[Updated Constantly]

HERE

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 9 Exam Answers

1. 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

2. 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**

3. 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.**

4. 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**

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

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

6. 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.**

7. 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.

8. 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.**

9. Which encryption algorithm is an asymmetric algorithm?

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

10. 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.

11. What is the focus of cryptanalysis?

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

12. 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.

13. 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.

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

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

15. 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

16. 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

17. 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

18. 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.**

19. What role does an RA play in PKI?

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

20. 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

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

- accounting
- **authenticity**
- compression

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

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

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

23. 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

24. 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**

25. 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