CCNA Security v2.0 Chapter 7 Exam Answers

itexamanswers.net/ccna-security-v2-0-chapter-7-exam-answers.html

February 9, 2016

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. What is the purpose of a nonrepudiation service in secure communications?

- to ensure that encrypted secure communications cannot be decoded
- to confirm the identity of the recipient of the communications
- to provide the highest encryption level possible
- **to ensure that the source of the communications is confirmed***

Nonrepudiation uses the unique characteristics of the sender of a message to confirm that the reputed sender is in fact the actual sender.

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

- integrity
- authentication
- **confidentiality***
- availability

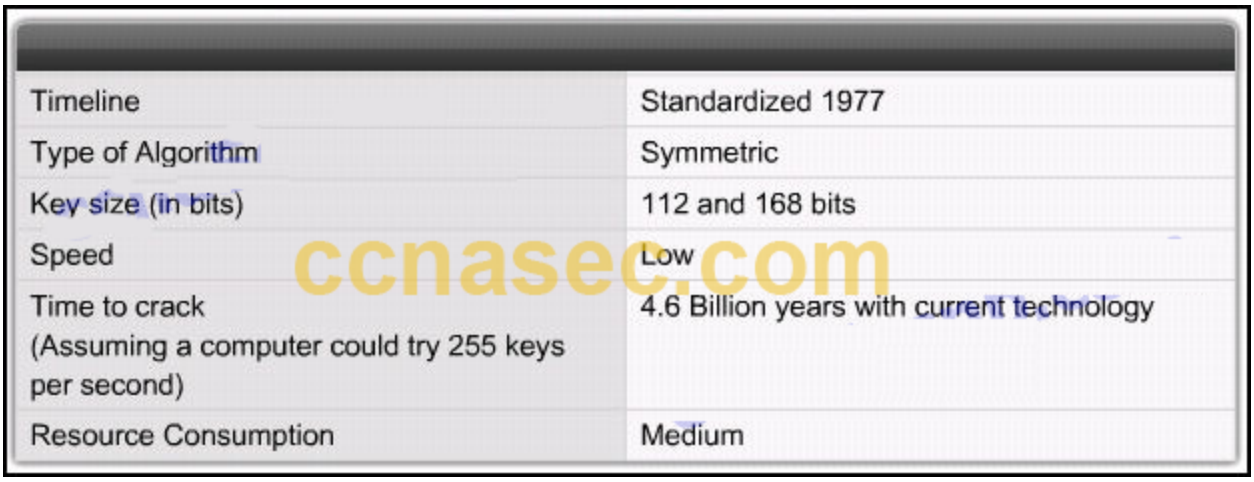
When data is encrypted, it is scrambled to keep the data private and confidential so that only authorized recipients can read the message. A hash function is another way of providing confidentiality.

3. Which encryption protocol provides network layer confidentiality?

- **IPsec protocol suite***
- Transport Layer Security
- Secure Hash Algorithm 1
- Secure Sockets Layer
- Keyed MD5
- Message Digest 5

Cryptographic encryption can provide confidentiality at several layers of the OSI model. For example, network layer protocols, such as the IPsec protocol suite, provide network layer confidentiality. Secure Sockets Layer (SSL) or Transport Layer Security (TLS), provide session layer confidentiality. MD5, Keyed MD5, and Secure Hash Algorithm 1 are examples of hash functions. They provide data integrity but not data confidentiality.

4. Refer to the exhibit. Which encryption algorithm is described in the exhibit?



- RC4
- AES
- **3DES***
- DES
- SEAL

3DES is a good choice to protect data because it has an algorithm that is very trusted and has security strength.

5. 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 unique shared secret known only by the retailer and the customer
- the public key of the retailer
- **the digital signatures***

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.

6. In which situation is an asymmetric key algorithm used?

- Two Cisco routers authenticate each other with CHAP.
- User data is transmitted across the network after a VPN is established.

- An office manager encrypts confidential files before saving them to a removable device.
- **A network administrator connects to a Cisco router with SSH.***

The SSH protocol uses an asymmetric key algorithm to authenticate users and encrypt data transmitted. The SSH server generates a pair of public/private keys for the connections. Encrypting files before saving them to a storage device uses a symmetric key algorithm because the same key is used to encrypt and decrypt files. The router authentication with CHAP uses a symmetric key algorithm. The key is pre-configured by the network administrator. A VPN may use both an asymmetric key and a symmetric encryption algorithm. For example in an IPSec VPN implementation, the data transmission uses a shared secret (generated with an asymmetric key algorithm) with a symmetric encryption algorithm used for performance.

7. Why is the 3DES algorithm often preferred over the AES algorithm?

- **3DES is more trusted because it has been proven secure for a longer period than AES.***
- AES is more expensive to implement than 3DES.
- 3DES performs better in high-throughput, low-latency environments than AES.
- Major networking equipment vendors such as Cisco have not yet adopted AES.

Despite its advantages, AES is a relatively young algorithm. An important rule of cryptography is that a mature algorithm is always more trusted. 3DES is therefore a more trusted choice in terms of strength, because it has been tested and analyzed for 35 years. AES can be used in high-throughput, low-latency environments, especially when 3DES cannot handle the throughput or latency requirements. AES is available in a number of Cisco VPN devices as an encryption transform.

8. What is the most common use of the Diffie-Helman algorithm in communications security?

- to create password hashes for secure authentication
- to provide routing protocol authentication between routers
- to encrypt data for secure e-commerce communications
- **to secure the exchange of keys used to encrypt data***

Diffie-Helman is not an encryption mechanism and is not typically used to encrypt data. Instead, it is a method to securely exchange the keys used to encrypt the data.

9. What is the focus of cryptanalysis?

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

10. How many bits does the Data Encryption Standard (DES) use for data encryption?

- 40 bits
- **56 bits***
- 64 bits
- 72 bits

DES uses a fixed length key. The key is 64-bits long, but only 56 bits are used for encryption. The remaining 8 bits are used for parity. A DES encryption key is always 56 bits long. When DES is used with a weaker encryption of a 40-bit key, the encryption key is 40 secret bits and 16 known bits, which make the key length 56 bits.

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

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

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.

12. Which encryption algorithm is an asymmetric algorithm?

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

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

13. Which type of encryption algorithm uses public and private keys to provide authentication, integrity, and confidentiality?

- symmetric
- shared secret
- IPsec
- **asymmetric***

An asymmetric encryption algorithm uses two keys, namely a public key and a private key. A symmetric encryption algorithm uses an identical key for both encryption and decryption. A shared secret is an example of using symmetric algorithm.

14. How do modern cryptographers defend against brute-force attacks?

- Use statistical analysis to eliminate the most common encryption keys.
- **Use a keyspace large enough that it takes too much money and too much time to conduct a successful attack.***
- Use an algorithm that requires the attacker to have both ciphertext and plaintext to conduct a successful attack.
- Use frequency analysis to ensure that the most popular letters used in the language are not used in the cipher message.

In a brute-force attack, an attacker tries every possible key with the decryption algorithm knowing that eventually one of them will work. To defend against the brute-force attacks, modern cryptographers have as an objective to have a keyspace (a set of all possible keys) large enough so that it takes too much money and too much time to accomplish a brute-force attack. A security policy requiring passwords to be changed in a predefined interval further defend against the brute-force attacks. The idea is that passwords will have been changed before an attacker exhausts the keyspace.

15. Which statement describes asymmetric encryption algorithms?

- They have key lengths ranging from 80 to 256 bits.
- They include DES, 3DES, and AES.
- They are also called shared-secret key algorithms.
- **They are relatively slow because they are based on difficult computational algorithms.***

DES, 3DES, and AES are examples of symmetric encryption algorithms (also known as shared secret key algorithms). The usual key length for symmetric algorithms is 80-256 bits. Asymmetric algorithms are relatively slow because they are based on difficult computational algorithms.

16. Which two non-secret numbers are initially agreed upon when the Diffie-Hellman algorithm is used? (Choose two.)

- binomial coefficient

- **generator***
- elliptic curve invariant
- **prime modulus***
- topological index
- pseudorandom nome

DH is a mathematical algorithm that allows two hosts to generate an identical shared secret on both systems without having communicated before. To start a DH exchange, both hosts must agree on two nonsecret numbers. The first number is a base number, also called the generator. The second number is a prime number that is used as the modulus. These numbers are usually public and are chosen from a table of known values.

17. What type of encryption algorithm uses the same key to encrypt and decrypt data?

- Diffie-Hellman
- **Shared-secret***
- Public-key
- Asymmetric

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

18. How many bits does the Data Encryption Standard (DES) use for data encryption?

- 40 bits
- **56 bits***
- 64 bits
- 72 bits

DES uses a fixed length key. The key is 64-bits long, but only 56 bits are used for encryption. The remaining 8 bits are used for parity. A DES encryption key is always 56 bits long. When DES is used with a weaker encryption of a 40-bit key, the encryption key is 40 secret bits and 16 known bits, which make the key length 56 bits.

19. In what situation would an asymmetric algorithm most likely be used?

- logging onto a computer
- **making an online purchase***
- uploading a networking book chapter using FTP
- transferring a large stream of data between two corporate locations

Asymmetric algorithms are slow, so they are commonly used in low-volume transactions such as making online purchases or logging into a financial website.

20. Why is asymmetric algorithm key management simpler than symmetric algorithm key management?

- It uses fewer bits.
- Only one key is used.
- Two public keys are used for the key exchange.
- **One of the keys can be made public.***

Asymmetric algorithms use two keys, a public and a private key. Key management is simpler because one of the keys can be made public.

21. What is the purpose of code signing?

- source identity secrecy
- **integrity of source .EXE files***
- reliable transfer of data
- data encryption

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.

22. Which algorithm can ensure data confidentiality?

- MD5
- PKI
- RSA
- **AES***

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

23. What is the purpose of a digital certificate?

- It guarantees that a website has not been hacked.
- **It authenticates a website and establishes a secure connection to exchange confidential data.***
- It provides proof that data has a traditional signature attached.
- It ensures that the person who is gaining access to a network device is authorized.

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.

24. Fill in the blank.
A shared secret is a **symmetric** key used in a encryption algorithm.

Download PDF File below:

[sociallocker id="54558"]

ITexamanswers.net – CCNA Security v2.0 Chapter 7 Exam Answers.pdf
703.06 KB 1819 downloads

...

Download

[/sociallocker]