CCNA Cyber Ops (Version 1.1) – Chapter 9 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-9-exam-answers-full.html

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. If an asymmetric algorithm uses a public key to encrypt data, what is used to decrypt it?

- DH
- **A private key**
- A digital certificate
- A different public key

A. When an asymmetric algorithm is used, public and private keys are used for the encryption. Either key can be used for encryption, but the complementary matched key must be used for the decryption. For example, if the public key is used for encryption, then the private key must be used for the decryption.

2. Which type of attack does the use of HMACs protect against?

- DoS
- DDoS
- Brute force
- **Man-in-the-middle**

D. Because only the sender and receiver know the secret key, only parties that have access to that key can compute the digest of an HMAC function. This defeats man-in-the-middle attacks and provides authentication of where the data originated.

3. Which algorithm can ensure data confidentiality?

- MD5
- **AES**
- RSA

- PKI

B. Data confidentiality is ensured through symmetric encryption algorithms, including DES, 3DES, and AES.

4. What is the purpose of code signing?

- Data encryption
- Reliable transfer of data
- Source identity secrecy
- **Integrity of source .EXE files**

D. Code signing is used to verify the integrity of executable files downloaded from a vendor website. Code signing uses digital certificates to authenticate and verify the identity of a website.

5. What are two symmetric encryption algorithms? (Choose two.)

- **3DES**
- MD5
- **AES**
- HMAC
- SHA

A, C. MD5, HMAC, and SHA are hashing algorithms.

6. What is the purpose of the DH algorithm?

- To provide non-repudiation support
- To support email data confidentiality
- To encrypt data traffic after a VPN is established
- **To generate a shared secret between two hosts that have not communicated before**

D. DH is an asymmetric mathematical algorithm that allows two computers togenerate an identical shared secret, without having communicated before. Asymmetric key systems are extremely slow for any sort of bulk encryption. It is common to encrypt the bulk of the traffic using a symmetric algorithm such as DES, 3DES, or AES, and use the DH algorithm to create keys that will be used by the symmetric encryption algorithm.

7. Which cryptographic technique provides both data integrity and nonrepudiation?

- 3DES
- **HMAC**

- MD5
- SHA-1

B. A Keyed-hash message authentication code (HMAC and KHMAC) is a type of message authentication code that uses an additional secret key as input to the hash function. This adds authentication to integrity assurance. When two parties share a secret key and use HMAC functions for authentication, the received HMAC digest of a message indicates that the other party was the originator of the message (non-repudiation), because it is the only other entity possessing the secret key. 3DES is an encryption algorithm, and MD5 and SHA-1 are hashing algorithms.

8. In a hierarchical CA topology, where can a subordinate CA obtain a certificate for itself?

- From the root CA only
- From the root CA or from self-generation
- From the root CA or another subordinate CA at the same level
- **From the root CA or another subordinate CA at a higher level**
- From the root CA or another subordinate CA anywhere in the tree

D. In a hierarchical CA topology, CAs can issue certificates to end users and to subordinate CAs, which in turn issue their certificates to end users, other lower level CAs, or both. In this way, a tree of CAs and end users is built in which every CA can issue certificates to lower level CAs and end users. Only the root CA can issue a self-signing certificate in a hierarchical CA topology.

9. Which objective of secure communications is achieved by encrypting data?

- Authentication
- Availability
- **Confidentiality**
- Integrity

C. When data is encrypted, it is scrambled to keep the data private and confidential so that only authorized recipients can read the message. A hash function is another way of providing confidentiality.

10. Which statement describes the use of hashing?

- Hashing can be used to prevent both accidental and deliberate changes.
- Hashing can be used to detect both accidental and deliberate changes.
- **Hashing can be used to detect accidental changes, but does not protect against deliberate changes.**

- Hashing can be used to protect against deliberate changes, but does not detect accidental changes.

C. Hashing can be used to detect accidental changes only. It is possible for an attacker to intercept a message, change it, recalculate the hash, and append it to the message. The receiving device would validate the appended hash.

11. Which IETF standard defines the PKI digital certificate format?

- X.500
- **X.509**
- LDAP
- SSL/TLS

B. To address the interoperability of different PKI vendors, IETF published the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 2527). The standard defines the format of a digital certificate.

12. Which two statements correctly describe certificate classes used in the PKI? (Choose two.)

- **A class 0 certificate is for testing purposes.**
- A class 0 certificate is more trusted than a class 1 certificate.
- The lower the class number, the more trusted the certificate.
- A class 5 certificate is for users with a focus on verification of email.
- **A class 4 certificate is for online business transactions between companies.**

A, E. A digital certificate class is identified by a number. The higher the number, the more trusted the certificate. The classes include the following:
Class 0 is for testing purposes in which no checks have been performed.
Class 1 is for individuals with a focus on verification of email.
Class 2 is for organizations for which proof of identity is required.
Class 3 is for servers and software signing for which independentverification and checking of identity and authority is done by the issuing certificate authority.
Class 4 is for online business transactions between companies.
Class 5 is for private organizations or governmental security.

13. Alice and Bob want to use a CA authentication procedure to authenticate each other. What must be obtained first?

- **CA self-signed certificate**
- Self-signed certificates of two CA authorities
- Self-signed certificate of the other device and the CA certificate
- Self-sig

A. In the CA authentication procedure, the first step when contacting the PKI is to obtain a copy of the public key of CA itself, called the self-signed certificate. The CA public key verifies all the certificates issued by the CA.

14. Which algorithm is used to automatically generate a shared secret for two systems to use in establishing an IPsec VPN?

- SSL
- DES
- AH
- **DH**
- ESP
- 3DES

The Diffie-Helman (DH) algorithm is the basis of most modern automatic key exchange methods. It is a mathematical algorithm that allows two computers to generate an identical shared secret on both systems without having communicated before. DH is commonly used when data is exchanged using an IPsec VPN.

15. A security specialist is tasked to ensure that files transmitted between the headquarters office and the branch office are not altered during transmission. Which two algorithms can be used to achieve this task? (Choose two.)

- 3DES
- HMAC
- AES
- **SHA-1**
- **MD5**

The task to verify that messages are not altered during transmission is to ensure data integrity, which can be implemented using hash function. HMAC can be used for ensuring origin authentication. AES and 3DES are encryption algorithms.

16. In which way does the use of HTTPS increase the security monitoring challenges within enterprise networks?

- HTTPS traffic can carry a much larger data payload than HTTP can carry.
- HTTPS traffic is much faster than HTTP traffic.
- HTTPS traffic does not require authentication.
- **HTTPS traffic enables end-to-end encryption.**

HTTPS enables end-to-end encrypted network communication, which adds further challenges for network administrators to monitor the content of packets to catch malicious attacks.

17. What technology has a function of using trusted third-party protocols to issue credentials that are accepted as an authoritative identity?

- hashing algorithms
- digital signatures
- symmetric keys
- **PKI certificates**

Digital certificates are used to prove the authenticity and integrity of PKI certificates, but a PKI Certificate Authority is a trusted third-party entity that issues PKI certificates. PKI certificates are public information and are used to provide authenticity, confidentiality, integrity, and nonrepudiation services that can scale to large requirements.

18. Which three algorithms are designed to generate and verify digital signatures? (Choose three.)

- IKE
- **DSA**
- **RSA**
- **ECDSA**
- AES
- .3DES

There are three Digital Signature Standard (DSS) algorithms that are used for generating and verifying digital signatures:Digital Signature Algorithm (DSA)
Rivest-Shamir Adelman Algorithm (RSA)
Elliptic Curve Digital Signature Algorithm (ECDSA)

19. What are two properties of a cryptographic hash function? (Choose two.)

- Complex inputs will produce complex hashes.
- Hash functions can be duplicated for authentication purposes.
- **The hash function is one way and irreversible.**
- The input for a particular hash algorithm has to have a fixed size.
- **The output is a fixed length.**

A cryptographic hash function should have the following properties:The input can be any length.
The output has a fixed length.
The hash value is relatively easy to compute for any given input.
The hash is one way and not reversible.
The hash is collision free, meaning that two different input values will result in different hash values

20. Which statement is a feature of HMAC?

- HMAC uses a secret key that is only known to the sender and defeats man-in-the-middle attacks.
- HMAC uses protocols such as SSL or TLS to provide session layer confidentiality.
- **HMAC uses a secret key as input to the hash function, adding authentication to integrity assurance.**
- HMAC is based on the RSA hash function.

A keyed-hash message authentication code (HMAC or KHMAC) is a type of message authentication code (MAC). HMACs use an additional secret key as input to the hash function, adding authentication to data integrity assurance.

21. Which two statements describe the characteristics of symmetric algorithms? (Choose two.)

- **They are commonly used with VPN traffic.**
- They use a pair of a public key and a private key.
- They are commonly implemented in the SSL and SSH protocols.
- They provide confidentiality, integrity, and availability.
- **They are referred to as a pre-shared key or secret key.**

Symmetric encryption algorithms use the same key (also called shared secret) to encrypt and decrypt the data. In contrast, asymmetric encryption algorithms use a pair of keys, one for encryption and another for decryption.

22. Which encryption algorithm is an asymmetric algorithm?

- AES
- SEAL
- **DH**
- 3DES

DH is an asymmetric algorithm. AES, 3DES, and SEAL are all symmetric algorithms.

23. Which statement describes the use of certificate classes in the PKI?

- Email security is provided by the vendor, not by a certificate.
- A vendor must issue only one class of certificates when acting as a CA.
- **A class 5 certificate is more trustworthy than a class 4 certificate.**
- The lower the class number, the more trusted the certificate.

The higher the certificate number, the more trustworthy the certificate. Class 1 certificates are for individuals, with a focus on email verification. An enterprise can act as its own CA and implement PKI for internal use. In that situation, the vendor can issue certificates as needed

for various purposes.

24. What is the focus of cryptanalysis?

- developing secret codes
- **breaking encrypted codes**
- implementing encrypted codes
- hiding secret codes

Cryptology is the science of making and breaking secret codes. There are two separate disciplines in cryptology, cryptography and cryptanalysis. Cryptography is the development and use of codes. Cryptanalysis is the breaking of those secret (encrypted) codes.

25. Two users must authenticate each other using digital certificates and a CA. Which option describes the CA authentication procedure?

- **The users must obtain the certificate of the CA and then their own certificate.**
- The CA is always required, even after user verification is complete.
- CA certificates are retrieved out-of-band using the PSTN, and the authentication is done in-band over a network.
- After user verification is complete, the CA is no longer required, even if one of the involved certificates expires.

When two users must authenticate each other using digital certificates and CA, both users must obtain their own digital certificate from a CA. They submit a certificate request to a CA, and the CA will perform a technical verification by calling the end user (out-of-band). Once the request is approved, the end user retrieves the certificate over the network (in-band) and installs the certificate on the system. After both users have installed their certificate, they can perform authentication by sending their certificate to each other. Each site will use the public key of the CA to verify the validity of the certificate; no CA is involved at this point. If both certificates are verified, both users can now authenticate each other.

26. When implementing keys for authentication, if an old key length with 4 bits is increased to 8 bits, which statement describes the new key space?

- The key space is increased by 3 times.
- The key space is increased by 8 times.
- **The key space is increased by 15 times.**
- The key space is increased by 16 times.

A key length with 4 bits will provide a key space of 2^4=16 keys. The new key length with 8 bits can provide a key space of 2^8=256 keys. The key space with 256 keys is 15 times larger than a key space with 16 keys.

27. What is the service framework that is needed to support large-scale public key-based technologies?

- **PKI**
- RSA
- 3DES
- HMAC

The service framework that is needed to support large-scale public key-based technologies is a PKI (public key infrastructure). SHA and HMAC are hashing algorithms. RSA is an asymmetric encryption algorithm.

28. What are the two important components of a public key infrastructure (PKI) used in network security? (Choose two.)

- symmetric encryption algorithms
- **certificate authority**
- intrusion prevention system
- **digital certificates**
- pre-shared key generation

A public key infrastructure uses digital certificates and certificate authorities to manage asymmetric key distribution. PKI certificates are public information. The PKI certificate authority (CA) is a trusted third-party that issues the certificate. The CA has its own certificate (self-signed certificate) that contains the public key of the CA.

29. A company is developing a security policy to ensure that OSPF routing updates are authenticated with a key. What can be used to achieve the task?

- SHA-1
- **HMAC**
- AES
- MD5
- 3DES

The task to ensure that routing updates are authenticated is data origin authentication, which can be implemented using HMAC. HMAC is MD5 or SHA-1 plus a secret key. AES and 3DES are two encryption algorithms. MD5 and SHA-1 can be used to ensure data integrity, but not authentication.

30. An online retailer needs a service to support the nonrepudiation of the transaction. Which component is used for this service?

- the private key of the retailer
- **the digital signatures**

- the unique shared secret known only by the retailer and the customer
- the public key of the retailer

Digital signatures, generated by hash function, can provide the service for nonrepudiation of the transaction. Both public and private keys are used to encrypt data during the transaction. Shared secrets between the retailer and customers are not used.

31. Which statement describes the Software-Optimized Encryption Algorithm (SEAL)?

- It uses a 112-bit encryption key.
- It requires more CPU resources than software-based AES does.
- It is an example of an asymmetric algorithm.
- **SEAL is a stream cipher.**

SEAL is a stream cipher that uses a 160-bit encryption key. It is a symmetric encryption algorithm that has a lower impact on the CPU resources compared to other software-based algorithms, such as software-based DES, 3DES, and AES.

32. What role does an RA play in PKI?

- a super CA
- **a subordinate CA**
- a backup root CA
- a root CA

A registration authority (RA) is a subordinate CA. It is certified by a root CA to issue certificates for specific uses.

33. What technology allows users to verify the identity of a website and to trust code that is downloaded from the Internet?

- encryption
- asymmetric key algorithm
- **digital signature**
- hash algorithm

Digital signatures provide assurance of the authenticity and integrity of software codes. They provide the ability to trust code that is downloaded from the Internet.

34. Which three services are provided through digital signatures? (Choose three.)

- accounting
- **authenticity**

- compression
- **nonrepudiation**
- **integrity**
- encryption

Digital signatures use a mathematical technique to provide three basic security services:Integrity
Authenticity
Nonrepudiation

35. What are two methods to maintain certificate revocation status? (Choose two.)

- subordinate CA
- **OCSP**
- DNS
- LDAP
- **CRL**

A digital certificate might need to be revoked if its key is compromised or it is no longer needed. The certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP), are two common methods to check a certificate revocation status.

36. The following message was encrypted using a Caesar cipher with a key of 2:

fghgpf vjg ecuvng

What is the plaintext message?

- invade the castle
- **defend the castle**
- defend the region
- invade the region

The Caesar cipher was a simple substitution cipher. In this example, if the key is 2, the letter d was moved two spaces to the right, resulting in an encoded message that used the letter f in place of the letter d. The letter g would be the substitute for the letter e, and so on. So, the resulting plaintext is f=d, g=e, h=f, g=e, p=n, f=d, v=t, j=h, g=e, e=c, c=a, u=s, v=t, n=l, g=e.

37. What is the purpose of a digital certificate?

- It ensures that the person who is gaining access to a network device is authorized.
- It provides proof that data has a traditional signature attached.
- It guarantees that a website has not been hacked.

- **It authenticates a website and establishes a secure connection to exchange confidential data**

Digital signatures commonly use digital certificates that are used to verify the identity of the originator in order to authenticate a vendor website and establish an encrypted connection to exchange confidential data. One such example is when a person logs into a financial institution from a web browser.

38. A company is developing a security policy for secure communication. In the exchange of critical messages between a headquarters office and a branch office, a hash value should only be recalculated with a predetermined code, thus ensuring the validity of data source. Which aspect of secure communications is addressed?

- data integrity
- non-repudiation
- **origin authentication**
- data confidentiality

Secure communications consists of four elements:Data confidentiality – guarantees that only authorized users can read the message
Data integrity – guarantees that the message was not altered
Origin authentication – guarantees that the message is not a forgery and does actually come from whom it states
Data nonrepudiation – guarantees that the sender cannot repudiate, or refute, the validity of a message sent