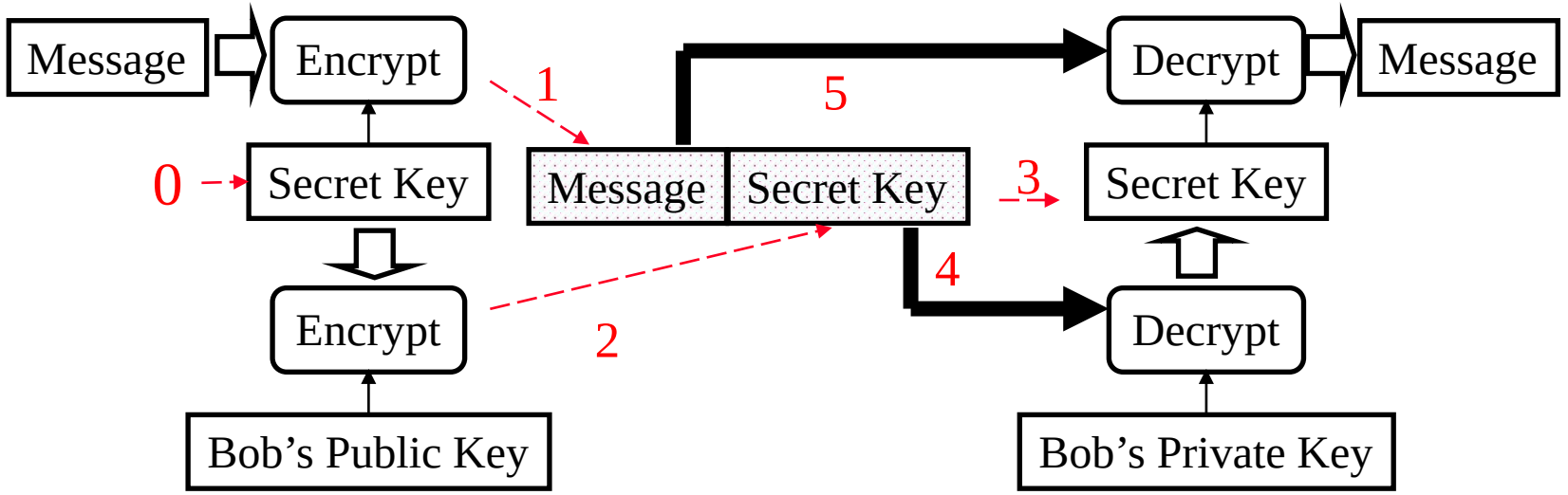
Whatever is in the cleartext is public knowledge.

- The e-mail 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 e-mail?

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

- Why not encrypt e-mail with Bob's public key as well? Why the extra secret key K_S? Because if somehow we can decrypt Bob's public key, we can get the secret key K_S easily? I don't see the extra protection.

Public key encryption or large messages is computationally expensive.

- Does the secret key need to follow some format? How to generate?

Yes. There are details about not using a weak key.

- What algorithm is used to generate Alice's random secret key?

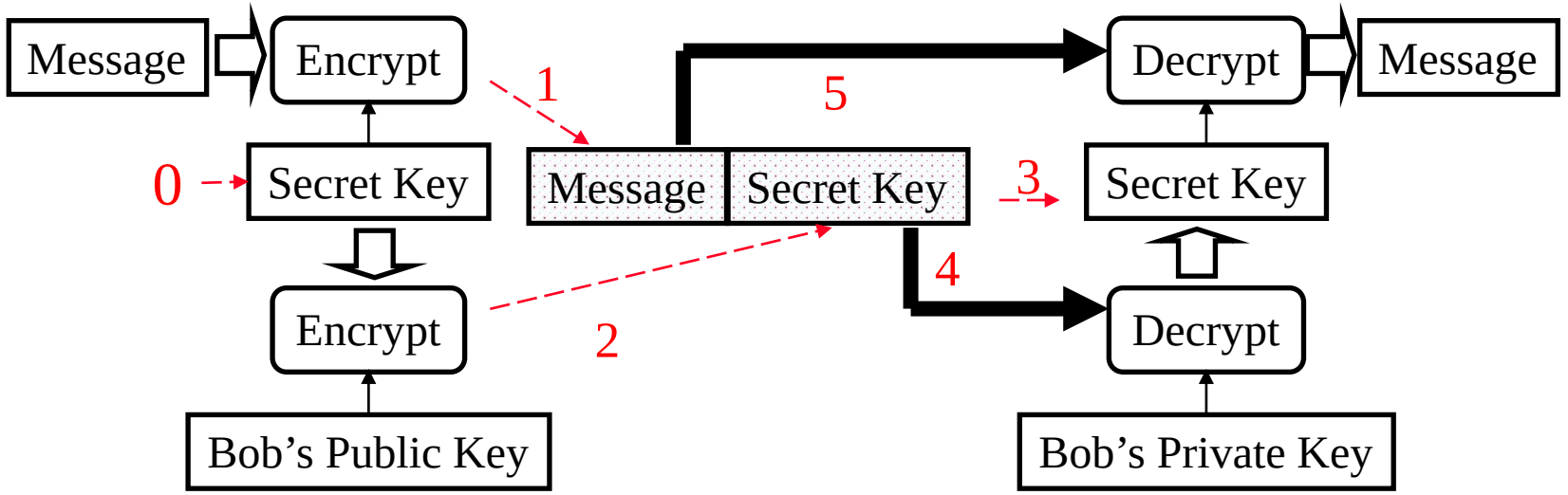
See above.

- Are all the e-mails encrypted in this way?

No. Nothing is encrypted unless you use a secure e-mail option.

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 message

Student Questions

- To send a secure message, do you need the receiver's public key and digital certificate?

Yes. The receiver must be in your contact list, where that certificate is stored in Outlook.

- Is efficiency the only reason we use a randomly generated secret key to encrypt the message instead of directly using the public/private key?

Yes, if you define efficiency as less computational cost.

- What if the encrypted secret key is compromised?

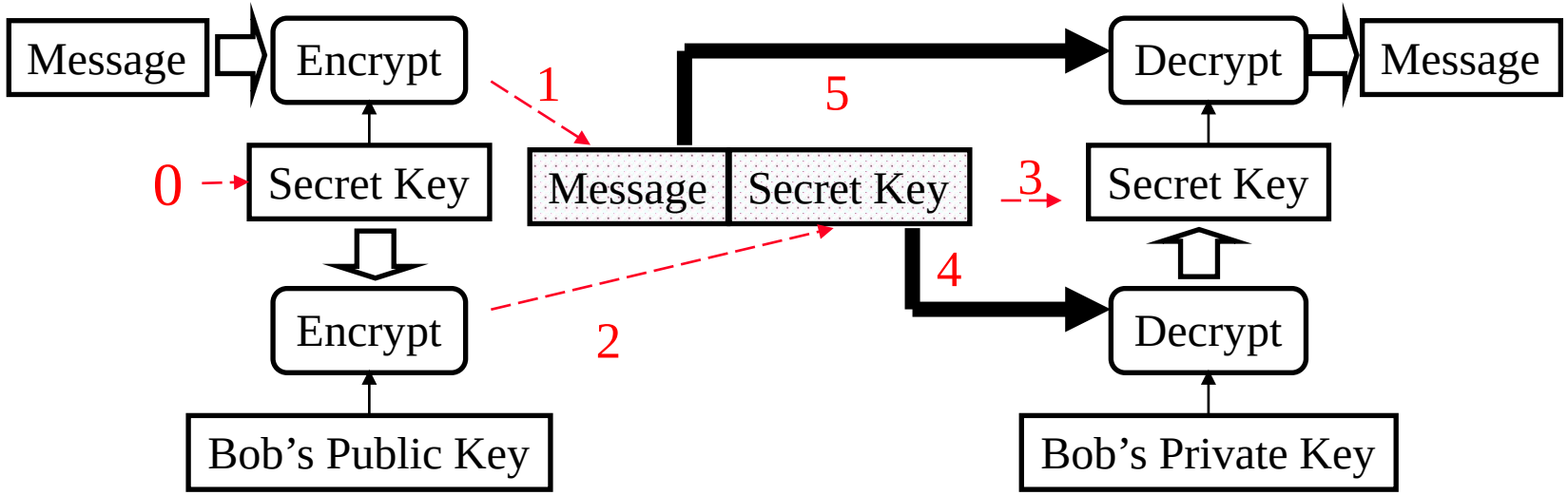
If a key is compromised, all information encrypted with it is compromised.

- Why do we have to use outlook to send secure messages, not other apps like Mail?

Sorry, We did not want to write instructions for all possible mail programs. So we wrote instructions for Outlook. You can use Mail and supply instructions for others to use it too.

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 message

Student Questions

- How long are keys?

No standard. You select. 64-bit is too small for today.

- Is a new secret key generated every time an e-mail is sent?

Yes. This reduces the number of ciphertexts available to the attacker to analyze.

- Is K_S regenerated for every e-mail or stay the same if the e-mail is sent to Bob?

See above.

- How to securely distribute public keys?

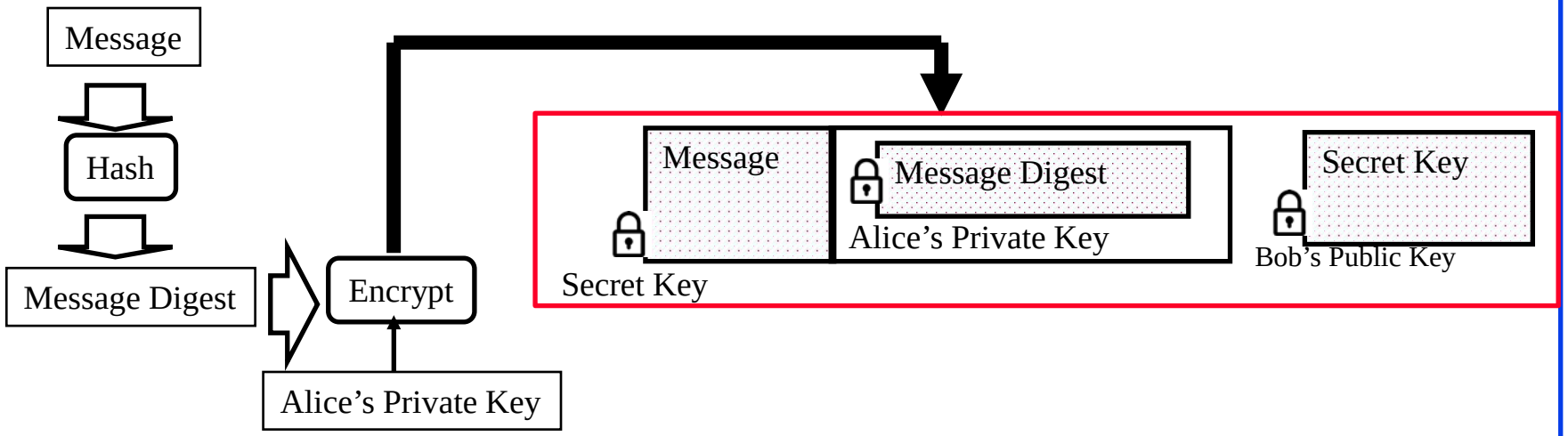
Public Keys are distributed in clear. Simple CRC protection is enough.

- If someone impersonates Bob and sends Alice his public key, can that person receive Alice's message to Bob? How to solve this security risk?

The first time when you talk to someone, make sure you are talking to the right person. After that, you save their certificate for future use.

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 the 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.

- So, the hash functions for each client in the whole e-mail system are identical?

Yes. Everyone uses the standard, e.g., SHA-2.

- Could you explain the word "sign" in this context?

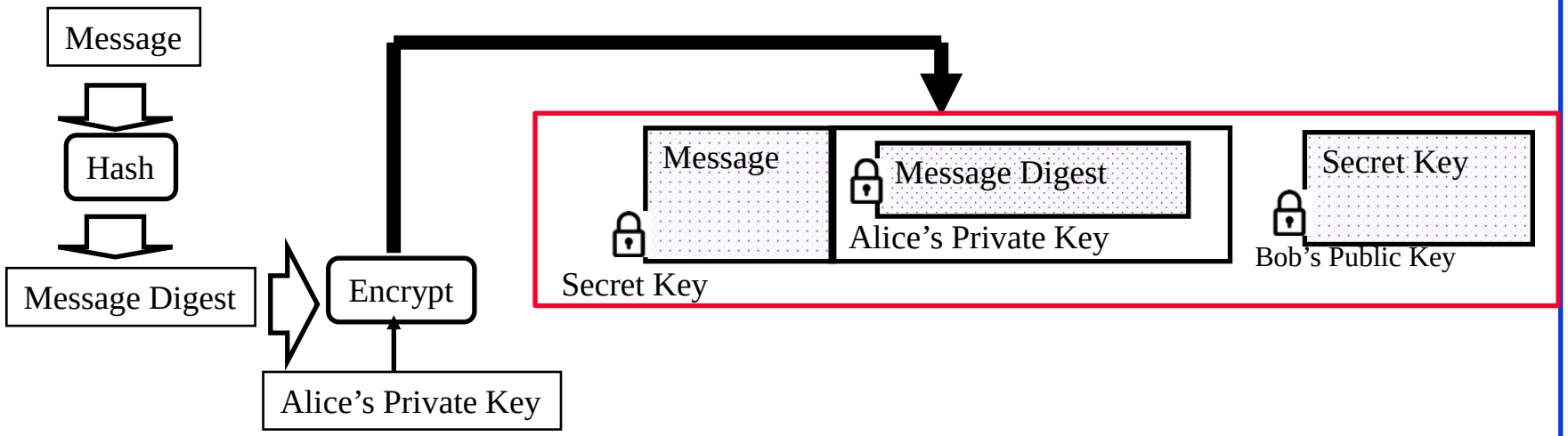
It should stand up in a court of law. The receiver should be able to prove using non-repudiation.

- Why is message digest used as a signature instead of PID or host IP?

Many users use a computer. You can't prosecute a computer or process.

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

- We need to do encryption, decryption, and sending keys together with the message. Will all these steps be done automatically by some application, or the sender and the receiver need to do everything manually?

Most e-mail applications, e.g., Outlook, do it automatically if you select the option.

- How could Alice's message be tampered with? Also, if Bob is using Alice's public key to verify the message came from Alice, couldn't someone else send a message using Alice's public key?

The message is encrypted using Alice's private key. Only Alice can send it.

- How can we overcome the challenge of encrypting the entire message instead of just a segment?

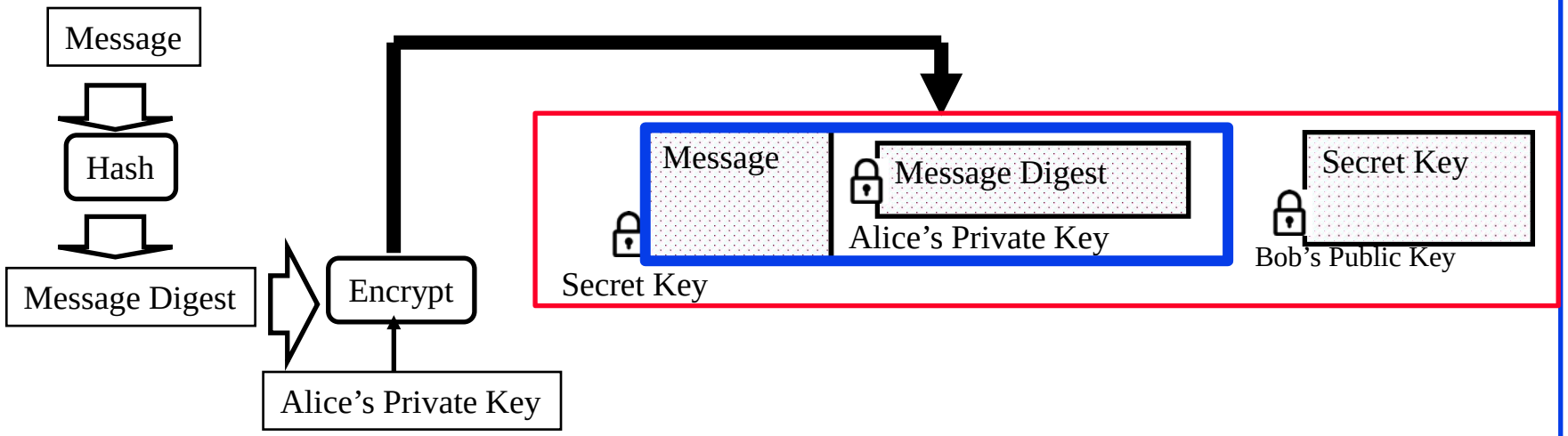
You could send the message in pieces, encrypt only some pieces, and send others clearly if that is what you want.

- Where is the Message Digest put?

See Figure. The red outline indicates the complete message.

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

- Is the Secret key only Encrypted the Message or Message and Message Digest?

Key names are indicated under the lock. As shown, the secret key is used to encrypt the message and message digest.

- What is the application of Message-Digest?

The message digest is used as a signature.

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

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 e-mail or when something is embedded in the message itself?

Yes.

- Why was 40-bit encryption the limit to what you could send outside the country? Was this number picked arbitrarily, or is there a reason that 40-bit is the limit?

US government wanted to be able to decrypt all international communications. Those times are not past.

- Do we still use PGP today?

Some people do.

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

Student Questions

- Is Gnu Privacy Guard (GPG) an implementation of PGP?

GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also known as PGP) [gnupg.org]

- Is PGP not used today, and what is its replacement?

Outlook and its competitors.

- Is it called "Pretty Good Privacy" because some features or privacy concerns are not met?

Mainly because it is free.

- Is this technique profitable?

No. This is free.

- Is the web of trust concept no longer used in any form? If a sufficient number of users do not trust a site, are there any consequences for that website?

Web of Trust is there but not there. Twitter, Facebook messages, Blacklists, and other social media instruments point out bad sites.

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.
- **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

- How can I verify if I successfully sent a secure e-mail?

Add the acknowledgment receipt option.

- I still have a question about lab 8. After importing the personal key to outlook, the encrypted appendix file is gone. Does that look right?

Yes. It is deleted so that no one else can get the secret key in a secure locker.

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

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

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

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

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

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

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

5. Examining your Certificate

From the references below.

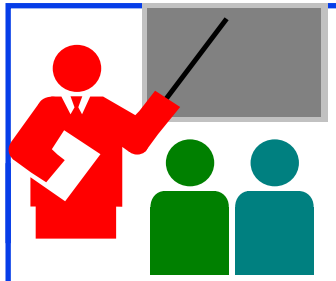
- In Windows, use Run → Certmgr.msc
- In the window that opens, look for Personal → Certificates
- Double-click on the new certificate. Go to the Details tab. Scroll down to find "Enhanced Key Usage." Click on it to see the results in the bottom pane. Please copy and paste it to your e-mail reply to 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

- So there is no secret key encryption in this Lab?

Yes. You need an e-mail certificate. WUSTL is still working on it. In the past, we used some sites that give free certificates. We can use it for class exercises if you find one, but not for business.



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

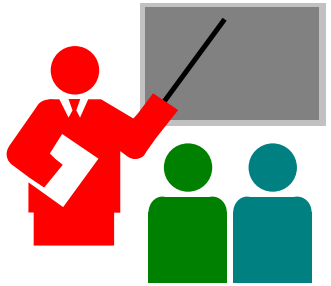
Student Questions

- Are e-mails sent during an HTTPS session not confidential?

All messages exchanged during an HTTPS session are secure.

Ref: Section 8.5, Review question R19

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 two rankings?
- *Not too many changes.*

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

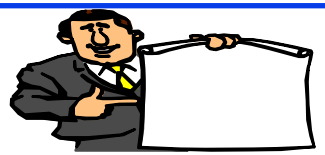
Digital certificates are public. You can post yours and others on your website. No security is required. It would help if you kept the private key in a safe. The private key is not there in the certificate.

- Basically, every ~~level~~ layer has its security approach; is that correct?

Yes. Every application has its security approach depending on the context it is used in.

End of Part 2

Next Q 8-97

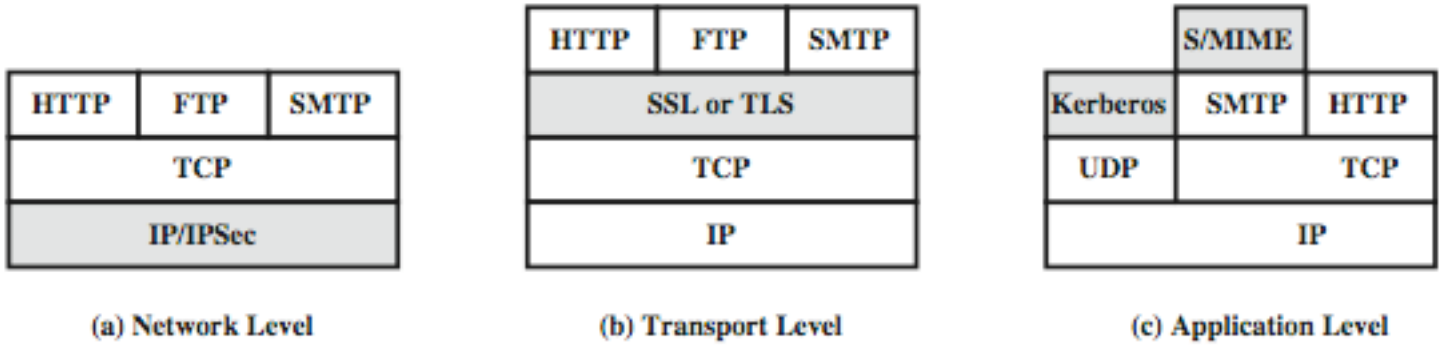


Transport Layer Security (TLS)

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

Student Questions

Web Traffic Security Approaches



(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

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

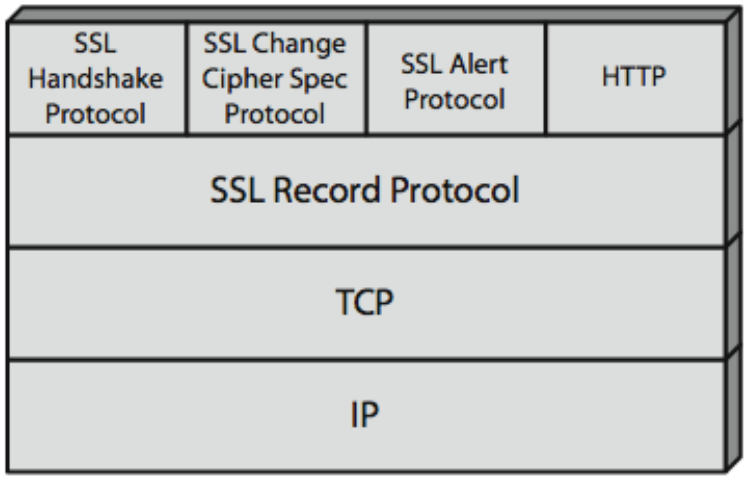
- What's the organization overseeing TLS? Is it the IEEE?

IETF

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

- Does the SSL/TLS handshake use ACKs?

SSL runs on TCP. TCP uses acks. Also, all SSL messages have responses, so missing messages are easily detected.

- Book Section 8.6 question: Is there is way to tell if a site where one might make a transaction is not authenticated (i.e., cannot be trusted)?

Their certificate will not be authentic and not be accepted. If they have a bad reputation, it will not be detected.

- Generally, what is a handshake? Does it mean some data exchange between a transmitter and a receiver?

See Slides 8-58.

SSL/TLS Handshake Protocol

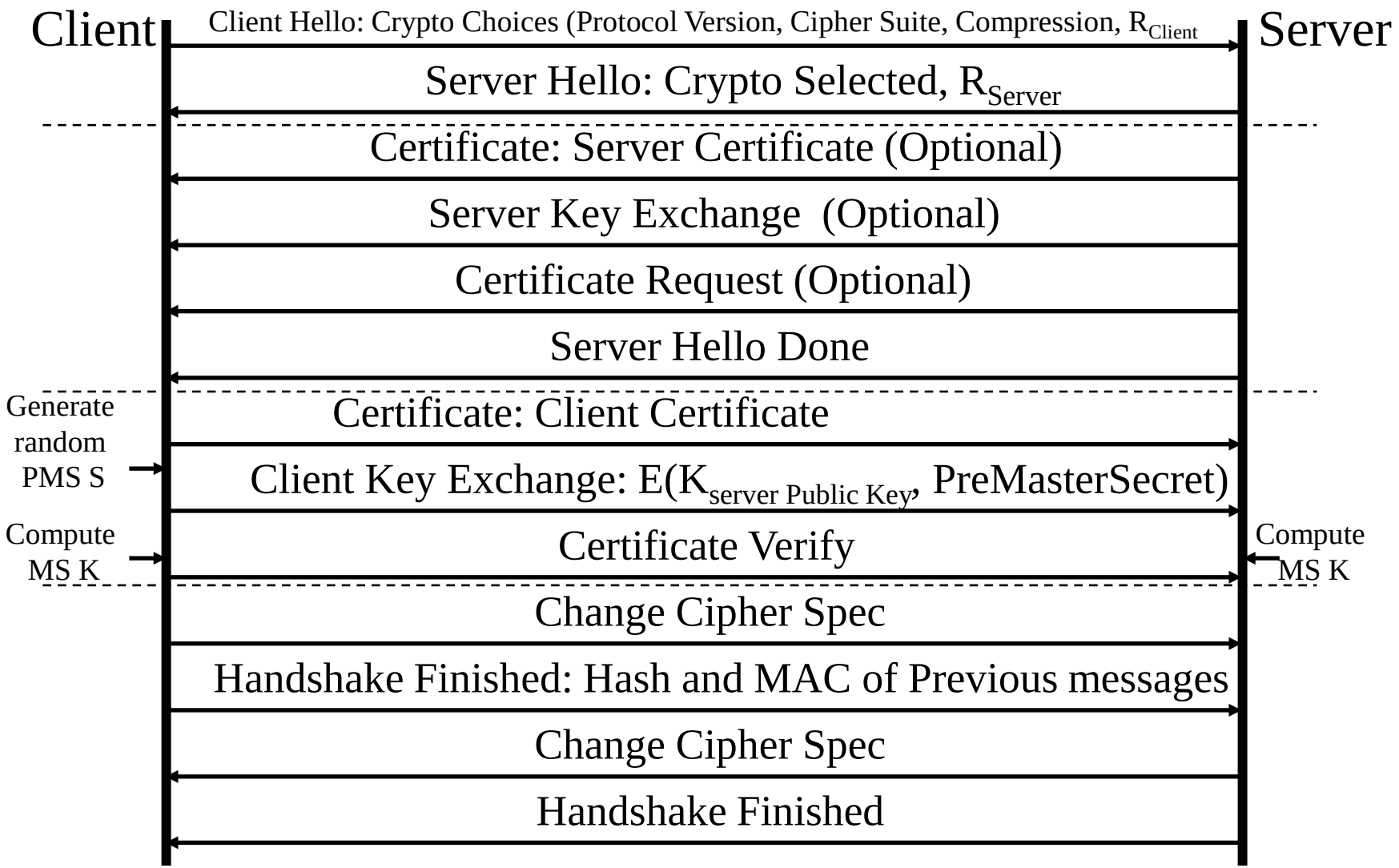
- Allows server and client to:
  - Authenticate each other
  - To negotiate encryption & MAC algorithms
  - To negotiate cryptographic keys to be used
- Comprises a series of messages in phases
  1. Establish Security Capabilities
  2. Server Authentication
  3. Client Authentication and Key Exchange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

Student Questions

- Are the cryptographic keys generated same for the client and the server?

Some are same and some are different. See Slide 8-59.

SSL/TLS Handshake Protocol Actions



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

- Does SSL/TLS handshake happen after TCP handshake?

Yes. SSL requires a TCP connection.

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

- Is there a protocol similar to TLS that works with UDP?

Yes. DTLS. It is not covered in this course.

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)

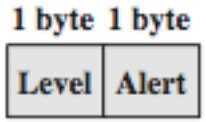
42 Bad certificate (warning or fatal)

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

- Is HTTPS encryption unique to each request being sent?

No. But the key is changed frequently—every few minutes.

- In the textbook it claims that for SSL, a closure SSL record must be sent before closing the TCP connection to prevent truncation attacks. What happens on an unexpected SSL disconnect?

The closure request results in a timely release of resources. Without closure, both sides will release resources after a timeout. And maybe subject to "truncation attack."

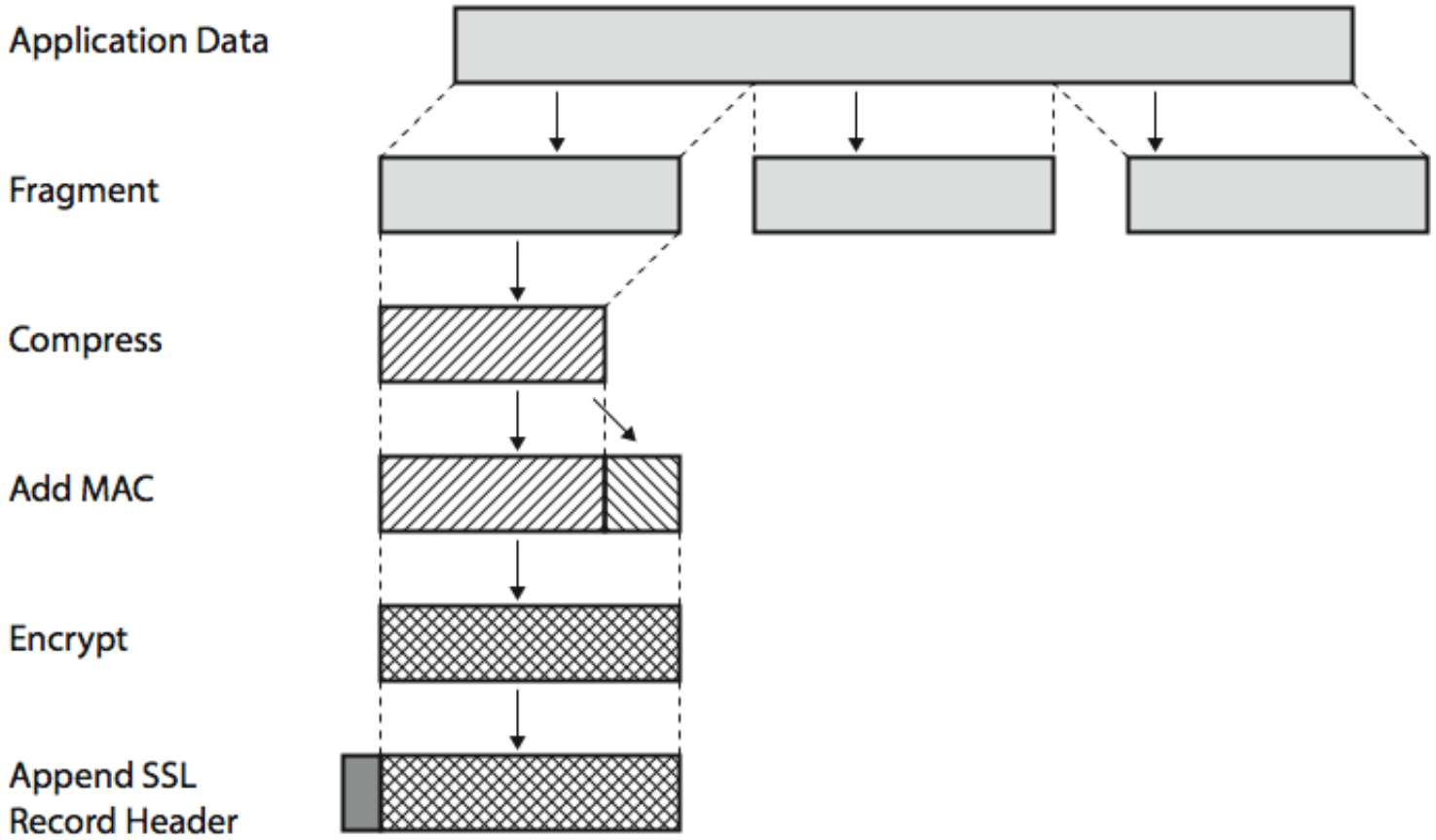
- Can you explain this sentence: "hash of the data plus the HMAC key MB plus the current sequence number" on page 648 of the book?.

MD5(Data||HMAC Key||Seq #)

MB is Bob's HMAC key.

MD5 is just an example of a hash used here.

SSL/TLS Record Protocol Operation



Student Questions

- Is there still active development in TLS? What's the organization overseeing the protocol?

Yes. IETF.

What's the organization overseeing TLS? Is it the IEEE?

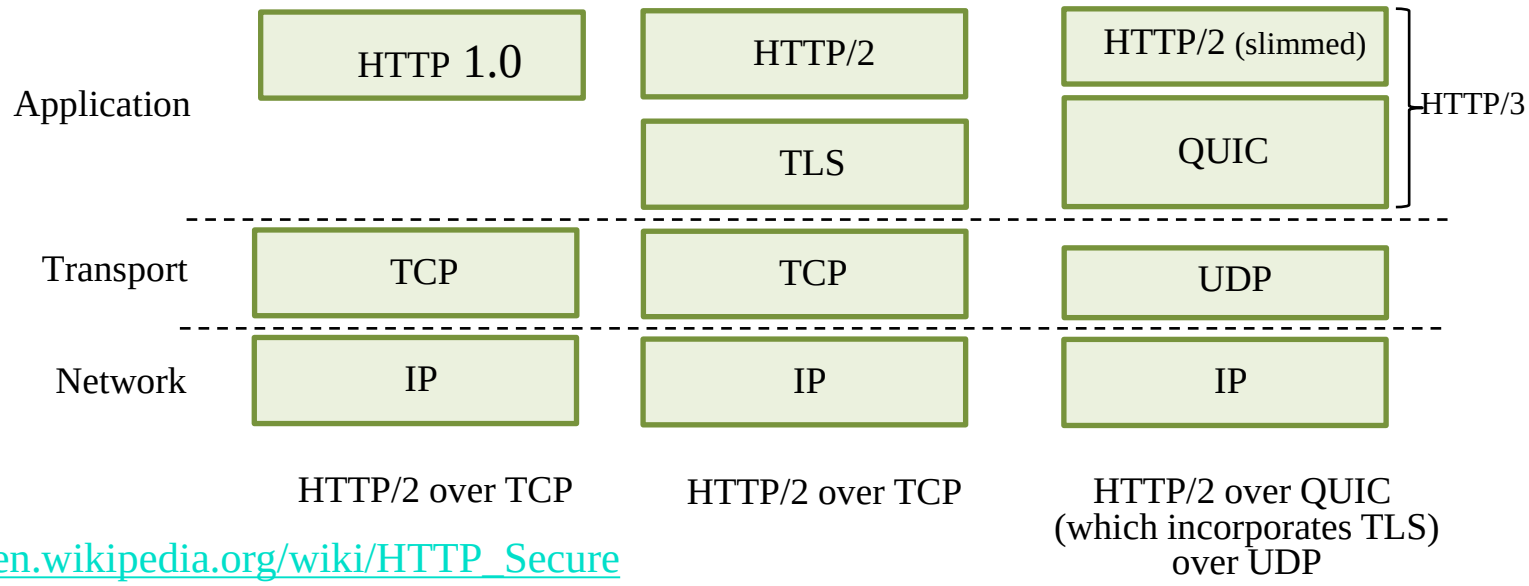
No. IETF.

- Does the TLS session start when the Master Secret (MS) is created?

See Slide 8-58. Generally, the start would be defined as the first message at the top.

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

Student Questions

- In the diagram, why is TLS(in QUIC) a part of HTTP/3 but not a part of HTTP/2?

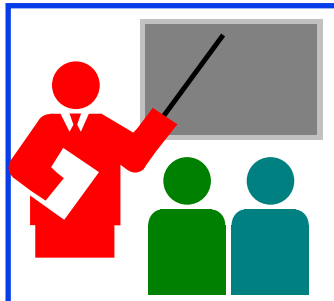
QUIC is a new Transport Layer Protocol that includes TLS.

- I remember reading somewhere that a hacker can still analyze/sniff traffic encrypted with HTTPS via Wireshark to extract useful information. Is this true?

You may be able to get traffic flow information by monitoring the number and length of messages.

- Does HTTPS use symmetric encryption? If so, how do both sides know the secret?

TLS handshake is used to share the secret.



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

- Does the TLS EMS ever change during a TLS session?
- *TLS keys are changed frequently to avoid giving too much data for the attacker to analyze.*
- Is the TLS sequence number initialized to zero?
- *I am not sure, but common sense would say that the initial sequence number would be random.*
- What does it mean for a key to be symmetric?

The secret key is symmetric. Public Key is asymmetric.

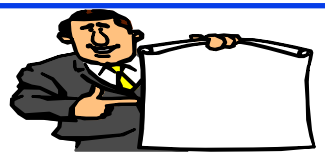
- Does TLS's API be the same as TCP's?

The APIs may be similar but not identical. TLS is a different protocol than TCP.

- How long are these four keys for TLS? Will it be costly?

Key lengths are chosen by the user depending upon the level of security required. Longer keys require more computation power.

Ref: Read Section 8.6 and Exercises R20-R23



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

- What is the difference between VPN and VPS?

VPS=Virtual Private Server
VPS is a server on the cloud. It is used not for security but to avoid the expense of having a physical server.

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

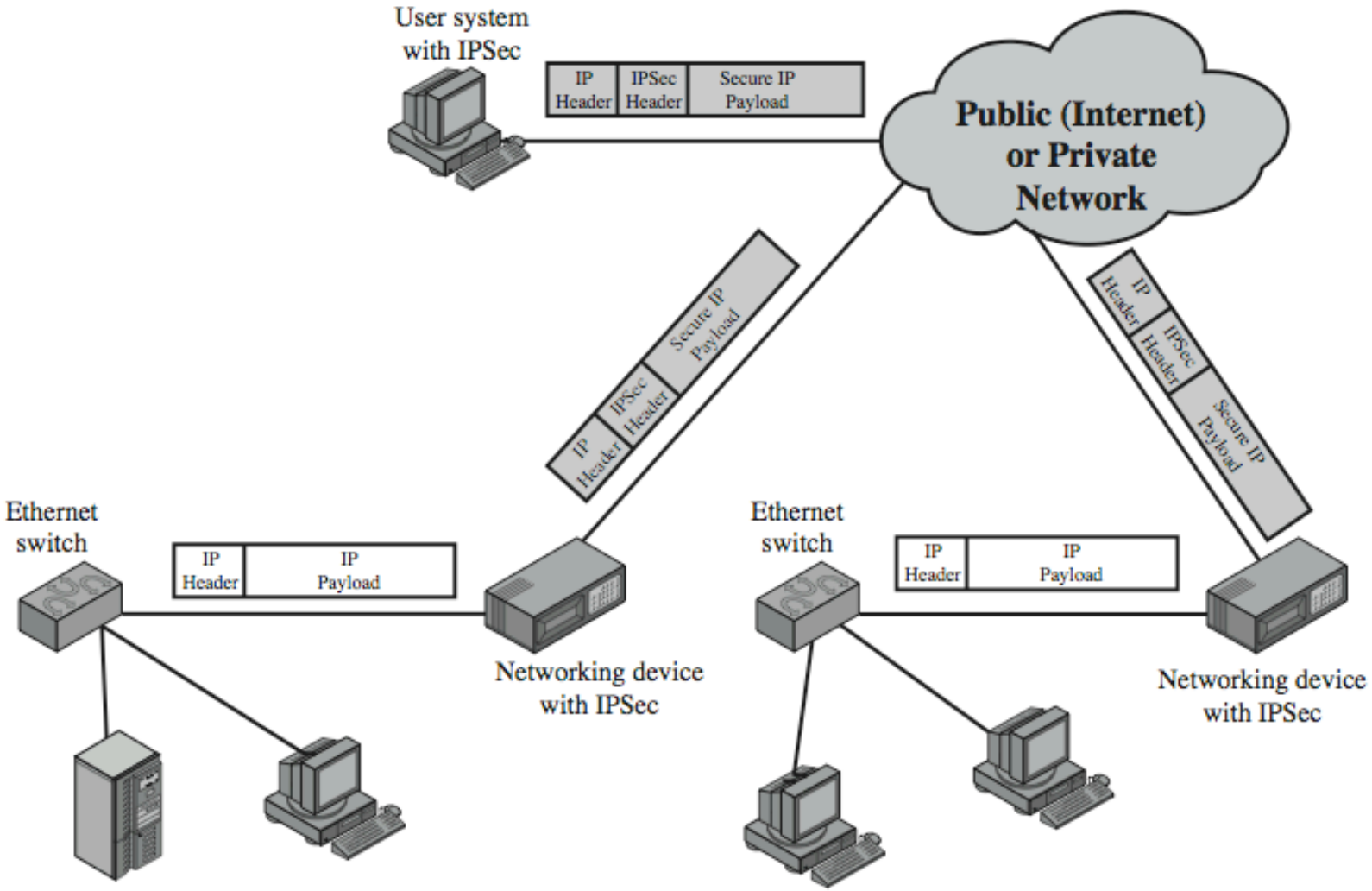
Ref: http://en.wikipedia.org/wiki/IPsec

Student Questions

- Are VPNs one type of IPsec application, or are IPsec applications also called VPNs?

VPN is one type of application of IPsec. You can use IPsec for other applications. See the list at the bottom of this slide.

IP Security Applications



Student Questions

- How are VPNs used to make websites think you are in a different location? Does the VPN company send your request from a server that is physically in that location?

All your requests are sent to the VPN server, communicating with the destination. So the world sees all messages coming/going from the server location.

- Are all users of a VPN communicating to the same IP address?

The VPN server is like any other server. It can have a fixed IP address or a rotating IP address (remember google.com address?). It can also be a set of servers behind a load balancer.

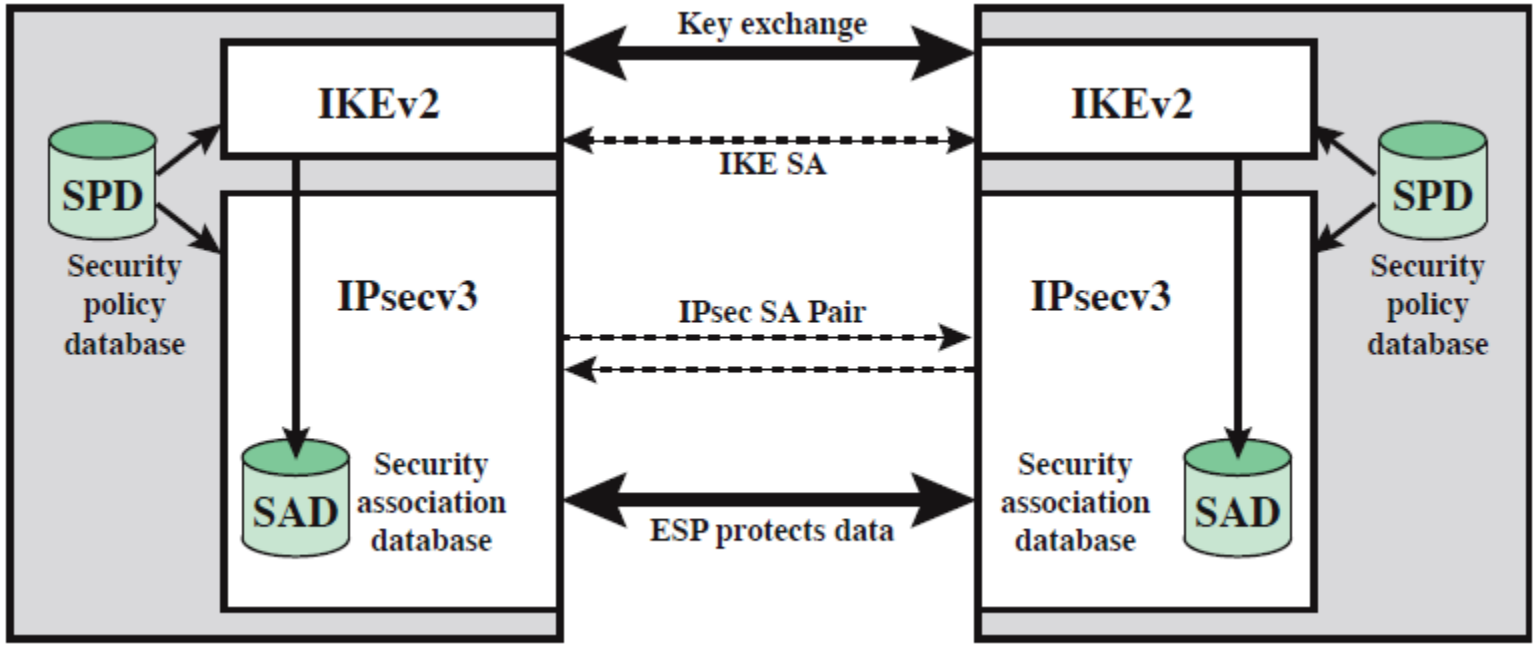
- Is this the reason that the VPN is exposed?

"VPN is exposed" if the government finds out that you are VPNing to some site banned by the government. Yes.

- If we want to set up a VPN, do we need DNS? *Yes, if you use the VPN server name. You can use the IP address directly and not use DNS.*

IP Security Architecture

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



Student Questions

- Is this like a firewall?

No. Firewalls do not encrypt traffic.

- Why do we need both SAD and SPD?

SPD is for the policies which remain the same over the long term and is a smaller database. SAD is for the current connections, which change as new connections are set up and old ones closed. Implementors can decide to keep them on the same "database," but they have a different purposes and durability.

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

- Are there security association databases for each network or server? Also, who manages the SAD?

Each device keeps and manages its databases. For example, if you have a security camera, it will maintain a SAD and SPD. The phone you use to connect to it will have its own SAD and SPD.

- If we had two senders and one receiver, would there be only 1 SAD for the sender-receivers, or would it be two separate SADs for each sender-receiver pair?

Each association is one-way and one-to-one. So, there would be two associations. Since each sender is also a receiver, there will be four associations.

- Why would two entities use one unidirectional SA and not two?

They will generally use two SAs.

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

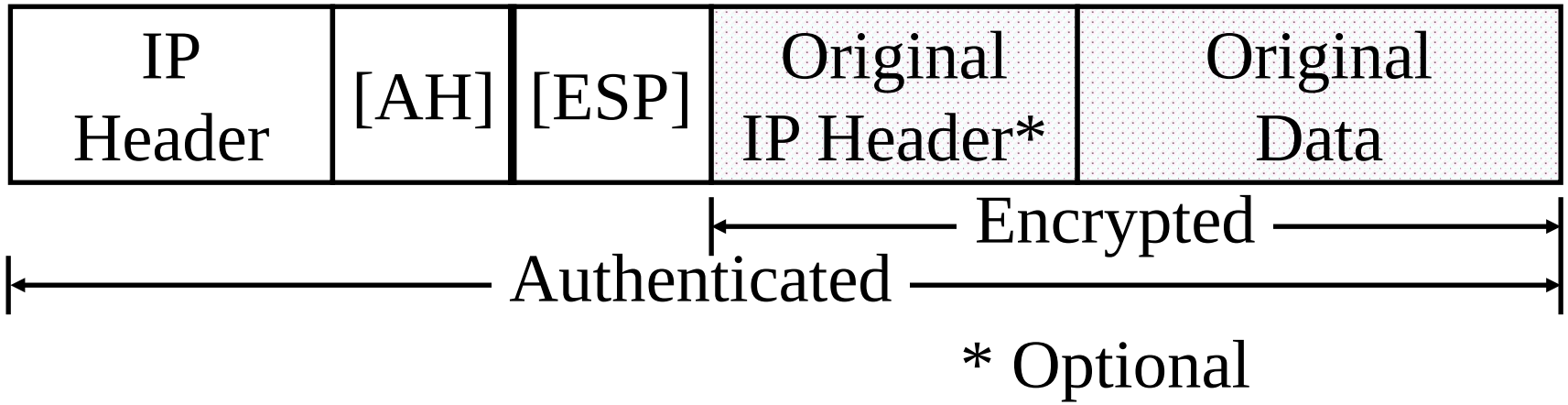
Student Questions

- Can you go over SPD again?

What's not clear?

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

- Will there be overlapping information since the new IP header, and original IP header exist simultaneously?

Routers look at the outer header only. The Inner header is in the payload. It will be looked only at the destination of the IPsec.

- For each layer, when should we choose encryption and when not?

Each application chooses its layer for security. If you want to secure all applications, you use IPsec. If you want to secure just one application, say, HTTP, you use HTTPS.

- Does UDP have a related encryption protocol?

Yes. DTLS.

- Can UDP use IPsec? Does UDP + IPsec make sense in security?

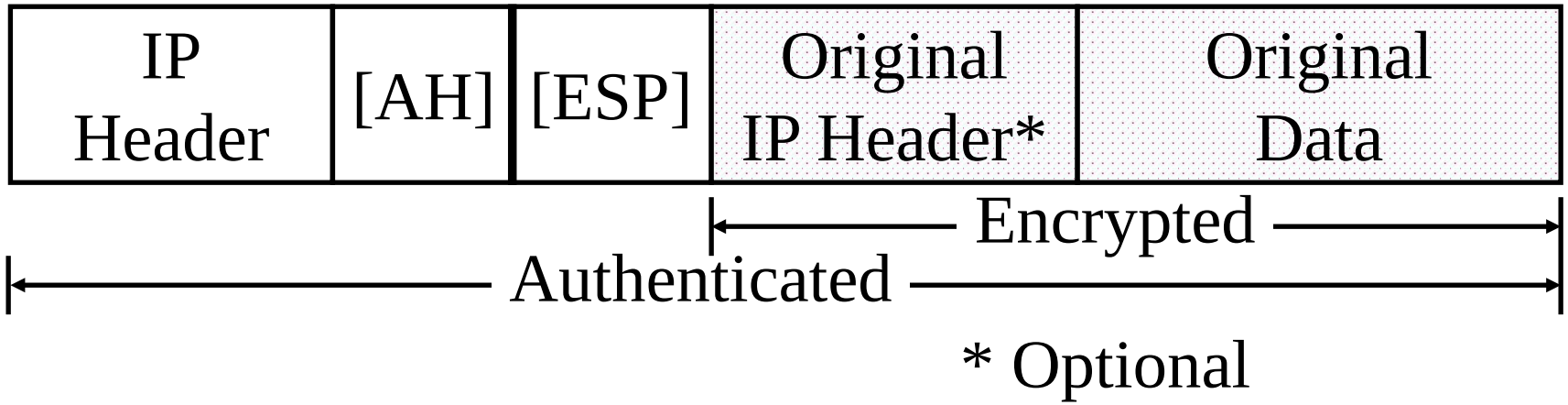
Yes. UDP is protected using IPsec, for example, in VPNs.

- Can you go into detail about the two ways of IP security?

Yes. AH, and ESP are covered next.

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

- Could you explain Quiz Question 3: IPSec secures all Ethernet applications.

Ethernet is Layer 2, and IP is Layer 3. The IP cannot secure things it does not see.

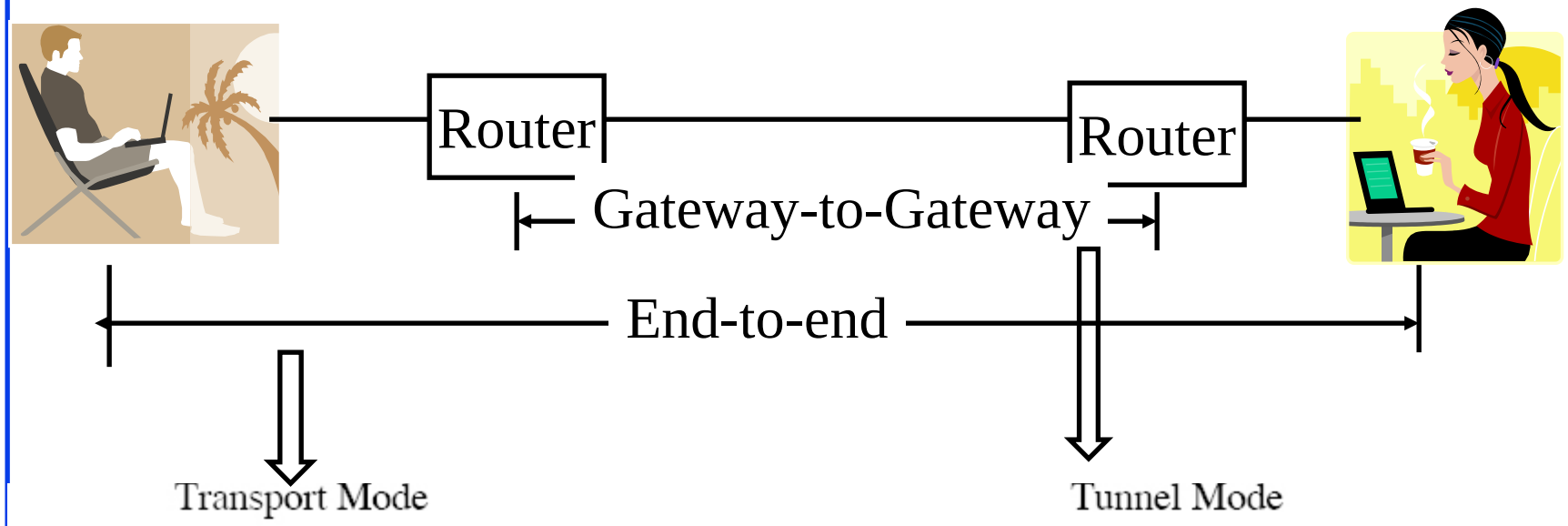
- The last question in the quiz in Canvas has no content in the choices.

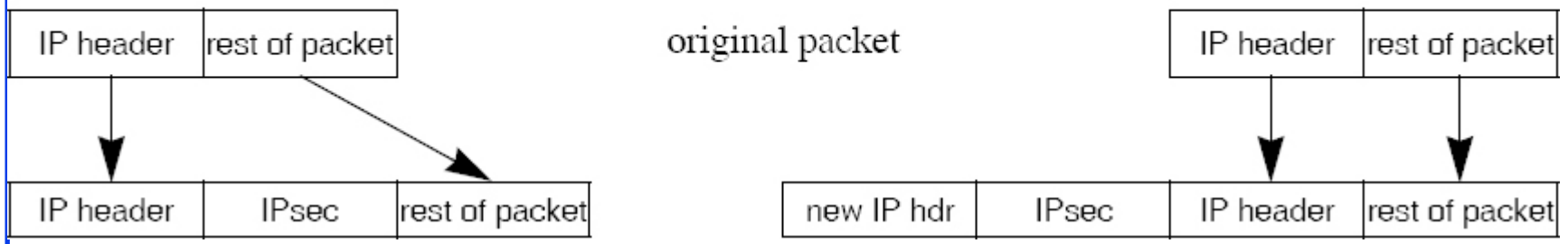
Sorry. Canvas does not allow me to correct the mistake now. We will add 2 points to everyone who took the quiz.

End of Part 3

Tunnel vs. Transport Mode

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





Student Questions

- To communicate via the transport method, how does one set up that communication channel? Wouldn't transport methods be made up of several tunnels since several routers must exist between, say, two communication hosts? Could you explain this in more depth?

Routers are not involved in the transport method. They forward the packets using the outer IP header, which is in clear.

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

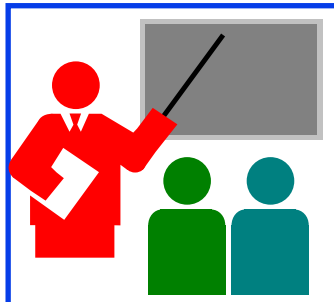
Student Questions

- Why does IKE use Diffie-Hellman during the first exchange of messages over RSA?

It was not covered in this course. We did not cover Diffie-Hellman.

- Why is IKE not used to encrypt messages since it's used to handle key generation?

IPsec consists of two parts: IKE and Encryption. Each part has its defined function.

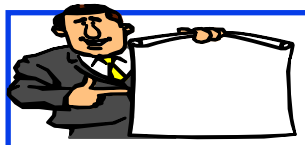


Summary: IPsec

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



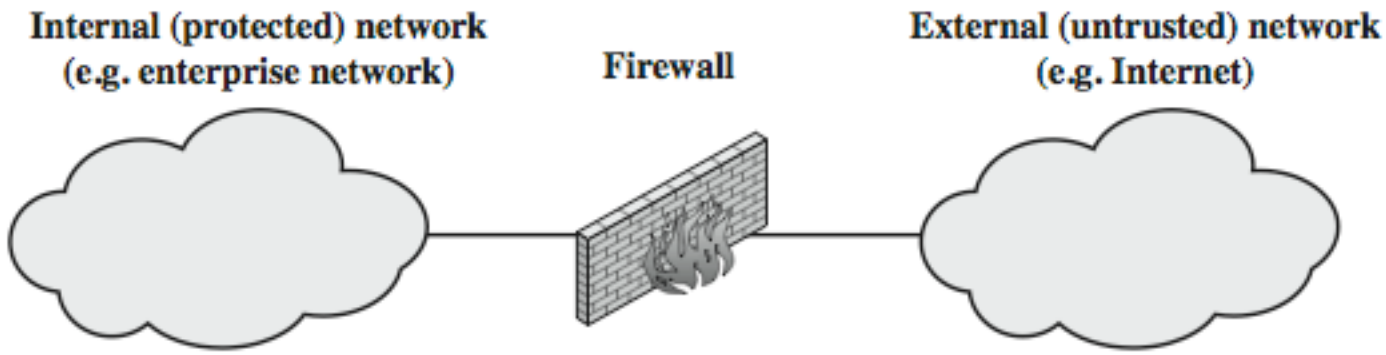
Firewalls and IDS

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



Student Questions

- Will a firewall create a false sense of security if it is not designed correctly?

Yes.

- From the slides, the Firewall blocks packets by identifying their sender/receiver hosts and ports. Is there any way of blocking by identifying the contents of a packet?

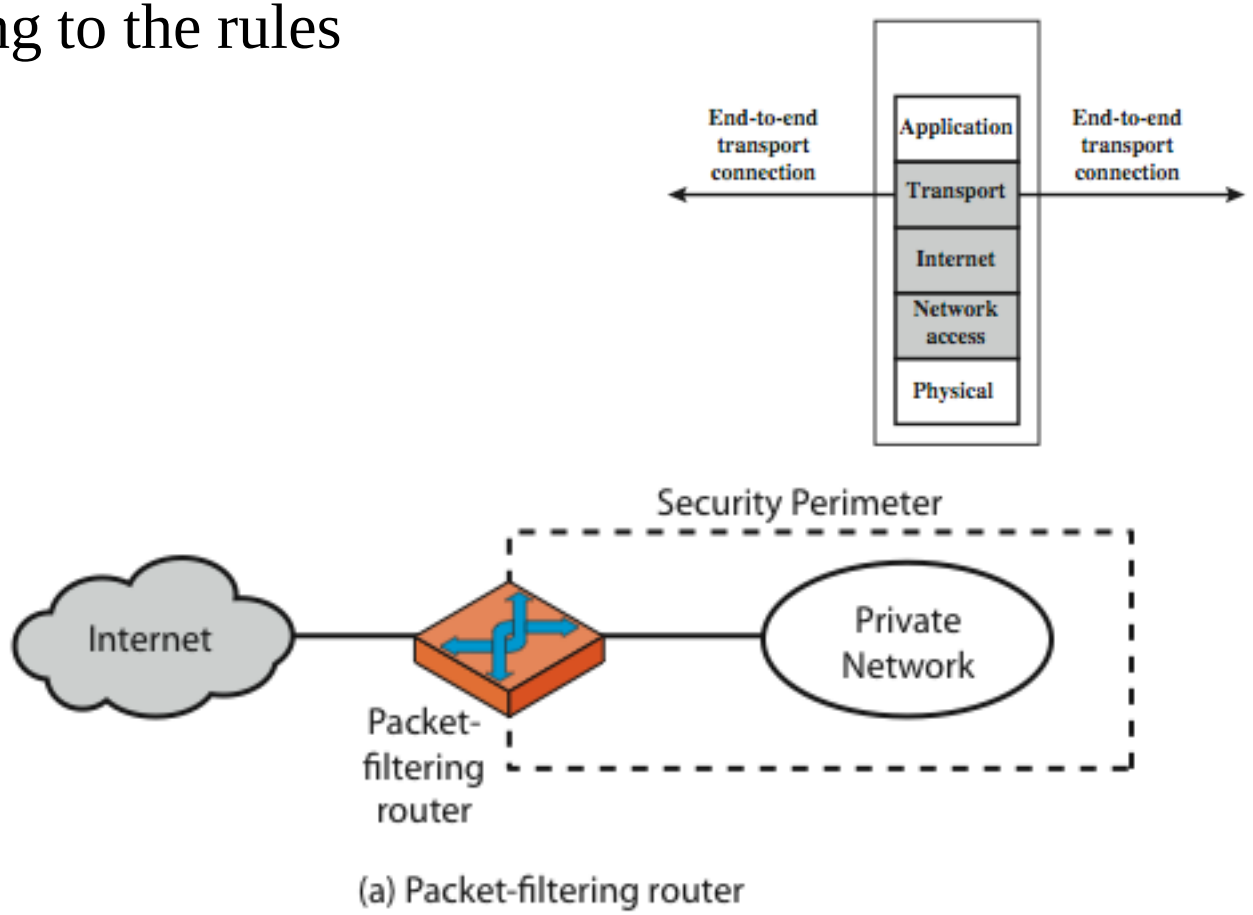
Yes. See Application-Level Gateway in Slide 8-85.

- So Firewall drops IP datagrams with untrusted IP addresses?

Yes.

Firewalls – Packet Filters

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



(a) Packet-filtering router

Student Questions

- Which layer does Firewall work on?

Application

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

- In the packet filter, can an external address-based policy protect datagrams whose source addresses are spoofed?

If you are concerned about source addresses, then you would use something that has origin authentication so the source addresses cannot be spoofed.

- Does a Windows Firewall "inspecting limited application data" technically give Microsoft a way to snoop on Windows users' data?

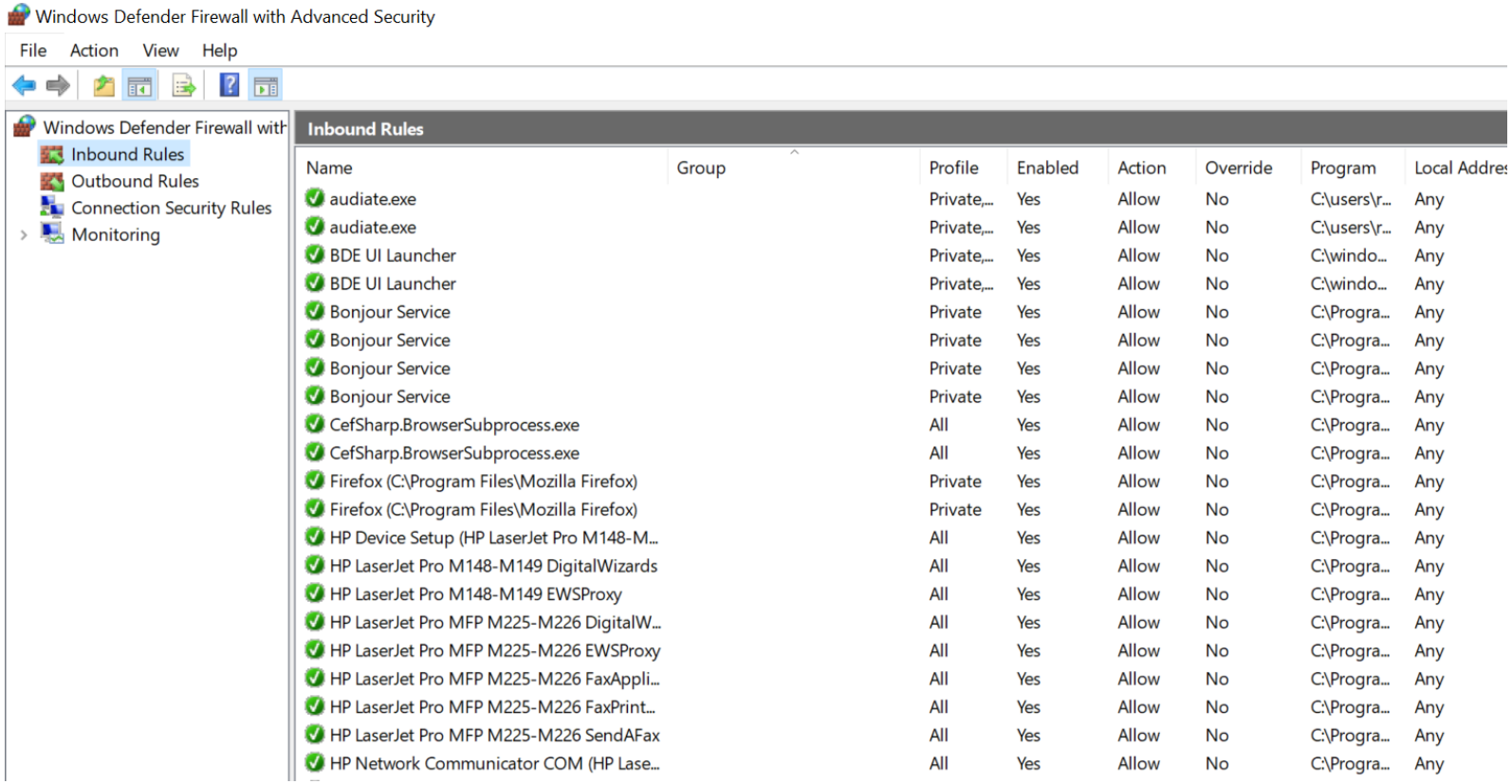
Yes.

- What does the firewall examine? The content of the packet or the source address?

Every field that you specify.

Packet Filter Example: Windows Firewall

- Windows Defender Firewall with Advanced Security → Inbound Rules



Student Questions

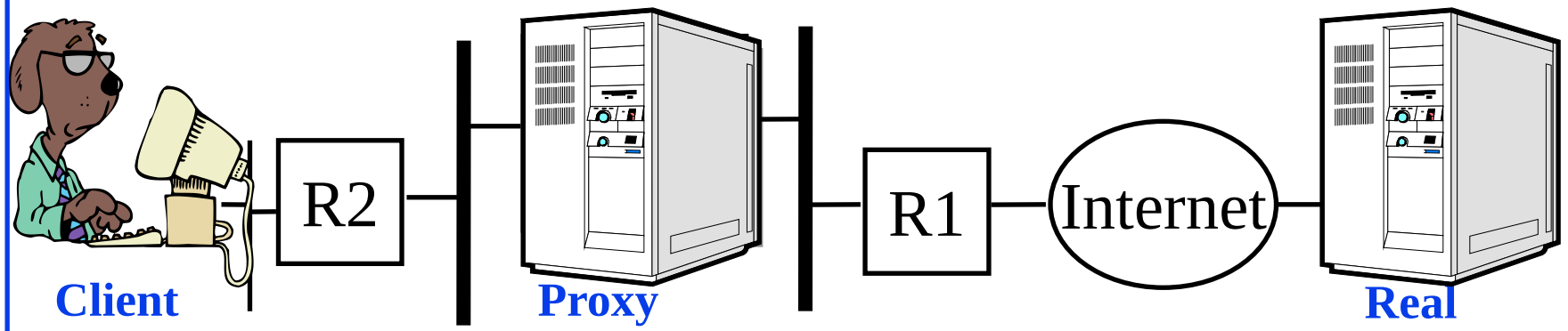
Firewalls – Stateful Packet Filters

- 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

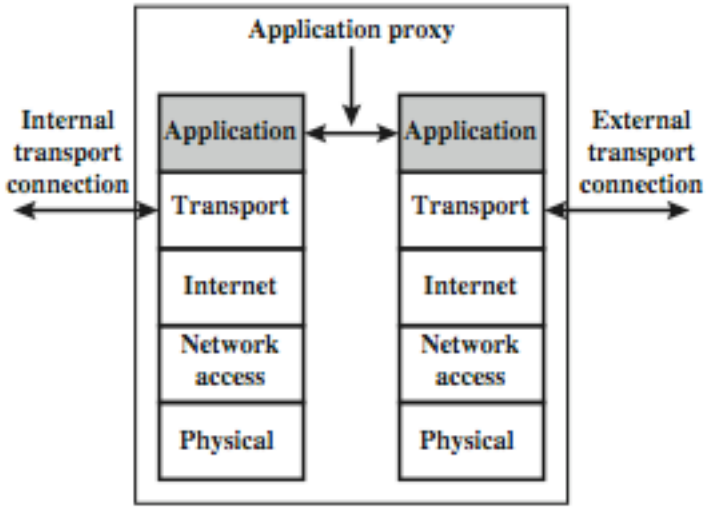


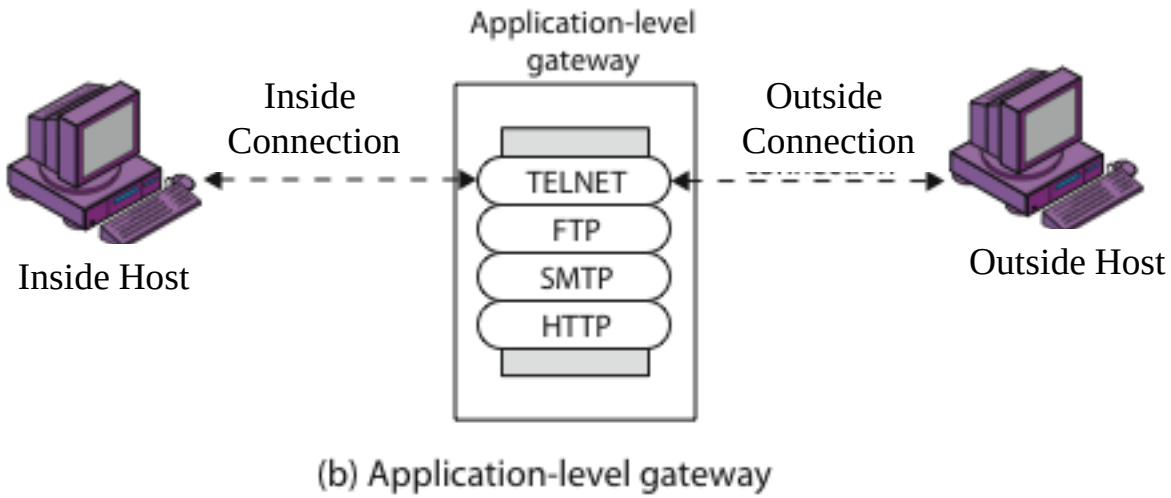
Student Questions

- Can a client know they are connecting to a proxy?

No. However, many organizations require clients to use their proxy. There you can't get out without the proxy.

Application Level Gateway (Cont)



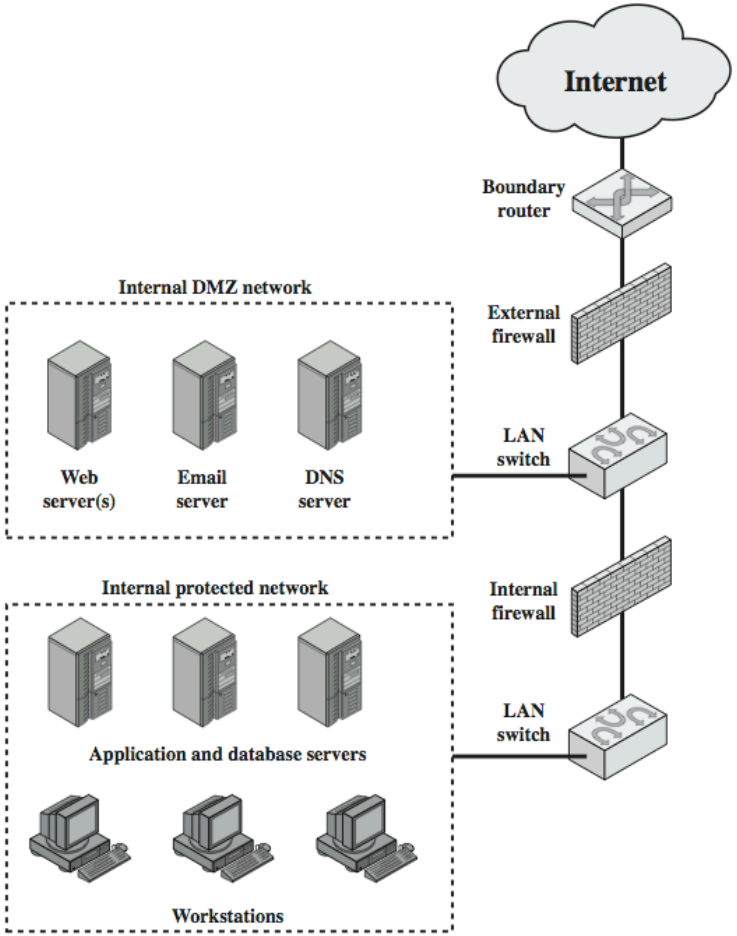


(b) Application-level gateway

Student Questions

DMZ Networks

- Demilitarized Zone



Student Questions

- Why not keep the stuff in the DMZ zone within another layer of security in the internal group?

Essentially, this is what is being done, if you define "internal group" as the entire enterprise/home network.

- Do external firewalls and internal firewalls use different packet filters?

Yes. External mostly checks the destination and application. Internal is more thorough.

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

- Can intruders make tons of false flags attacks to confuse our Anomaly-Based IDS? What's the countermeasure for such attacks?

False flags can be detected by origin authentication. You will need a mechanism like IPsec that provides origin authentication.

- What are PDAs?

Personal Digital Assistants – smartphones, iPads, etc.

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

- Can intruders make tons of false-flag attacks to confuse our Anomaly-Based IDS? What's the countermeasure for such attacks?

Not sure how you confuse our anomaly-based IDS. It is not based on frequency. It is based on the IDS designer's view of what is normal.

- How are Anomaly-Based IDS different than Statistical Detection (Since statistical detection also looks for abnormal cases)?

They are similar. However, anomaly-based IDS generally have preset rules. They are somewhere between rule-based and statistical analysis.

Honeypots

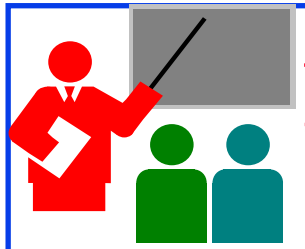
- Decoy systems to lure attackers
  - Away from accessing critical systems
  - To collect information about their activities
  - To encourage the attacker to stay on the system so the administrator can respond
- Are filled with fabricated information
- Instrumented to collect detailed information on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

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

Student Questions

- Are honeypots commonly used? They seem like a bad idea because to direct an intruder towards the honeypot, you probably have to put an intentional weakness on your network's edge that, when exploited, gives access to the honeypot. The wrong idea is intentionally putting a weakness.

Yes, they are used commonly. The weakness is in an area that is outside "your network."



Firewalls and IDS: Summary

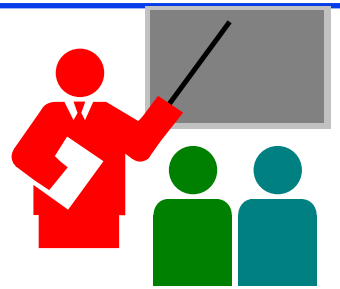
1. Firewalls separate networks of different trust levels
2. Some traffic, such as laptops, smartphones, and wireless can bypass the firewall
3. A firewall can be a simple packet filter or an application-level proxy
4. Intruders can be both internal, external or organized
5. IDS can be signature based,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

Student Questions

- Do most operating systems have a native IDS or is it that a license needs to be purchased for one or one needs to find a standalone open-source one like Snort?

Initially, most OS did not come with IDS. Now, most do. Snort is used for networks of systems.

Ref: Section 8.9 and Exercises R28-R32



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

- Would you please clarify the range of Exam 3?

All sections mentioned at the bottom of summary slides in Chapters 7 and 8. For example, see the bottom left of this slide.

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

- Should we expect all of the information we have covered (including the "extra" security information) to be on the exam?

The exam is based on the "Union of slides and the book."
Some things like details of the generation of a master secret were included in the slides with the caveat that you do not need to remember the formula but know roughly how it is done.

- If we've taken the first two exams, is the 3rd one optional?

Yes. Yes (in the 1st Lecture). Yes (after every exam), Yes (in Piazza Note this week).

- When can we expect to see what our final letter grade will be?

18th May 2022.

- How many blanks and judgments are in this exam?

Not determined yet.

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

- Would you like two more classes?