浙江大学 2019–2020 学年 春 学期

《网络安全原理与实践》课程期末考查

课程号：21191581，开课学院：__计算机学院_____

诚信考试，沉着应考，杜绝违纪。

考生姓名：_____学号：_____所属院系：_____

题序	一 25	二 15	三 10	四 10	五 10	六 10	七 10	八 10	总 分
得分									
评卷人									

Answer table for Section One:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25					

一、(25 points)There are 25 questions or uncompleted statements in this section. Beneath every subject there are a few phrases or statements marked A, B, C, and D. Choose the statement that answers the question correctly, or the phrase that best completes the sentence. (***Please write your answers in above answer table.***)

( ) 1. The sequence of cryptography properties __, __, __, and __ offers protection of secrecy, accuracy, ascription, and liability, respectively.

A. Confidentiality, Integrity, Authentication, Non-repudiation
B. Confidentiality, Authentication, Non-repudiation, Integrity
C. Authentication, Confidentiality, Integrity, Non-repudiation
D. Non-repudiation, Authentication, Integrity, Confidentiality

( ) 2. Given a key of 10111011, what is the ciphertext of message 01101101 following OTP?

A. 00101001 B. 10111011 C. 11010110 D. 01101101

( ) 3. DES is a __ cipher with __-bit plaintext/ciphertext and __-bit key.

A. Stream, 128, 128 B. Block, 64, 56 C. Block, 64, 64 D. Stream, 56, 64

( ) 4. Which of the following items is not included in a root certificate?

A. CA Name B. Public Key C. Signature D. Issuer's CA Name

( ) 5. Consider when Alice and Bob secretly communicate using RSA. Alice's public key is (5, 14) and private key is (11, 14). If Bob wants to send a message of 3 to Alice, what is the ciphertext?

A. 243 B. 5 C. 4 D. 3

( ) 6. If you find this piece of code in a bitcoin blockchain: "scriptSig":"304502 042b2d…", what does the sequence 304502 mean?

A. Value of bitcoin
B. Signature of sender
C. Public key of sender
D. Public key of recipient

( ) 7. Given an attacker hijacking the communication channel of Alice and Bob, which of the following cases is not a successful MITM attack?

A. Alice and Bob use a shared key, the attacker eavesdrops the key.

B. Alice and Bob follow public key encryption and exchange their public keys, the attack eavesdrops both public keys.

C. Alice sends Bob shared key k1, the attacker replaces k1 with another key k2, which is sent to Bob.

D. Alice and Bob follow public key encryption. The attacker hijacks Alice's public key, and sends its own public key k_{pub} to Bob. Meanwhile, the attacker hijacks Bob's public key, and sends k_{pub} to Alice.

( ) 8. Towards a secure connection, the techniques of __, __, and __ are used to protect communication against eavesdropping, manipulation, and impersonation, respectively.

A. Encryption, Integrity (MAC), Signature
B. Signature, Encryption, Integrity (MAC)
C. Integrity (MAC), Signature, Encryption
D. Encryption, Signature, Integrity (MAC)

( ) 9. In blockchain, how many blocks to wait before accepting transactions in a block?

A. 5 B. 6 C. 8 D. 10

( ) 10. In a SERVER HELLO message of HTTPS, which of the following information is not necessarily included?

A. Session ID B. Server Certificate C. Client Certificate Request D. SSL Protocol Version

( ) 11. Which of the following properties is not provided by Proof of Stake?

A. Resistance to 51% attack
B. Resistance to double spending
C. Less computation than Proof of Work
D. None of the above

( ) 12. Among all delivery schemes, __ is the dominant form of message delivery on Internet, __ delivers a message to a group of nodes, and __ delivers a message to a group of nodes based on geographic location.

A. unicast, multicast, geocast
B. broadcast, anycast, multicast
C. multicast, unicast, anycast
D. anycast, multicast, geocast

( ) 13. Which of the following components is not part of the AES encryption?

A. SubBytes B. Whitener C. MixColumns D. AddRoundKey

( ) 14. The purpose of a server's certificate is to vouch for the __ key that is signed by the __ key and verified by the __ key.

A. server's private, server's pubic, CA's public
B. server's public, CA's private, CA's public
C. CA's public, CA's public, CA's public
D. server's public, server's private, server's pubic

( ) 15. Which layer should the routing information of an overlay network communication reside?

A. Data Link Layer B. Network Layer C. Transport Layer D. Application Layer

( ) 16. Which of the following statements about Triple DES is NOT correct?

A. Apply DES three times to each block.
B. Encryption keys K1, K2, K3 must be different with each other.
C. Runs slower than DES.
D. Number of iterations in the implementation is triple of DES.

( ) 17. Which of the following properties of wireless communication does not cause a higher security risk?

A. Broadcast Communication B. Limited Resource C. Higher Mobility D. Constrained Accessibility

( ) 18. In IEEE 802.11i, which of the following schemes requires additional hardware support to secure data transmission?

A. MPDU B. CCMP C. TKIP D. RC4

( ) 19. Which of the following entities does not involve in the authentication phase of 802.11i?

A. AP B. AS C. End Station D. STA

( ) 20. Which of the following statements is not a weakness of WEP?

A. STA does not authenticate to AP.
B. It uses only 24-bit IV in plaintext, which is vulnerable to cracking.
C. The adopted CRC for message integrity is an unkeyed function.
D. Week seeds used for RC4 cipher is more vulnerable to keystream cracking.

( ) 21. Which of the following statements is correct for blockchain and Bitcoin?

A. Each block contains only one transaction.
B. A user cannot transfer bitcoin to himself.
C. A transaction can have more than one recipient.
D. A transaction is accepted right after the block containing it is created.

( ) 22. Which of the following items is not included in a certificate?

A. Domain Name B. Private Key C. CA Signature D. Certificate Date

( ) 23. Which of the following protocols is not a WLAN protocol for security enhancement?

A. WEP B. HTTPS C. WPA D. WPA2

( ) 24. Which of the following schemes is effective against jamming attacks?

A. The sender and receiver use a highly secure encryption protocol to encrypt their messages.

B. The sender and receiver agree upon a pre-defined sequence of frequencies. During each time period, they use one of the frequencies for communication and use the next one in the next time period.

C. The sender and receiver use the distance bounding protocol to make sure that they are sufficiently close to each other upon communication.

D. The sender and receiver adopt a proxy to relay their messages. Meanwhile, they use also proxy re-encryption.

( ) 25. Which of the following operations is not involved in the operation flow of 802.11i?

A. Discovery B. Authentication C. Key exchange D. Data transfer

二、(15 points)

(1). What is the key difference between symmetric cryptography and asymmetric cryptography? Given that either of them can protect security, why should we still need both of them? Accordingly, how are they usually used in combination?

(2). Provide an example to showcase how a DNS hijacking attack works.

(3). Describe the two critical techniques that can be jointly used to protect network communication against replay attacks.
How do they mitigate replay attacks in combination?
What are their respective limitations?

三、**(10 points)**

(1). Describe an attack scenario of a relay attack over wireless communication. Use illustration to ease the explanation if necessary.

(2). How does the distance bounding protocol protect wireless communication against a relay attack?
What is the limitation of distance bounding?

四、(10 points)

(1). How does blockchain address double spending?

(2). What is the difference between proof of work and proof of stake?

五、(10 points)

(1). Given the four important fields in a certificate (Domain Name, Public Key, CA Name, and CA Signature), please describe the process of how to verify the certificate. (Note that additional information/certificate might be used for verification.)

(2). What are the two ways for a client to know whether a certificate is revoked or not?
What are the security drawback of Certificate Revocation List (CRL)-based validity check?

六、(10 points)

(1). Consider when Alice and Bob communicates via three relay routers A, B, and C using onion routing. The shared keys for Alice to communicate with A, B, and C are k_A, k_B, and k_C, respectively. Assume Alice plans to send a message msg to Bob. Let $E(msg)_k$ denote the encrypted msg using key k. Describe the content of the packet payload RECEIVED on each hop:

A	
B	
C	
Bob	

(2) Please describe the advantage and disadvantage of anonymizing proxy.

七、(10 points)

(1). What is the difference between a Rogue AP and an Evil Twin AP?

(2). Describe the process of WEP encryption and decryption.

八、(10 points = 6 + 4)

(1). Please draw the Feistel cipher per round with L_{I-1} and R_{I-1} as inputs and L_I and R_I as outputs.

(2). Please explain how S-box works in DES.

Wow, you made it! Thank you.