Security 2021 Midterm

1. Types of Malicious Software (5)

a. Zombie
   A program that secretly takes over another Internet-attached computer and then uses that computer to launch attacks that are difficult to trace to the zombie's creator
b. Worm
   Unwanted program that replicates itself in multiple locations on the disk or across network connection
c. Virus
   Piece of software that infects programs
d. Trojan Horses
   Attractive program with hidden side-effects (like a game or upgrade)
e. Logic Bombs
   Embedded code into some program, triggered when specific condition is met
f. Trapdoors
   Secret entry point into a program

2. What types of attacks prevented by Message Authentication? (or Message Authentication Requirements should be preventing these attacks)

a. Masquerade
   Insertion of message into the network from a fraud source
b. Content Modification
   Change in content of the message (data)
c. Sequence Modification
   Change in sequence of data sent
d. Timing Modification
   Change in timing of sent data. Like capturing a sent message, and forwarding it at a later time

3. Phases of the Virus & describe each

a. Dormant: The virus is idle. Waiting for some event to occur.
b. Propagation: The virus copies itself into other programs or into the system disk.
c. Triggered: Virus is activated by some event.
d. Execution: Virus function is being executed, doing what it was supposed to do, whether harmless or not.

4. Draw DES Round

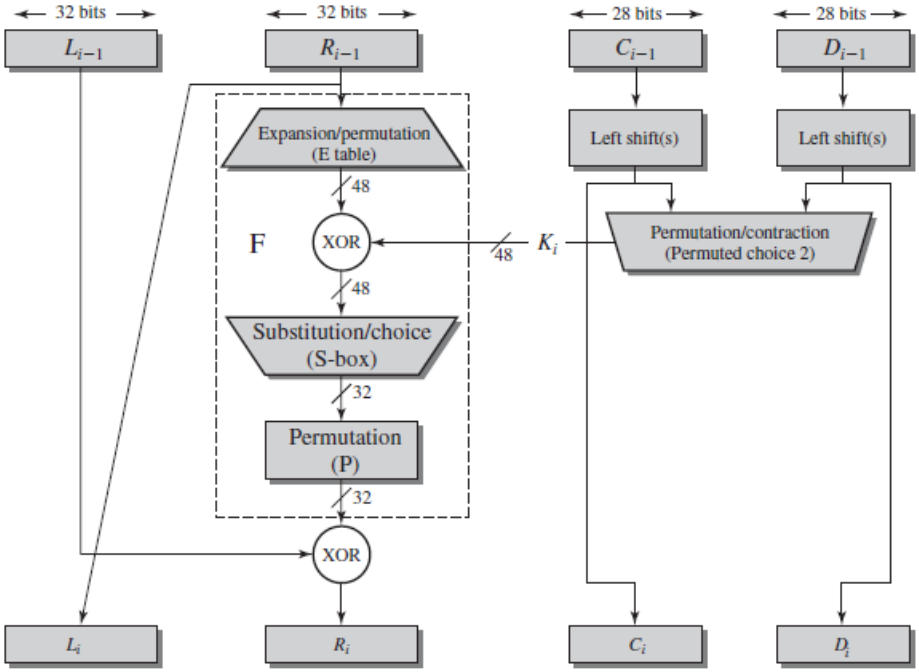


Figure 3.6 Single Round of DES Algorithm

5. Hash Function requirements

a. Variable Input: Any input data size should be valid
b. Fixed Output Length: Output of H should have a fixed size
c. Efficiency: H(x) should be relatively easy to compute, both software and hardware should be practical and applicable
d. Preimage resistant: For any hash value h, it's computationally infeasible to find y such that H(y) = h
e. Second preimage resistant: Given x, It's computationally infeasible to find y != x, and H(x) = H(y)
f. Collision resistant: It's computationally infeasible to fine any pair(x, y) such that H(x) = H(x)
g. Pseudorandomness: Output of H meets standard tests for psuedorandomness

6. Authentication Requirements

a. Protects message integrity
b. Validates identity of originator
c. Provides non-rejection of origin

7. Describe SSL services in one sentence

A web security mechanism, implemented at the transport layer.

8. Draw SSL Protocol Stack (architecture?)

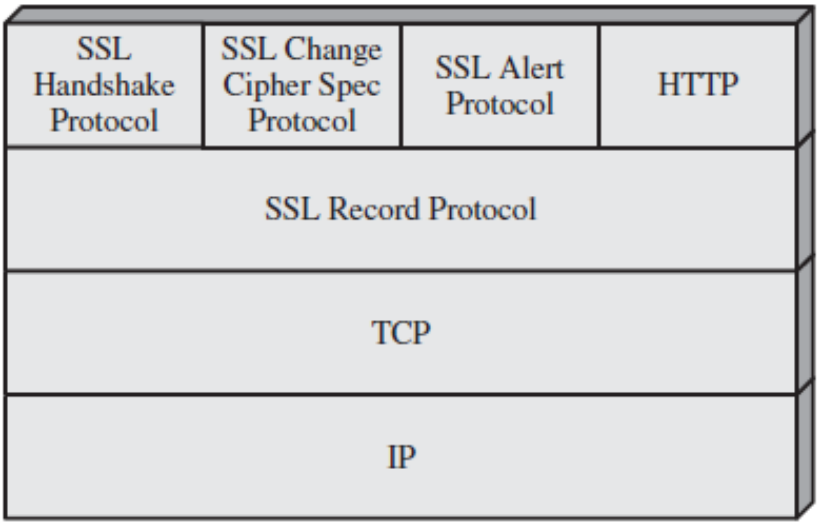


Figure 16.2 SSL Protocol Stack

9. Write Operations of SSL record protocol

Fragment
Compress
Add MAC
Encrypt
Append SSL Record Header

10. SSL security records & its security services

Confidentiality
Message integrity

11. Provide Function for each of:

a. **SSL Alert:** Conveys SSL-related alerts to peer entity
b. **SSL Handshake:**
   Allows server & client to authenticate each other, negotiate encryption & MAC algorithms, and cryptographic keys to be used
c. **SSL Cipher Change:** Cause the pending state to be copied into the current state, which updates the cipher suite to be used on this connection

12. Compare Between:

a. Stream & Block Cipher

Stream cipher: Ciphertext output is produced bit-by-bit, or byte-by-byte from a stream plaintext input.

Block Cipher: Ciphertext output is produced in blocks, parallel or in series. Plaintext is considered in blocks too.

b. Diffusion & Confusion

Diffusion: Considers statistical structure of plaintext over bulk of ciphertext

Confusion: Makes relationship between ciphertext and key as complex as possible.

c. Steganography & encryption

Steganography: Hiding the message in some way so it's invisible to direct sight, like using an invisible ink.

Encryption: Encrypting a message so it won't be understandable, but plainly visible.

d. Active & Passive Attacks

Activate Attacks: They capture the message and reply later

Passive Attacks: They can only read the messages sent but changes nothing

e. Monoalphabetic & Polyalphabetic encryption

Monoalphabetic: The relationship between a character in the plain text and the characters in the cipher text is one-to-one.

Polyalphabetic: The relationship between a character in the plain text and the characters in the cipher text is one-to-many.

f. SSL Connection & SSL Session

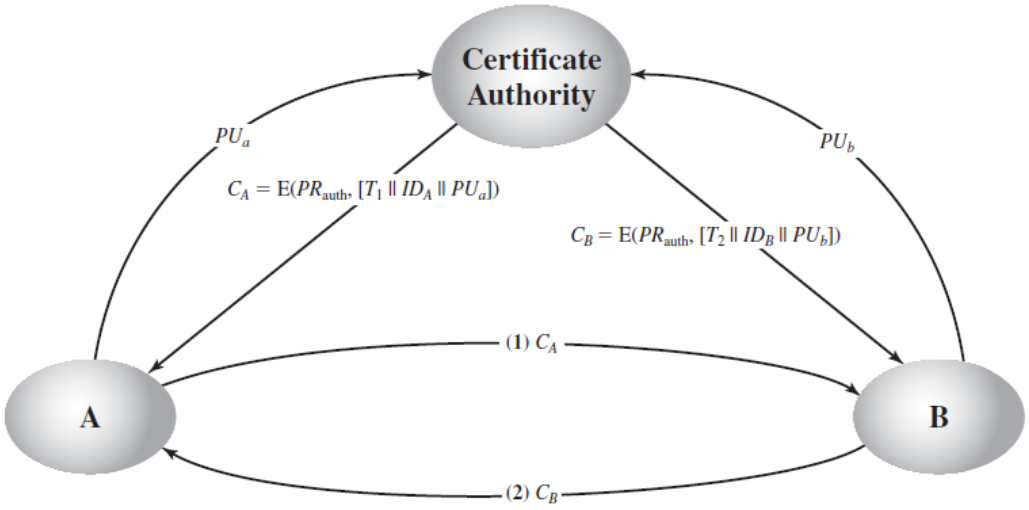
SSL connection: A transport that provides a suitable type of service. In SSL, they are Peer-to-Peer relationship. The connection is transient, and each connection is associated with one session.

SSL session: An association between a client and a server. Sessions are created by Handshake Protocol. And are defined as set of cryptographic.

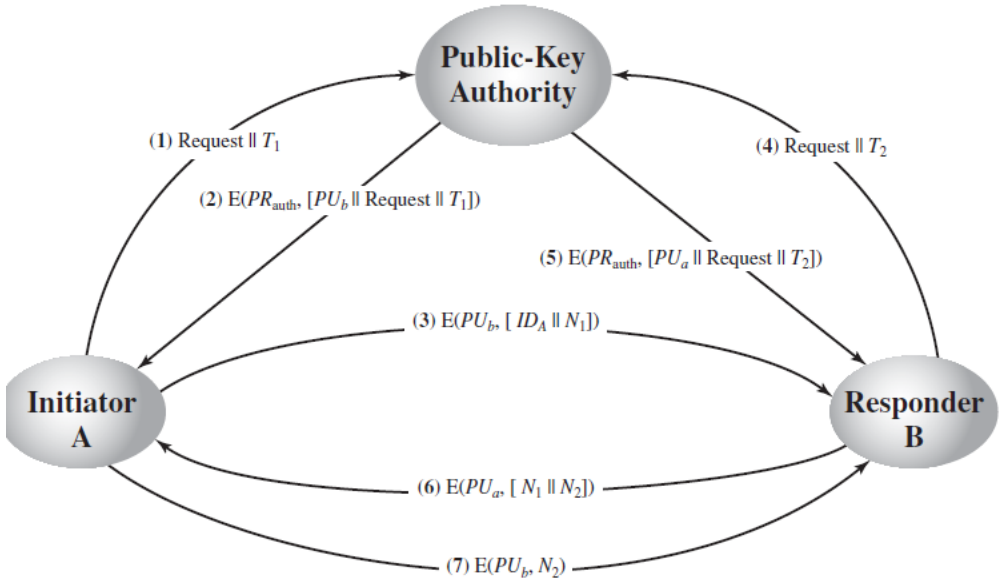
13. List 4 requirements needed in any certificate issued by a certificate authority

a. Any participant can read a certificate to determine the name and the public key of the certificate owner
b. Any participant can verify that the certificate originated from the certificate authority and not a counterfeit
c. Any participant can verify that currency of the certificate
d. Only the certificate authority can create or update certificates

14. Draw Certificate Authority Diagram



15. Draw Public-key authority diagram



16. True & False:

a. **Alice is sending a message to Bob using asymmetric encryption. She will encrypt using Alice's public Key.** (False)
b. **In asymmetric encryption, both encryption and decryption use the same key.** (False)
c. **Ceasar cipher is considered polyalphabetic cipher** (False ... monoalphabetic cipher)
d. **If a plain text is successfully hashed, then its confidentiality is ensured** (False)
e. **Block ciphers encryption modes used in stream ciphers** (True ... not sure, bs I mean the part CFB where it's considered both block or stream)

f. **In symmetric key encryption we use public channel for key exchange** (True)
g. **Digital Signature can be verified using sender's public key** (True)
h. **Properly used, a MAC provide both confidentiality and Integrity** (True)

17. Define:

a. **One-way function**
   The system stores the value of the function of the user's password only, and when the user enters his password, the system compares the function's value to the one previously stored, without needing to store the password itself or comparing it.
   OR
   It's one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible.
b. **Authorization**
   Granting access to specific services and/or resources based on the authentication

18. [MCQ] Which of the following are Reducible in GF(2):

a. **X3 + X2 + 1**
b. **X3 + X + 1**
c. **None**
d. **All of Above**

19. Certificate Authority verify/authenticate (I don't get what is the question)

a. **Hash Function**
b. **Public Key**
c. **Shared Key in session key**
d. **Digital Signature**

20. [MCQ] p and q for RSA are ...

a. **coprime**
b. **primes**
c. **all of the above**
d. **none of the above**

21. MCQ: Which is false about ECB

a. **used in short data**
b. **encryption can be executed in parallel**
c. **[illegible]ks can be repeated or swapped without being noticed by the receiver**
d. **none of the above**

22. Which 2 encryption mode permits the block cipher encryption function to be called before the data is available?

OFB & CTR

23. DES Cipher consists of 16 rounds

24. Which DES is used operating short data?

ECB

25. Round key is … bit, and round input is … bit

56 … 64 (m4 3rfa hna l round key yt2al eno 56 or 48)

26. In block cipher operations, during the transmission of C3 (the third cipher block) an error in the 5th bit occurred. How many plaintext blocks will be affected, if we are using:

a. **16-bit CFB mode? Explain why?**

   Assuming block size is 64, Number of blocks affected after P3 = 64/16 = 4
   Total number of affected blocks are 5 (P3, P4, P5, P6, and P7)
   This happened due to the shift register in the CFB

b. **8-bit OFB mode? Explain Why?**

   P3 only, because in OFB, encryption output is the one forwarded to the following block and not the cipher block.

27. Additive inverse of 15 mod 17

17 – 15 = 2

28. For a short message, which is best to use for encryption/decryption:

a. **OFB**
b. **CBC**
c. **CFB**
d. **ECB**

29. GCD of 1234 and 4321

GCD	Q	R
GCD(4321, 1234)	3	619
GCD(1234, 619)	1	615
GCD(619, 615)	1	4
GCD(615, 4)	153	3
GCD(4, 3)	1	1
GCD(3, 1)	3	0