Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/7/2022 8:14:51 pm • Time spent: 03:51

Score: 80% Passing Score: 80%

Question 1: ✔ Correct

When a cryptographic system is used to protect data confidentiality, what actually takes place?

- Data is available for access whenever authorized users need it.
- ➡ Unauthorized users are prevented from viewing or accessing the resource.
- Data is protected from corruption or change.
- Encrypted data transmission is prohibited.

EXPLANATION

Cryptography is the science of converting data into a secret code to hide a message's meaning during transmission. Cryptography systems provide the following security services:

- Confidentiality by ensuring that only authorized parties can access data.
- Integrity by verifying that data has not been altered in transit.
- Authentication by proving the identity of the sender or receiver.
- Non-repudiation by validating that communications have cone from a particular sender at a particular time.

REFERENCES

7.1.2 Cryptography Facts

7.1.5 Symmetric and Asymmetric Encryption Facts

q_cryp_concepts_basic_secp7.question.fex

Question 2: ✔ Correct

Which term means a cryptography mechanism that hides secret communications within various forms of data?

- Ciphertext
- Algorithm
- Steganography
- Cryptanalysis

EXPLANATION

Steganography is the cryptography mechanism that hides secret communications within various forms of data.

Ciphertext is the encrypted form of a message that makes it unreadable to all but those the message is intended for.

Cryptanalysis is the method of recovering original data that has been encrypted without having access to the key used in the encryption process.

A cipher or algorithm is the process or formula used to convert a message or otherwise hide its meaning.

REFERENCES

7.1.2 Cryptography Facts

q_cryp_concepts_stegano_secp7.question.fex

Question 3: ✔ Correct

Which of the following algorithms are used in asymmetric encryption? (Select two.)

- [ ] AES
- [x] RSA
- [ ] Twofish
- [ ] Blowfish
- [x] Diffie-Hellman

EXPLANATION

RSA and Diffie-Hellman are asymmetric algorithms. RSA, one of the earliest encryption algorithms, can also be used for digital signatures. The Diffie-Hellman Protocol was created in 1976 but is still in use today in technologies such as SSL, SSH, and IPsec.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_asym_02_secp7.question.fex

Question 4: ✕ Incorrect

A receiver wants to verify the integrity of a message received from a sender. A hashing value is contained within the digital signature of the sender.

Which of the following must the receiver use to access the hashing value and verify the integrity of the transmission?

- Receiver's public key
- Sender's private key
- Sender's public key
- ~~Receiver's private key~~

EXPLANATION

Digital signatures are created using the sender's private key. Therefore, only the sender's public key can be used to verify and open any data encrypted with the sender's private key. The recipient's private and public keys are not involved in this type of cryptography situation. Often, the hashing value of a message is protected by the sender's private key (their digital signature). The recipient must extract the original hashing value.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

7.2.5 Cryptographic Implementation Facts

7.3.1 Hashing

7.3.2 Hashing Algorithms

7.3.3 Hashing Facts

7.3.4 Using Hashes

7.3.5 Compare an MD5 Hash

q_asys_sys_encrypt_hash_secp7.question.fex

Question 5: ✕ Incorrect

Mary wants to send a message to Sam in such a way that only Sam can read it. Which key should be used to encrypt the message?

- Sam's public key
- ~~Sam's private key~~
- Mary's private key
- Mary's public key

EXPLANATION

Sam's public key should be used to encrypt the message. Only the corresponding private key, which only Sam has, can be used to decrypt the message.

Mary cannot use Sam's private key because only Sam has that key. Anything encrypted with the private key can be decrypted by anyone with the public key.

Encrypting the message using Mary's private key would mean that anyone could read the data using Mary's public key. Encrypting with Mary's public key would mean that only Mary would be able to decrypt it using her private key.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_key_01_secp7.question.fex

Question 6: ✔ Correct

Above all else, what must be protected to maintain the security and benefit of an asymmetric cryptographic solution, especially if it is widely used for digital certificates?

- Cryptographic algorithm
- ➡ Private keys
- Hash values
- Public keys

EXPLANATION

The strength of an asymmetric cryptographic system lies in the secrecy and security of its private keys. A digital certificate and a digital signature are little more than unique applications of a private key. If the private keys are compromised for a single user, for a secured network, or for a digital certificate authority, the entire realm of trust is destroyed.

REFERENCES

7.1.2 Cryptography Facts

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_secret_01_secp7.question.fex

Question 7: ✔ Correct

Which of the following algorithms are used in symmetric encryption? (Select two.)

- [ ] Diffie-Hellman
- [x] 3DES
- [x] Blowfish
- [ ] RSA
- [ ] ECC

EXPLANATION

3DES and Blowfish are symmetric encryption algorithms.

RSA, Diffie-Hellman, and ECC are asymmetric encryption algorithms.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_sym_01_secp7.question.fex

Question 8: ✔ Correct

Which of the following encryption mechanisms offers the least security because of weak keys?

- AES
- TwoFish
- IDEA
- DES

EXPLANATION

DES offers the least encryption security of all the cryptography systems in this list. DES has a limitation of 56-bit keys, the weakest of those listed here. The strength of a cryptosystem lies not only in long keys but in the algorithm, initialization vector or method, the proper use of the keyspace, and the protection and management of keys.

AES (128-, 192-, and 256-bit keys), TwoFish (up to 256-bit keys), and IDEA (128-bit keys) all support stronger keys than DES.

REFERENCES

7.1.5 Symmetric and Asymmetric Encryption Facts

q_asys_sys_encrypt_weak_01_secp7.question.fex

Question 9: ✔ Correct

Which of the following can be classified as a stream cipher?

- ➡ (●) RC4
- ( ) Twofish
- ( ) Blowfish
- ( ) AES

EXPLANATION

The most frequently used implementation of symmetric key stream ciphers is Rivest's cipher v4, known as RC4. RC4 uses a variable key up to 256 bits and is commonly used with WEP and SSL. It uses the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA).

Blowfish, Twofish, and AES are all block ciphers.

REFERENCES

7.1.7 Cryptography Algorithms Facts

q_cryp_algorithm_stream_secp7.question.fex

Question 10: ✔ Correct

Which type of password attack employs a list of pre-defined passwords that it tries against a login prompt?

- Downgrade attack
- Collision attack
- Dictionary attack
- Birthday attack

EXPLANATION

A dictionary attack is a type of brute-force attack. A hacker uses a list of words and phrases to try to guess the decryption key.

- Dictionary attacks work well if weak passwords are used.
- Using longer and uncommon passphrases is the best way to secure data against these attacks.

A collision attack tries to find two inputs that produce the same hash value. This type of attack is often used on digital signatures.

A birthday attack combines a collision attack and brute-force attack. The name is taken from the birthday probability math problem.

A downgrade attack forces the system to use an older, less secure communication protocol.

REFERENCES

7.1.13 Cryptographic Attack Facts

q_cryp_attacks_dict_secp7.question.fex