Keys are marked with an "*".

CHAPTER 1

TEXTBOOK CHAPTER REVIEW QUESTIONS

1. Which can protect data through an *obscurity* solution?
A) Steganography *
B) Symmetric cryptography
C) Message authentication function
D) Hashing
E) Sponge function

2. The following are benefits of VPN EXCEPT:
A) VPN offers flexibility in forming and terminating secure connections over the Internet.
B) When an organization maintains a large contingent of mobile workers, telecommuters, or branch offices, cost savings could be significant.
C) VPN supports anytime, anywhere, and any-to-any accessibility.
D) VPN performance is unaffected by Internet congestions. *
E) VPN uses tunneling to securely transport IP packets.

3. Which is CORRECTLY paired between a VPN standard and its operational layer?
A) IPSec: internet, SSL: data link
B) IPSec: internet, SSL: application
C) IPSec: transport, SSL: data link
D) IPSec: internet, SSL: transport *
E) IPSec: transport, SSL: application

4. The four components of a cryptography system include the following EXCEPT:
A) plaintext
B) ciphertext
C) digital signature *
D) key value
E) encryption algorithm

5. The PKI (Public Key Infrastructure) is maintained and operated by _____.
A) governments
B) certificate authorities *
C) Internet engineering task force
D) Internet service providers
E) WAN service providers

6. When a digital signature is used for authentication, a session key can be utilized concurrently to _____.
A) generate a message digest by the sender
B) encrypt the original message and digital signature *
C) generate a digital signature by the sender

D) generate a digital signature by the receiver
E) generate a message digest by the receiver

7. Choose an ACCURATE statement on the asymmetric vs. symmetric key encryption.
A) In the asymmetric key encryption, both parties encrypt and decrypt messages using the same single key.
B) In the symmetric key encryption, each party should have two keys -- a public key and a private key.
C) In the asymmetric key encryption, only one key must be shared between communicating parties.
D) Symmetric keys are longer than asymmetric keys.
E) The asymmetric key encryption is slower than the symmetric key encryption. *

8. An applicant is sending an encrypted message with her/his digital signature appended. To authenticate the sender, the verifier (message receiver) uses a/the _____.
A) private key of the verifier
B) public key of the verifier
C) private key of the applicant
D) public key of the applicant *
E) session key

9. The X.509 standard defines information items to be included in the _____.
A) digital signature
B) digital certificate *
C) public key encryption
D) symmetric key encryption
E) message digest

10. The digital certificate _____.
A) is an alternative authentication method when encryption is unavailable
B) validates the owner of a particular public key *
C) delivers a private key to its owner
D) is a method to securely exchange session keys
E) is an electronic receipt of an online transaction

11. The digital signature attached to a message can authenticate _____.
A) both the message sender and the message itself *
B) the message sender only
C) the message only
D) both the message sender and receiver
E) both the message receiver and message itself

12. What type of cipher can take a character and replaces it with another character, working one character at a time?
A) stream cipher *
B) block cipher
C) Triple Data Encryption System (3DES)

D) RSA cipher
E) Elliptic Curve Cryptography (ECC)

13. Which is NOT a characteristic of hashing?
A) The results of a hash function should not be reversed as it is a one-way function.
B) The hash value of a particular standard (ex. MD5) should always be the same fixed size.
C) Collisions between two hash values of two different hash algorithms are normal. *
D) A message cannot be produced from a predefined hash value.
E) Hashing creates a unique digital fingerprint of data or message.

14. Which describes the transport mode of IPSec?
A) IPSec servers are placed at the boundary of local sites.
B) Hosts internal to a site are not aware of IPSec servers.
C) When a packet in transition is in a corporate network, it remains unencrypted.
D) It is a popular choice for implementing intranet-based site-to-site VPNs.
E) The data field of an IP packet is protected by encryption, but not the IP header. *

15. When Bob needs to send Alice a message with a digital signature, which two technologies can be used by the *Bob's device*?
A) SHA-512 and Alice's private key
B) SHA-512 and Bob's public key
C) MD5 and Bob' public key.
D) SHA-512 and Alice's public key
E) MD5 and Bob's private key *

16. Cryptography can be a tool for:
A) confidentiality and authentication
B) authentication and integrity
C) integrity and confidentiality
D) confidentiality, authentication, and integrity *
E) confidentiality

17. Which of the following uses an asymmetric cryptography?
A) Data Encryption Standard (DES)
B) Elliptic curve cryptography (ECC) *
C) Advanced Encryption Standard (AES)
D) Blowfish
E) Triple Data Encryption Standard (3DES)

18. Which system uses the hybrid approach that utilizes both symmetric and asymmetric cryptography technologies to make the most of their strengths?
A) RSA cryptography
B) Elliptic curve cryptography (ECC)
C) Triple Data Encryption Standard (3DES)
D) Advanced Encryption Standard (AES)
E) Pretty Good Privacy (PGP) *

19. The WPA standard has one major advantage over WAP2/WPA3. What can it be?
A) WPA offers stronger authentication than WPA2/WPA3.
B) WPA offers better a quality of service than WPA2/WPA3.
C) Wireless NICs that support WEP can be upgraded to WPA, but not to WPA2/WPA3. *
D) WPA has been standardized by IEEE but WPA2/WPA3 has not.
E) WPA is supported by more Wi-Fi standards including 802.11g and 802.11n than WPA2/ WPA3.

20. Which information may NOT be included in a digital certificate?
A) Owner's private key *
B) Issuer company
C) Expiration date
D) Name of its owner
E) Owner's public key

21. Which VPN requires additional purchase and installation of security software in user computers?
A) SSL in the tunnel mode
B) IPSec in the transport mode *
C) IPSec in the tunnel mode
D) IPSec in the site-to-site mode
E) SSL in the regular mode

22. The framework for all of the entities (e.g., software, hardware, roles, policies, protocols, procedures) involved in the digital certificate and asymmetric cryptography management is called:
A) certificate authority standards
B) certificate authority policy
C) public key infrastructure *
D) asymmetric cryptography Infrastructure
E) digital certificate management

23. _____ is a popular security standard built into web browsers.
A) SSH (Secure shell)
B) PPTP (point-to-point tunneling protocol)
C) SSL (Secure socket layer) *
D) SET (Secure electronic transaction)
E) IPSec (IP security)

24. Choose a CORRECT statement regarding VPN standards.
A) SSL offers the most secure VPN solution among available standards.
B) The IPSec's tunnel mode is more cost-effective to implement than its transport mode. *
C) Implementing the IPSec's tunnel mode requires software installation in each user computer.
D) The IPSec's security software is embedded in web browsers.
E) When SSL is combined with HTTP, the mutual authentication of both client and server is mandated.

25. When a person has a 20MB message to transmit electronically, how can she add a digital signature for sender authentication?
A) By scanning her handwriting signature
B) By encrypting the message with her own public key
C) By encrypting the message with her own private key
D) By encrypting the message digest with her own public key
E) By encrypting the message digest with her own private key *

TEXTBOOK HANDS-ON EXERCISES

Exercise 10.3

1. Whereas the pre-shared key is permanently used with WEP, it is dynamically changed periodically with WPA/WAP2/WPA3 making them much more difficult to break than WEP.
2. With the PSK mode, the authentication of a client host is performed by a wireless access point. In the enterprise mode, the host authentication is carried out by the central authentication server and the role of access point is merely relaying authentication information.
3. WPA is an interim solution for the ultimate migration to WPA2 (then WPA3) from WEP, and therefore WPA is not an official IEEE standard. Meanwhile, WPA2 is an official security standard known as IEEE 802.11i offering government grade security. Another difference between WPA and WPA2/3 is the preferred choice of authentication technology.
4. SSID and hosts MAC address
5. A popular standard protocol that enables the centralized authentication between hosts and the authentication server.
6. Use of passwords or passphrases
7. hosts and wireless access points
8. authentication and data encryption

ADDITIONAL TEST BANK QUESTIONS

Choose a CORRECT statement regarding the VPN (virtual private network) technology.
A) VPN generally costs high on network maintenance and administration.
B) VPN allows anywhere, anytime, and any-to-any connectivity because of the Internet's ubiquity.*
C) VPN lacks flexibility in adding suppliers or customers of a firm to its enterprise network.
D) VPN offers reliable quality of services (QoS) for mission-critical applications over the Internet.
E) VPN is generally safer than leased lines in transporting sensitive data.

When a company tries to connect its suppliers through site-to-site VPNs to exchange invoices electronically, the _____ standard would be the most secure choice.
A) PPTP
B) IPsec*

C) SSL
D) PPP
E) DES

When IPv6 is in full swing, _____ technology is expected to become a requirement to protect data communications.
A) PPTP
B) IPsec*
C) SSL
D) PPP
E) DES

When IPsec and SSL technologies are compared:
A) IPsec and SSL technologies are defined at the internet layer
B) IPsec software should be installed in each user station in the "tunnel" mode, but SSL software is built into the web browser.
C) SSL has higher overhead than IPsec in setup, maintenance and update.
D) SSL is considered as secure as IPsec.
E) IPsec is considered technically more complex than SSL in implementing VPN. *

When the IPsec standard is used for VPN, both communicating parties exchange a(n) _____ for mutual authentication.
A) digital certificate *
B) digital signature
C) IPsec gateway
D) IPsec-enabled web browser
E) session key

The IPsec technology can be deployed in _____ modes.
A) site-to-site and remote access
B) tunnel and transport *
C) tunnel and site-to-site
D) transport and remote access
E) site-to-site and transport

Choose a CORRECT statement regarding SSL.
A) The technology is defined in the internetwork layer
B) Its usage requires that necessary software be separately purchased and installed.
C) It generally provides a higher level of security than IPsec.
D) It can be used for both site-to-site and remote access VPNs.*
E) The software should be installed and maintained in each user station.

The following are descriptions of IPsec tunnel mode EXCEPT:
A) IPsec servers are placed at the boundary of local sites securing all inter-site transactions.
B) Internal hosts are unaware of the IPsec server's existence, making it transparent to the hosts.
C) Packets inside of a corporate network remain unencrypted.
D) The tunnel mode is popular in implementing both remote access and site-to-site VPNs.

E) It provides end-to-end (or host-to-host) security. *

Which information may NOT be contained in the digital certificate?
A) Owner's name or alias
B) Owner's public key
C) Issuer's name
D) Owner's private key*
E) Issuer's digital signature

Which reflects a correct sequence of security standards from weak to strong?
A) WPA, WEP, WPA2
B) WPA2, WEP, WPA
C) WEP, WPA2, WPA
D) WEP, WPA, WPA2*
E) WPA, WPA2, WEP

The main components of a cryptography system include the following EXCEPT:
A) Plaintext
B) Ciphertext
C) Digital signature *
D) Key value
E) Encryption algorithm

The hash function is used to derive a _____ from an original message.
A) message digest
B) digital certificate
C) session key
D) public key
E) private key

X.509 issued by ITU (International Telecommunications Union) defines a ____ standard.
A) digital signature
B) digital certificate*
C) public key
D) message digest
E) access control list

The following figure summarizes information items included in the _____.

Version: 3
Serial number: 123456
Algorithm: RSA
Issuer name: VeriSign
Validity period: start / expiration dates
Subject name: John Doe
Subject public key: XXXXXXXXXXX
CA digital signature: XXXXXXXX

A) Digital signature
B) Digital certificate*
C) Public key
D) Message digest
E) Access control list

Web browsers including Internet Explorer and Firefox have a built-in support for _____.
A) Packet Sniffing Detection
B) IP Spoofing Prevention
C) IP Spoofing Detection
D) Access Control List
E) SSL/TLS *

MD5 and SHA-1 are standards of:
A) encryption technologies
B) hashing algorithms (or functions)
C) digital certificate standards
D) well-known worms
E) well-known Trojan horses

Choose an INCORRECT statement about the digital signature.
A) The message digest is a short message calculated from an original message.
B) A hash function is generally used to produce a message digest from the original message.
C) The message digest is encrypted with a receiver's public key, resulting in a digital signature.*
D) The receiver computer decrypts the sender's digital signature using the sender's public key.
E) The receiver computer produces its own message digest based on the delivered message for comparison purpose.

Choose the LEAST accurate statement of the public key encryption.
A) When A sends a message to B, A encrypts it with B's public key.
B) After A encrypts a message with B's public key, A can decrypt it using the same B's public key. *
C) When A needs authentication to B, A encrypts a message with A's private key.
D) If A and B send messages to each other, each encrypts with the other's public key.
E) If A encrypts a message with B's public key, B's private key will decrypt it.

Choose a CORRECT statement regarding Wi-Fi standards.
A) WPA is an official IEEE standard.
B) WPA and WPA2 rely on the same encryption standard.
C) With WPA, the pre-shared key is permanently used making it vulnerable for password cracking.
D) The home network relies on centralized authentication between hosts and an authentication server.
E) To derive pre-shared keys in WEP or WPA-PSK, passwords/passphrases are heavily used. *

In total, how many different keys should be used for secure communication between two parties

when it relies on the asymmetric key encryption?
A) 0
B) 1
C) 2
D) 4*
E) 8

The PKI servers of a certificate authority perform the following functions except:
A) create digital certificates
B) maintain a certificate revocation list
C) distribute digital certificates
D) securely distribute private keys
E) perform security testing of a business system*

The cipher text is _____.
A) a message digest produced from an original text
B) a message digest produced from an encrypted text
C) an original text to be encrypted.
D) an encrypted text *
E) an encrypted text that has been compromised.

How to combine asymmetric and symmetric key encryptions to make the most of their strengths? Choose the LEAST accurate statement in describing the procedure from A to E.
A) Party A creates a single key for a session (called session key).
B) Party A encrypts the session key using Party B's private key and sends it to Party B. *
C) Party B decrypts that secret session key with Party B's private key.
D) Both parties now encrypt data with the session key.
E) With the session key, encryption and decryption are faster than using the asymmetric key system.

Which is CORRECT about hashing?
A) Hashing takes an input of any lengths and produces a variable-length hash value.
B) The hash function is also known as a *message digest*.
C) A dataset cannot be created in order to produce a predefined hash value. *
D) The probability of different messages to produce the same hash value is zero.
E) A hash value can be reversed to restore the original input.