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/cse473-25/

Student Questions

- For chapter 8, P77 - the summary part we say ESP for confidentiality and integrity, but we know that ESP could used for confidentiality, integrity and authentication if we configure it according to our purpose. So if ESP completely replaces AH?
- Page #655 8.7.4 Will IPsec transport mode work across NAT?
- What security measures/methods are likely to last a long time without ever getting broken?

©2025 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

©2025 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

- 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.

©2025 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

- Does the telegram violate the principle: Non-repudiation? Because when I talk to someone in telegram, I can delete the message from both his (her) devices and my devices.

Yes, if what you said is true.

©2025 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

- Does Quantum Computing threaten the encryption methods utilized within network security? Is there work on post-quantum encryption methods within computer networking?

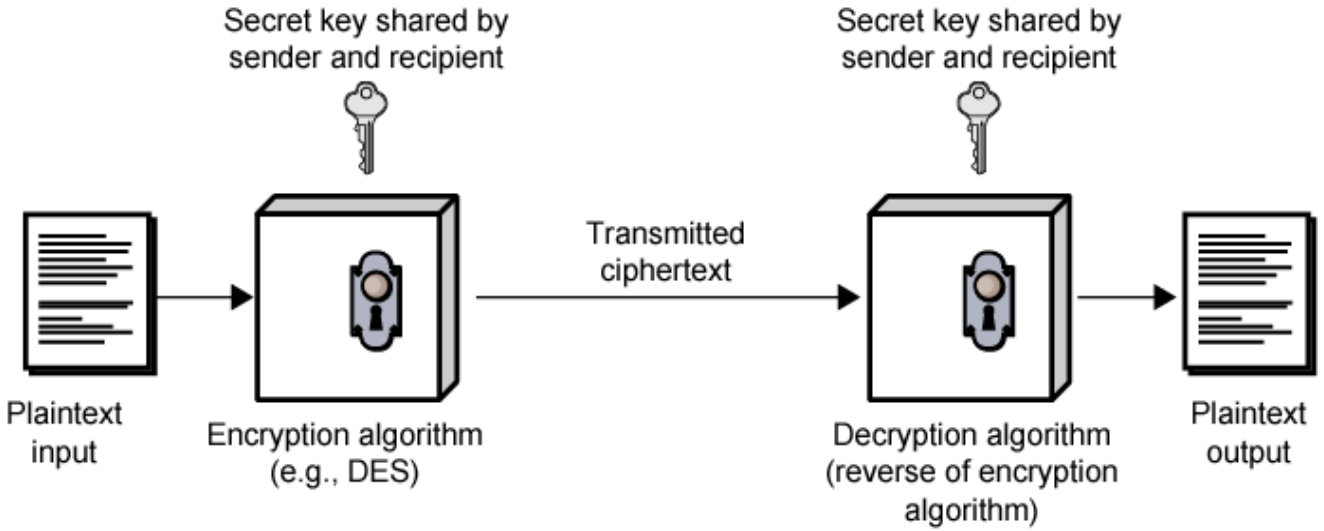
Yes. Please see our publications and talks on my website.

©2025 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

- What are the disadvantages of secret key encryption?

1. *The secret is known to two people. Either person can lose 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?

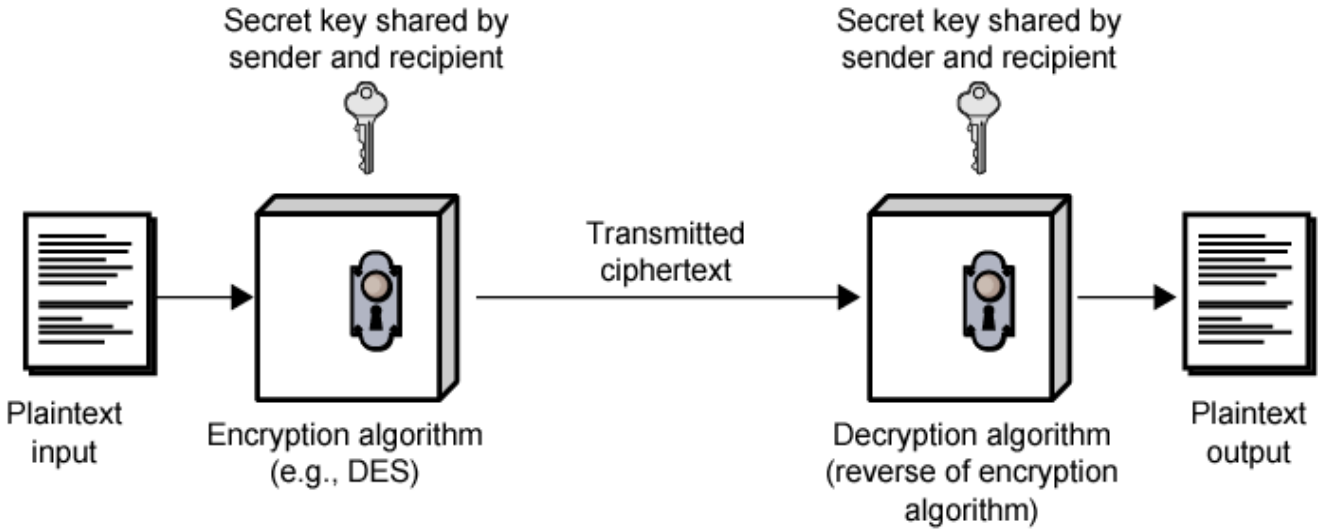
The key is not sent in the clear over the network, so network sniffers will not work. If you infect the sender's computer, you may be able to get the key.

©2025 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

- 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.

- Do we transmit keys with encrypted messages together?

This is discussed later in encrypted emails.

©2025 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

- 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.

- How to decrypt polyalphabetic encrypted messages?

See the example above.

- Does polyalphabetic mean substitution using the word rather than the letter, or are there multiple substitution rules?

Word substitution will make the tables shorter.
See the example in the first question above.

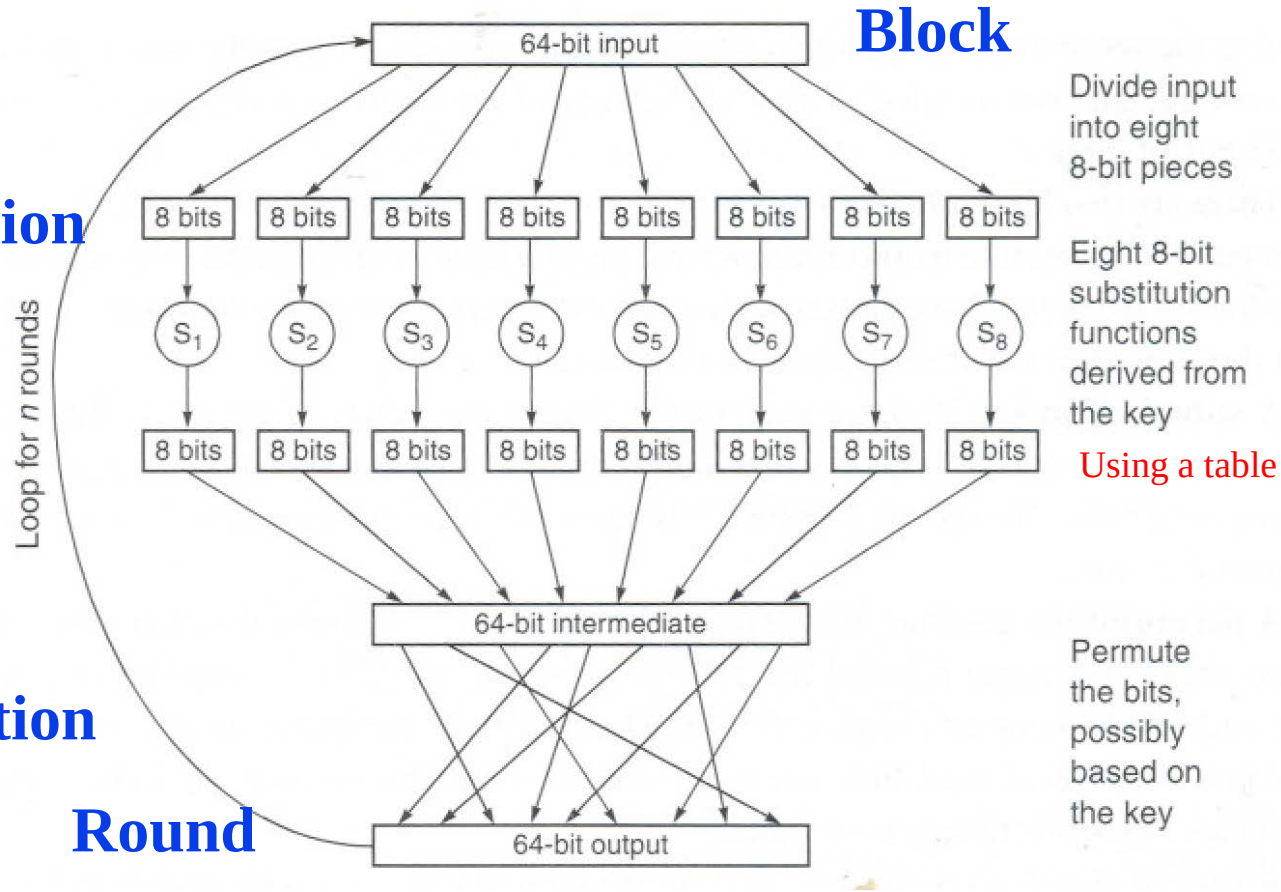
- Is the Vigenere cipher an example of a polyalphabetic cipher?

Yes. The key decides substitution.

©2025 Raj Jain

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.

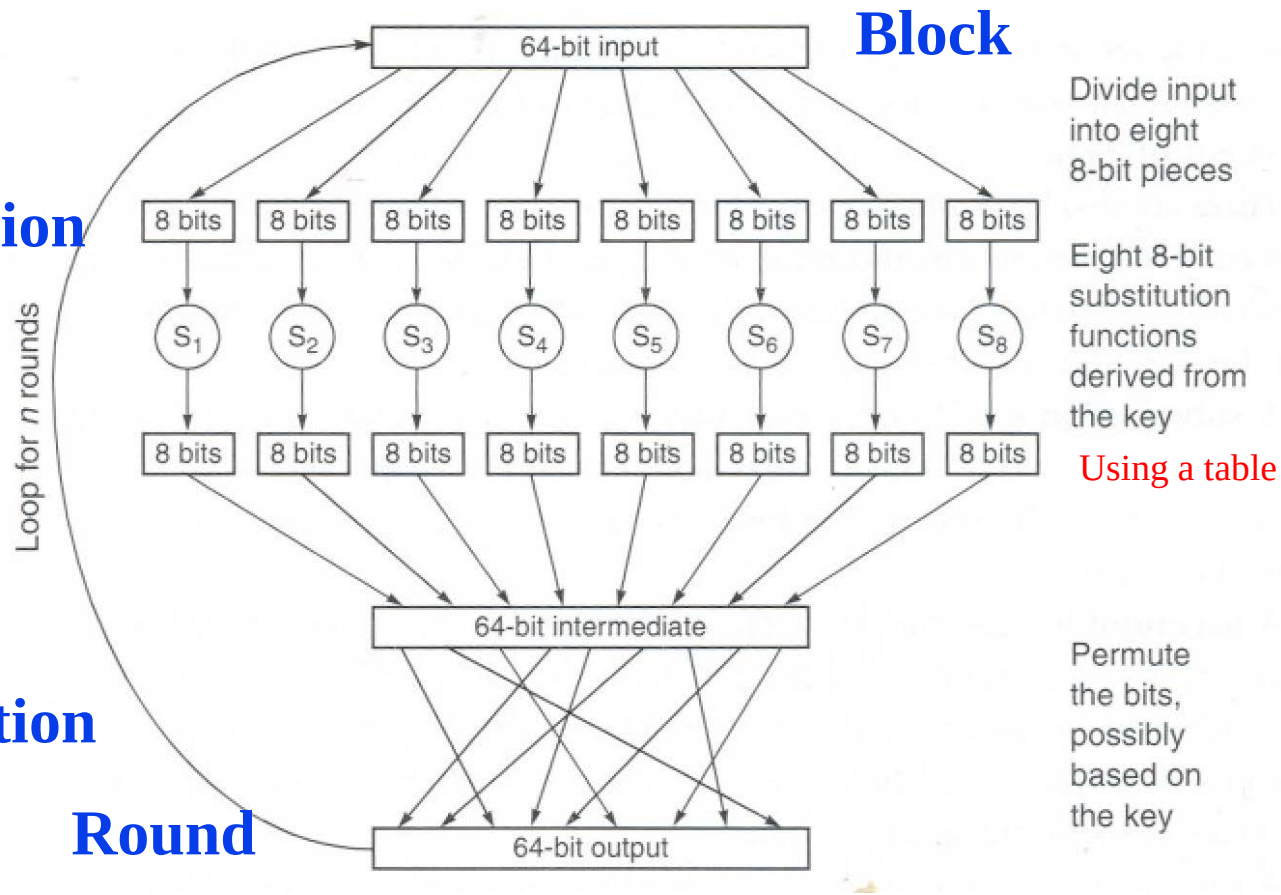
- What is the secret key in Block Encryption? Is the permutation step related to the secret key?

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

©2025 Raj Jain

Block Encryption

- Block Encryption



Student Questions

- Are a block and a frame the same thing?

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

- Do we do the block encryption for all 16 rounds each? Is it doing more rounds means more security? *Yes. Yes.*
- How secure is Block Encryption compared to other Encryption methods?

Block is the most common.

- What happens when the block of data is not perfect for 64-bit?

It is padded to a 64-bit boundary.

- Is the bit permutation scheme always the same to permit decryption?

Permutation is based on rules so that everyone comes up with the exact encrypted text.

- Could you explain why changing one bit will affect all 64 bits again? *Sure*
- How many rounds are commonly used in popular block encryption techniques?

AES uses 10 rounds for 128-bit keys, 14 rounds for 256-bit keys, …

©2025 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

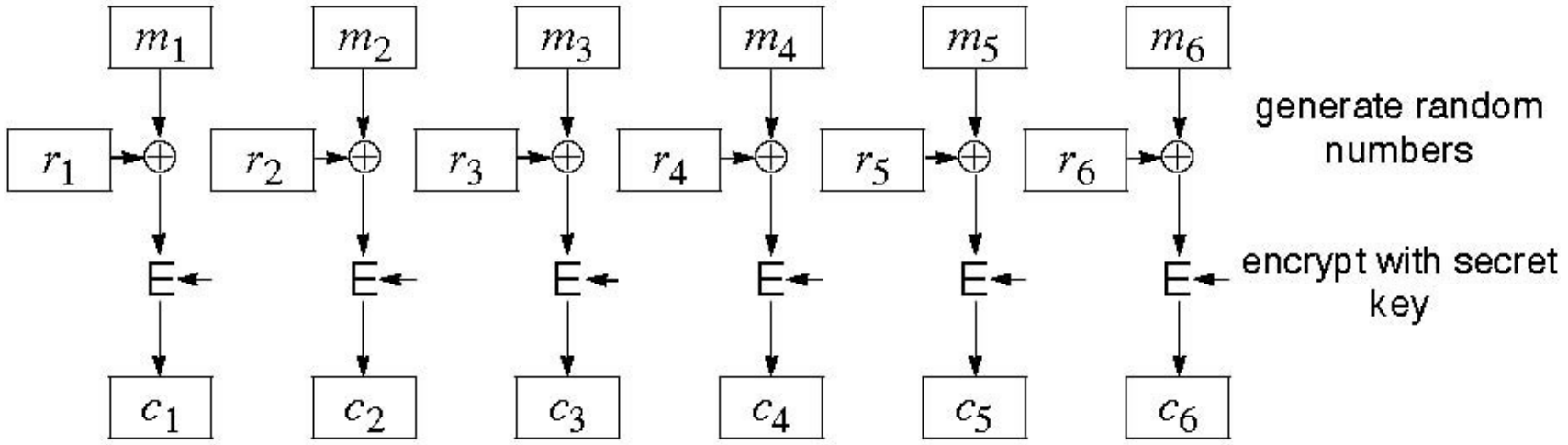
- What is the table?

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

©2025 Raj Jain

Cipher Block Chaining (CBC)

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



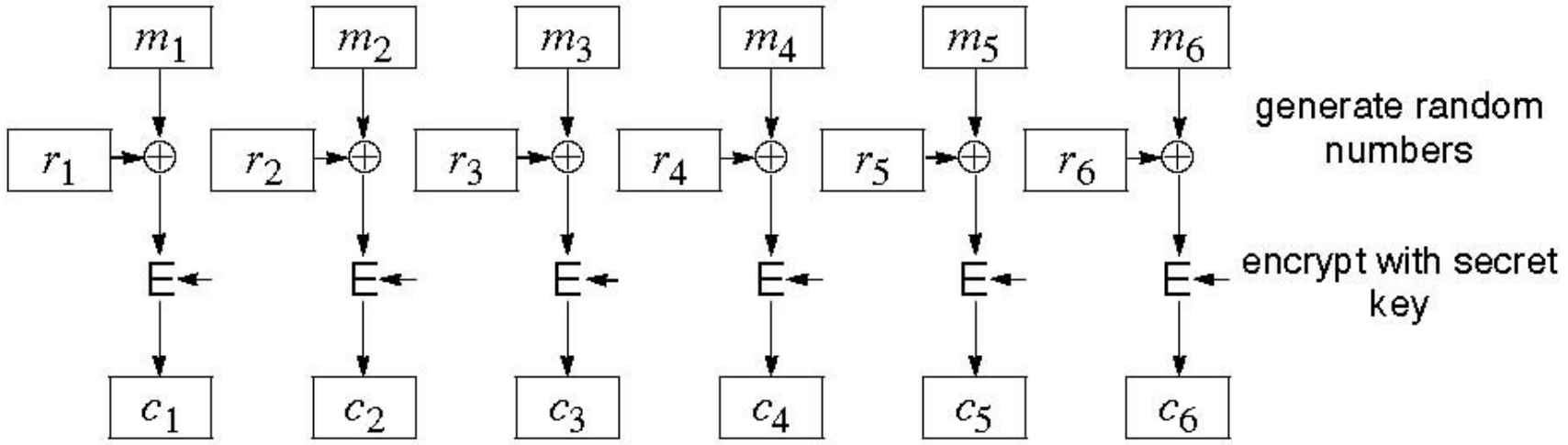
Student Questions

- 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.
  - Can I use CRC to create the indexes for a hash table?
    Yes. See the above question.
  - How does the receiver know which random number the sender uses?
    It is shown in the next slide

©2025 Raj Jain

Cipher Block Chaining (CBC)

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



Student Questions

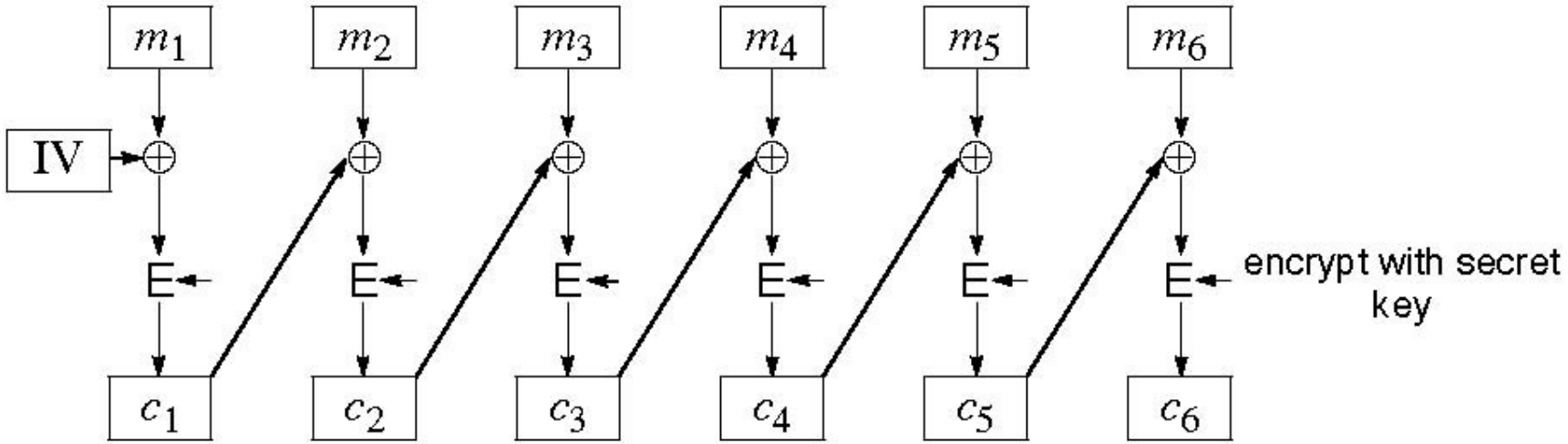
- For CBC, if the encryption changes every time based on a random number, how will the decoder update to decode the message? Does the decoder need to know the random number?

Yes, the decode can generate the same random numbers.

©2025 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

- 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 the 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 the 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.*
- How would you decide the value for IV?

Any random number is a good IV.

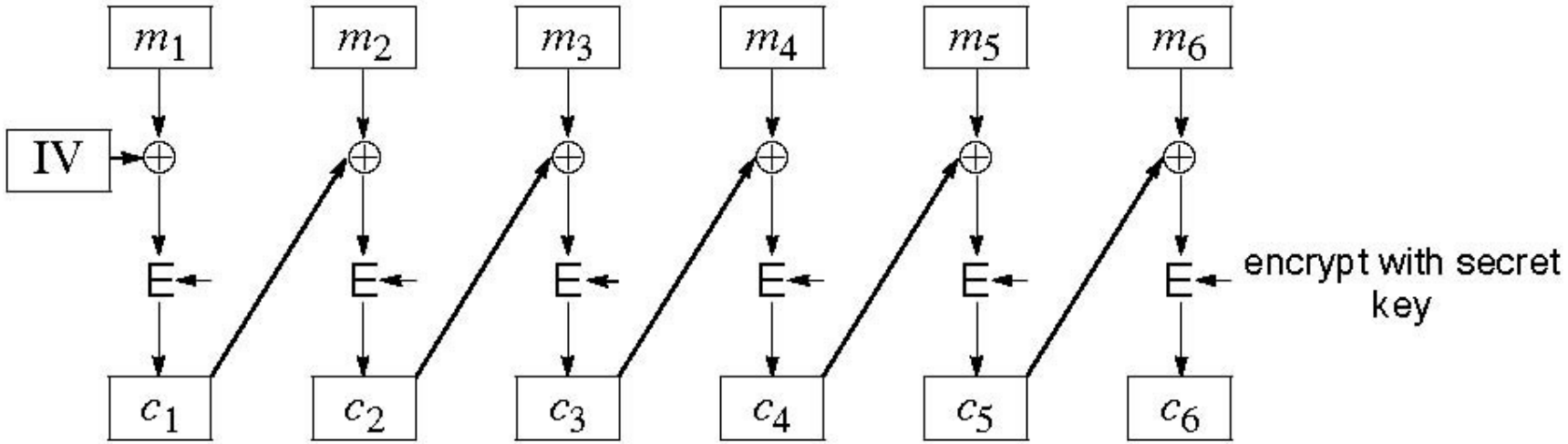
- What is the IV use different from the R1R2?

R1=IV, R2 is generated from the encryption.

©2025 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

- It seems that the security of the encryption depends on the initial value. If so, how can we trust the initial value?

All random values for IV are equally secure.

- What is Continue Holding and Start Bombing?

Example of messages

- Since we can use the encryption method in digital signatures and certificates, is there a specific reason to use the random number method described here?

Yes. This is used to strengthen the encryption.

- How is Cipher Block Chaining different then the methods that Blockchain uses?

No relationship. Blockchain is simply a linked list.

- So, c1 is subtracted from m2 before the application of the secret key during decryption?

Exclusive-or'ed. Yes.

- How is the IV chosen?

Randomly.

- Is the process of decoding CBC the same on the receiver side, provided they have the initial value?

©2025 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

- 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

- Why do we need triple DES?

More secure than DES

- Should the 3rd nested DES statement in the red say "key3" instead of "key1"? Why are only two keys needed vs. 3?

It is key1. Someone showed that it is equally strong.

©2025 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

- How effective is Triple DES in improving security?

56-bit vs 112 bits. Still used.

- How exactly is it determined whether or not something is secure?

It is insecure if a reasonable computer can decrypt it in a reasonable time.

- Can the security of DES be increased infinitely by chaining it more?

Probably. But better methods have been invented.

- When it says "for commercial and unclassified" use, does that mean that classified data uses a different encryption method? What do they use? *AES.*

©2025 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

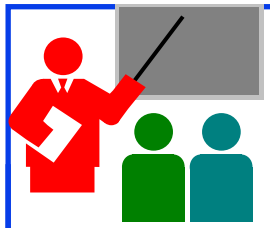
- What do you mean by 9-bits to store a byte?

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

- If you use a larger/different key length, would the block length also change? Or is it always 128 bits?

Block size is always 128 bits in AES.

©2025 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

- In today's world, which encryption technique do we use most extensively? Is it AES?

AES is most common for secret key encryption.

- If we use the secret key encryption technique rather than any more advanced one, will we be more vulnerable to attackers?

The main problem with the secret key is how to send the key. More advanced techniques help solve this problem.

©2025 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

©2025 Raj Jain



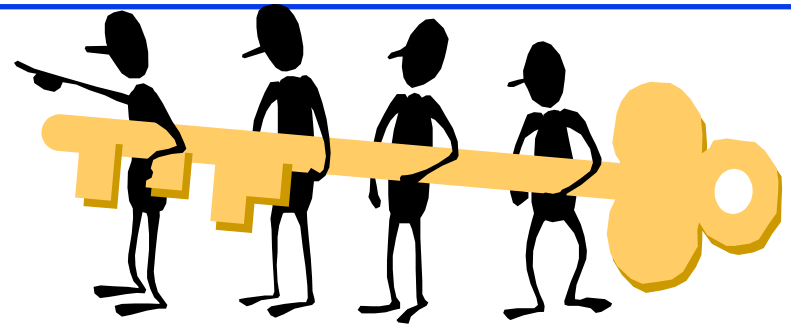
Public Key Encryption

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

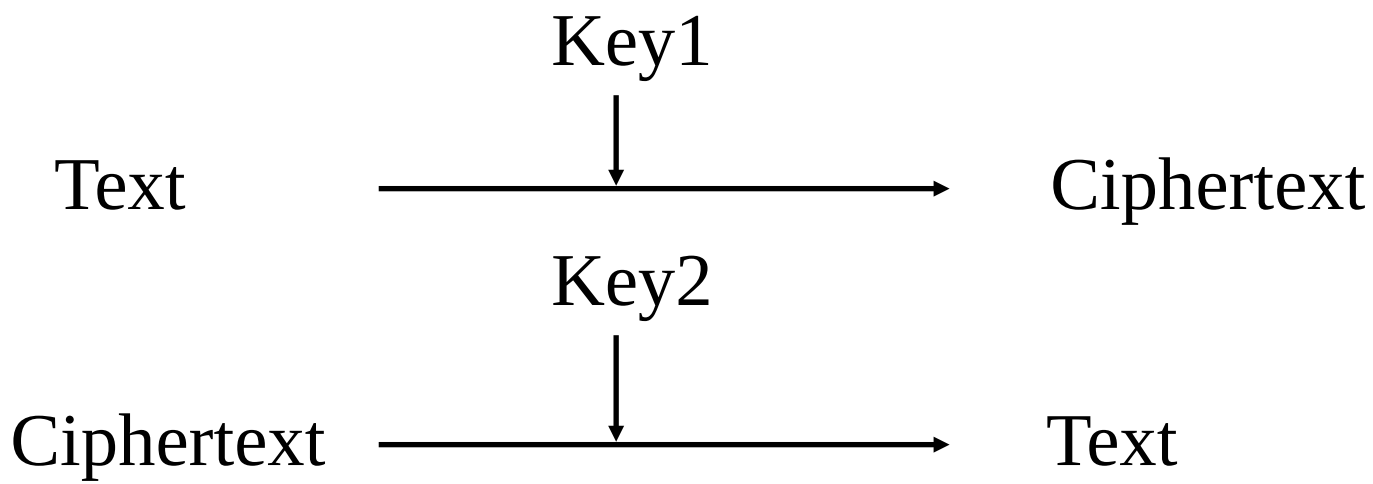
Student Questions

©2025 Raj Jain

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?

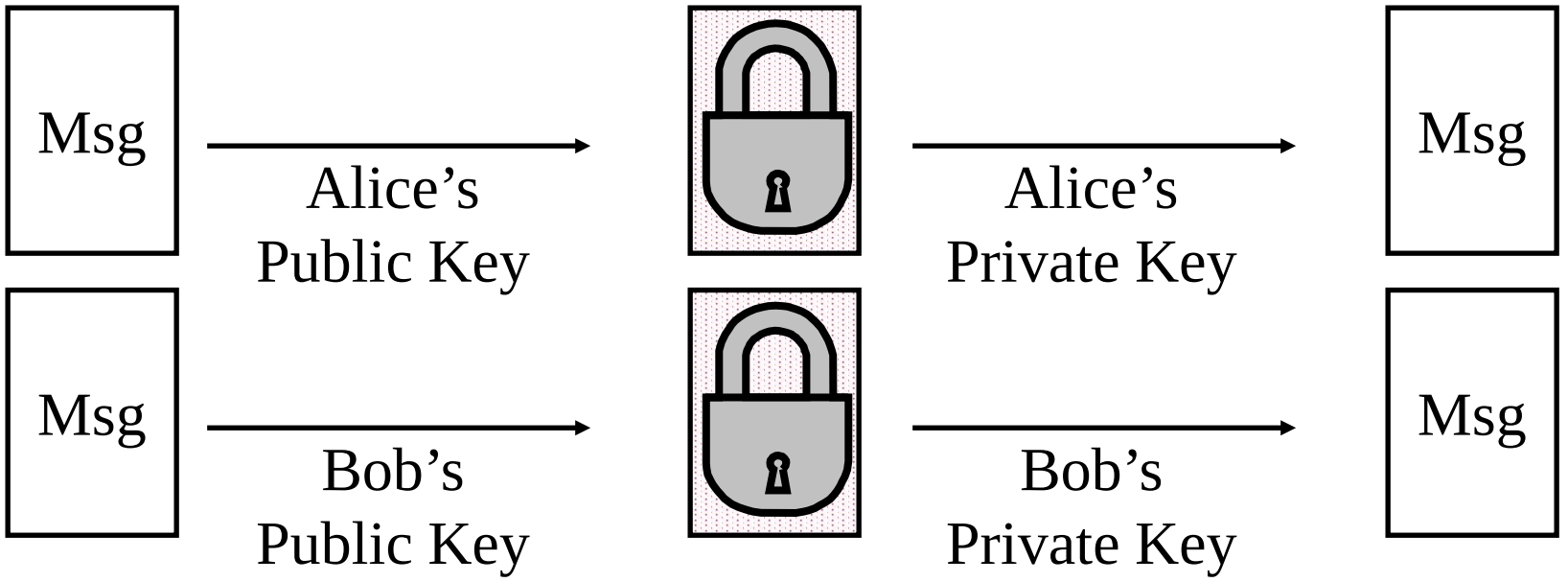
You cannot get any more information from ciphertext than from their lengths. Given two plaintexts of equal length and their two respective ciphertexts, cannot determine which ciphertext belongs to which plaintext.
Perfect Secrecy: No information at all.

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

©2025 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

- What are the disadvantages of public key encryption?

A 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 are private keys 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.

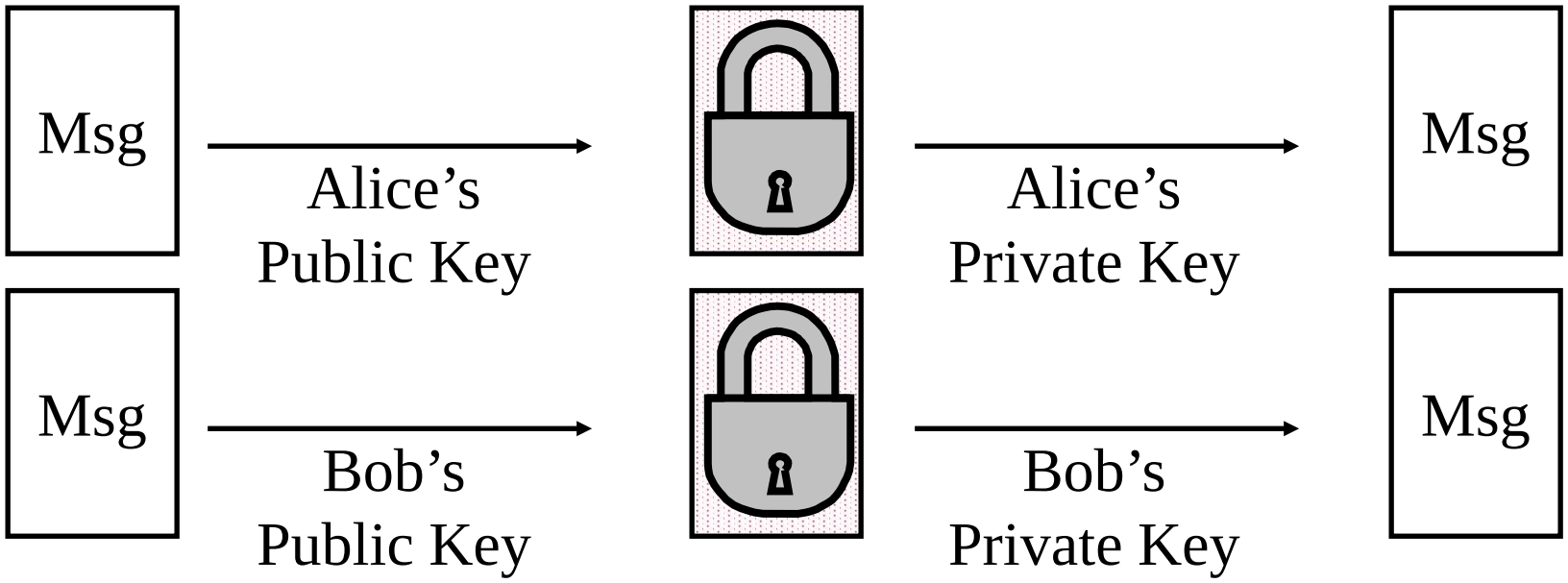
- Does the public key the same for Alice and Bob?

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

©2025 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 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.

- How can you guarantee the public key is not changed when transported over the network when accessing it from a website?

If my public key is changed, it does not hurt me.

- If "Encrypted with the private key can be decrypted by the public key," is it more vulnerable because everyone can have a public key?

No. Everyone can encrypt text so that only you can read it.

- What happens if you want to send a message to several people? Would you use multiple public keys?

Group keys.

- Is the only reason that somebody would encrypt information with their private key for verification of ownership? Are there any other uses cases for that technique?

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, and 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.

- How does the computer handle RSA mod so there's no overflow?

Precisely as indicated in this slide.

©2025 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

- Can you clarify the notation in the box? If x = y mod z, does that mean that z/y has a remainder of x?

Yes

- How does x = y mod z mean y = x mod z? If z is 23 and x is 4, then y is 3 because 23/4 has a remainder of 3. But 23/3 has a remainder of 2 which is not equal to x.

In "mod 4" arithmetic:
23 mod 4 = 3
3 mod 4 = 23

©2025 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

- 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.

- 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.

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

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

©2025 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

- How are p and q chosen?

Huge primes

©2025 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

- 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.

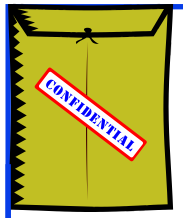
- What algorithm is used to calculate d in real-life implementations?

Chinese remainder theorem

- What algorithm is used to calculate d in real-life implementations?

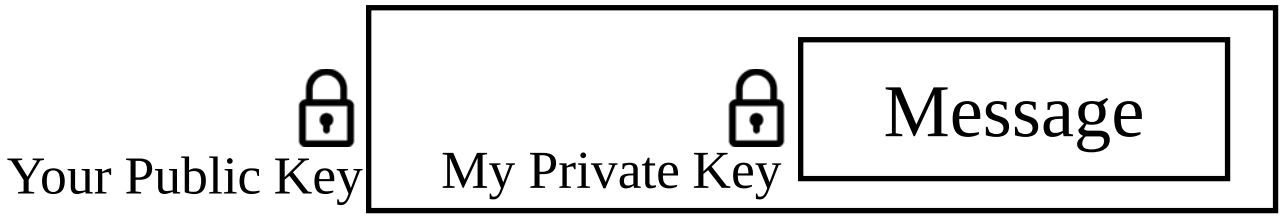
Chinese remainder theorem

©2025 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

- 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.

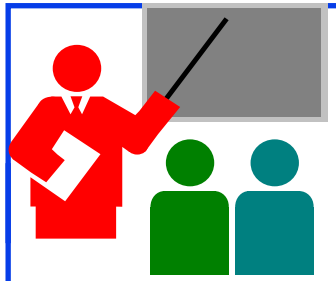
- Can you go over non-repudiation?

My private key is known only to me, so I must have sent this message. I cannot deny it.

- Whose signature is on the message? Yours or Mine?

Sender's signature

©2025 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

- 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?

- Are private keys and public keys permanent or new keys get generated for each session?

Session keys are different from public/private keys. Session keys are generated several times during a session.

©2025 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

©2025 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

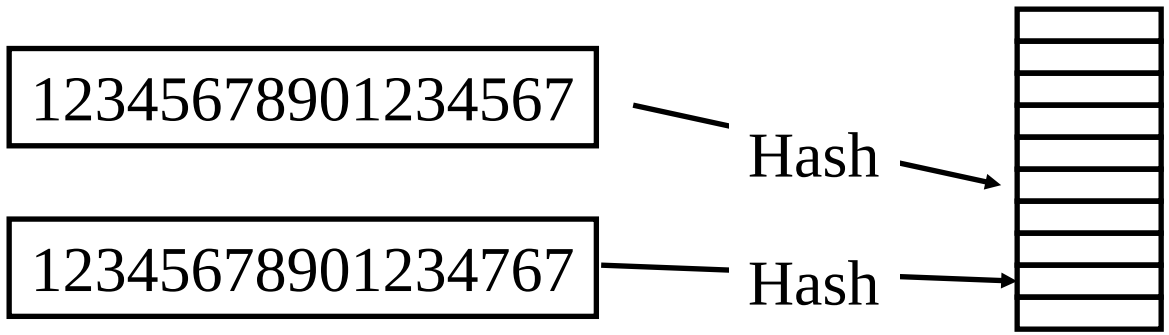
Student Questions

- Could you rank the safety between RSA, AES, and MD5?

RSA =Public/Private Key
AES is an encryption method
MD5 is a hash function
There is no overlap

©2025 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

- 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.

©2025 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

- 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.

- What does 32-bit operation mean? What kind of operation, to be specific?

All operations (Add, multiply, etc.) use 32 bits.

- Is MD5 still considered an excellent hash?

It is used extensively in file exchange.

- How do people tell when a hash algorithm is no longer secure? Is there a way to mathematically determine if an algorithm is insecure?

©2025 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

- 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 than 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.

- What does the passes mean? *Rounds*
- Does OS keep the private keys used for all secure communication via the network?

Yes.

- Why SHA-1 Algorithm is relatively not safe compared to other encryption methods like SHA-256?

SHA-256 is revised version of SHA-1

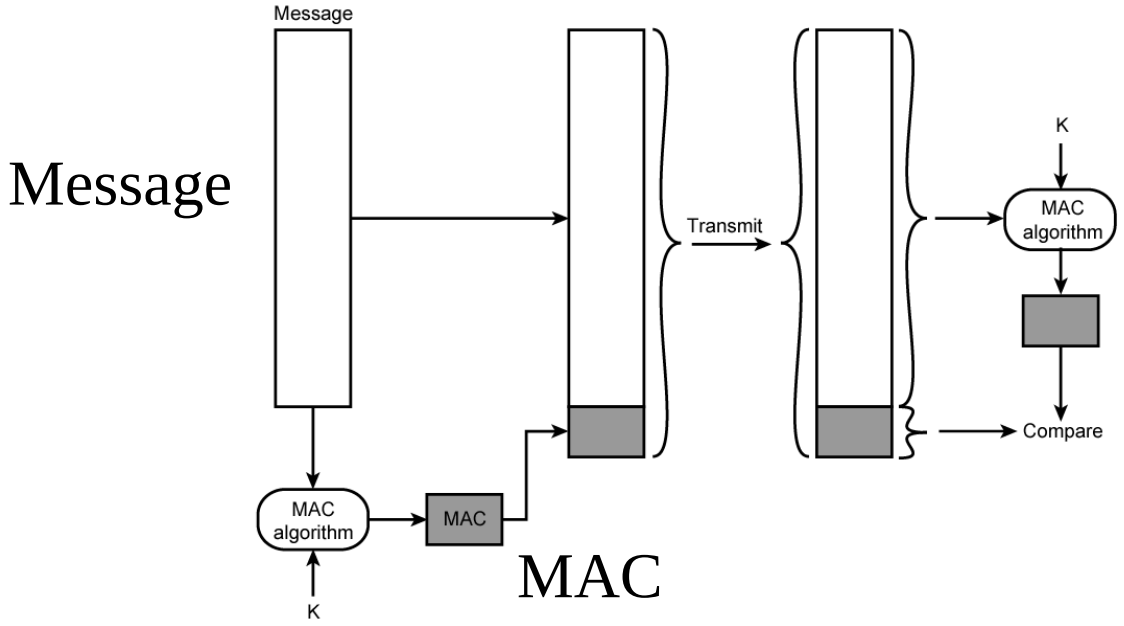
- How is SHA-256 improved from SHA-1?

SHA-256 is a 256-bit version of SHA-2. Details are taught in Security courses.

©2025 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
- $\text{Encrypt}_{\text{secret key}}\{\text{Message, CRC, Time Stamp}\}$
- $\text{Message} + \text{Encrypt}_{\text{secret key}}(\text{Hash})$
  Or, $\text{Message} + \text{Encrypt}_{\text{Source's private key}}(\text{Hash})$



Student Questions

- Does CRC here is used for checksum?

Here CRC is used as an example of hash.

- Page 684 P14 Why a MAC would be better than a digital signature given a MAC can be spoofed?

©2025 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

- Why is AES considered a hash function? Isn't it an encryption standard?

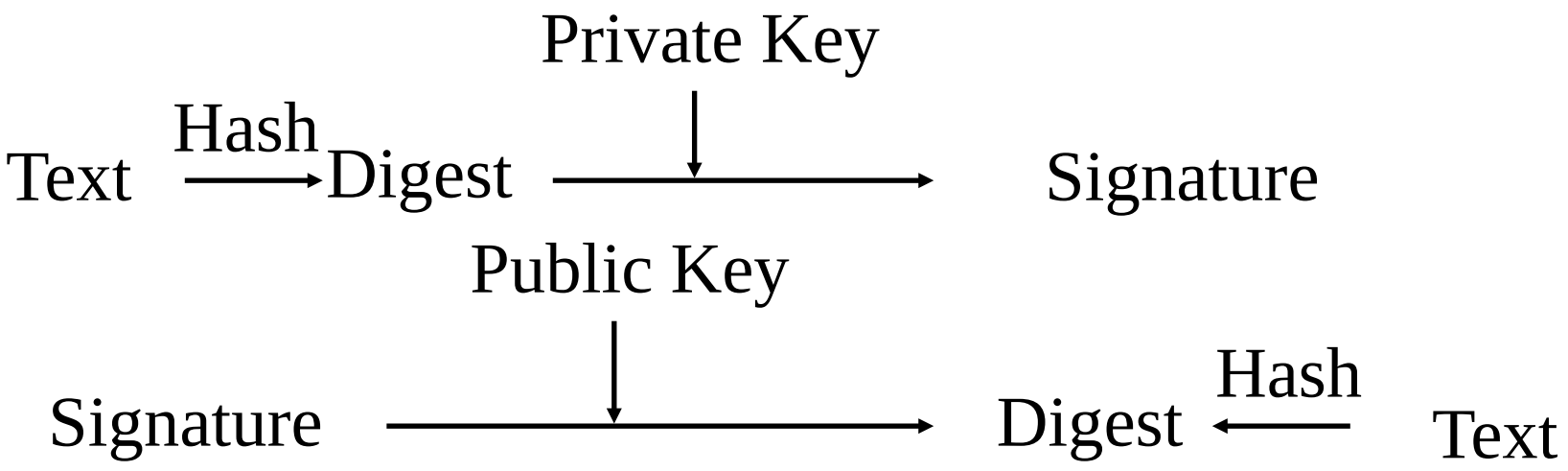
HMAC-AES is a hash function. AES is not.

©2025 Raj Jain



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.

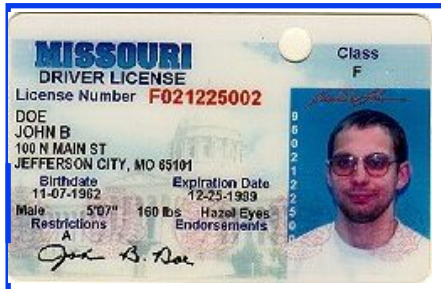
- So, will a person have a unique digital signature for each message they send/sign?

Yes. If the message is changed, the signature will be invalid.

- Are there hash function standards similar to encryption standards?

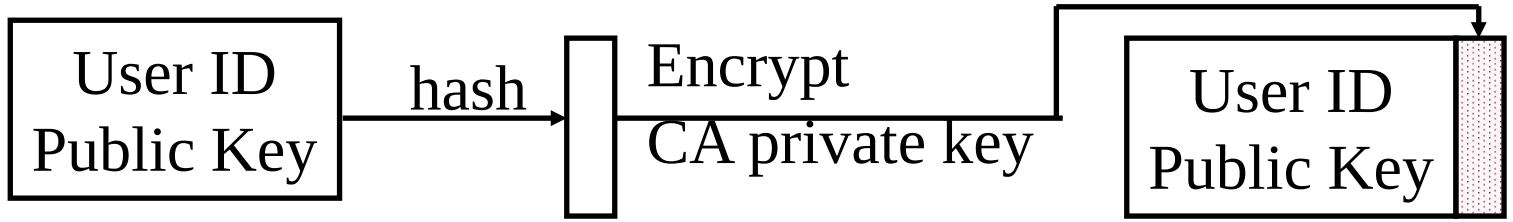
Yes. SHA-1, SHA-2, SHA-3, MD-4, MD5, etc are hash function standards.

©2025 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

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

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

- Who is at the top of the CA hierarchy?

Any well-known CA.

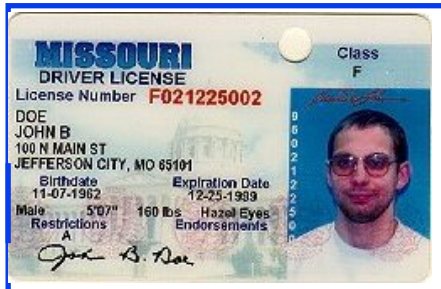
- If your CA turns out to be untrustworthy, does a digital signature renew itself somewhere else, or do you have to do it?

All signatures done using an invalid CA are invalid.

- Who is allowed to become a CA? If I want to authenticate my website, do I go to any available CA?

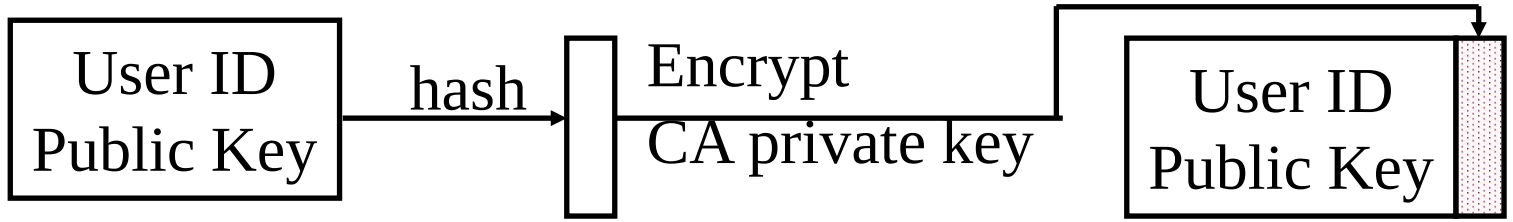
Yes. Going to the most popular (trusted) CA would be best. These CAs are included in operating systems such as Windows, MAC, Linux, etc.

©2025 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

- Can a CA ever become compromised?

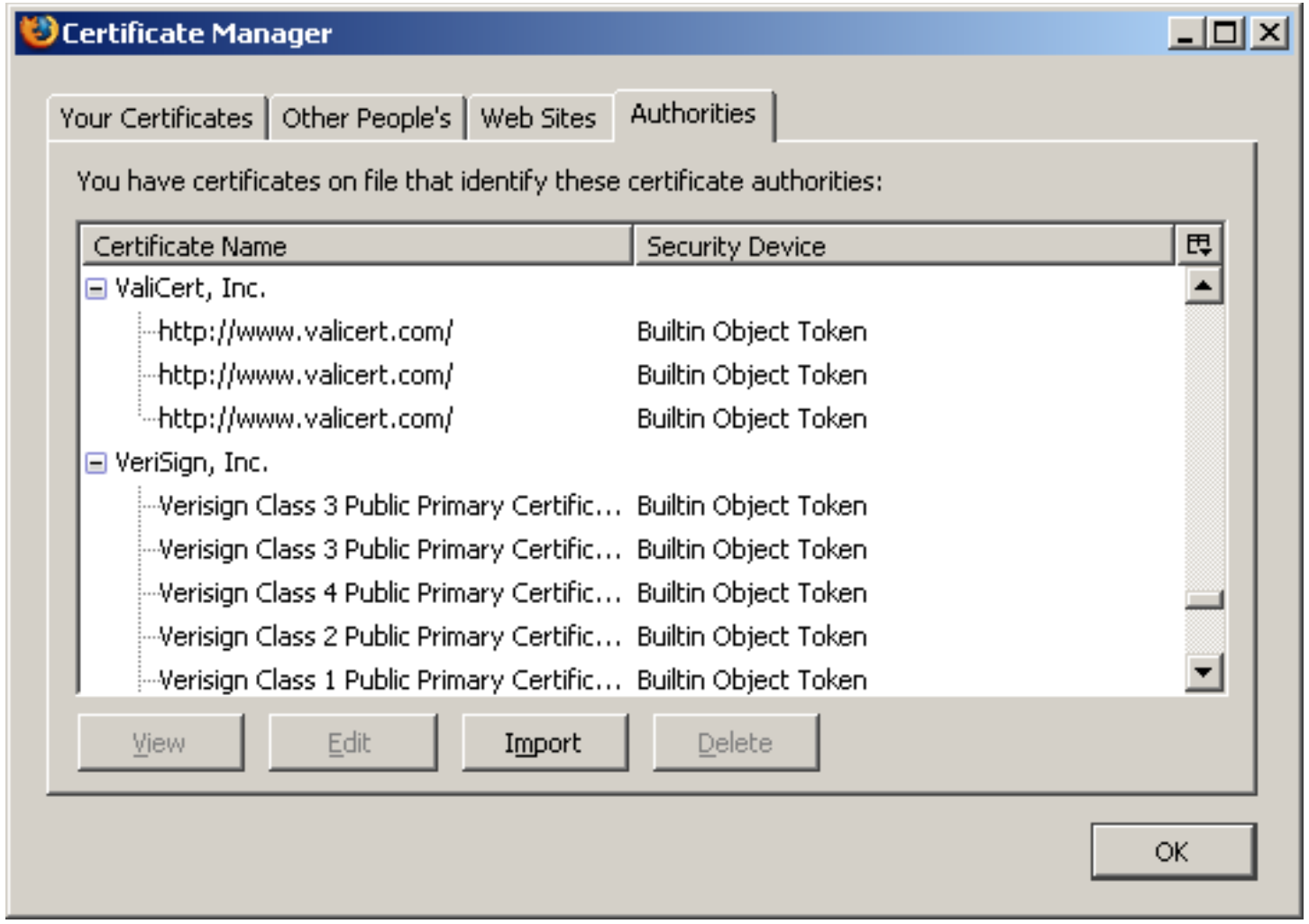
Yes. They often are. A list of such CA keys is also built into every operating system.

- How can I get a free certificate?

https://letsencrypt.org/
https://app.zerossl.com/signup/free
https://www.sslforfree.com/

©2025 Raj Jain

Oligarchy Example



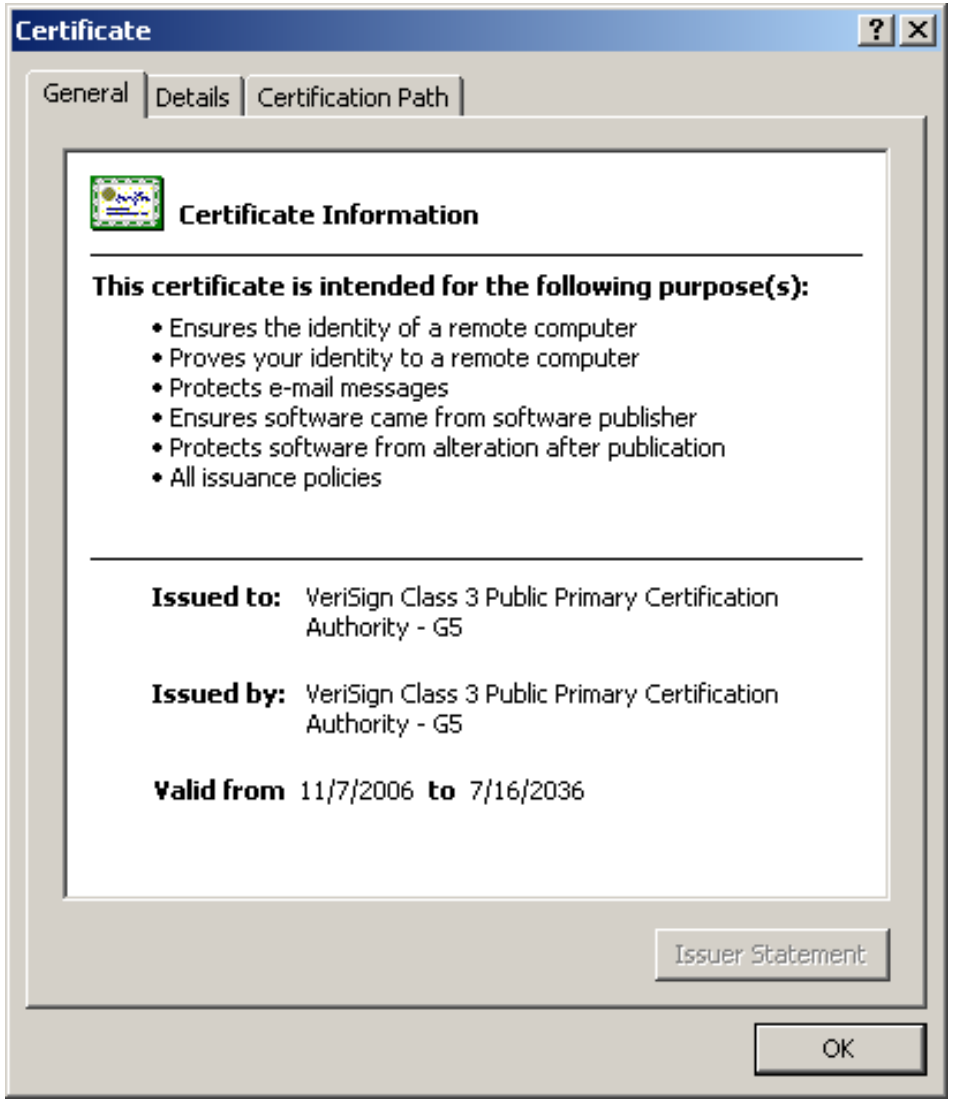
Ref: Windows: http://smallbusiness.chron.com/see-security-certificates-stored-computer-54732.html
MAC: https://superuser.com/questions/992167/where-are-digital-certificates-physically-stored-on-a-mac-os-x-machine

Student Questions

©2025 Raj Jain

Sample X.509 Certificate

- Certmgr.msc in Windows



Student Questions

©2025 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

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

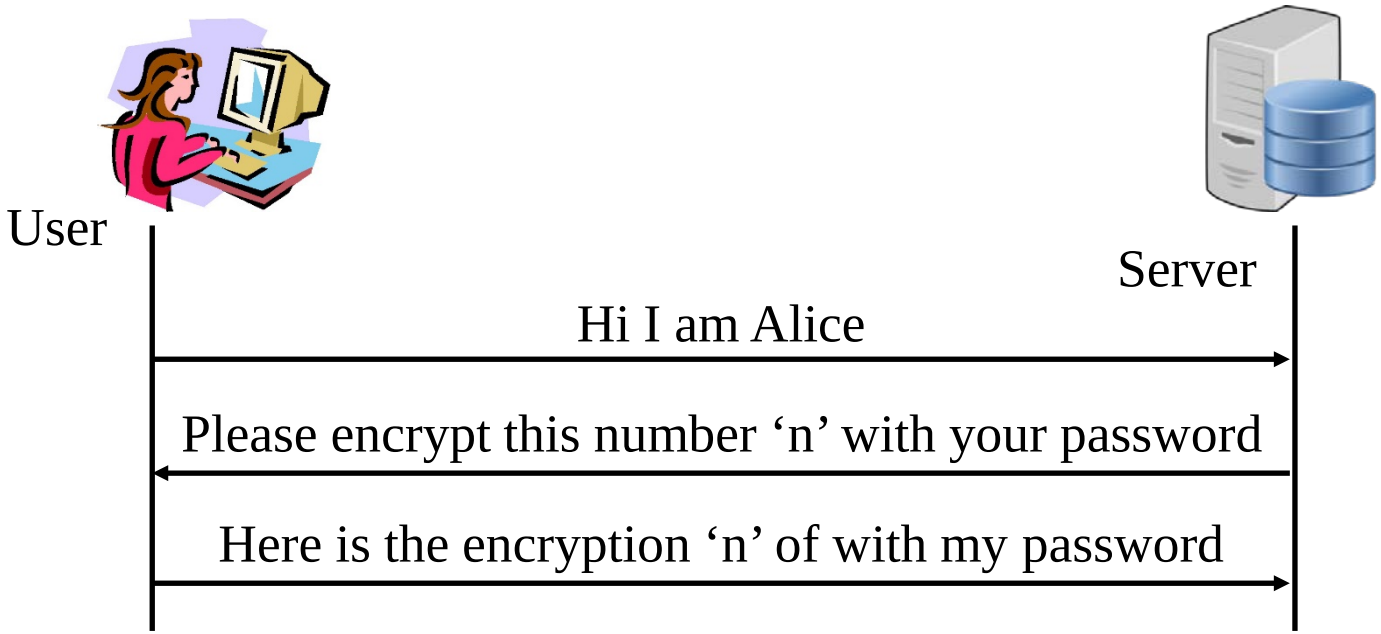
Yes. This is why it is important to synchronize your clock to the world clock.

- Does a server set the nonce on HTTP cookies for further requests? If so, how is this safe?
- Is the absence of a CA what operating systems like Windows use to warn users that a piece of software is unknown/unauthenticated by them?

Yes.

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, so it has no value. Yes, someone can pose as the server, so server authentication is required before itself.

- Is nonce the same as salt?

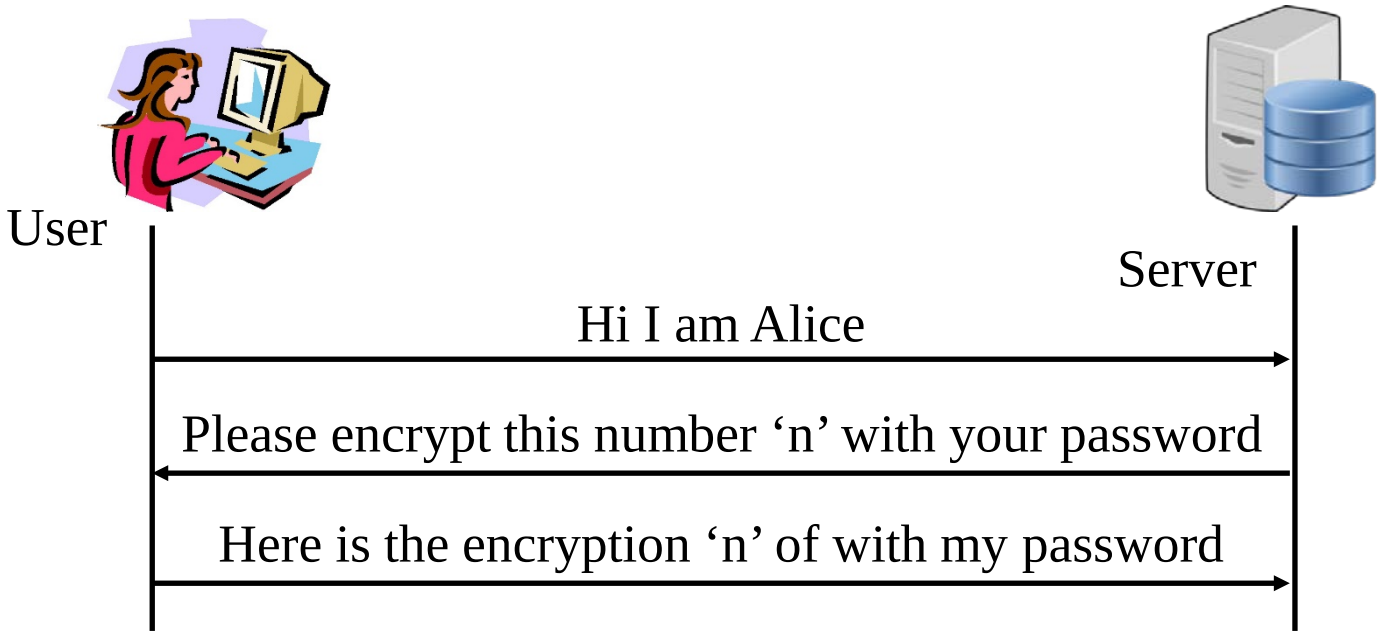
No. Salt is used in hashing inside the server. Nonce is sent on the network.

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

No. Never. There are several alternatives.

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 for security and passwords?

Nonce is 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 weak that a small number of ciphertexts can reveal the secret, it should not be used.

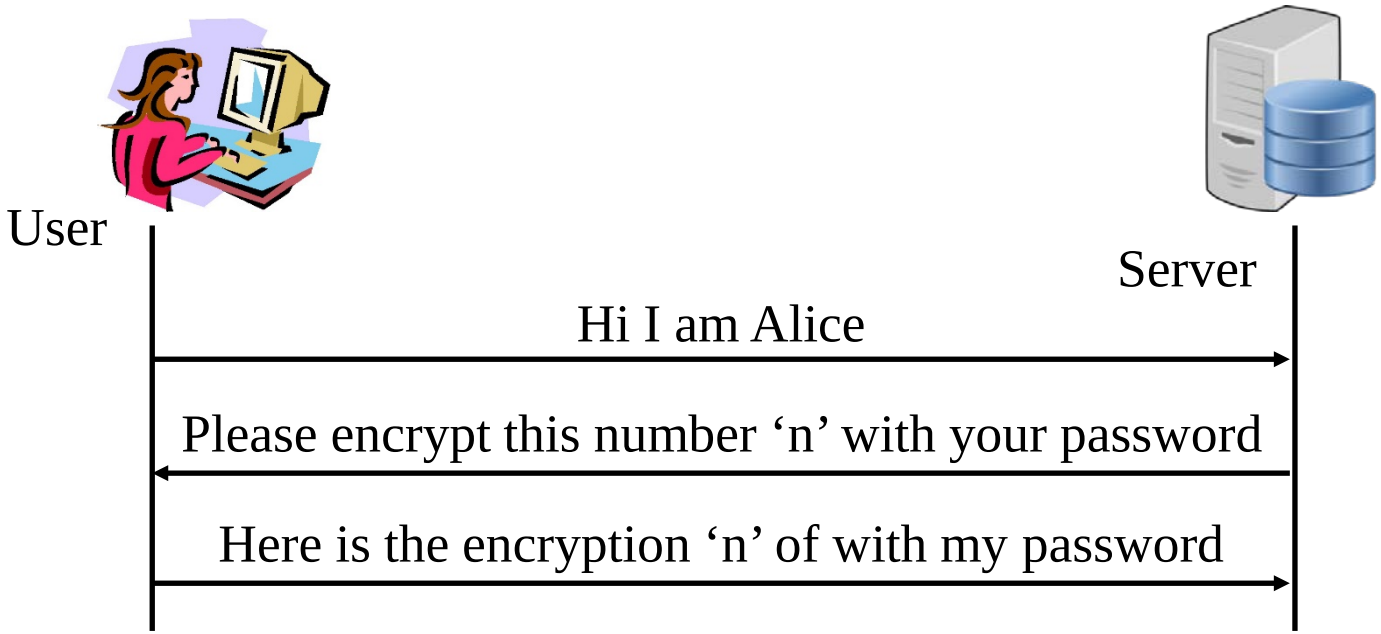
- So what exactly is saved in the server? If it's encryption, isn't each encryption different as a different nonce is used each time?

A hash of the password is saved on the server.

©2025 Raj Jain

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

- 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 cryptocurrencies, not security.

- How can the server validate the encryption of the nonce if it doesn't store the password itself?

As indicated, the server does store the password.

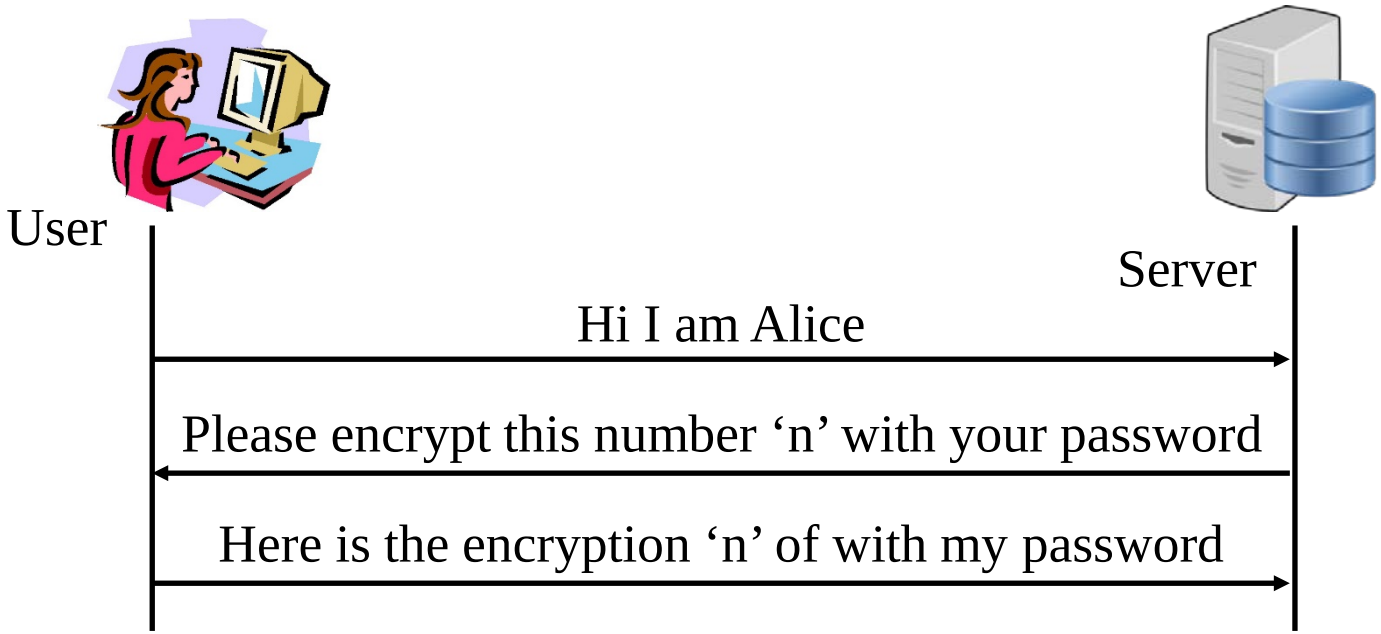
- So the encrypted 'n' should match the *expected* encrypted 'n' on the server's side to authenticate the user? *Yes.*
- Why would we use this protocol instead of using something like a digital signature instead?

Digital signatures came much later. Also, digital signatures require a public key which is computationally complex.

©2025 Raj Jain

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

- The textbook describes the different authentication protocols "ap" and the versions before ap4.0, which uses the nonce. Are there any newer versions of "ap" since 4.0?

AP is not an actual protocol. It is the author's way of explaining step by step.

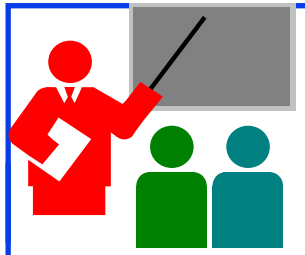
- How is the password initially sent to the server?

It is send using a secure channel such as https: (using public key).

- What is the purpose of nonces if we already store a hash of the password on the server (i.e., not in plaintext)? Is this just to add an extra layer of authentication security?

The server needs to verify that the user knows the password.

©2025 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

- ❑ Can cyber criminals fake Digital Certificates and pretend that their 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.

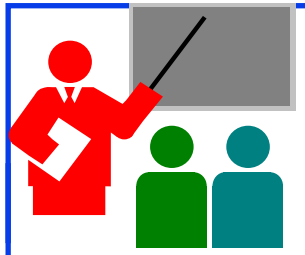
- ❑ What are "root authorities"?

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.

©2025 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

- ❑ 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.

- ❑ Will MD5 change when we change the original file?

Of course. Any change in the file by anyone will invalidate the MD5 hash.

- ❑ Would there ever be any value in encrypting a hash or hashing an encrypted message?

Yes. Encrypting a hash is done for signatures. Hashing an encrypted message is done for integrity.

- ❑ How do you prove that a hash function is impossible to decrypt?

Hash functions cannot be inverted easily. It can be done by challenge-response.

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

©2025 Raj Jain



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 shares 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.

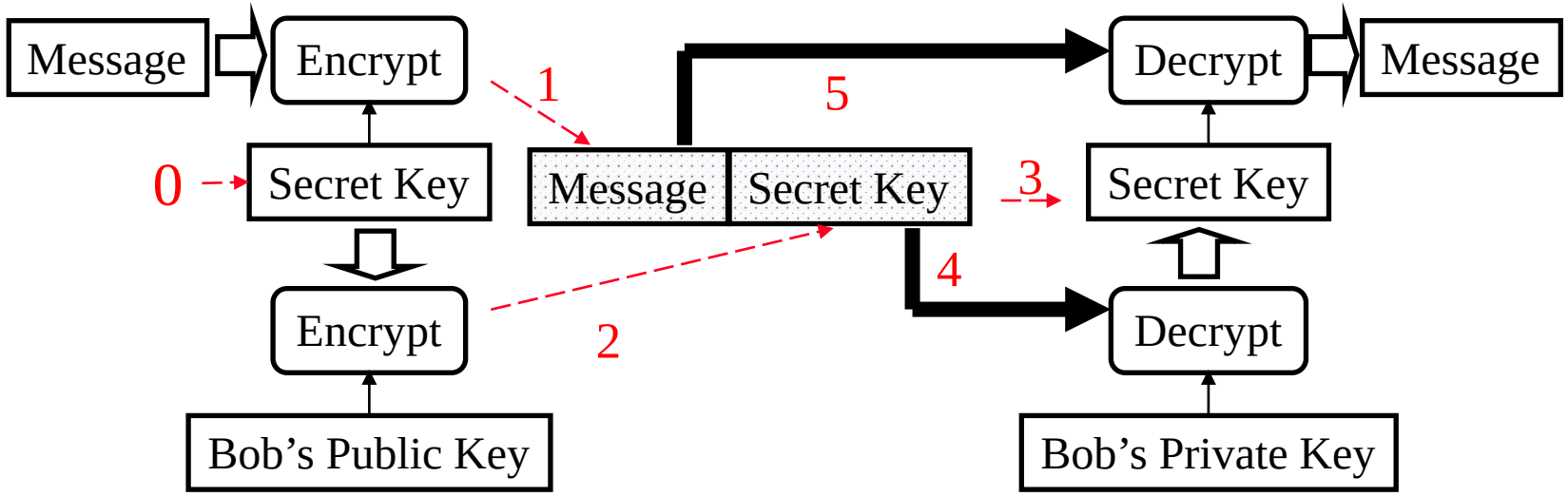
❑ The e-mail envelope consisting of the sender, receiver, and timestamps appears to be unencrypted. Why is this information not encrypted along with the message?

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

©2025 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

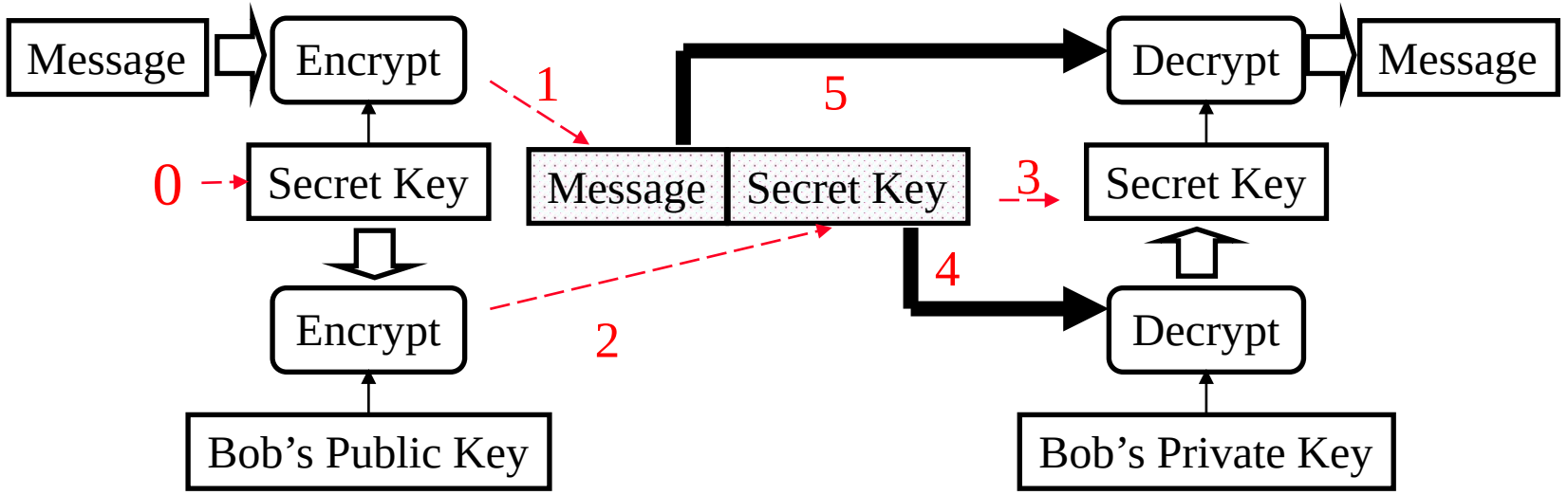
Student Questions

- 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.
- What if the encrypted secret key is compromised?
  If a key is compromised, all information encrypted with it is compromised.

©2025 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

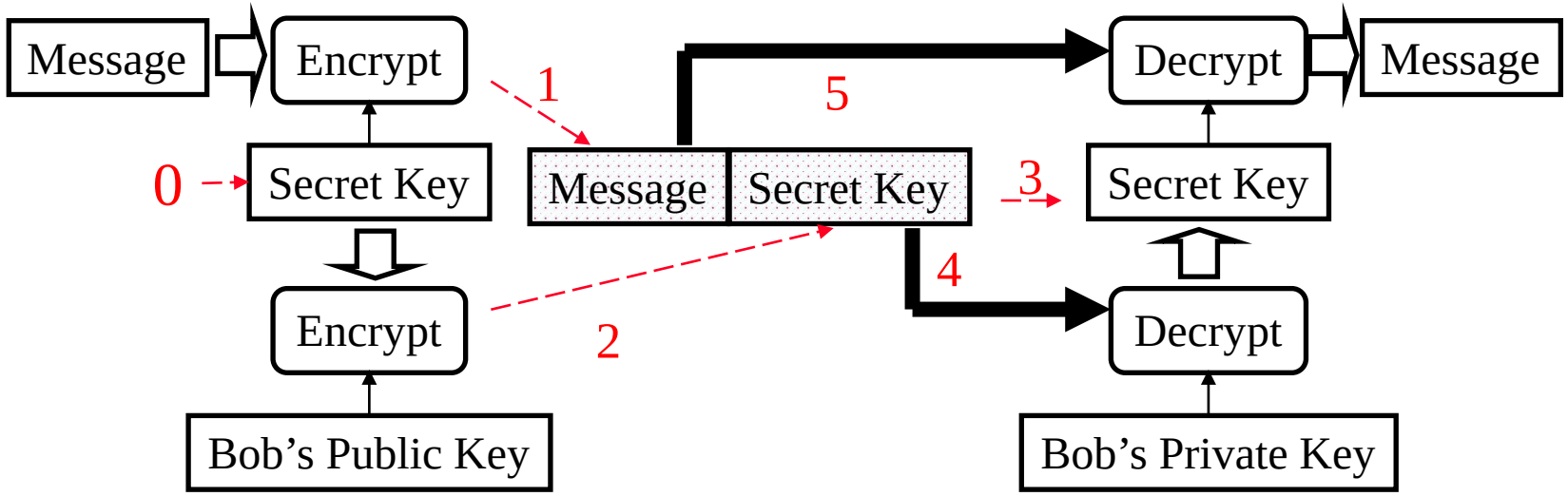
Student Questions

- 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 does it stay the same if the e-mail is sent to Bob?
  See above.
- How to securely distribute public keys?
  Public Keys are distributed in the 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.
- 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.

©2025 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

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

Yes, if you define efficiency as less computational cost.

- How is Bob able to recover the message from K_S?

Anyone can recover the message if they know the secret key.

- How hard is it to decrypt secure email? What are some techniques that attackers/hackers might use to decrypt secure emails?

As hard as AES.

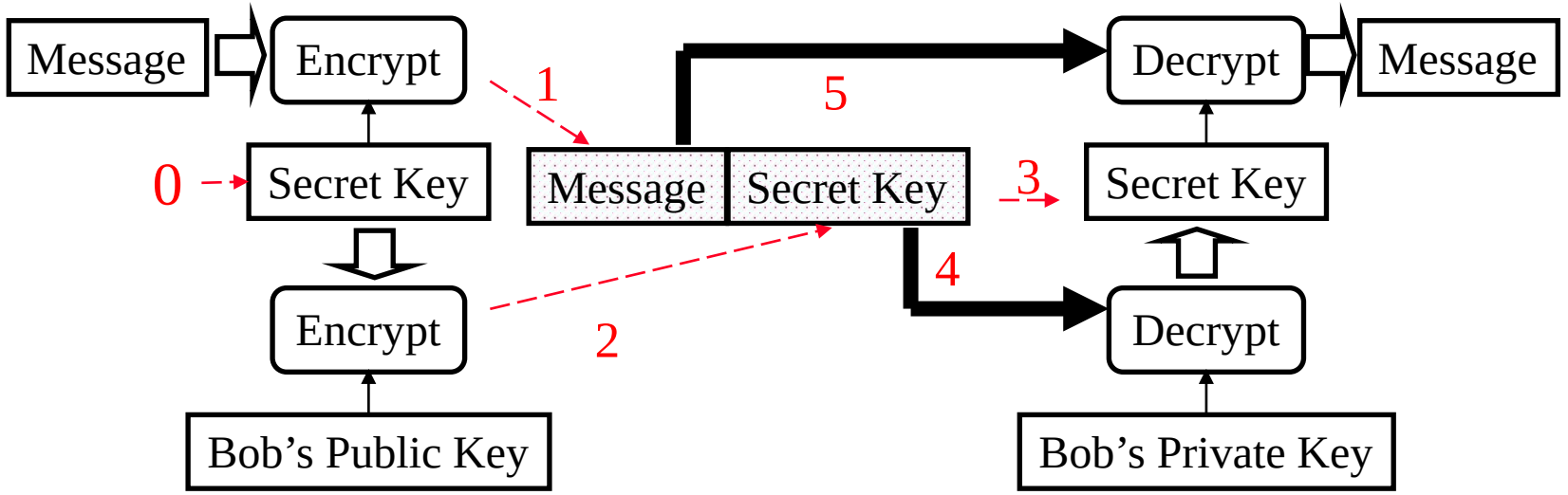
- What is the purpose of sending a random secret key with the message? Why not just encrypt the message with Bob's public key?

Public key encryption is computationally complex. It is done as little as required.

©2025 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

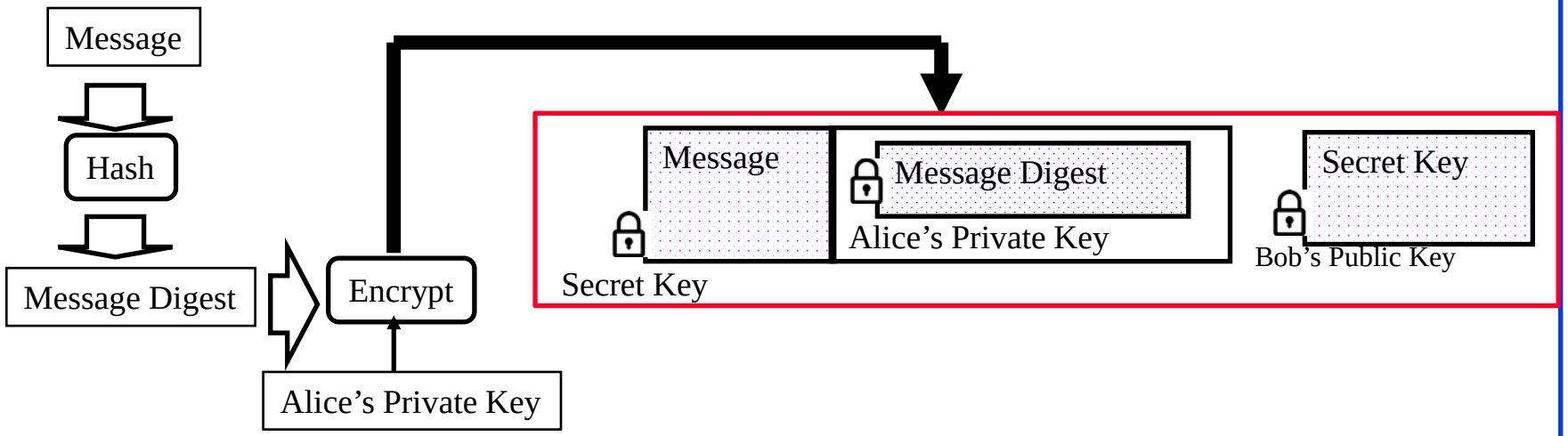
Student Questions

- If something is encrypted with a user's public key, will the user's private key be the only one able to decrypt it? I thought everyone had access to the public key.
  Yes. Only the private key can decrypt it.
- If the public key encrypts the message, is it always decrypted by the private key? How could it be?
  This was an innovation worth several billion dollars to Ron Rivest of RSA.

©2025 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

- 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.

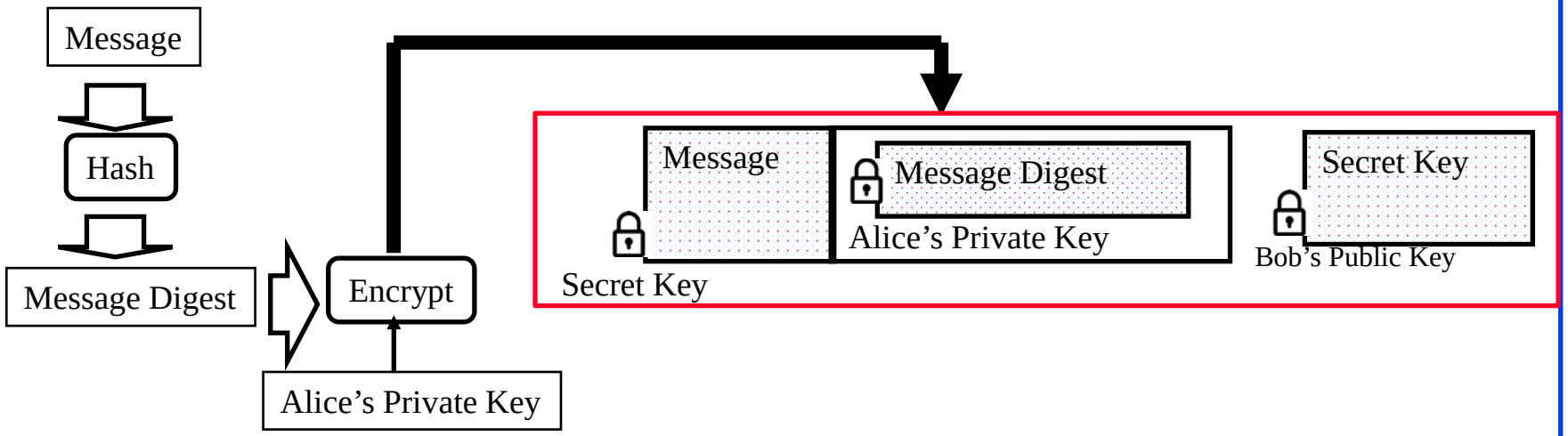
- Why is message digest used as a signature instead of PID or host IP?

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

©2025 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

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

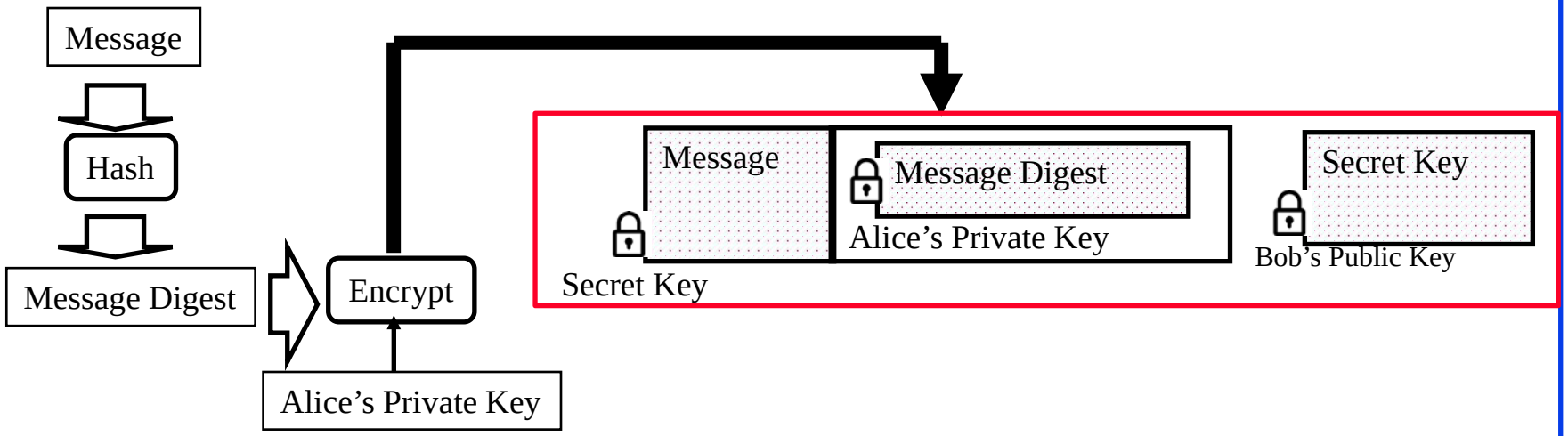
- How can we overcome the challenge of encrypting the entire message instead of just a segment?

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

©2025 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

- Where is the Message Digest put?

See Figure. The red outline indicates the complete message.

- Why must we hash the message into a digest and then encrypt it with the private key? Can we encrypt the plaintext with the private key?

Public Key computation is expensive.

- Why does Alice need to both hash and encrypt the message?

Hash is used during the signature process.

- How does Bob verify the message digest?

By hashing the message and comparing it with the digest.

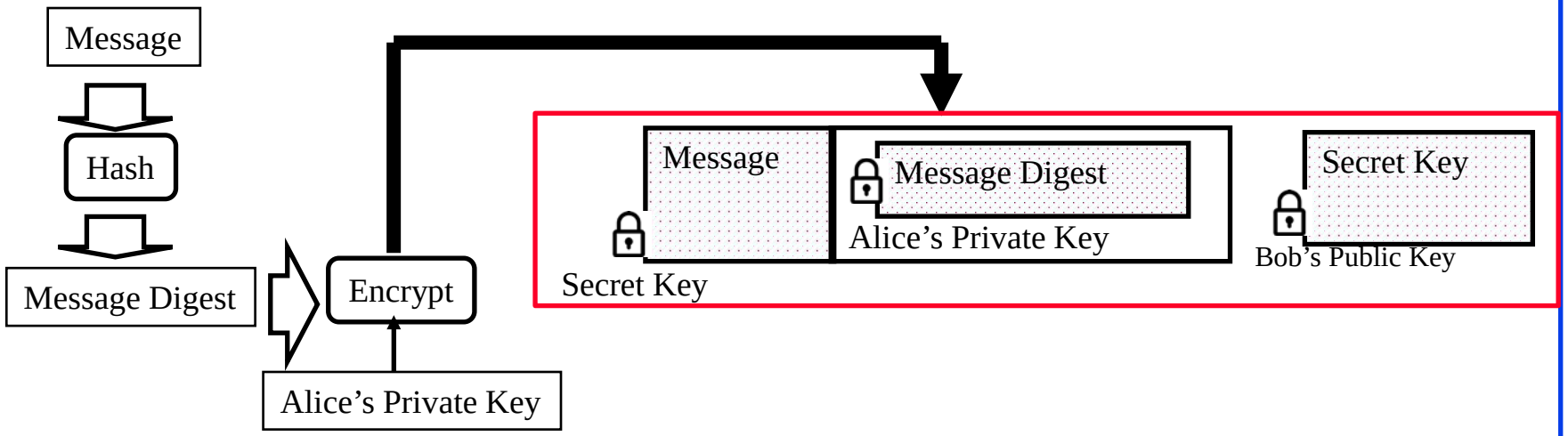
- When using Outlook, are messages not encrypted by default with TLS or some other mechanism?

TLS is used to secure it on the network between the hosts. It can still be sniffed on the host.

©2025 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

- So, does the new secret key get longer every time?

The words under the lock show the key used to lock that part of the message.

- Is this the same process as secure or encrypted messaging?

This could be used. But every system has its way of securing messages.

©2025 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

©2025 Raj Jain

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?

The 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.

- 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.

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

©2025 Raj Jain

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 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, Black lists, and other social media instruments point out bad sites.

- What does OCRable mean?

OCR=Optical Character Recognition

- In a web of trust system, do users/agents with different levels of trust have different privileges or abilities?

No difference in abilities. But you may trust someone with 0.999 more than someone with a trust level of 0.5.

It is like Social Security Card vs. Driver's License vs. a Passport for identification.

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

©2025 Raj Jain

Student Questions

- What sort of vetting process do large organizations have for issuing Certificates? Is it likely that Microsoft will accidentally issue a certificate to a malicious actor?

All sorts of physical vetting is done. For example, government website require id.me verification which requires you to send a picture of yourself and your driver license. Some websites require answering facts related to the id from public records.

- How is the web of trust started since no one is trusted at the start?

The person proposing it started it.

- How does the web of trust- certificates work? How is it different from CA?

I have not seen it used much.

- Is this used in any practical sense or only for academic demonstrations and hobbyists?

PGP is used quite a bit in practice.



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

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

Add the acknowledgment receipt option.

©2025 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

©2025 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

©2025 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

©2025 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

©2025 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

©2025 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

©2025 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

©2025 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.

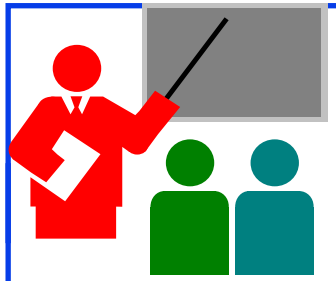
Ref: https://www.top-password.com/blog/view-installed-certificates-in-windows-10-8-7/
https://www.digicert.com/kb/code-signing/mac-verifying-code-signing-certificate.htm

Student Questions

- 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.

©2025 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

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

All messages exchanged during an HTTPS session are secure.

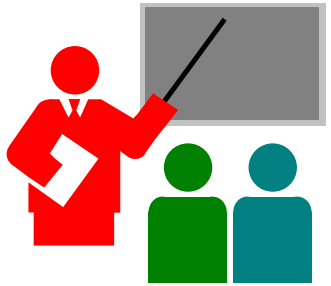
- Why could anyone not get access to the secret keys

Secret keys are generated and destroyed after each use. They are not stored or reused.

Ref: Section 8.5, Review question R19

©2025 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

Student Questions

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

No = 0 points

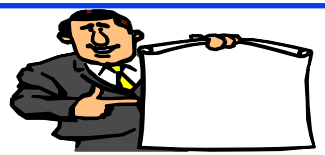
Yes = 4 points

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

- Is there a graph for regraded exam 2 rankings? *Not too many changes.*
- How do we secure the digital certificate system itself from attacks?

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

©2025 Raj Jain



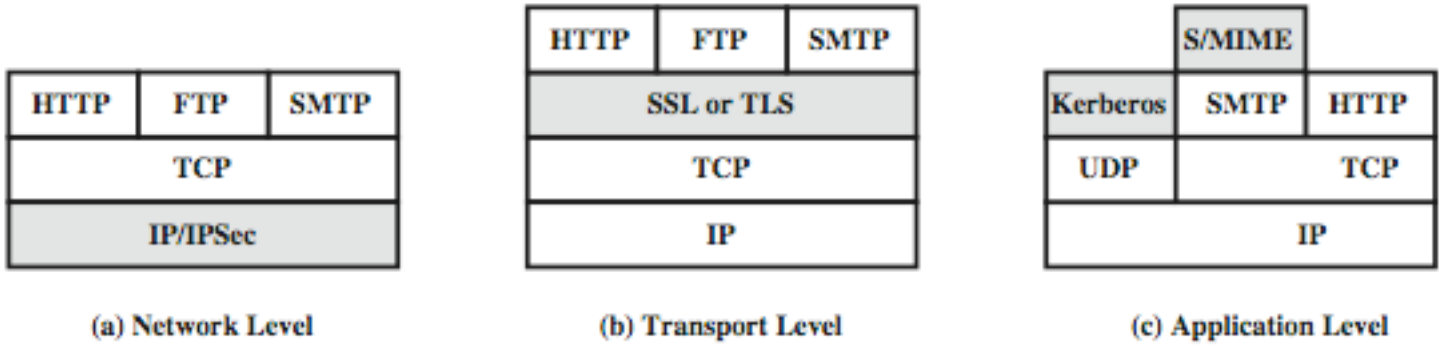
Transport Layer Security (TLS)

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

Student Questions

©2025 Raj Jain

Web Traffic Security Approaches



(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

- Does SSL here stand for Secure Shell?

SSL=Secure Socket Layer

TLS = Transport Layer Security

- What goes into the negotiation? Is it just the highest security algorithm that the client and server support?

Encryption and Hash methods.

©2025 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

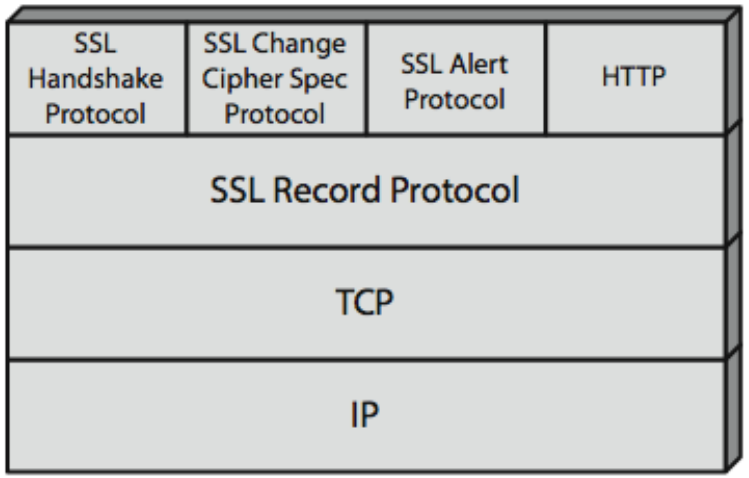
Student Questions

©2025 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

- 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.

- Why is the record protocol on another layer? What does this imply about its relationship with the other three protocols?

All protocols on the top layer need and use record protocol.

- Why is the record protocol on a different layer?

Because other components use it.

©2025 Raj Jain

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 the same for the client and the server?

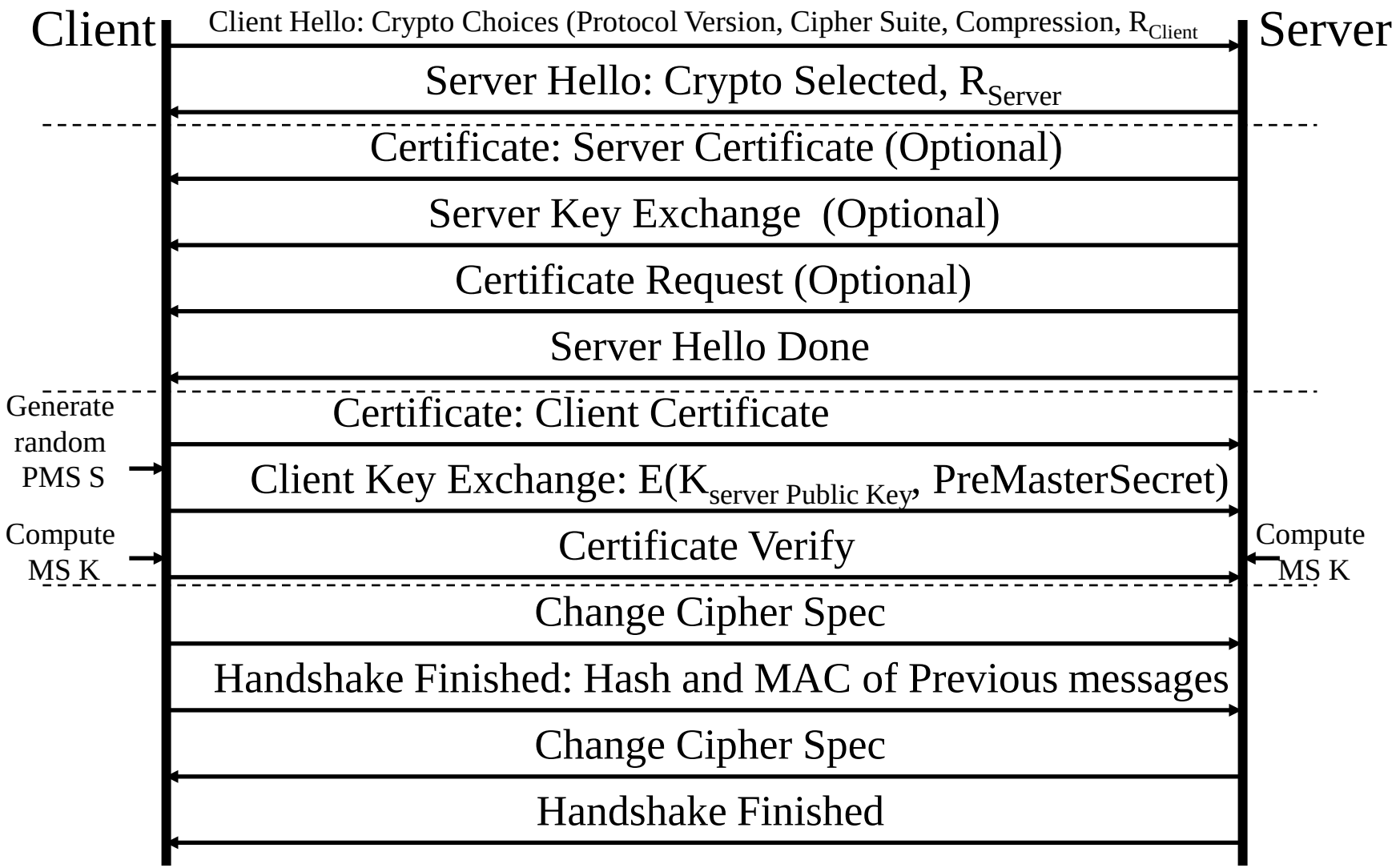
Some are the same, and some are different. See Slide 8-59.

- Is anything currently built into TLS to compute/use post-quantum encryption methods? Or will TLS be broken with the advent of a sufficiently large quantum computer?

Quantum computers are quite a bit away. See http://www.cse.wustl.edu/~jain/talks/qb_tt.htm

©2025 Raj Jain

SSL/TLS Handshake Protocol Actions



Student Questions

- In phase 2, the top three are optional. What are the benefits if we use them?

The server is not authenticated, which was common initially.

Do you authenticate the police when they arrest you?

- What is stopping someone in the middle which changes messages in the handshake from also changing the hash message to match the messages they changed to?

This is called a "man-in-the-middle (MIM)" attack. Handshake finished message was added to avoid MIM caused by changing to a weak cipher suite

- How is the certificate verified in the last step of phase 3? By checking, is the MS computed the same?

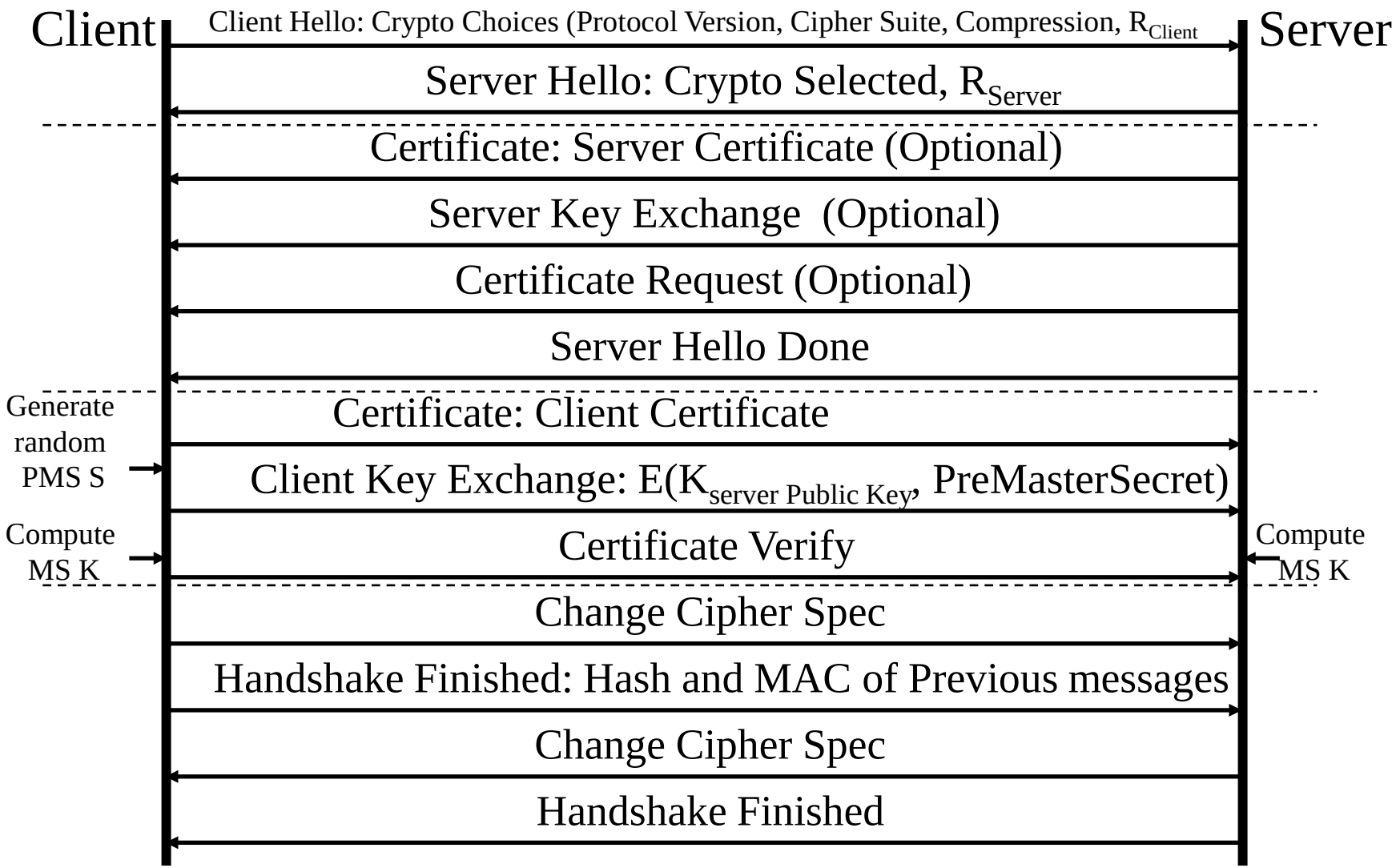
Its meaning is "Certificates Verified." It is like an ack to say I am done with this phase.

- How does SSL/TLS handshake different from other handshakes?

See the figure in this slide.

©2025 Raj Jain

SSL/TLS Handshake Protocol Actions



Student Questions

- Is this a standard form of "x-way handshake," as we have seen before? If so, what would x be here?

It is NOT called a 13-way handshake. It is two-way authentication.

- What are some common challenges and limitations of implementing client certificate authentication in SSL/TLS connections?

Certificates require public key computation, which is complex.

- How can a Server Certificate be optional?

Initially, they used only client authentication, e.g., free public Wi-Fi at airports. But now, we also use server authentication.

- Is the "certificate verify" step used to ensure the sender and receiver have calculated the same master secret?

Yes.

©2025 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

- Does SSL/TLS handshake happen after a TCP handshake?

Yes. SSL requires a TCP connection.

- So, after the server receives the encrypted version of PMS, it decrypts the PMS with server's private key. Then both server and client compute the MS and check if they have computed the same MS?

They both compute the MS. There is no need to check that they have the same MS. If they have different MS, decryption will result in garbage and they will have resync.

©2025 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

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

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

©2025 Raj Jain

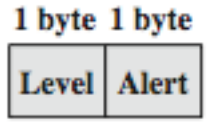
SSL/TLS Alert Protocol

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

©2025 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

- 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 a "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?

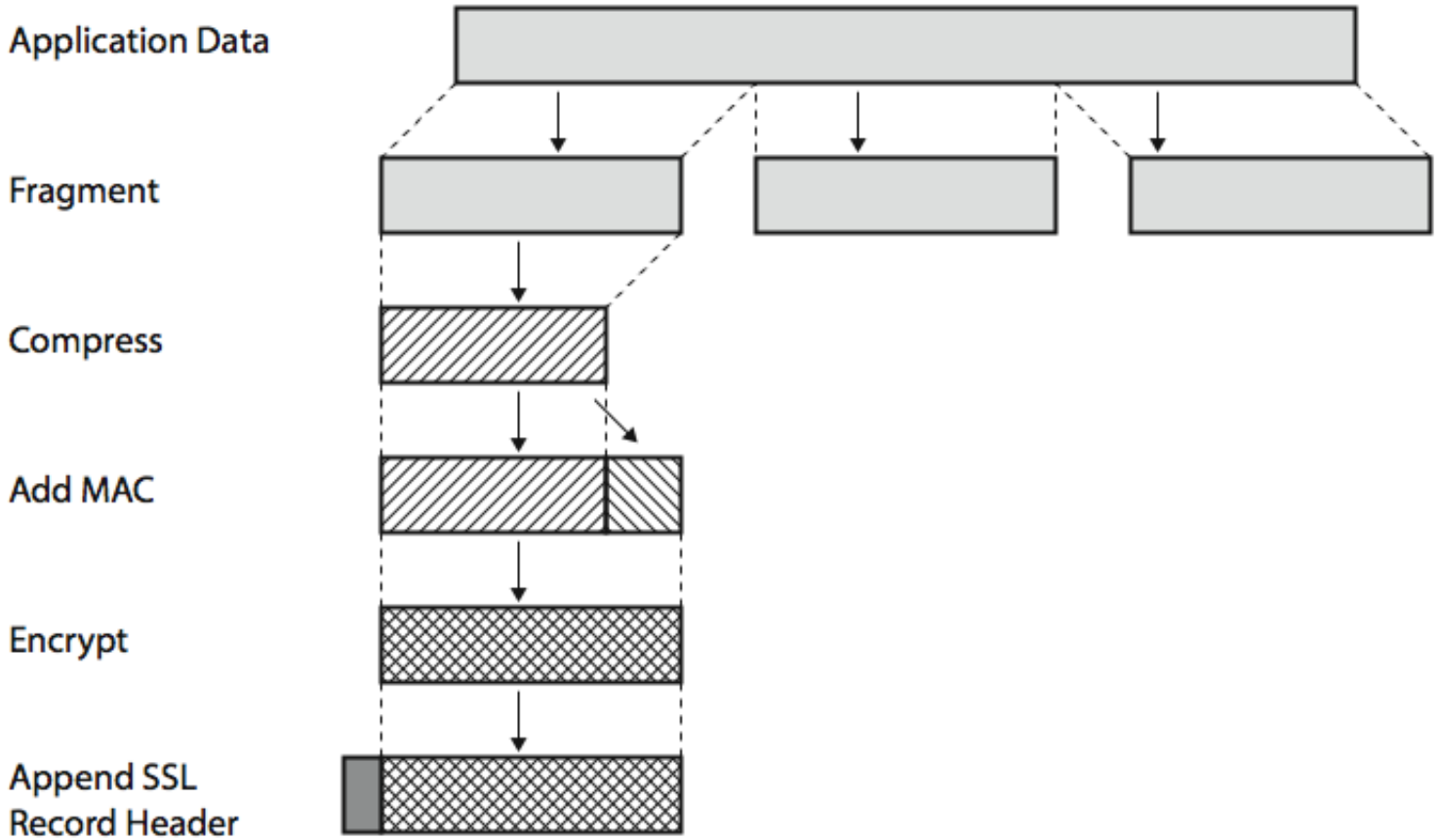
MD5(Data||HMAC Key||Seq #)

MB is Bob's HMAC key.

MD5 is just an example of a hash used here.

©2025 Raj Jain

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.

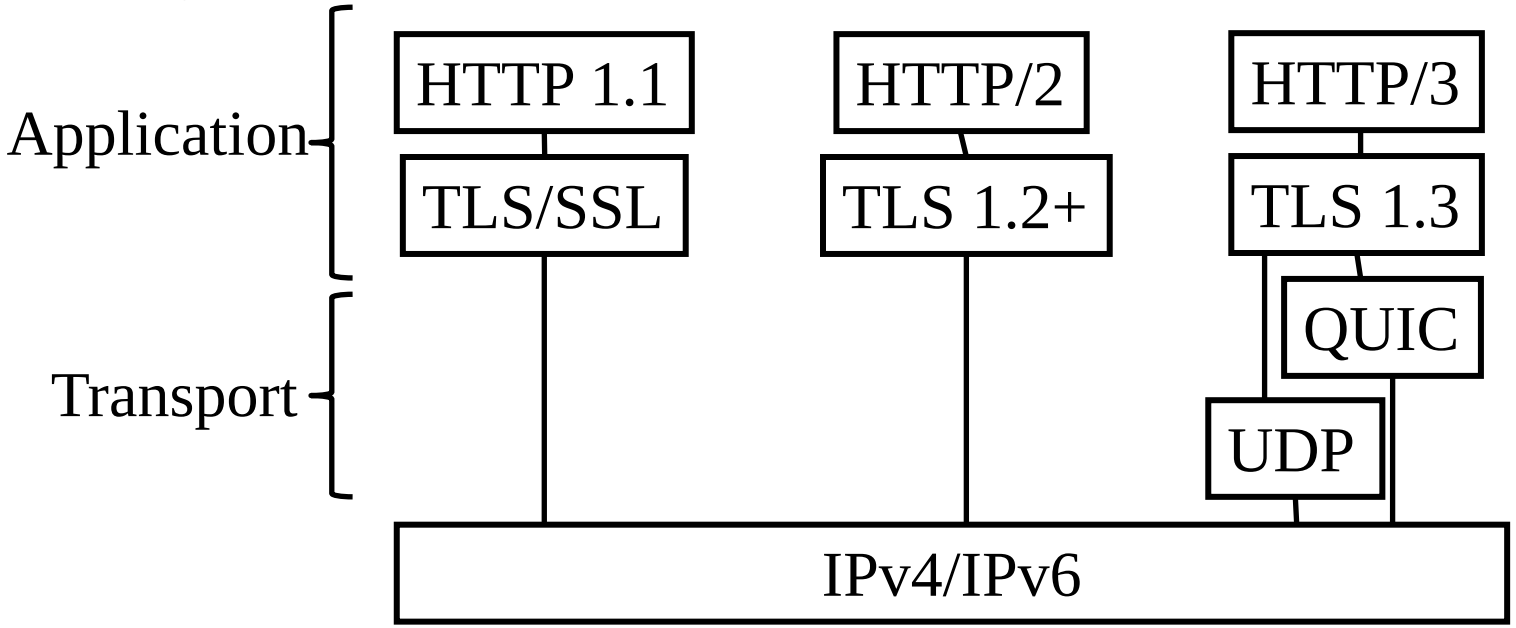
- Does the TLS session start when the Master Secret (MS) is created?

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

©2025 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

- 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.

- Why there's a need to have both HTTP and HTTPS?

Many websites do not require security.

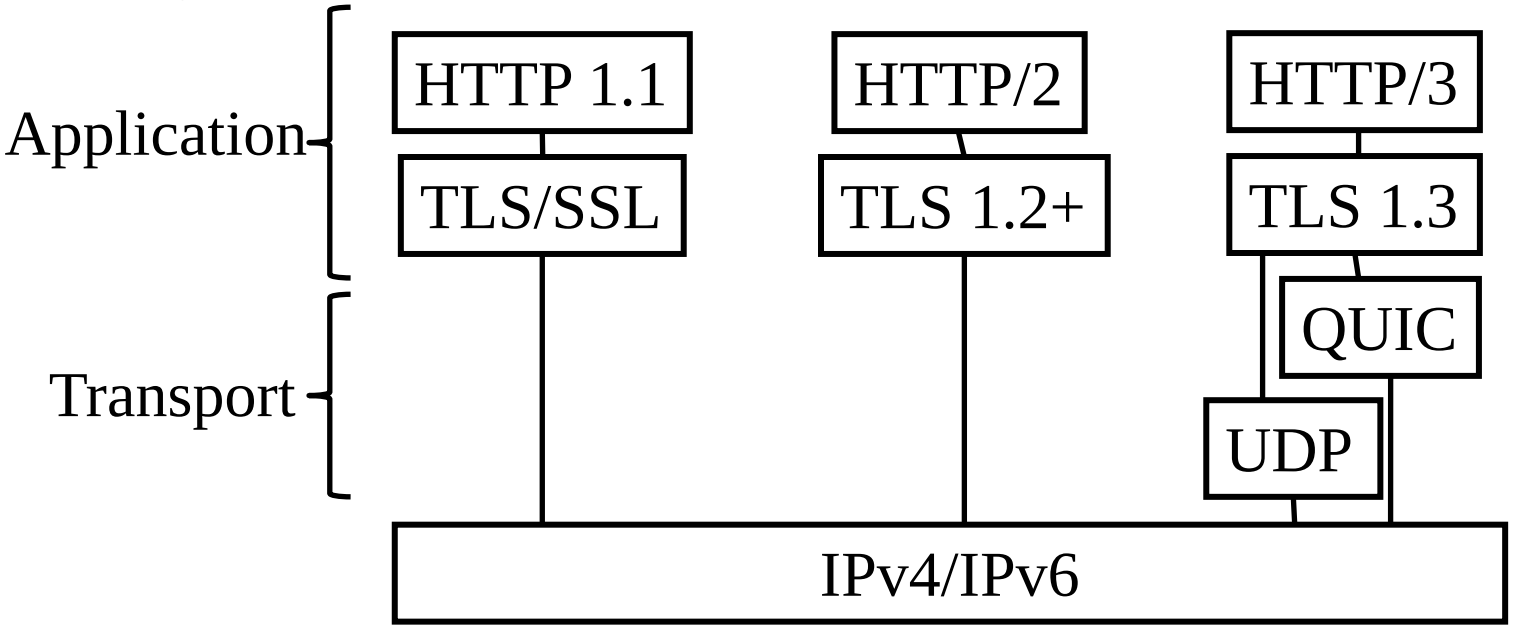
- you answered that QUIC is a new Transport Layer Protocol that includes TLS, but it is shown as application layer protocol on the slides. Which one is correct?

QUIC is a transport protocol like TCP. Some part of TLS uses UDP.

©2025 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

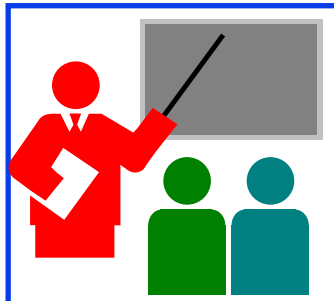
- Textbook page 632 If it is straightforward for anyone to make a website that has a certificate from a CA allowing them to use HTTPS, why are certificates helpful?

To authenticate the website.

- So is SSL/TLS a layer added between application layer and transportation layer to add security functionalities?

Yes

©2025 Raj Jain



TLS: Summary

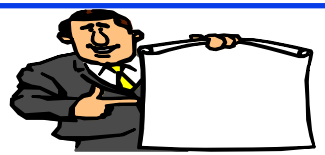
1. Netscape invented SSL to secure web transactions
2. TLS is a revised version of SSL V3
3. TLS provides
   a. Crypto negotiation,
   b. Secure key exchange,
   c. Privacy via encryption, and
   d. Integrity using a keyed hash.
4. HTTP over TLS is also called HTTPS

Student Questions

- ❑ 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 on the level of security required. Longer keys require more computation power.*

Ref: Read Section 8.6 and Exercises R20-R23

©2025 Raj Jain



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.

©2025 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

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

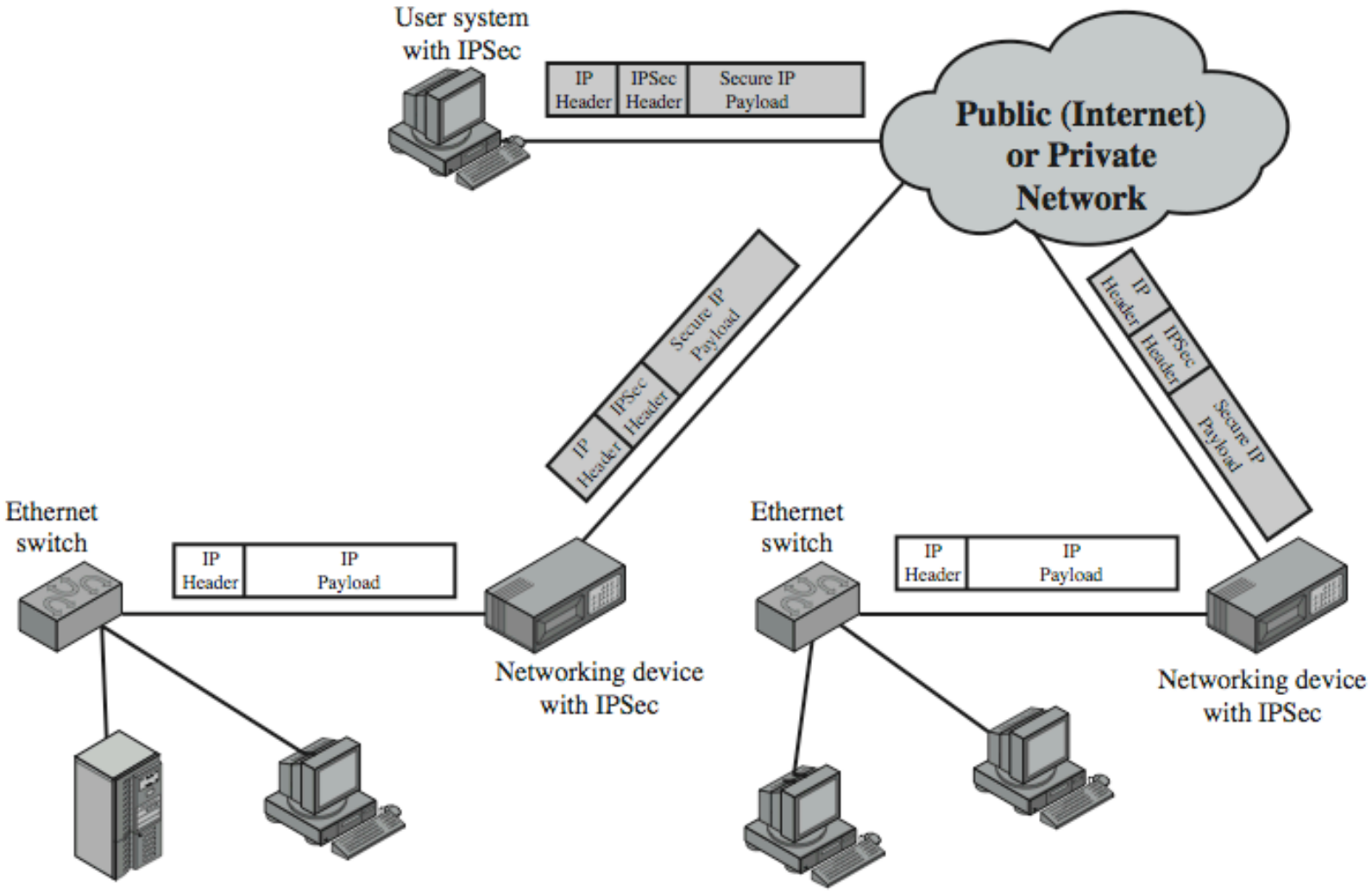
VPN is one type of application of IPsec. You can use IPsec for other applications. See the list at the bottom of this slide.

- How is the rejection of replayed packets enforced? *Secure timestamps/sequence numbers are one way.*
- So in daily life, most packets going over the internet never get encrypted if we do not explicitly ask the software to do the encryption. *Yes.*
- Is IPSec automatically enabled on most end systems? *No.*
- Does IPsec not ensure others cannot infer information from the traffic flow? *Yes.*
- Is there IP security when one switches to a private browser, or how does that work?

To get security, you can use HTTPS in any browser in private or public mode. Private mode disables add-ons in the browser.

©2025 Raj Jain

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?

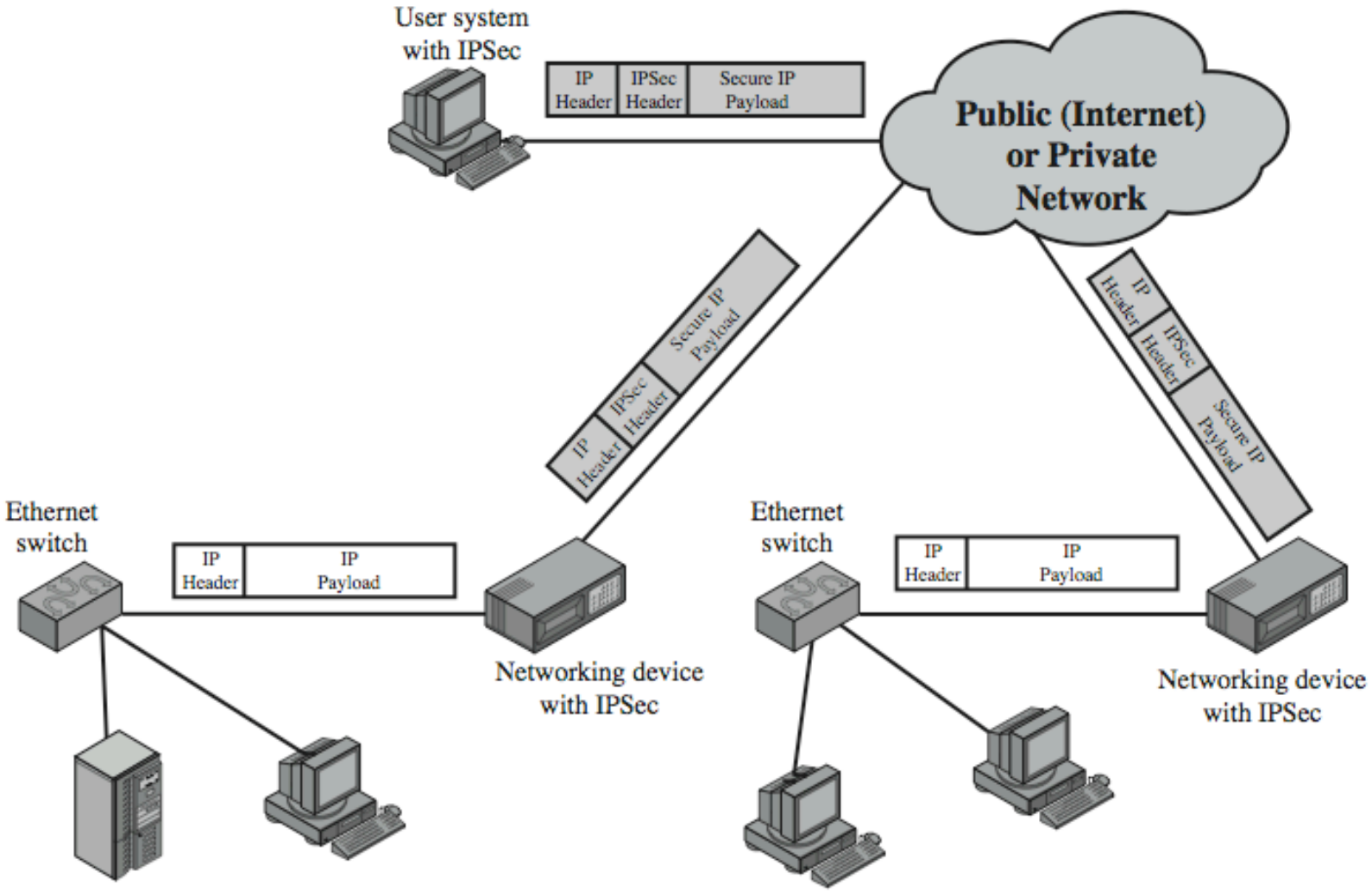
"VPN is exposed" if the government finds out that you are VPNing to some site banned by the government. Yes.

- Where does the "virtual" in VPN come from?

VPN is a virtual replacement for a private network or private line.

©2025 Raj Jain

IP Security Applications



Student Questions

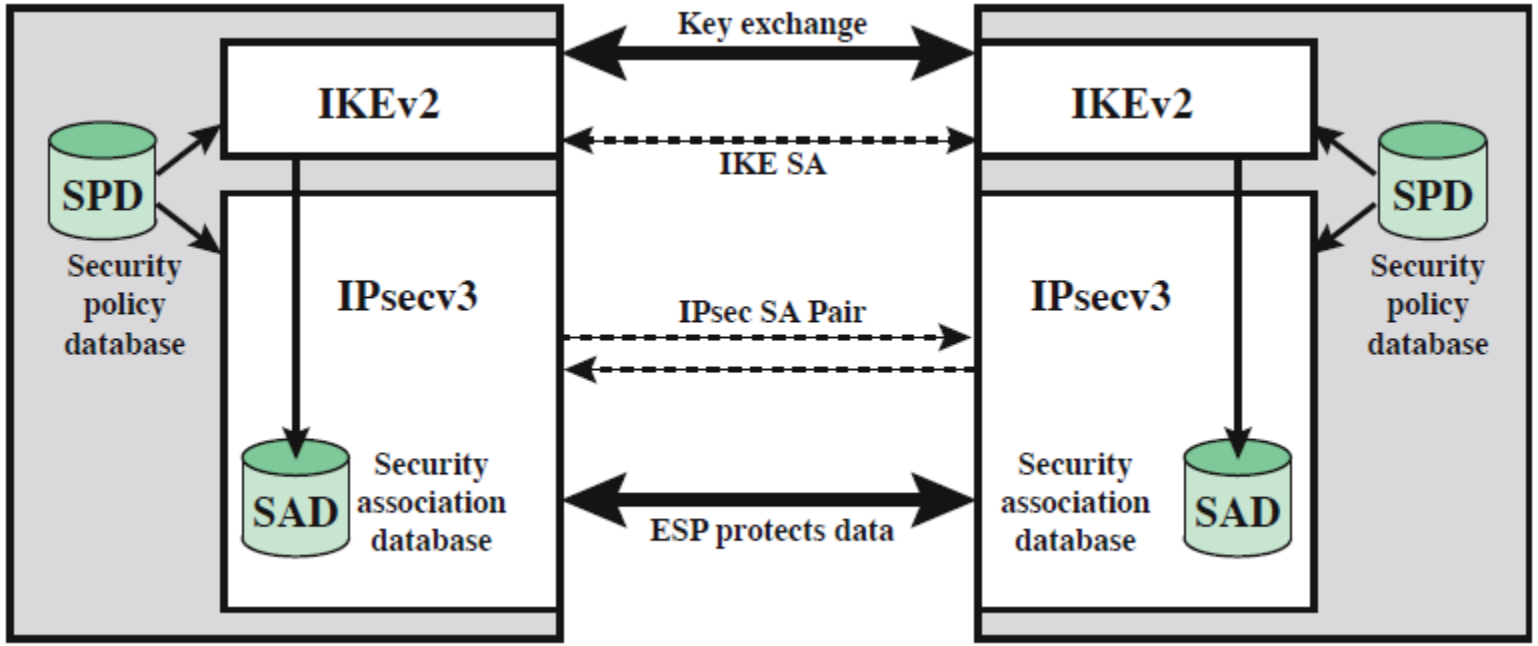
- If we want to set up a VPN, do we need DNS?

Yes, if you use the VPN server name. You can use the IP address directly and not use DNS.

©2025 Raj Jain

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 are closed. Implementors can decide to keep them on the same "database," but they have different purposes and durability.

©2025 Raj Jain

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
  - The 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.*
- How many bytes are the AH and ESP?

Not critical for this course.

©2025 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

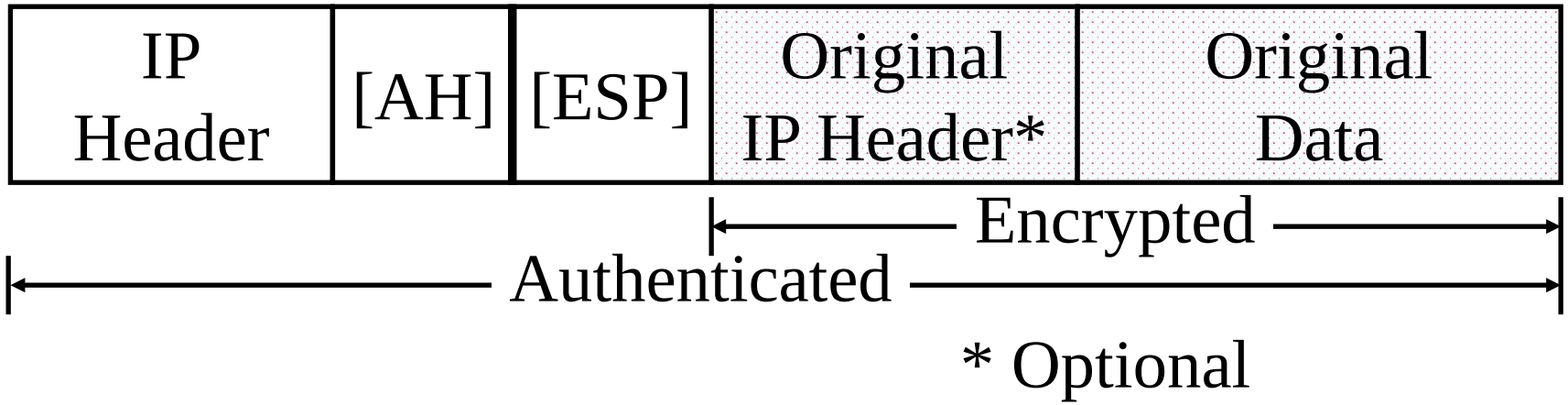
- Can you go over SPD again?

What's not clear?

©2025 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

- 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.

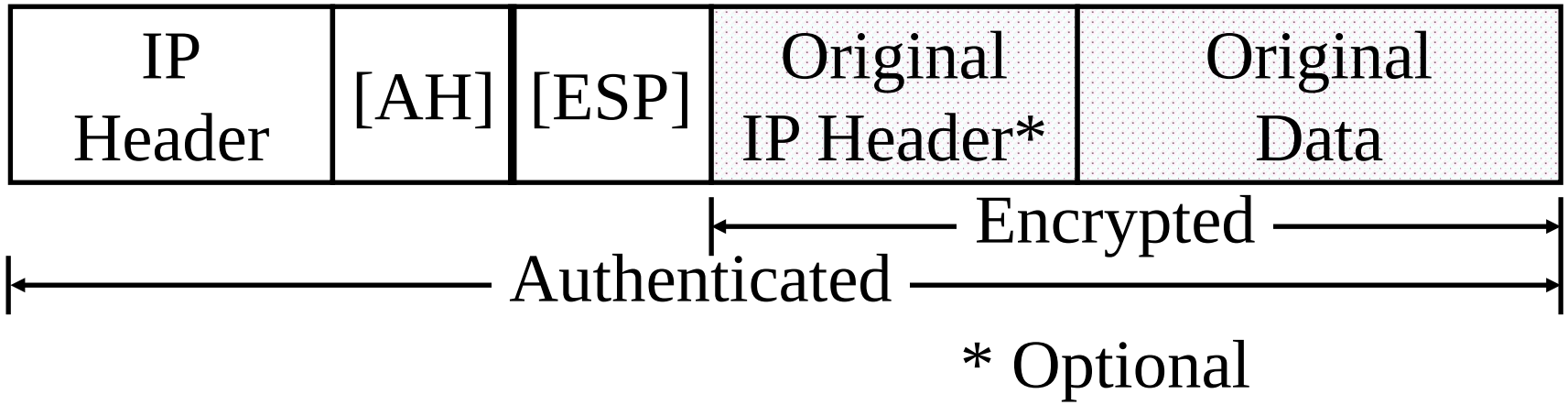
- Can you go into detail about the two ways of IP security?

Yes, AH and ESP are covered next.

©2025 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

- 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.

- Do all transport protocols have some encryption protocol?

No, e.g., TCP w/o SSL.

- Is SSL and IP security in different situations could be used simultaneously?

Yes, e.g., HTTPS on a VPN.

- I thought tunneling was only for an IPv6 packet being transmitted by an IPv4 router. Is this the same kind of tunneling, and is it always used for both IPv4 and IPv6?

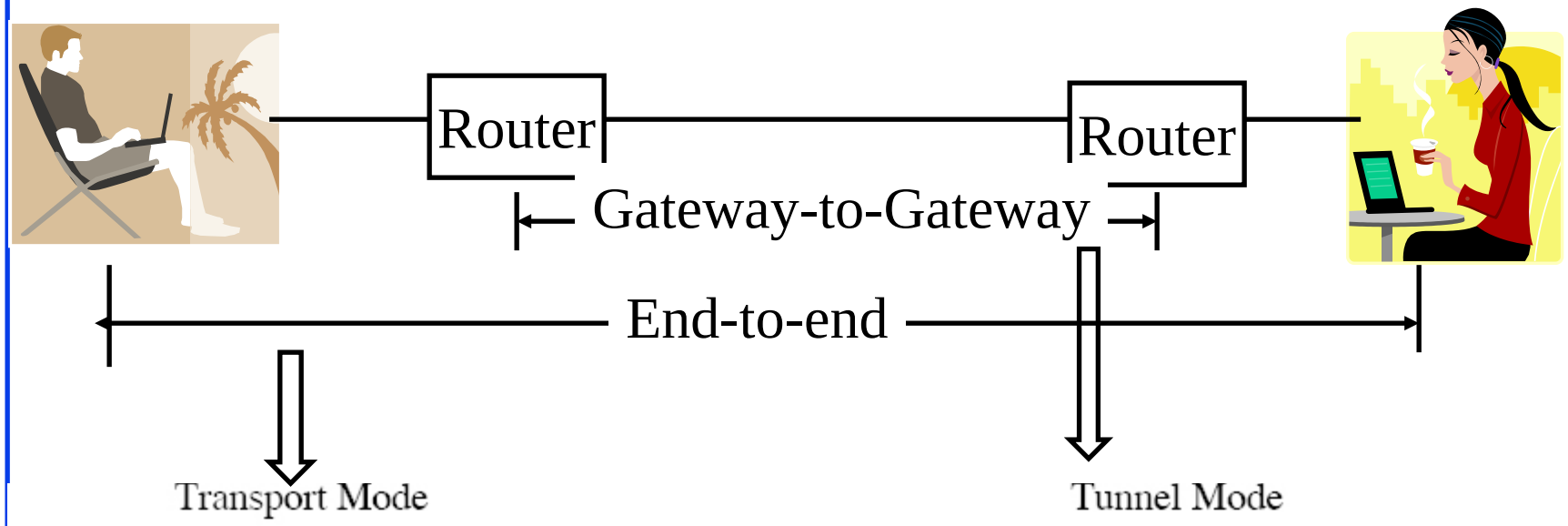
Tunneling is used whenever a protocol has to be transported in a region where that protocol is not spoken, e.g., IPv4 over IPv6, IPv6 over IPv4, IPv4 with security over insecure regions, etc.

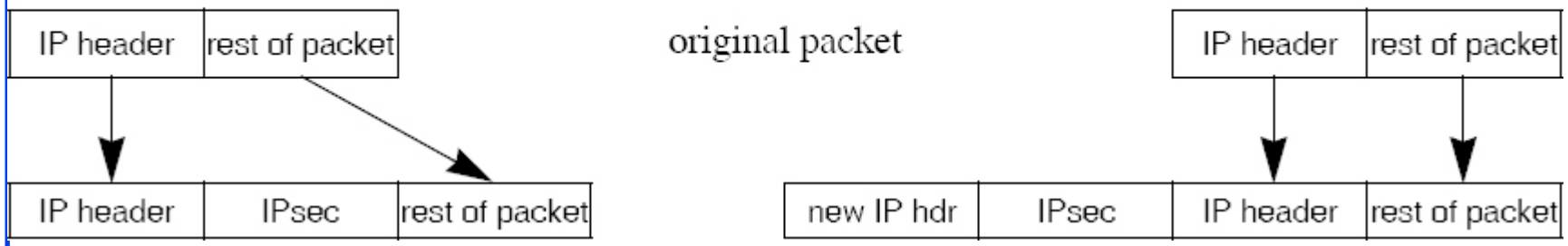
End of Part 2

©2025 Raj Jain

Tunnel vs. Transport Mode

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





Student Questions

- how do we pick those ways and use end-to-end in WUSTL?

When you browse or connect to the medical campus from the Danforth campus, you are using tunnel mode. When you use HTTPS, you are using transport mode.

- Does the decryption process happen in the transport mode?

Yes, routers do encryption and decryption.

- What advantages does transport mode have over tunnel mode? *Transport mode protects against insider attacks.*
- Transport mode's datagram will not have a new IP header? Because the source and destination address will not change?

Yes.

©2025 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

- Since MAC is associated with a packet, why have an ICV? MAC itself could ensure integrity.

ICV can be a simple hash or include digital signature. If it includes signature, it is called MAC.

- AH doesn't provide confidentiality. How does ESP do this, and why does AH leave this feature unimplemented?

AH is used when confidentiality is not required. It is similar to signing your message but not encrypting it.

- Can you explain why one key is needed for confidentiality and another for integrity?

Integrity keys can be shared more widely than confidentiality keys.

- Where is the Authentication header inserted? What does it contain?

See Slide 8.72.

©2025 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

- How is AH both connectionless and using a shared secret key? I would assume having a shared secret key would mean an established connection, the duration of which is how long the secret key is valid.

For the network layer, the term connectionless applies only for routing. The path does not follow a preset circuit as in MPLS.

- Can the AH stop someone from intercepting and changing the data before it gets to you?

Yes. That's precisely what it does.

©2025 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

- Can you explain TFC?

TFC=You cannot figure out if and how much information has been transmitted.

- What is an anti-replay service?

You can't use old captured responses.

- Why is TFC limited?

Padding can hide size differences.

©2025 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

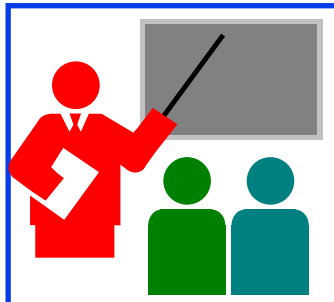
- Is using keys for integrity similar to the error detection process of CRC?

Yes.

- If the two devices already know the shared secret key, does IKE still requires two pairs of keys then?

No. IKE is used to get the keys across.

©2025 Raj Jain



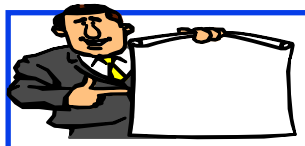
Summary: IPsec

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

©2025 Raj Jain



Firewalls and IDS

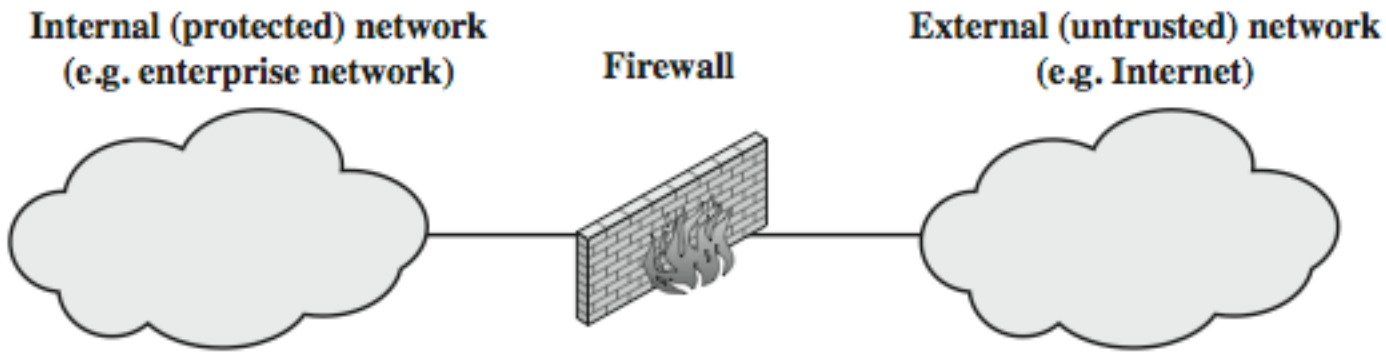
1. What is a Firewall?
2. Types of Firewalls
3. Intrusion Detection Systems
4. Honeypots

Student Questions

©2025 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

- 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.*
- How do firewalls differ in behaviors?

By having different rules

- What will happen if we do not have firewalls for websites?

They will be hacked, and data leaked.

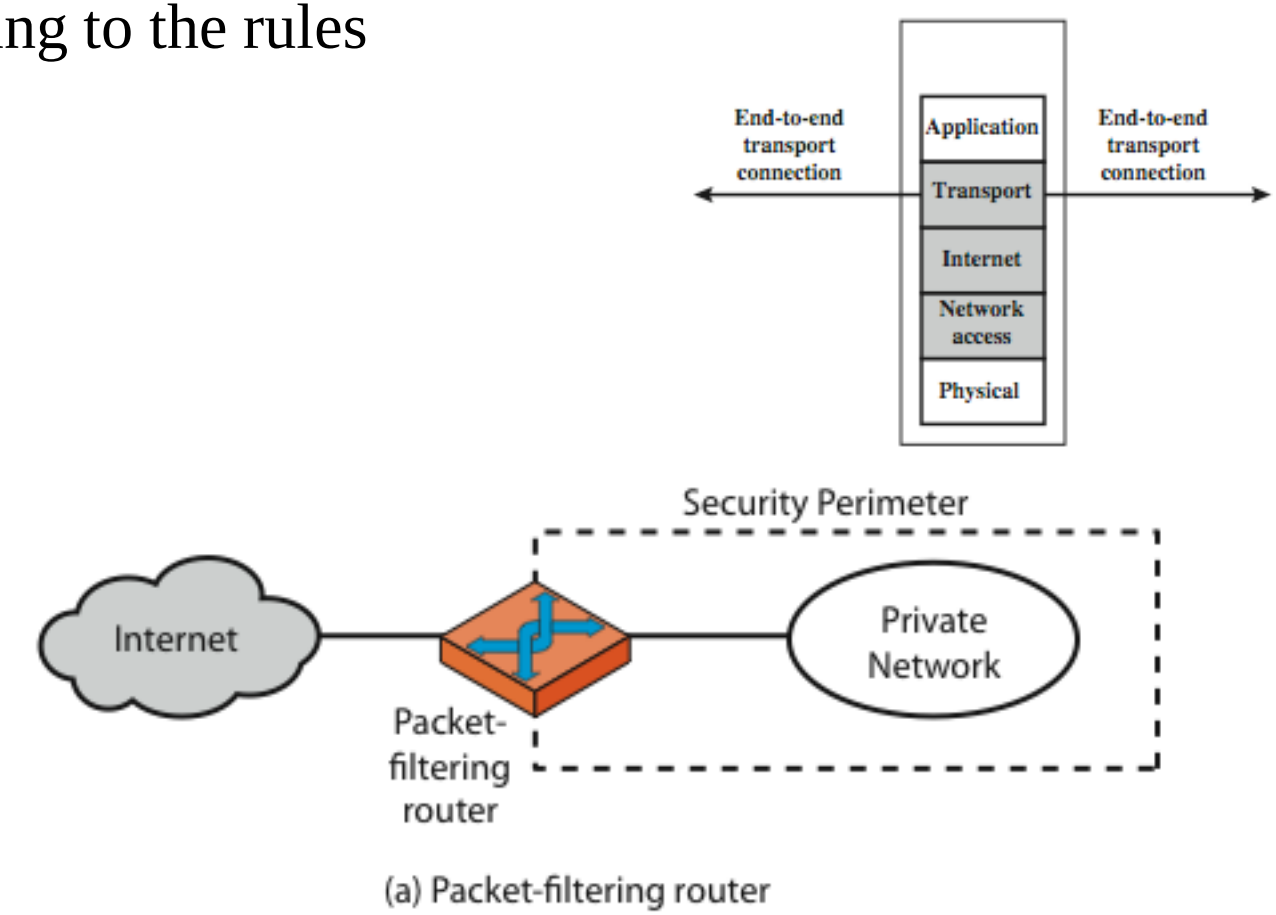
- What does it mean by firewall implements VPN? Why would firewall have VPN?

Firewalls may allow only certain traffic to enter/exit the system.

©2025 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

- Who defines the firewall rules?

Administrator. For your computer, you are the admin.

- What happens after the firewall filters out a packet? Does the sender resend the packet? What happens to the recipient application that was supposed to receive the packet?

The application disconnects after a limited number of retries.

- When an IP address is 'blacklisted,' is that the firewall?

Yes.

- Where is the firewall implemented? Is it a router or a switch?

A firewall can be a separate box, software in a router, or the host.

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

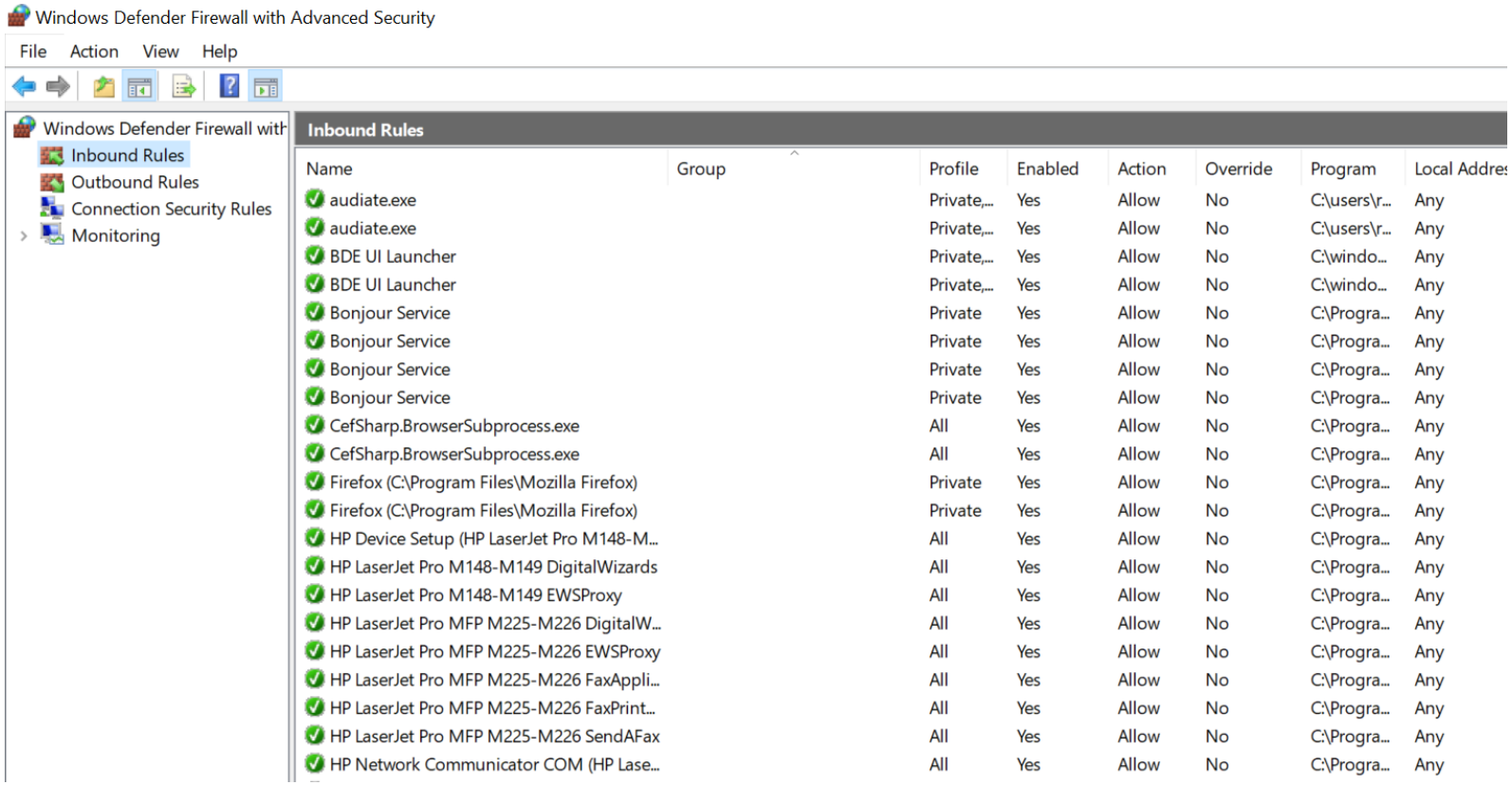
Student Questions

- 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

- You said you play with these rules every day? What are you doing? How much does this need to be changed on a day-to-day basis?

Not every day. But to allow certain remote operations, you need to first change the firewall.

- Are these rules implemented in the hardware or software?

Software.

- Can we play with the firewall on the MacOS system?

On your Mac, choose Apple menu > System Settings, click Network in the sidebar, then click Firewall. (You may need to scroll down.)

©2025 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

- In terms of efficiency, what is the overhead of turning on the firewall and letting it examine every packet?

There is some overhead.

- Are stateful packet filters more secure than regular packet filters? *Yes.*
- What would happen if the data exceeds the limitation? *It may not be inspected.*
- How does a firewall maintain its state, and where does it remember these rules? Like in the router?

Each computer has a firewall. The rules are on the computer. Each company/home network has a firewall. These rules are in the boundary routers.

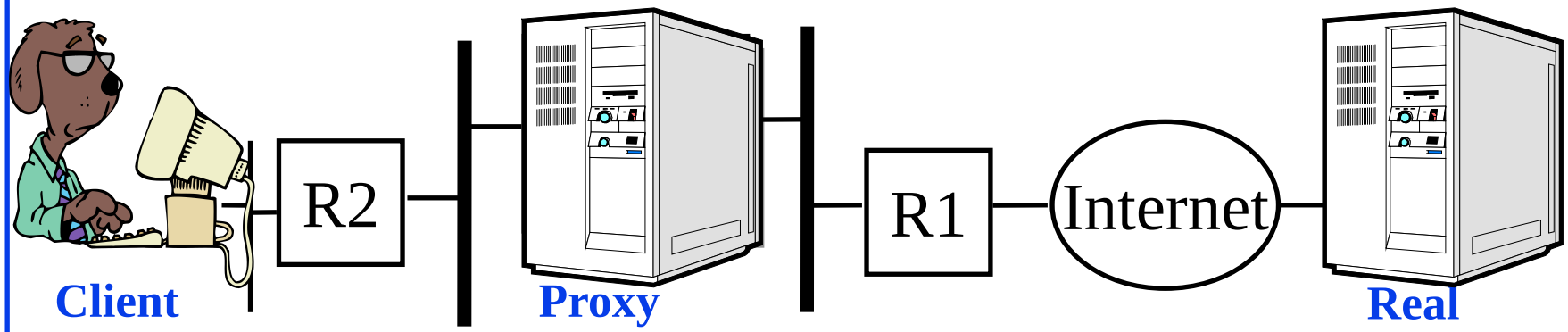
- Can firewalls be hijacked (i.e., rules manipulated by a hacker)?

Yes, firewalls can be hacked.

©2025 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

- Does this proxy server also have a function of improving traffic? Or does it just purely serve as a firewall?

It can do either or both.

- How do proxy servers benefit organizations in terms of security, performance, and user experience?

Improves performance and security.

- What is the difference between a proxy server and a firewall?

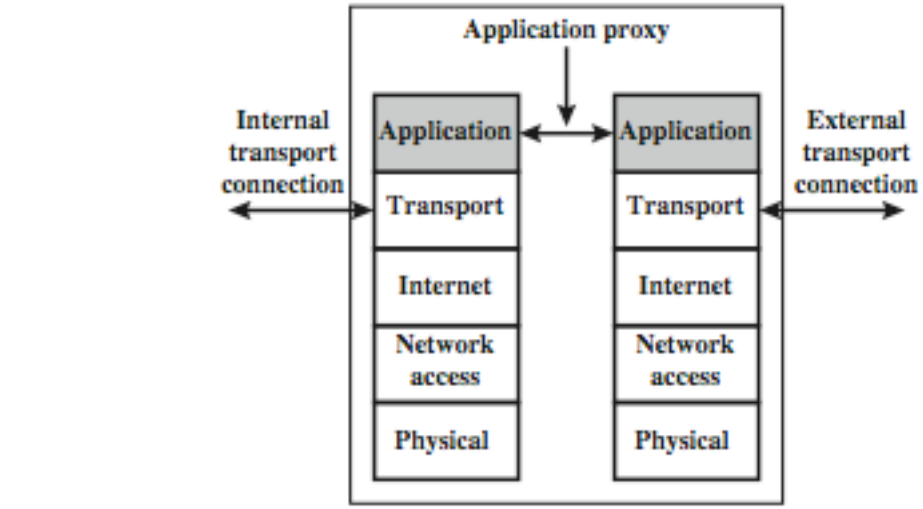
Proxy servers are often used for performance and not for firewalling.

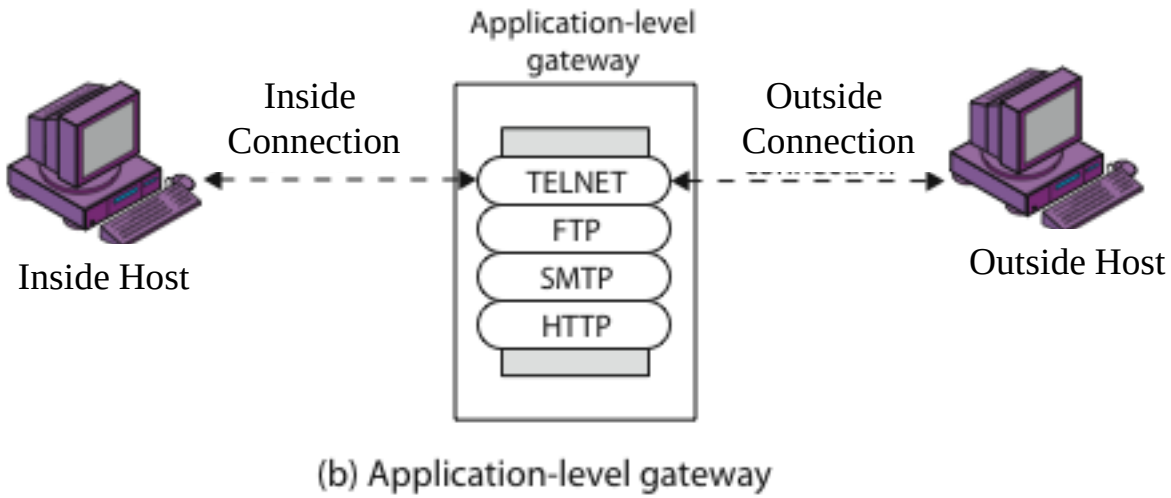
- What is the difference between a proxy and a firewall?

Proxy primarily provides performance improvement. Security may or may not be on.

©2025 Raj Jain

Application Level Gateway (Cont)





(b) Application-level gateway

Student Questions

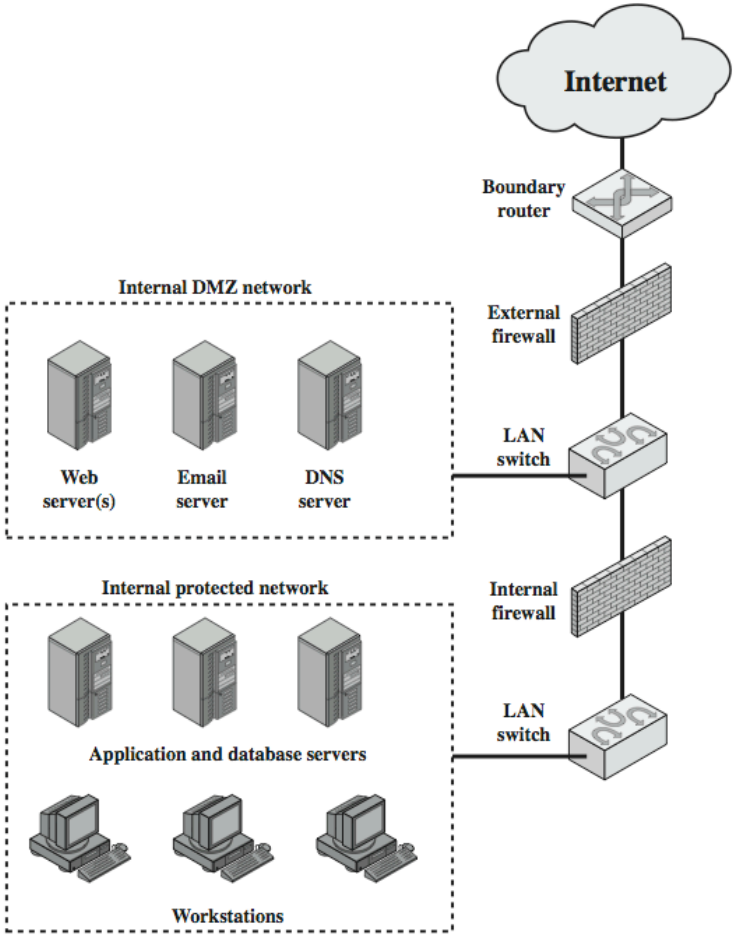
- How do firewall implementations typically differ based on the entity they're implemented on? For example, a proxy server firewall (which I assume is stateful), say a laptop firewall?

A firewall can only protect the traffic passing through it. A network-based firewall can protect all nodes, while a laptop firewall can only protect itself.

©2025 Raj Jain

DMZ Networks

- Demilitarized Zone



Student Questions

- What does the external firewall do if "the whole world can reach the DMZ network"?

Implements the rules for who can do what on the DMZ network.

- DMZ and protected which is harder to enter? *Protected.*
- What differences are there between the external and internal firewalls?

Internal firewall rules are more restrictive.

- Can only server be in DMZ? Why don't we put routers in DMZ as well for more protection?

Boundary routers have their own job. It may include firewall.

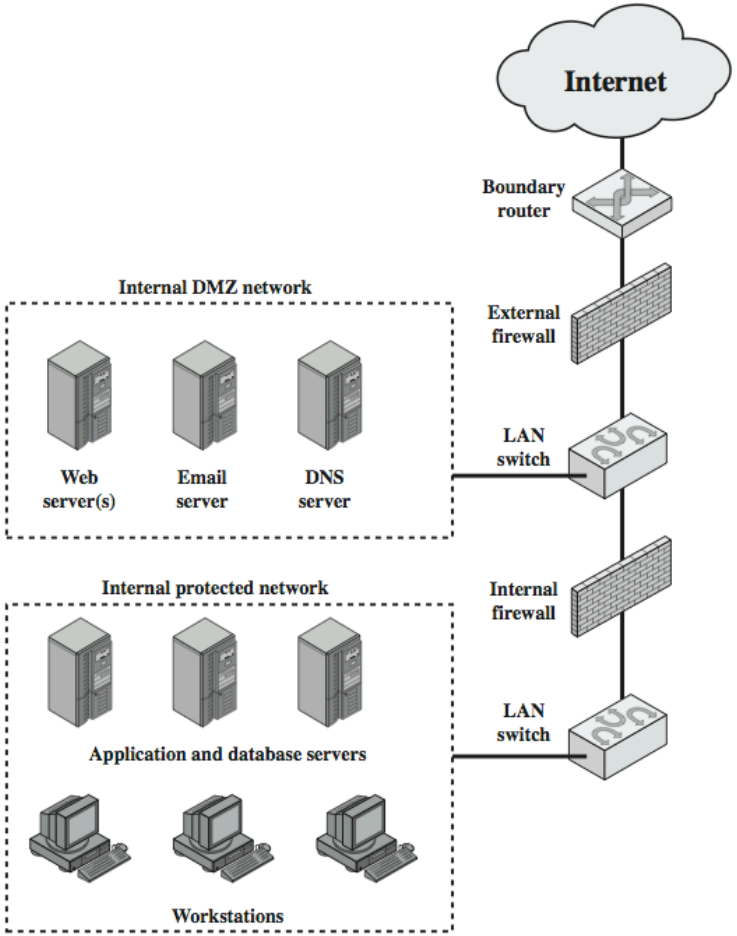
- Would you want to have additional firewalls within the DMZ network that could prevent devices from spreading harmful content to each other? Perhaps if some malicious attacker gained physical access to one device of a large internal DMZ?

Yes. Each server has its own internal firewall.

©2025 Raj Jain

DMZ Networks

- Demilitarized Zone



Student Questions

- Do the demilitarized zone networks use stateful firewalls?

All firewalls can be stateful or stateless.

- Why do we need two external and internal firewalls here?

External allows uninvited traffic, while internal does not.

- P677. Usually when we say DMZ in home routers, it would expose all port of a specific server inside the network. Is it the same DMZ here as it seems that it is referring to a group of servers?

Same. One server or many.

©2025 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, 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.

- Why wireless LAN access attacks can not be protected by a firewall while wired can.

Wireless LANs are easier to listen to.

- What is sneakernet? *People messengers*
- What files/computer systems would you initially start with to debug an infected computer? *Operating systems*
- What is a sneakernet?

See Above

- How can trusted services like SSL/SSH be involved in attacks bypassing firewalls?

An SSL message can invoke something unsafe, e.g., write on a read-only database.

©2025 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

- Doesn't a firewall do intrusion and extrusion detection? What's the difference between a firewall and these concepts?

A firewall may do one or both.

- What is the primary function of extrusion detection systems?

Check information leak

- How do we inspect all of the files on our computer?

Use malware detection software. Several operating systems provide it. On others, you have to buy it.

©2025 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

- How are signature-based IDS derived from code, and how are some recognizable as malware?

Here, signature = pattern
Not a cryptographic signature.

  - How exactly is Rule-based different from signature-based? Don't they both require previous attack knowledge?

Signature based is mostly pattern recognition. Rule-based is a table or conditions (rules) to validate.

©2025 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

- if you have a honeypot set up, what is the process for making practical use of the data you collect from that honeypot site?

Catch the hackers

- How would non-attackers interact with the honeypot systems?

They would act normally.

- What are some common types of honeypots used in industry, and what are the advantages and limitations of each type? *Too detailed for this course.*
- The honey pot uses a real address, but it's only used to detect malicious traffic. How does it prevent valid IP addresses from being blocked?

Honeypot may or may not block.

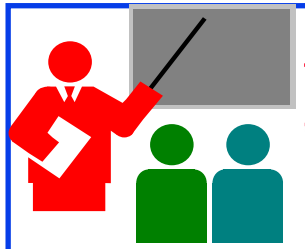
- Can a non-website server with decoy files, information, etc., be used to distract an attacker who has already breached the network?

Yes.

- What serves as a lure for honeypots? Is there dummy-sensitive information or something like that?

Yes. Dummy sensitive information.

©2025 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

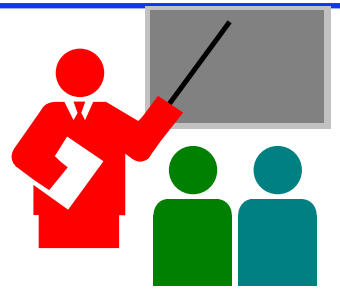
Student Questions

- How does VPN work around firewall?

Firewall rules are set to allow VPN traffic.

Ref: Section 8.9 and Exercises R28-R32

©2025 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

- Are there ways to detect/counteract security defects below the transport layer?

Yes. There may be utilities to reset or debug firewalls.

©2025 Raj Jain



Wireless Security

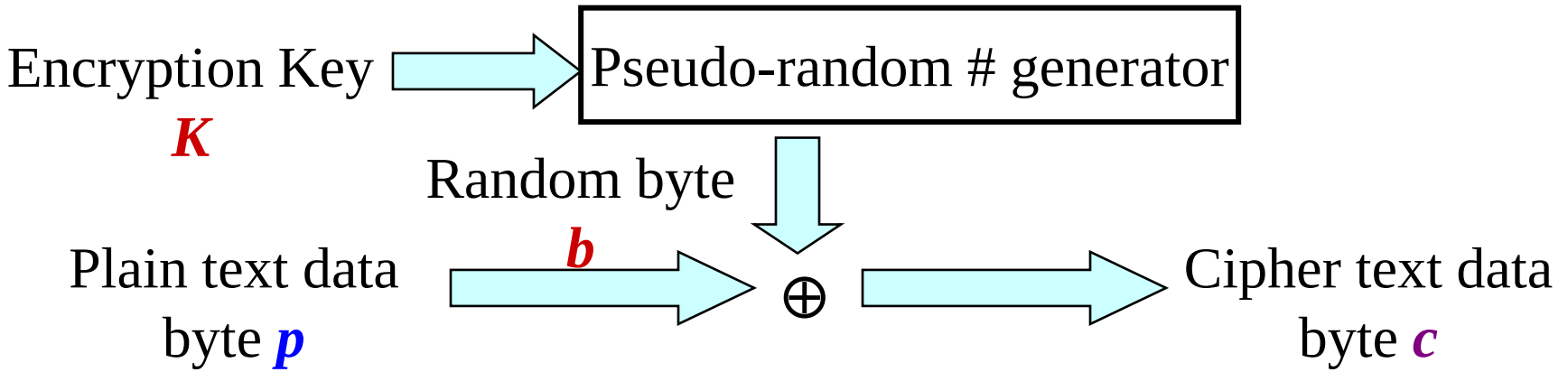
1. Ron's Cipher 4 (RC4)
2. Extensible Authentication Protocol (EAP)
3. RADIUS
4. Wired Equivalent Privacy (WEP)
5. Problems with WEP Authentication
6. 802.11i Wireless LAN Security
7. Authentication and Key Derivation
8. WPA2 Four-Way Handshake
9. Authentication and Key Management in 4G/5G

Student Questions

©2025 Raj Jain

Ron's Cipher 4 (RC4)

- Developed by Ron Rivest in 1987. Trade secret. Leaked 1994.
- Stream Cipher
  - A pseudo-random stream is generated using a given key and xor'ed with the input
- Pseudo-random stream is called a **One-Time pad**
- Key can be 1 to 256 octets
- See the C code in the reference.



Ref: Brad Conte, "Implementation of RC4 in C," 2006, http://bradconte.com/rc4_c

©2025 Raj Jain

Student Questions

- Can you explain the one-time pad in detail?

Random #: 00100011 10110110

Data: 11111011 10001001

Encrypted: 11011000 00111111

- Why does the random number generator need a specific seed? Is the seed used later?

Generators use a formula.

$$x_n = f(x_{n-1})$$

You need to provide the first number x_0 to start. This is the seed. It is not used again.

$$x_n = 5x_{n-1} + 1 \mod 16$$

Starting with x_0=5:
The first 16 numbers obtained by the above procedure: 10, 3, 0, 1, 6, 15, 12, 13, 2, 11, 8, 9, 14, 7, 4, 5

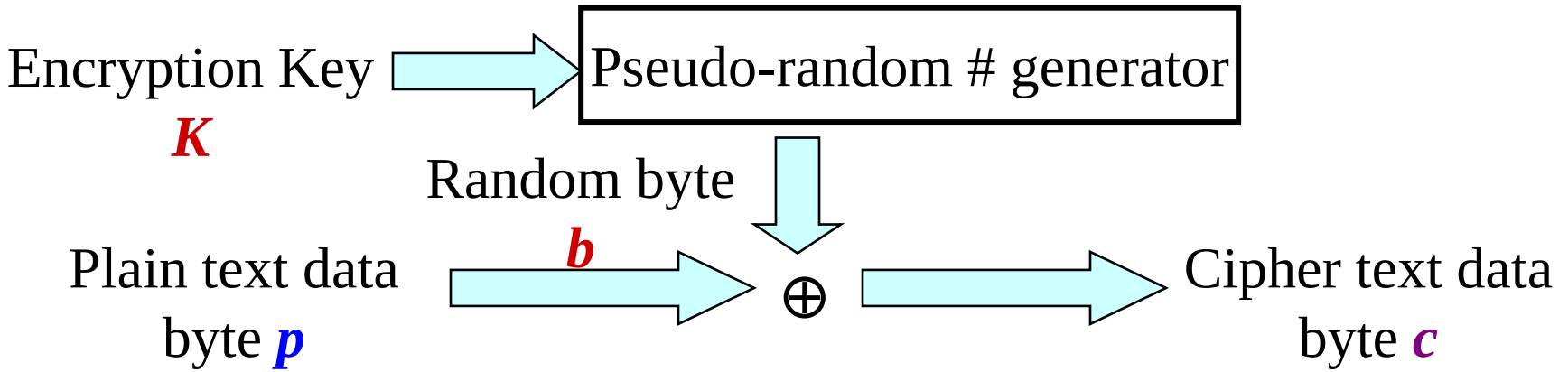
- When is Ron's Cipher used?

In WEP and WPA1

- Is the implementation of RC4 required in this exam? *No*

Ron's Cipher 4 (RC4)

- Developed by Ron Rivest in 1987. Trade secret. Leaked 1994.
- Stream Cipher
  - A pseudo-random stream is generated using a given key and xor'ed with the input
- Pseudo-random stream is called a **One-Time pad**
- Key can be 1 to 256 octets
- See the C code in the reference.



Ref: Brad Conte, "Implementation of RC4 in C," 2006, http://bradconte.com/rc4_c

©2025 Raj Jain

Student Questions

- Is there a specific reason we see this in the slides' wireless section?

No. RC4 is used in wired networks also. It is where it is mentioned in the book for the first time.

- What encryption is used in Bitcoin, or blockchain in general? What makes cryptocurrencies secure?

Bitcoin uses public key encryption. It is not RSA but even stronger elliptic curve cryptography.

- How are Bitcoin transactions verified?

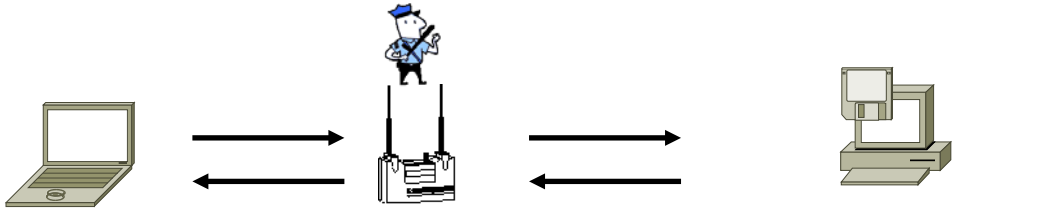
All transactions are signed by the user. Their public key is their ID.

- How does RSA differ from RC4?

RSA is a public key method, while RC4 is a secret key method.

Extensible Authentication Protocol (EAP)

- Old Methods: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP)
- Each authentication protocol required a new protocol
  ⇒ Extensible Authentication Protocol
- Allows using many different authentication methods
- Components: **Supplicant**: User, **Authenticator**: Network edge device, **Authentication Server.**



- Authenticator does not have to know all the authentication methods

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

Student Questions

- Why does the authenticator not have to know all authentication methods? Which parts of the authentication methods it needs to be aware of?

It is a simple pass-through.

- Why are there so many old methods? Why are they not just adjusting to the existing ones but making a different method?

Little increments may result in significant changes.

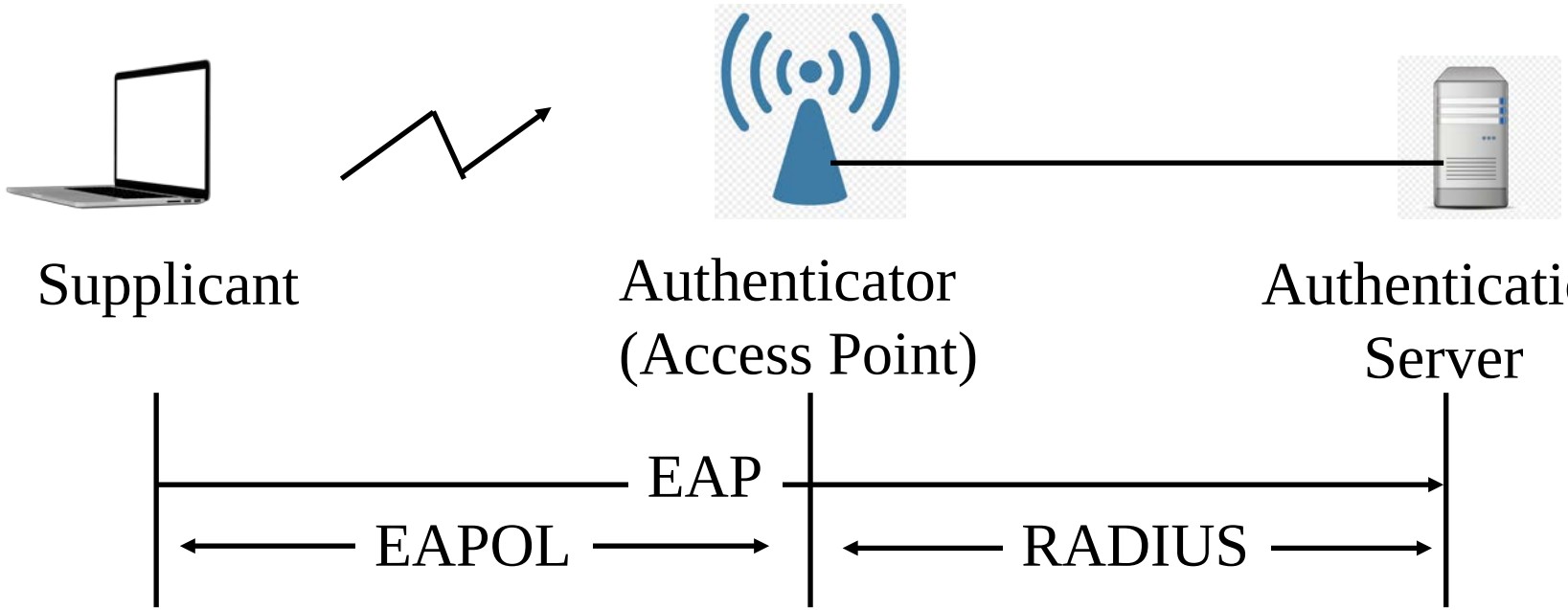
- Is EAP still used in wireless networks or just in 5G?

EAP is used in all wired and wireless networks.

©2025 Raj Jain

EAP over LAN (EAPOL)

- EAP was designed for Point-to-point line
- IEEE extended it for LANs ⇒ EAPOL
- Added a few more messages and fields
- EAPOL is part of EAP that runs over IEEE 802 protocols.



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

Student Questions

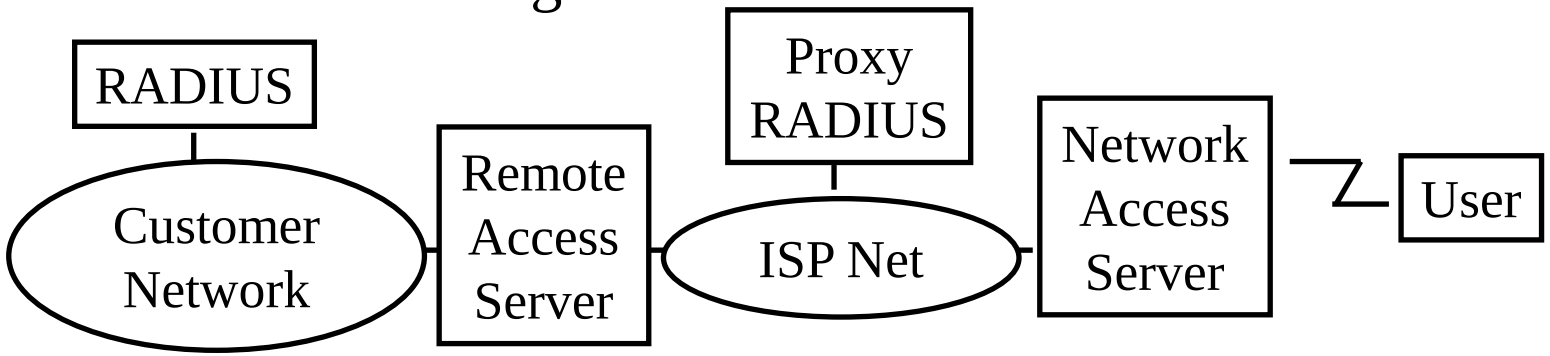
- The textbook says EAPOL is used between the station and the access point, and RADIUS is used between the access point and the authentication server. So where are the access point and authentication server on the diagram on this slide?

RADIUS is used between the Access server and the authentication server. EAP allows dumb access servers. Your home network has a shared password. Office networks require a user's unique password before connecting to Wi-Fi. The unique password is stored on the Authentication server.

©2025 Raj Jain

RADIUS

- Remote Authentication Dial-In User Service
- Central point for Authorization, Accounting, and Auditing data ⇒ **AAA** server
- Network **Access** servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances
- Uses UDP: In case of server failure, the request must be re-sent to backup ⇒ Application-level retransmission required
  - TCP takes too long to indicate failure



- Ref: http://en.wikipedia.org/wiki/RADIUS

Student Questions

- What is the benefit of adding a RADIUS/DIAMETER server and protocol to the EAP messages?

RADIUS came before EAP. It simply allows all secrets to be stored in a central place and used at multiple access servers. EAP allowed dumb authenticators.

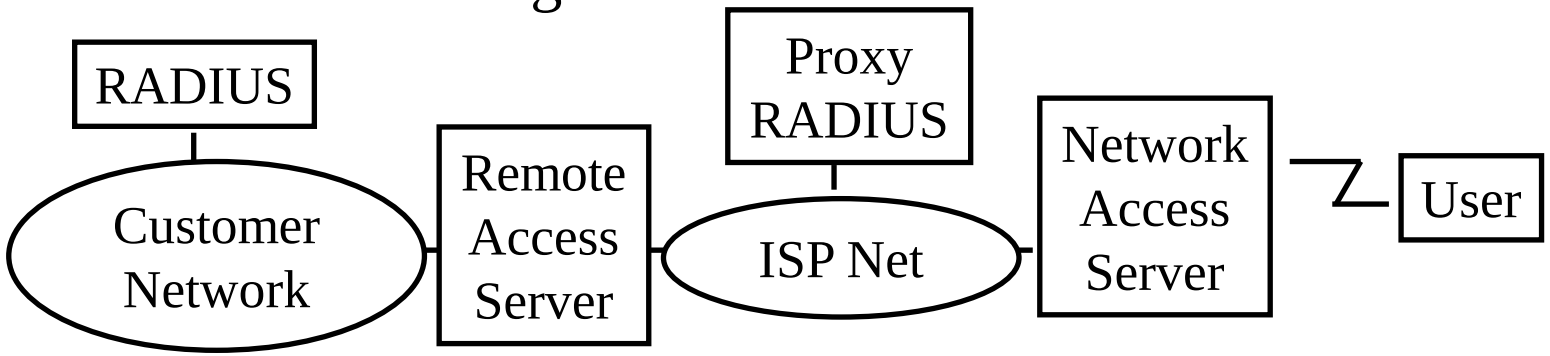
- If both EAP and RADIUS allow the authenticator not to know the authentication methods, what are their difference? *RADIUS access servers were more than pass-through.*
- So EAP allows the authenticator to be dumb in that it does not know either methods or information, while RADIUS only allows the access servers to be ignorant about authentication information but not methods?

Yes.

©2025 Raj Jain

RADIUS

- Remote Authentication Dial-In User Service
- Central point for Authorization, Accounting, and Auditing data ⇒ **AAA** server
- Network **Access** servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances
- Uses UDP: In case of server failure, the request must be re-sent to backup ⇒ Application-level retransmission required
  - TCP takes too long to indicate failure



- Ref: http://en.wikipedia.org/wiki/RADIUS

Student Questions

- Does DIAMETER provide the same, slightly improved functionality as RADIUS, or does it allow for a "dumb" authenticator like EAP?

It is a significant extension of RADIUS. That is why it has a different name. Yes, it allows EAP.

Ref: https://en.wikipedia.org/wiki/Diameter_(protocol)

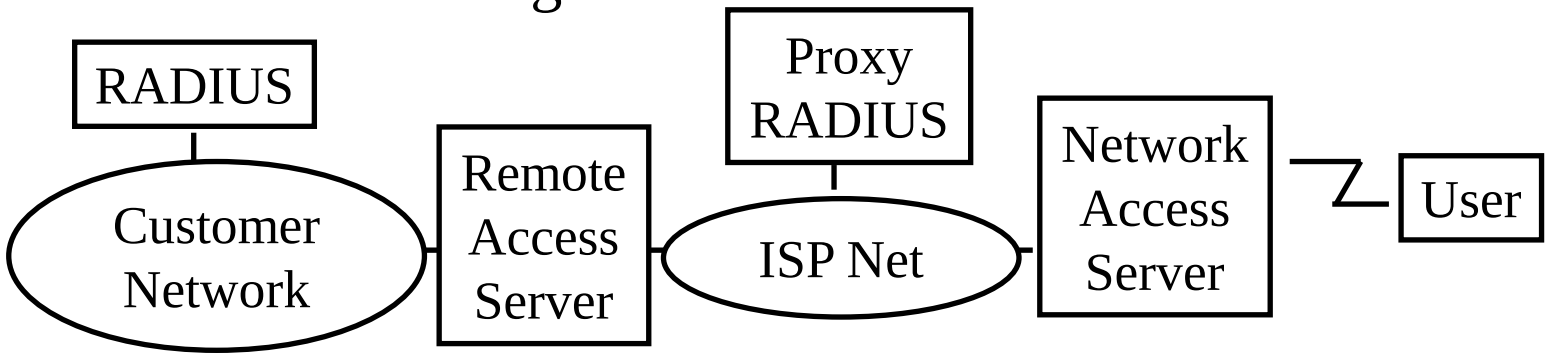
- Can you explain why TCP takes too long to indicate failure but an application-level transmission isn't?

Some applications prefer their loss-recovery mechanisms, and some don't. DIAMETER, for example, uses TCP.

©2025 Raj Jain

RADIUS

- Remote Authentication Dial-In User Service
- Central point for Authorization, Accounting, and Auditing data ⇒ **AAA** server
- Network **Access** servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances
- Uses UDP: In case of server failure, the request must be re-sent to backup ⇒ Application-level retransmission required
  - TCP takes too long to indicate failure



- Ref: http://en.wikipedia.org/wiki/RADIUS

Student Questions

- Is the proxy radius like the proxy servers in that they help with performance and security?

Yes

- Is RADIUS for authentication servers and EAP for authenticators?

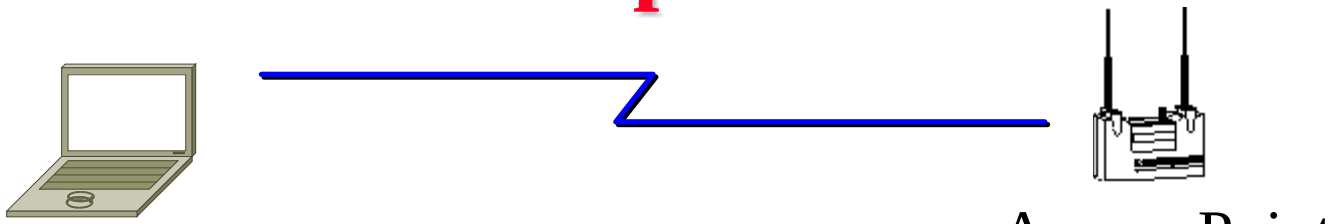
RADIUS allows authentication to be centralized. EAP allows authenticators to be dumb.

- Can you explain the purpose of an authenticator when it doesn't seem like it's doing any real work?

Authenticator is a trusted guard at the edge that checks the ID of users. Without that you will have to direct dial the Access server.

©2025 Raj Jain

Wi-Fi Operation



Station

Access Point

- Access Points (APs) periodically broadcast a beacon with SSID (service set ID) and security level
- Subscriber stations listen to these beacons, measure signal strength and determine which AP to join
- Subscribers can also send a "Probe" to find APs in the neighborhood
- AP authenticates the subscriber station using shared keys
- Subscriber stations and AP exchange encrypted packets
- Subscriber station send a "Disassociate" message and log off

Student Questions

- What is the point of sending a probe if all APs broadcast a beacon with SSID and security level? Wouldn't the subscriber already have all the information that a probe would tell them?

Some high-security APs do not advertise their SSIDs.

©2025 Raj Jain

Wired Equivalent Privacy (WEP)

- WEP ⇒ Privacy similar to a wired network
- First encryption standard for wireless. Defined in 802.11b
- Provides authentication and encryption
- Shared Key Authentication
  ⇒ All users and access points share a single key.

Student Questions

- If everyone has the same shared key, how do we distinguish one user from another?

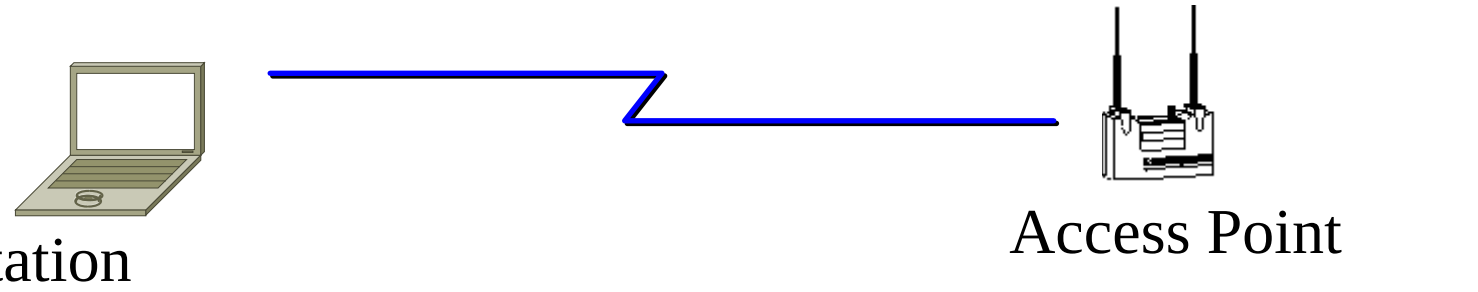
By MAC addresses.

©2025 Raj Jain

End of Part 4

Problems with WEP Authentication

- Record one challenge/response
- Both plain text and encrypted text are available to an attacker
- XOR the two to get the keystream
- Use that keystream and IV to encrypt any subsequent challenges



Student Questions

- The textbook said that since RC4 uses a limited range of IV, the attacker can get the keystream of a byte. How does the attacker exploit the fact to do something harmful because the same IV can repeat quickly?

Random number generators cycle through the same sequence again and again.

©2025 Raj Jain

WEP Problems

- No centralized key management
  Manual key distribution ⇒ Difficult to change keys
- Single set of Keys shared by all ⇒ Frequent changes necessary
- No mutual authentication
- No user management (no use of RADIUS)
- Directly uses the master key
- No protection against replay

Student Questions

- What do you mean by manual key distribution? Who distributes the keys, and why is it hard to change keys?

It is what is done in your home. If you change your Wi-Fi password, you must tell all family members.

- How would you know the correct length for the IV value?

The random number generator determines the length of the IV value.

Ref: http://en.wikipedia.org/wiki/Wireless_security, http://en.wikipedia.org/wiki/Wireless_LAN_security, http://en.wikipedia.org/wiki/Cracking_of_wireless_networks

©2025 Raj Jain

802.11i Wireless LAN Security

- Wi-Fi Alliance **Wi-Fi Protected Access (WPA)**
  Software modification to existing WEP systems
  Temporal Key Integrity Protocol (TKIP)
  - Key mixing function to generate per packet key
  - Sequence Number to protect against replay attacks
  - 64-bit message integrity check (MIC)
  - Uses the same RC4 encryption
- 802.11i **Robust Security Network (RSN) or WPA2**
  Requires hardware replacement
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - AES encryption with counter mode

Ref: http://en.wikipedia.org/wiki/IEEE_802.11i-2004, http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol, http://en.wikipedia.org/wiki/CCMP

©2025 Raj Jain

Student Questions

- Which part of the hardware needs to be upgraded? *Encryption logic.*
- From Textbook: In Figure 8.31 on Page 662, how do the mobile device and the authentication server establish a shared secret key?

Secret=f(nonce1,nonce2, password)

Secret key, public/private key can be used in place of password.

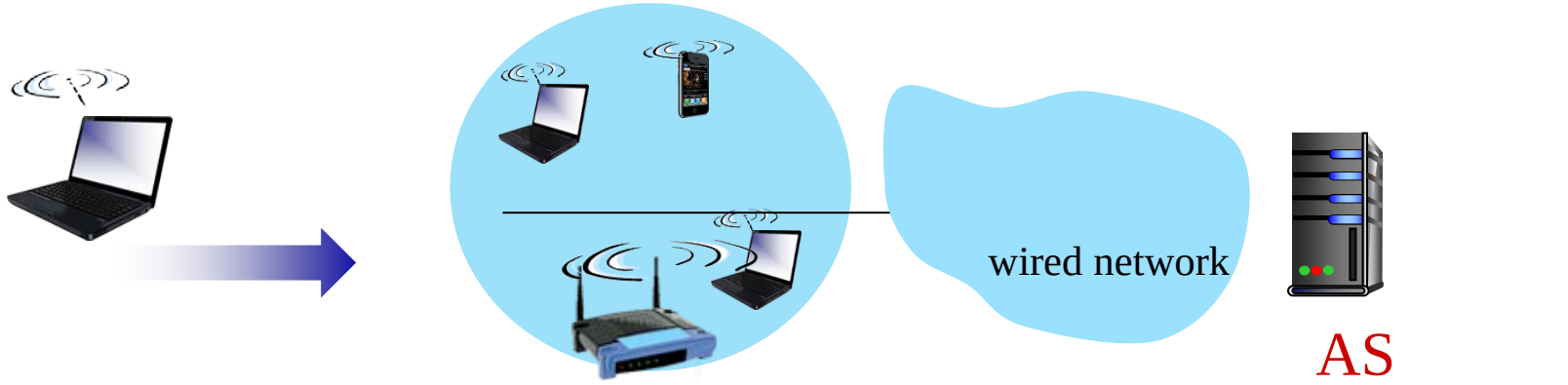
- Can you explain again when/how are shared common secrets distributed?

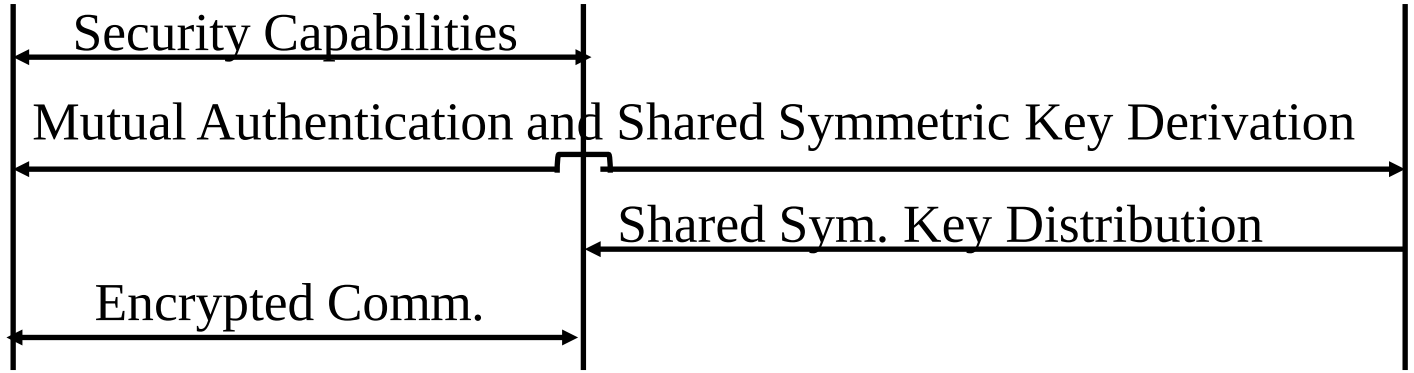
See the previous question.

- Could you go over the fifth quiz question: "WPA requires hardware modification and so cannot be implemented in older WEP systems."

WPA was designed for software upgradeability of older WEP systems.

Authentication and Key Derivation





Student Questions

- Are keys generated in the mobile device or the base station?

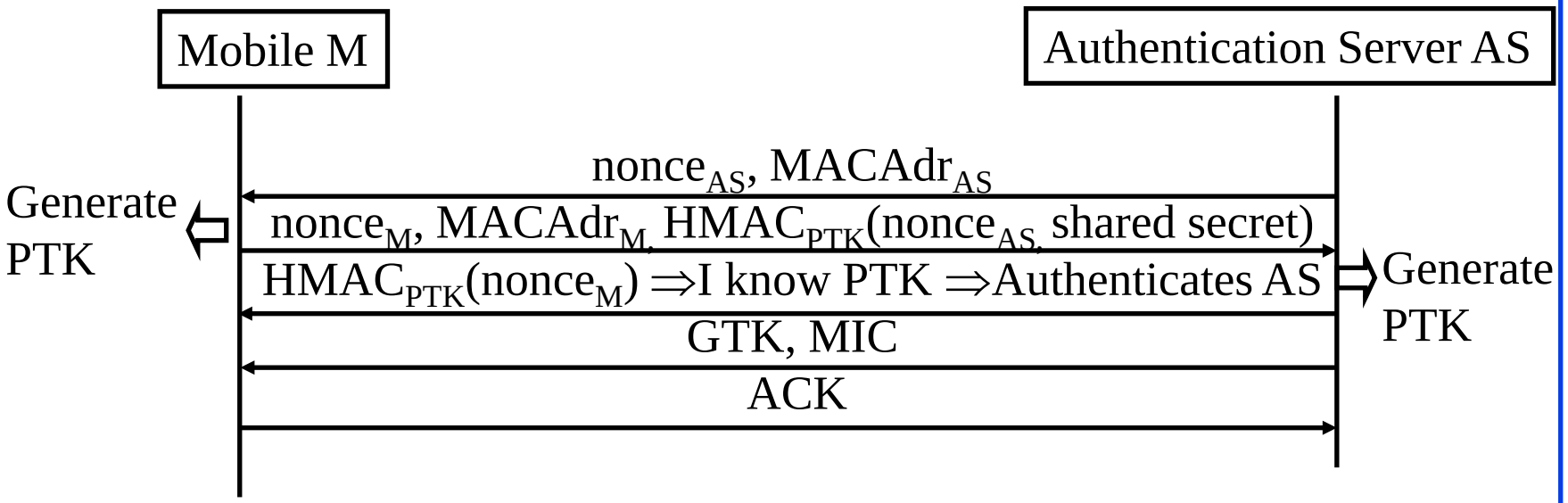
Both generate and come up with the same key.

- Page 661: The book mentions that Authentication Servers are used to authenticate the mobile device. Does this apply to only mobile cell phone devices? Or also to laptops/portable computers with wireless connectivity?

Users are authenticated in WiFi. SIM is authenticated in 4G/5G.

©2025 Raj Jain

WPA2 Four-Way Handshake



- Pair-wise transient key (PTK)
  =f(shared secret, Nonce$_{AS}$, MACAdr$_{AS}$, Nonce$_{M}$, MACAdr$_{M}$)
- PTK is used for unicasts.
  Group Temporal Key (GTK) is used for multicast

Ref: http://en.wikipedia.org/wiki/IEEE_802.11i-2004

Student Questions

- How does WPA3 improve on WPA2?

Removes the need for a shared password and uses the latest encryption

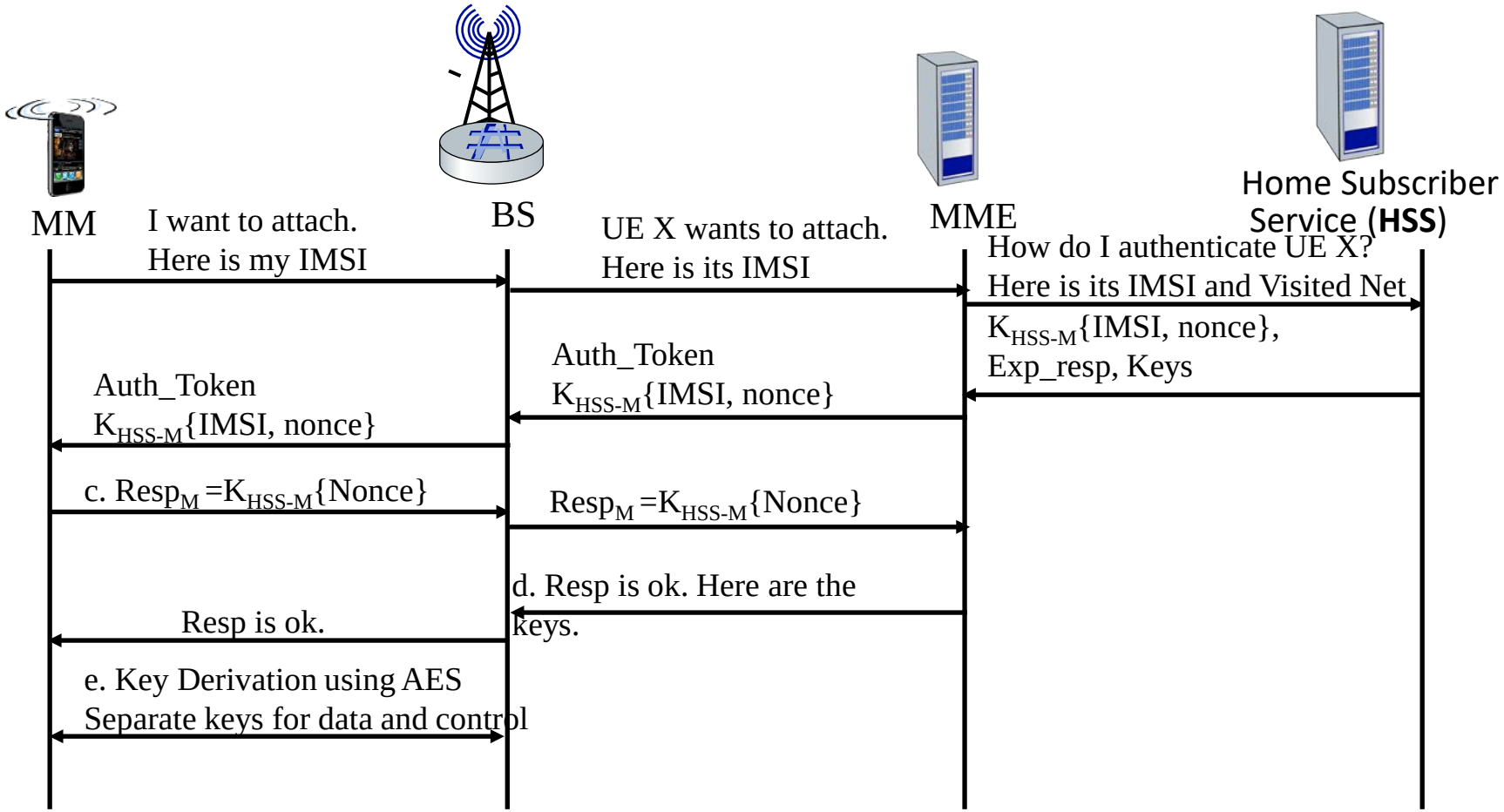
https://www.netspotapp.com/blog/wifi-security/what-is-wpa3.html#What_is_WPA3

- What is WPA3?

It is a stronger version of WPA2 and is the current standard since 2020. It removes several weak components of WPA such as TKIP and uses stronger encryptions.

©2025 Raj Jain

Authentication and Key Management in 4G



- K_{HSS-M} is the secret shared by HSS and Mobile

Student Questions

- The answer to the quiz says that the MME serves as the authentication server in 4G, while the slides show that the MME serves as the authenticator and the HSS servers as the authentication server. Which one is correct?

HSS is the authentication server. The quiz has been corrected to give points to either answer.

- What is the function of Keys from HSS?

These are nonces that are used in key derivation.

- What is Exp_resp?

Expected Response

- Could you please re-explain this diagram?

Sure.

©2025 Raj Jain

Authentication and Key Management in 5G

- Several options:

1. Same as in 4G
2. 4G scheme implemented using EAP. So the authenticator does not know the secret or the algorithm.
3. IoT device authentication. No pre-shared keys.
4. Use Public Key so IMSI is not transmitted in clear text.

Student Questions

- Book Page 666: What are the new authentication and key agreement protocols used in 5G? How do they differ from 4G protocol?

Beyond the scope of this course.

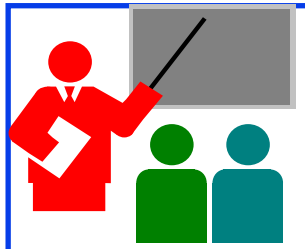
- How are SIM cards hacked, i.e., what kind of software/hardware is needed to read/write one?

Beyond the scope of this course.

- What kind of trouble does not sending IMSI out in the open over 5G save us from?

IMSI is your phone's social security number (ID).

©2025 Raj Jain



Review: Wireless Security

1. RADIUS allows the use of centralized authentication servers.
2. EAP allows authenticators not to know the secrets or the algorithm.
3. Wi-Fi's initial security using WEP failed and resulted in several inventions in authentication and key management
4. WPA2 used stronger encryption, dynamic keys, and several keys derived from the shared secrets. It also used the RSA algorithm in place of RC4
5. In 4G/5G, HSS serves as the authentication server and MME as an authenticator
6. In 5G, additional methods for IoT have been introduced. Also, EAP is allowed.

Review Section 8.8 and do R19 through R27

Student Questions

- Are signed and encrypted emails used often in the corporate world?

Yes. Some people sign their messages by default.

End of Part 3

©2025 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

©2025 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

©2025 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

©2025 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

©2025 Raj Jain

Scan This to Download These Slides



Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse473-25/i_8sec.htm

Student Questions

- Would you please clarify the range of Exam 3?

All sections are mentioned at the bottom of summary slides in Chapters 7 and 8.

- When would I receive the total grade?

Along with all other grades. Two weeks after Exam 3.

©2025 Raj Jain

Scan This to Download These Slides



Raj Jain
http://rajjain.com

http://www.cse.wustl.edu/~jain/cse473-25/i_8sec.htm

Student Questions

©2025 Raj Jain

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

©2025 Raj Jain