



開始於 2021年 06月 21日(一) 15:30

作答狀態 已經完成

完成於 2021年 06月 21日(一) 17:30

所用時間 2 小時

分數 得**89.83**分(滿分為100.00分)

試題**1**

答對

得分 2.00/配分2.00

In order to support multiple application processes, what are the 4-tuples used as a TCP demux key?

單選或多選：

- ☐ a. destination web address
- ☒ b. source port number ✓
- ☐ c. destination MAC address
- ☒ d. destination IP address ✓
- ☒ e. destination port number ✓
- ☐ f. source MAC address
- ☒ g. source IP address ✓

你答對了!

正確答案： source port number, destination port number, source IP address, destination IP address

試題2

答對

得分 2.00/配分2.00

How does TCP compute AdvertisedWindow for flow control

單選：

- ☐ a. $\text{MaxSendBuffer} - (\text{LastByteWritten} - \text{LastByteAcked})$
- ☒ b. $\text{MaxRcvBuffer} - (\text{NextByteExpected} - 1 - \text{LastByteRead})$ ✓
- ☐ c. $\text{LastByteSent} - \text{LastByteAcked}$
- ☐ d. $\text{MaxRcvBuffer} - (\text{LastByteRcvd} - \text{LastByteRead})$

你答對了!

正確答案： $\text{MaxRcvBuffer} - (\text{NextByteExpected} - 1 - \text{LastByteRead})$

試題3

答對

得分 2.00/配分2.00

Suppose that the CongestionWindow of a TCP connection is 8 when a timeout occurs. What is the updated CongestionWindow for TCP with fast recovery?

單選：

- ☐ a. 16
- ☒ b. 4 ✓
- ☐ c. 7
- ☐ d. 1

你答對了!

正確答案：4

試題4

答錯

得分 0.00/配分2.00

Suppose that the CongestionWindow of a TCP connection is 8 when an ACK arrives. What is the updated CongestionWindow for TCP in the slow start mode?

單選：

- ☐ a. 7
- ☐ b. 10
- ☒ c. 16 ✖
- ☐ d. 9

你答錯了!

正確答案：9

試題5

答對

得分 2.00/配分2.00

What is the main reason for TCP to estimate RTT?

單選：

- ☐ a. EffectiveWindow
- ☒ b. Timeout ✔
- ☐ c. CongestionWindow
- ☐ d. AdvertisedWindow

你答對了!

正確答案：Timeout

試題6

答錯

得分 0.00/配分2.00

What are the flags used for a normal TCP connection setup?

單選或多選：

- ☒ a. SYN ✓
- ☒ b. RESET ✗
- ☐ c. ACK
- ☐ d. URG
- ☒ e. FIN ✗

你答錯了!

正確答案： SYN, ACK

試題7

答對

得分 2.00/配分2.00

When should Nagle's self-clocking algorithm be turned off?

單選：

- ☐ a. emails
- ☐ b. bank transactions
- ☒ c. online gaming ✓
- ☐ d. web browsing

你答對了!

正確答案： online gaming

試題8

答對

得分 2.00/配分2.00

What does RED do when a packet arrives and AvgLen is not greater than MinThreshold?

單選：

- ☐ a. drop the packet
- ☐ b. drop the packet with a certain probability
- ☒ c. enqueue the packet ✓

你答對了!

正確答案：enqueue the packet

試題9

答對

得分 2.00/配分2.00

What is the main objective of TCP flow control?

單選：

- ☐ a. guarantee flow rate
- ☐ b. avoid congestion in the network
- ☐ c. correct packet errors
- ☒ d. not to overrun the receiver ✓

你答對了!

正確答案：not to overrun the receiver

試題10

答對

得分 2.00/配分2.00

Since TCP is full-duplex, what the two main fields in a TCP header are needed in order to keep packets to be transmitted and received in-order?

單選或多選：

- ☒ a. Acknowledgment ✓
- ☒ b. SequenceNum ✓
- ☐ c. Checksum
- ☐ d. AdvertisedWindow

你答對了!

正確答案： SequenceNum, Acknowledgment

試題11

答對

得分 2.00/配分2.00

Nonce is a number that is used once. It is to protect the playback attack.

選擇一個：

- ☒ 是 ✓
- ☐ 非

正確答案為"是"

試題**12**

答對

得分 2.00/配分2.00

There are three kinds of frames in MPEG. Which one of them can be decoded independently?

單選：

- ☐ a. B frames
- ☐ b. P frames
- ☒ c. I frames ✓

你答對了!

正確答案：I frames

試題**13**

答對

得分 3.00/配分3.00

Suppose seven frames encoded by MPEG are I, B, B, P, B, B, and I frames. What is the sequence that these seven frames are transmitted?

單選：

- ☐ a. I B B P B B I
- ☐ b. I B B I B B P
- ☒ c. I P B B I B B ✓
- ☐ d. I I P B B B B

你答對了!

正確答案：I P B B I B B

試題14

答對

得分 5.00/配分5.00

Suppose a DNS server contains the following records:

(cs.princeton.edu, gnat.cs.princeton.edu, NS, IN)
(ee.princeton.edu, helios.ee.princeton.edu, NS, IN)
(gnat.cs.princeton.edu, 192.12.69.5, A, IN)
(helios.ee.princeton.edu, 128.196.28.166, A, IN)
(jupiter.physics.princeton.edu, 128.196.4.1, A, IN)
(saturn.physics.princeton.edu, 128.196.4.2, A, IN)
(mars.physics.princeton.edu, 128.196.4.3, A, IN)
(venus.physics.princeton.edu, 128.196.4.4, A, IN)

Suppose a request for the resolution of saturn.ee.princeton.edu.
What is the response of the DNS?

單選：

- ☐ a. Do nothing
- ☒ b. It sends a pointer to another name server ee.princeton.edu with the IP address 128.196.28.166 of that name server. ✓
- ☐ c. It sends a pointer to another name server cs.princeton.edu with the IP address 192.12.69.5 of that name server.
- ☐ d. It sends the resolved IP address 128.196.28.161

你答對了!

正確答案：It sends a pointer to another name server ee.princeton.edu with the IP address 128.196.28.166 of that name server.

試題**15**

答對

得分 2.00/配分2.00

HTTP 1.0 uses persistent TCP connections to fetch objects. On the other hand, HTTP 1.1 uses non-persistent TCP connections for the entire HTTP session.

選擇一個：

- ☐ 是
- ☒ 非 ✓

正確答案為"否"

試題16

答對

得分 5.00/配分5.00

Consider two (publicly known) parameters 2 and 5 for the Diffie-Hellman key agreement

(2 is the generator of the group $\{1,2,3,4\}$). Suppose Bob selects 3 as his secret number and Alice selects 2 as her secret number.

單選或多選：

- ☒ a. Bob sends 3 to Alice. ✓
- ☐ b. The common secret number (key) is 3.
- ☒ c. Alice sends 4 to Bob. ✓
- ☐ d. Bob sends 2 to Alice.
- ☐ e. Alice sends 3 to Bob.
- ☒ f. The common secret number (key) is 4. ✓

你答對了!

正確答案： Alice sends 4 to Bob., Bob sends 3 to Alice., The common secret number (key) is 4.

試題17

答對

得分 5.00/配分5.00

A sequence of data contains five symbols A, B,C,D, and E.
Suppose that A appears in the data with probability 0.3,
B appears in the data with probability 0.25,
C appears in the data with probability 0.2,
D appears in the data with probability 0.15, and
E appears in the data with probability 0.1.
Use the Huffman coding to represent these five symbols.
The average number of bits per symbol is

單選：

- ☐ a. 2.00
- ☒ b. 2.25 ✓
- ☐ c. 3.00
- ☐ d. 2.50
- ☐ e. 2.15

你答對了!

正確答案：2.25

試題**18**

答對

得分 5.00/配分5.00

Consider the following LZ encoded binary sequence

0001000000110101100001000010

Suppose the indexes are encoded using 3 bits. Please decode it to find the original sequence.

單選：

- ☐ a. 1011010100110
- ☒ b. 1011010100010 ✓
- ☐ c. 1011010100011
- ☐ d. 1011010101010

你答對了!

正確答案：1011010100010

試題19

答對

得分 5.00/配分5.00

Suppose that there are two flows sharing one unit of bandwidth. Packet 1 of flow 1 arrives at time 0 and its packet length is 5 (units of bandwidths), i.e., it takes 5 units of time to transmit this packet. Packet 2 of flow 1 arrives at time 2 and its packet length is 6. Packet 1 of flow 2 arrives at time 1 and its packet length is 8. Find the packet departure times of these three packets under the **fair queueing** policy.

單選或多選：

- ☒ a. Packet 1 of flow 2 departs at time 13. ✓
- ☐ b. Packet 1 of flow 1 departs at time 4.
- ☐ c. Packet 2 of flow 1 departs at time 18.
- ☒ d. Packet 1 of flow 1 departs at time 5. ✓
- ☒ e. Packet 2 of flow 1 departs at time 19. ✓

你答對了!

正確答案：Packet 1 of flow 1 departs at time 5., Packet 1 of flow 2 departs at time 13., Packet 2 of flow 1 departs at time 19.

試題**20**

答對

得分 10.00/配分
10.00

Consider two primes $p=5$ and $q=7$ for the RSA algorithm. Choose an encryption key $e=7$. Consider a message $M=3$.

單選或多選：

- ☐ a. The decryption key $d=8$.
- ☒ b. The encrypted message C for M is 17. ✓
- ☐ c. The decryption key $d=6$.
- ☐ d. The encrypted message C for M is 13.
- ☒ e. The decryption key $d=7$. ✓
- ☐ f. The encrypted message C for M is 19.

你答對了!

正確答案：The decryption key $d=7$., The encrypted message C for M is 17.

試題**21**

部分答對

得分 1.33/配分2.00

Please select the correct statements for RSVP.

單選或多選：

- ☒ a. The RESV message contains the Tspec and Rspec. ✓
- ☐ b. The source sends the PATH message with Rspec to receivers.
- ☐ c. The RESV message is used for reserving resource for a receiver.
- ☒ d. RSVP is a resource reservation protocol. ✓

你的答案是部分答對

你答對了 2題。

正確答案： RSVP is a resource reservation protocol., The RESV message contains the Tspec and Rspec., The RESV message is used for reserving resource for a receiver.

試題**22**

答對

得分 2.00/配分2.00

Please select the correct statements.

單選或多選：

- ☐ a. Admission control is to decide whether a packet should be admitted.
- ☐ b. Policing is to determine whether a flow violates the flow specification.
- ☒ c. Admission control is to decide whether a flow should be admitted. ✓
- ☒ d. Policing is to determine whether a packet violates the flow specification. ✓

你答對了!

正確答案： Admission control is to decide whether a flow should be admitted., Policing is to determine whether a packet violates the flow specification.

試題**23**

答錯

得分 0.00/配分5.00

Suppose that the RTT of a TCP connection is 100ms. Each TCP segment is 1500 bytes.

The segment drop probability is 0.0001. Use the TCP equation to compute the throughput of this TCP connection,

單選：

- ☐ a. 16.68Mbits/sec
- ☐ b. 14.64 Mbits/sec
- ☐ c. 10 Mbits/sec
- ☒ d. 12 Mbits/sec ❌

你答錯了!

正確答案：14.64 Mbits/sec

試題**24**

部分答對

得分 1.50/配分2.00

Select the correct statements

單選或多選：

- ☒ a. The RTP standard actually defines a pair of protocols: RTP and RTCP ✓
- ☒ b. RTCP uses feedback data for rate-adaptive applications ✓
- ☐ c. RTP uses timestamps for synchronization
- ☒ d. RTP is on top of UDP ✓

你的答案是部分答對

你答對了 3題。

正確答案： RTP is on top of UDP, The RTP standard actually defines a pair of protocols: RTP and RTCP, RTCP uses feedback data for rate-adaptive applications, RTP uses timestamps for synchronization

試題**25**

答對

得分 2.00/配分2.00

Please select the correct statements

單選或多選：

- ☒ a. The home agent uses IP tunneling to deliver the packet to the foreign agent ✓
- ☒ b. The foreign agent delivers the packet to the hardware address of the mobile node ✓
- ☒ c. There might be triangle routing ✓
- ☐ d. The home agent intercept packets by impersonating the mobile node via TCP

你答對了!

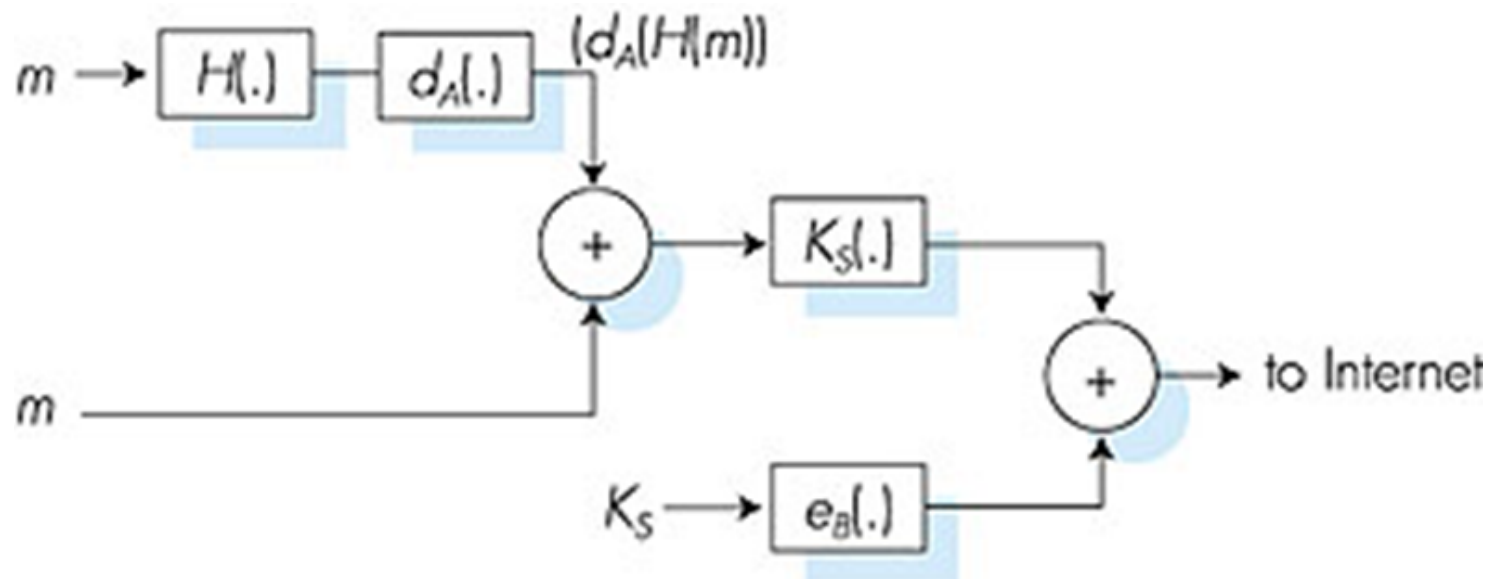
正確答案： The home agent uses IP tunneling to deliver the packet to the foreign agent,
The foreign agent delivers the packet to the hardware address of the mobile node,
There might be triangle routing

試題26

答對

得分 4.00/配分4.00

Consider the operations of PGP for sending an email from Alice to Bob. Assume that the public keys are available to each other. The email consists of two parts: one is a session key encoded by Bob's public key, and the other part, encoded by the session key, is the message and a digital signature signed by Alice.



Select the correct statements.

單選或多選：

- ☒ a. The email is digitally signed by Alice, i.e., Alice uses her private key to encode the message digest of the email. ✓
- ☐ b. Only Bob can use his public key to decode the session key
- ☒ c. PGP provides confidentiality, authentication and non-repudiation, and data integrity ✓
- ☒ d. If the two message digests are identical, then it must be Alice who sent the email and the email has not been altered. ✓

你答對了!

正確答案：The email is digitally signed by Alice, i.e., Alice uses her private key to encode the message digest of the email., If the two message digests are identical, then it must be Alice who sent the email and the email has not been altered., PGP provides confidentiality, authentication and non-repudiation, and data integrity

試題**27**

答對

得分 2.00/配分2.00

Select the services that use IP tunneling

單選或多選：

- ☒ a. IPSEC ✓
- ☒ b. Overlay networks ✓
- ☒ c. VPN ✓
- ☒ d. Mobile IP ✓

你答對了!

正確答案：Overlay networks, Mobile IP, IPSEC, VPN

試題**28**

答對

得分 2.00/配分2.00

Please select correct statements

單選或多選：

- ☐ a. The 52 upper- and lower-case letters, the 10 digits 0 through 9, and the special characters + and -
- ☒ b. Each 6-bit piece maps onto one of 64 valid ASCII characters ✓
- ☐ c. Base64 maps every two bytes of the original binary data into four ASCII characters
- ☒ d. MIME uses a straightforward encoding of binary data into the ASCII character set ✓

你答對了!

正確答案： MIME uses a straightforward encoding of binary data into the ASCII character set, Each 6-bit piece maps onto one of 64 valid ASCII characters

試題29

答對

得分 2.00/配分2.00

Please select the correct statements

單選或多選：

- ☒ a. IP spoofing is a security attack that transmit packets with false IP addresses. ✓
- ☒ b. The man-in-the-middle attack is an attacker who stays between two communicating users. ✓
- ☒ c. The attacker that uses the playback attack can record the encrypted message and play it back to a server. ✓
- ☒ d. DOS can use TCP SYNs (or other means) to jam a server ✓
- ☒ e. A packet sniffer is a program running in a network-attacked device that passively receives all data-link layer frames passing by the device's network interface. ✓

你答對了!

正確答案：IP spoofing is a security attack that transmit packets with false IP addresses., A packet sniffer is a program running in a network-attacked device that passively receives all data-link layer frames passing by the device's network interface., DOS can use TCP SYNs (or other means) to jam a server, The attacker that uses the playback attack can record the encrypted message and play it back to a server., The man-in-the-middle attack is an attacker who stays between two communicating users.

試題30

答對

得分 2.00/配分2.00

The RSA algorithm can be used for digital signature because the sender can use his private key to encrypt a digest and the receiver can use the public key of the sender to decrypt the coded message.

選擇一個：

- ☒ 是 ✓
- ☐ 非

正確答案為"是"

試題31

答對

得分 2.00/配分2.00

In JPEG, which step or steps will lose information?

單選：

- ☐ a. Encoding
- ☐ b. DCT
- ☒ c. Quantization ✓

你答對了!

正確答案：Quantization

試題**32**

答對

得分 2.00/配分2.00

Please select the correct statements

單選或多選：

- ☒ a. RIO can be used for AF ✓
- ☒ b. DiffServ code points (DSCP) is used to identify the PHB of packet ✓
- ☐ c. FIFO can be used for EF
- ☒ d. One of the main reasons for DiffServ is the scalability problem ✓

你答對了!

正確答案： One of the main reasons for DiffServ is the scalability problem, DiffServ code points (DSCP) is used to identify the PHB of packet, RIO can be used for AF

試題**33**

答對

得分 2.00/配分2.00

Please select correct statements.

單選或多選：

- ☐ a. SMTP runs on UDP
- ☒ b. SMTP uses ASCII ✓
- ☒ c. RFC 822 was extended in 1993 to allow email messages to carry many different types of data ✓
- ☒ d. SMTP is an application layer protocol ✓

你答對了!

正確答案：SMTP is an application layer protocol, RFC 822 was extended in 1993 to allow email messages to carry many different types of data, SMTP uses ASCII

試題**34**

答對

得分 2.00/配分2.00

Euler's totient function is defined as the number of positive integers that are less than n and relatively prime to n . Find the Euler's totient function for $n=91$.

單選：

- ☐ a. 91
- ☐ b. 70
- ☐ c. 80
- ☒ d. 72 ✓

你答對了!

正確答案：72

試題**35**

答對

得分 3.00/配分3.00

Suppose that the CongestionWindow of a TCP connection is 8 (MSS) when a TCP segment is received from the other end. The AdvertisedWindow of the received packet is 10 (MSS).

The LastByteSent pointer is at 15 (MSS) and the LastByteAcked pointer is at 11 (MSS).

單選：

- ☐ a. The EffectiveWindow is 2
- ☒ b. The EffectiveWindow is 4 ✓
- ☐ c. The EffectiveWindow is 8
- ☐ d. The EffectiveWindow is 6

你答對了!

正確答案：The EffectiveWindow is 4