Contents

[1 王铁民 + 李茂川 2](#_Toc417329369)

[2 张楠 + 卜野 5](#_Toc417329370)

[3 胡志愷 + 何双 6](#_Toc417329371)

[4 张淳阳+ 陈怡斐 8](#_Toc417329372)

[5 肖瀚 + 王一如 9](#_Toc417329373)

[6 乔赫良+ 陈晓宇 11](#_Toc417329374)

[7 Clyde + 赵子懿 13](#_Toc417329375)

[8 吴真 +杨海钰 14](#_Toc417329376)

**Chapter 3, 43 questions**

**------------------------Owner for Q 1-30-------------------**

# 王铁民 + 李茂川

**1.**

**a.** Define cryptography.

**b.** What is confidentiality?

**c.** Distinguish between plaintext and ciphertext.

**d.** Which is transmitted across the network—the plaintext or the ciphertext?

**e.** What is a cipher?

**f.** What is a key?

**g.** What must be kept secret in encryption for confidentiality?

**h.** What is a cryptanalyst?

**2.** Complete the enciphering in Figure 3-2.

**3.**

**a.** Which leaves letters unchanged—transposition or substitution ciphers?

**b.** Which leaves letters in their original positions—transposition or substitution ciphers?

**4.** Complete the enciphering in Figure 3-3.

**5.**

**a.** In codes, what do code symbols represent?

**b.** What is the advantage of codes?

**c.** What are the disadvantages?

**6.** Finish encoding the message in Figure 3-4.

**7.**

**a.** Why is the word *symmetric* used in symmetric key encryption?

**b.** When two parties communicate with each other using symmetric key encryption, how many keys are used in total?

**c.** What type of encryption cipher is almost always used in encryption for confidentiality?

**8.**

**a.** What is the best way to thwart exhaustive searches by cryptanalysts?

**b.** If a key is 43 bits long, how much longer will it take to crack it by exhaustive search if it is extended to 45 bits?

**c.** If it is extended to 50 bits?

**d.** If a key is 40 bits long, how many keys must be tried, on average, to crack it?

**e.** How long must a symmetric encryption key be to be considered strong today?

**9.** Why is cryptography not an automatic protection?

**10.**

**a.** What are the two advantages of RC4?

**b.** Why is an RC4 key length of 40 bits commonly used?

**c.** Is this a strong key?

**11.**

**a.** How long is a DES key?

**b.** Is this a strong length?

**c.** Describe block encryption with DES.

**12.**

**a.** How does 3DES work?

**b.** What are the two common effective key lengths in 3DES?

**c.** Are these lengths strong enough for communication in corporations?

**d.** What is the disadvantage of 3DES?

**13.**

**a.** What is the big advantage of AES over 3DES?

**b.** What are the three key lengths offered by AES?

**c.** Which strong symmetric key encryption cipher can be used with small mobile devices?

**d.** Which symmetric key encryption cipher probably will dominate symmetric key encryption in the near future?

**14.**

**a.** It is claimed that new and proprietary encryption ciphers are good because cryptanalysts will not know them. Comment on this.

**b.** What is security through obscurity, and why is it bad?

**15.**

**a.** Distinguish between cryptography and cryptographic systems.

**b.** Distinguish between cryptographic systems and cryptographic system standards.

**c.** Why is the first handshaking stage the negotiation of security methods and options?

**d.** What is an impostor?

**e.** What is authentication?

**f.** What is mutual authentication?

**g.** Why is a secure keying phase necessary?

**16.**

**a.** What three protections do cryptographic systems provide on a message-by-message basis?

**b.** What is an electronic signature?

**c.** What two protections do electronic signatures usually provide?

**d.** Distinguish between the handshaking stages and ongoing communication.

**17.**

**a.** In SSL/TLS, what is a cipher suite?

**b.** Why do companies want to create policies that define security methods and options for a particular application that is used between corporate partners?

**18.**

**a.** In authentication, distinguish between the supplicant and the verifier.

**b.** What are credentials?

**c.** How many supplicants and verifiers are there in mutual authentication between two parties? Explain.

**19.**

**a.** In hashing, what is the hash?

**b.** Is encryption reversible?

**c.** Is hashing reversible?

**d.** Is hashing repeatable?

**20.**

**a.** Is MS-CHAP used for initial authentication or message-by-message authentication?

**b.** How does the supplicant create the response message?

**c.** How does the verifier check the response message?

**d.** What type of encryption does MS-CHAP use? (This is a trick question but an important one.)

**e.** In MS-CHAP, does the server authenticate itself to the client?

**21.**

**a.** When Alice sends a message to Bob, what key will she use to encrypt the message?

**b.** Why is “the public key” not a good answer to Question 21?

**c.** What key will Bob use to decrypt the message?

**d.** Why is “the private key” not a good answer to Question 21b?

**e.** In a classroom with 30 students and a teacher, how many public keys will there be?

**f.** How many private keys?

**22.**

**a.** What is the main drawback to public key encryption?

**b.** What is the most popular public key encryption cipher?

**c.** What is the other commonly used public key encryption cipher?

**d.** Which need to be longer—symmetric keys or public keys? Justify your answer.

**e.** How long are strong RSA keys?

**f.** How long are strong ECC keys?

**23.** Julia encrypts a message to David using public key encryption for confidentiality. After encrypting the message, can Julia decrypt it?

**24.** Explain how public key encryption can facilitate symmetric session key exchange.

**25.**

**a.** What is the purpose of Diffie–Hellman key agreement?

**b.** Can an attacker who captures the exchanged keying information compute the symmetric session key?

**26.**

**a.** In public key encryption for authentication, which key does the supplicant use to encrypt?

**b.** Does the verifier decrypt the ciphertext with the supplicant’s public key? (If not, explain what key it does use.)

**c.** Who is the true party?

**d.** What does the sender attempt to prove it knows that only the true party should know?

**27.**

**a.** In public key authentication, what must the sender know that an impostor should not be able to learn?

**b.** For what type of authentication is a digital signature used—initial authentication or message-by-message authentication?

**c.** How does the supplicant create a message digest?

**d.** How does the supplicant create a digital signature?

**e.** In public key encryption, what is “signing?”

**f.** What combined message does the supplicant send?

**g.** How is the combined message encrypted for confidentiality?

**h.** How does the verifier check the digital signature?

**i.** Does the verifier use the sender’s public key or the true party’s public key to test the digital signature?

**28.**

**a.** Besides authentication, what security benefit does a digital signature provide?

**b.** Explain what this benefit means.

**c.** Do most message-by-message authentication methods provide message integrity as a by-product?

**29.**

**a.** Contrast the key the sender uses for encryption in public key encryption for confidentiality and public key encryption for authentication.

**b.** Contrast the key the receiver uses for decryption in public key encryption for confidentiality and public key encryption for authentication. (Careful!)

**30.**

**a.** From what kind of organization can a verifier receive digital certificates?

**b.** Are most CAs regulated?

**c.** Does a digital certificate indicate that the person or firm named in the certificate is trustworthy?

Explain.

**------------------------Owner for Q 31-38-------------------**

# 张楠 + 卜野

**31.**

**a.** What are the two most critical fields in the digital certificate?

**b.** What field in a digital certificate allows the receiver of a certificate to determine if the certificate has been altered?

**c.** What three things must the receiver of a digital certificate check to ensure that a digital certificate is valid?

**d.** What are the two ways to check a certificate’s revocation status?

**32.**

**a.** Does a digital signature by itself provide authentication? Explain why or why not.

**b.** Does a digital certificate by itself provide authentication? Explain why or why not.

**33.**

**a.** What two cryptographic protections does an HMAC provide?

**b.** Do HMACs use symmetric key encryption, public key encryption, or hashing?

**c.** What is the benefit of HMACs over digital signatures?

**34.**

**a.** Why can’t HMACs provide nonrepudiation?

**b.** Why is it usually not a problem that HMACs fail to provide nonrepudiation?

**35.**

**a.** What is a replay attack?

**b.** Can the attacker read the contents of the replayed message?

**c.** Why are replay attacks attempted?

**d.** What are the three ways to thwart replay attacks?

**e.** How do time stamps thwart replay attacks?

**f.** How do sequence numbers thwart replay attacks?

**g.** How do nonces thwart replay attacks?

**h.** In what types of applications can nonces be used?

**36.**

**a.** What is quantum key distribution?

**b.** What are the two advantages of quantum key distribution?

**c.** Why is quantum key cracking a major threat to many traditional cryptographic methods?

**37.**

**a.** What is the definition of a VPN?

**b.** Why do companies transmit over the Internet?

**c.** Why do they transmit over untrusted wireless networks?

**d.** Distinguish between the three types of VPNs.

**e.** What does a VPN gateway do for a remote access VPN?

**f.** What does a VPN gateway do for a site-to-site VPN?

**g.** Which types of VPNs use VPN gateways?

**38.**

**a.** Distinguish between SSL and TLS.

**b.** For what type of VPN was SSL/TLS developed?

**c.** For what type of VPN is SSL/TLS increasingly being used?

**------------------------Owner for Q 39 - 46-------------------**

# 胡志愷 + 何双

**39.**

**a.** At what layer does SSL/TLS operate?

**b.** What types of applications can SSL/TLS protect?

**c.** What are the two commonly used SSL/TLS-aware applications?

**d.** Why is SSL/TLS popular?

**40.**

**a.** SSL/TLS was created for host-to-host (browser–webserver) communication. What device can turn SSL/TLS into a remote access VPN?

**b.** In SSL/TLS remote access VPNs, to what device does the client authenticate itself?

**c.** When a remote client transmits in an SSL/TLS VPN, how far does confidential transmission definitely extend?

**d.** What three services do SSL/TLS gateways commonly provide?

**e.** What is webification?

**f.** What software does the client need for basic SSL/TLS VPN operation?

**g.** For what purposes may the client need additional downloaded software?

**h.** Why installing the additional downloaded software on the browser may be problematic?

**i.** Why is SSL/TLS attractive as a remote access VPN technology?

**j.** What problems do companies face if they use it as a remote access VPN technology?

**k.** Which of the three types of VPNs can SSL/TLS support?

**41.**

**a.** At what layer does IPsec operate?

**b.** What layers does IPsec protect?

**c.** Compare the amount of cryptographic security in IPsec with that in SSL/TLS.

**d.** Compare centralized management in IPsec and SSL/TLS.

**e.** Why is IPsec’s transparent protection attractive compared with SSL/TLS’ nontransparent protection?

**f.** Which versions of IP can use IPsec?

**42.**

**a.** Distinguish between transport and tunnel modes in IPsec in terms of packet protection.

**b.** What are the attractions of each?

**c.** What are the problematic issues of each?

**43.**

**a.** What does an SA specify? (Do not just spell SA out.)

**b.** When two parties want to communicate in both directions with security, how many IPsec

SAs are necessary?

**c.** May there be different SAs in the two directions?

**d.** What is the advantage of this?

**e.** Why do companies wish to create policies for SAs?

**f.** Can they do so in SSL/TLS?

**g.** How does IPsec set and enforce policies?

**Chapter 4, 22 questions**

**1.**

**a.** Explain the four general goals for secure networking.

**b.** How can information be gathered from encrypted network traffic?

**c.** Give an example of how new technology has made networks less secure.

**d.** How does the castle model relate to secure networking?

**e.** What is meant by “death of the perimeter?”

**f.** How does the city model relate to secure networking?

**2.**

**a.** What is a denial-of-service attack?

**b.** Other than a DoS attack, what could cause a company’s webserver crash?

**c.** What are the main goals of DoS attacks?

**d.** Is a slow degradation of service worse than a total stoppage? Why?

**3.**

**a.** What is the difference between a direct and indirect DoS attack?

**b.** What is backscatter?

**c.** What types of packets can be sent as part of a DoS attack?

**d.** Describe a SYN flood.

**e.** How does a DDoS attack work?

**f.** What does a handler do?

**------------------------Owner for Q 4-11-------------------**

# 张淳阳 + 陈怡斐

**4.**

**a.** How does a P2P attack work?

**b.** How does a reflected attack work?

**c.** What is a DRDoS attack, and how does it work?

**d.** What is a Smurf flood?

**e.** What type of packet is sent in a Smurf flood? Why?

**f.** How could a malformed packet cause a host to crash?

**5.**

**a.** What is black holing?

**b.** Is black holing an effective defense against DoS attacks? Why?

**c.** How can the effects of SYN floods be mitigated?

**d.** What is a false opening?

**6.**

**a.** Why do hosts use ARP?

**b.** Can ARP poisoning be used outside the LAN? Why not?

**c.** Why do hosts send ARP requests?

**d.** What is ARP spoofing?

**e.** How could an attacker use ARP spoofing to manipulate host ARP tables?

**7.**

**a.** Explain ARP poisoning?

**b.** Why does the attacker have to send a continuous stream of unrequested ARP replies?

**c.** Do switches record IP addresses? Why not?

**d.** Does the attacker have to poison the gateway’s ARP tables too? Why?

**e.** Why does all network traffic go through the attacker after poisoning the network?

**8. a.** How can ARP poisoning be used as a DoS attack?

**b.** How can static IP and ARP tables be used to prevent ARP poisoning?

**c.** Can static IP and ARP tables be effectively used in large networks? Why not?

**d.** Why would limiting local access prevent DoS attacks?

**9.**

**a.** What is a SLAAC attack?

**b.** Why do host automatically prefer IPv6 addressing?

**c.** What has to be introduced to a network for a SLAAC attack to work?

**d.** Would a SLAAC attack work on an existing IPv6 network? Why not?

**e.** Could a rogue router direct internal traffic to an outside rogue DNS server? How?

**10.**

**a.** What is the main access control threat to Ethernet LANs?

**b.** What is the main access control threat to wireless LANs?

**c.** Why is the access control threat to wireless LANs more severe?

**d.** Is eavesdropping usually a concern for wired LANs, wireless LANs, or both?

**11.**

**a.** Why is 802.1X called Port-Based Access Control?

**b.** Where is the heavy authentication work done?

**c.** What are the three benefits of using a central authentication server?

**d.** Which device is the verifier? Explain. (Trick question.)

**e.** Which device is called the authenticator?

**------------------------Owner for Q 12-19-------------------**

# 肖瀚 + 王一如

**12.**

**a.** How does an EAP session start?

**b.** What types of messages carry requests for authentication information and responses to these requests?

**c.** Describe how the central authentication server tells the authenticator that the supplicant is acceptable.

**d.** How does the authenticator pass this information on to the supplicant?

**e.** In what sense is EAP *extensible*?

**f.** When a new authentication method is added, what device software must be changed to use the new method?

**g.** Why is there no need to change the operation of the authenticator when a new EAP authentication method is added or an old EAP authentication mode is dropped?

**h.** Why is this freedom from the need to make changes in the switch beneficial?

**13.**

**a.** What standard do most central authentication servers follow?

**b.** How are EAP and RADIUS related in terms of functionality?

**c.** What authentication method does RADIUS use?

**14.**

**a.** What is the most common attack against wireless networks? Why?

**b.** Which IEEE standard governs WLAN transmission?

**c.** Which device acts as a relay between wired and wireless networks?

**d.** What is the typical range of a WLAN?

**e.** What is the difference between an open network and a private network?

**f.** Who would set up a rogue access point? Why?

**g.** Give examples of both internal and external harm caused by unauthorized wireless access.

**h.** Are you liable if someone else uses your wireless network to commit a crime? Why, or why not?

**15.**

**a.** What man-in-the-middle attack is a danger for 802.11 WLANs?

**b.** Physically, what is an evil twin access point?

**c.** What happens when the legitimate supplicant sends credentials to the legitimate access point?

**d.** In what two types of attacks can the evil twin engage?

**e.** Are evil twin attacks frequent?

**f.** Where are they the most frequently encountered?

**g.** How can the danger of evil twin attacks be addressed?

**16.**

**a.** How would a wireless DoS attack be carried out?

**b.** What type of devices could be used to flood the transmission frequency for a WLAN?

**c.** What device could be used to identify a DoS flood if the entire frequency is being flooded by EMI?

**d.** What type of attack commands could be sent to cause a wireless DoS attack?

**e.** What would happen if a wireless network were flooded with CTS frames?

**17.**

**a.** Why is it impossible to extend 802.1X operation using EAP directly to WLANs?

**b.** What standard did the 802.3 Working Group create to extend 802.1X operation to WLANs with security for EAP?

**c.** For 802.11i, distinguish between outer and inner authentication.

**d.** What authentication method or methods does outer authentication use?

**e.** What two extended EAP protocols are popular today?

**f.** Distinguish between their options for inner authentication.

**g.** Is 802.11i security strong? Explain.

**18.**

**a.** What was the first core wireless security standard?

**b.** What encryption algorithm does it use?

**19.**

**a.** What prompted the Wi-Fi Alliance to create WPA?

**b.** Compare WPA and 802.11i security.

**c.** What does the Wi-Fi Alliance call 802.11i?

**d.** Despite its security weaknesses, why do many companies continue to use WPA instead of 802.11i?

**------------------------Owner for Q 20 – 22 + 1 – 5 in next chapter -------------------**

# 乔赫良+ 陈晓宇

**20.**

**a.** Why is 802.1X mode unsuitable for homes and small offices?

**b.** What mode was created for homes or very small businesses with a single access point?

**c.** How do users in this mode authenticate themselves to the access point?

**d.** Why is using a shared initial key not dangerous?

**e.** How are PSK/personal keys generated?

**f.** How long must passphrases be for adequate security?

**21.**

**a.** What is the purpose of a wireless IDS?

**b.** How do wireless IDSs get their data?

**c.** What is a rogue access point?

**d.** What are the two alternative to using a centralized wireless IDS?

**e.** Why are they not attractive?

**22.**

**a.** Does the use of spread spectrum transmission in 802.11 create security?

**b.** What are SSIDs?

**c.** Does turning off SSID broadcasting offer real security? Explain.

**d.** What are MAC access control lists?

**e.** Do they offer real security? Explain.

**Chapter 5 – 5.5, 21 questions**

**1. a.** List the AAA access controls.

**b.** Explain each in a sentence.

**c.** What are the four bases for authentication credentials?

**d.** What is two-factor authentication’s promise?

**e.** How can a Trojan horse defeat this promise?

**f.** How can a man-in-the-middle attack defeat this promise?

**g.** What is RBAC? (Do not just spell it out).

**h.** Why is RBAC less expensive than access control based on individual accounts?

**i.** Why is it less error-prone? (The answer is not specifically in the text.)

**j.** Why do technologically strong access controls not provide strong access control in real organizations?

**2.**

**a.** Distinguish between mandatory access controls and discretionary access controls.

**b.** What is multilevel security?

**c.** What are SBU documents?

**d.** Do they need to be considered in access controls?

**e.** Why are access control models needed?

**3.**

**a.** Why is having a single point of building entry important?

**b.** Why are emergency exits important?

**c.** What should be done about them?

**d.** List the four elements of entry authorization in CobiT.

**e.** Why is loading dock security important?

**f.** What access control rules should be applied to loading docks?

**g.** What steps should be taken to reduce the danger of environmental damage?

**h.** List rules for working in secure areas.

**4.**

**a.** What is siting?

**b.** Distinguish between UPSs and electrical generators.

**c.** If wiring cannot be run through walls, what should be done to protect the wiring?

**d.** What should be done to protect laptops taken off-premises?

**e.** What controls should be applied to off-site equipment maintenance?

**f.** What controls should be applied to equipment disposal or reuse?

**g.** What controls should be placed over employees taking equipment off-site?

**5.**

**a.** What special controls are required by terrorism threats?

**b.** Why is it necessary to prevent piggybacking?

**c.** What advice would you give a company about CCTV?

**d.** What is Dumpster™ diving?

**e.** How should trash bins be protected?

**f.** What can be done to reduce the dangers of desktop PC theft and unauthorized use?

**------------------------Owner for Q 6 – 13 -------------------**

# Clyde + 赵子懿

**6.**

**a.** What are reusable passwords?

**b.** Why is password cracking over a network difficult to do?

**c.** In what two ways can password-cracking programs be used?

**d.** Which is safer for the cracker? Why?

**7.**

**a.** Why is it a problem to use the same password at multiple sites?

**b.** Why is it difficult to enforce a policy of using a different password at each site?

**c.** Why are password duration policies important?

**d.** What are password resets?

**e.** Why are password resets dangerous?

**f.** How can password resets be automated?

**g.** Why are password reset questions difficult to create?

**h.** How may password resets be handled in high-risk environments?

**8.**

**a.** What is the book’s recommended password policy for length and complexity?

**b.** How can password-cracking programs be used to enforce password strength policy?

**c.** Before you run a password-cracking program on your company’s computers to check for weak passwords, what should you do?

**9.** What is the likely future of passwords?

**10.**

**a.** Distinguish between magnetic stripe cards and smart cards.

**b.** What are one-time-password tokens?

**c.** What are USB tokens?

**d.** What is the advantage of USB tokens compared to cards?

**e.** What is the attraction of proximity tokens?

**11.**

**a.** Why is it important to disable lost or stolen access devices?

**b.** Give an example of two-factor authentication not mentioned in the text.

**c.** What is a PIN?

**d.** Why can PINs be short—only four to six digits—while passwords must be much longer?

**12.**

**a.** What is biometric authentication?

**b.** On what two things about you is biometric authentication based?

**c.** What is the major promise of biometrics?

**13.**

**a.** Describe the three scanner actions in the enrollment process.

**b.** What are key features?

**c.** Why are they necessary?

**d.** What does the server do with the key features created by the enrollment scan?

**e.** What is a template?

**f.** What is user access data?

**g.** What are match indices, and how are they related to decision criteria?

**------------------------Owner for Q 14 – 21 -------------------**

# 吴真 + 杨海钰

**14.**

**a.** In biometrics, what is a match?

**b.** Distinguish between false acceptances and false rejections.

**c.** What are false acceptance rates (FARs) and false rejection rates (FRRs)?

**d.** For computer access, why is a false acceptance bad?

**e.** Why is a false rejection bad?

**f.** Which is worse from a security viewpoint?

**g.** Which is worse from a user acceptance viewpoint?

**15.**

**a.** For watch lists of criminals, what is a false acceptance?

**b.** For watch lists of criminals, which is worse from a security viewpoint, a false acceptance or a false rejection? Explain.

**c.** For watch lists of people who should be allowed to enter a room, which is worse from a security viewpoint, a false acceptance or a false rejection? Explain.

**16.** What is failure to enrol?

**17.**

**a.** Distinguish between verification and identification.

**b.** Which requires more matches against templates?

**c.** Which is more likely to generate a false acceptance? Why?

**d.** Compare identification with watch list matching.

**e.** Which is more likely to generate a false match? Why?

**18.**

**a.** Suppose that the probability of a false acceptance is one in a million, that there are

10,000 identities in the database, and that there is a watch list with 100 people. What will be the FAR for verification?

**b.** For identification?

**c.** For the watch list?

**19.**

**a.** Distinguish between error rates and deception in biometrics.

**b.** Why fingerprint scanning, which is often deceived, can be acceptable for entry into a supplies cabinet?

**c.** When it may not be sufficient?

**20.**

**a.** What is the advantage of fingerprint recognition?

**b.** What are the disadvantages?

**c.** For what type of use is fingerprint recognition sufficient?

**d.** What is the advantage of iris recognition?

**e.** What are the disadvantages?

**f.** Does iris scanning shoot light into your eye?

**21.**

**a.** What is the advantage of face recognition?

**b.** What does *surreptitious* mean?

**c.** Where is hand geometry recognition used?

**d.** What are the disadvantages of voiceprint recognition?

**e.** What are the most widely used forms of biometric authentication?

**f.** What is the most widely used form of biometrics?