Exam Report: 9.2.5 Practice Questions

Date: 1/28/2020 10:06:58 am
Time Spent: 7:47

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 20%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

Advanced cryptography includes various modes of operation.

Drag the mode of operation on the left to the appropriate definition on the right.

Each cipher text block is fed back into the encryption and then encrypts the next plaintext block.

~~Block Cipher Mode~~ Cipher Feedback Mode

Each plaintext block is added to the previous cipher text block and then the result is encrypted with the key.

~~Cipher Feedback Mode~~ Cipher Block Chaining Mode

This mode can encrypt or decrypt one fixed-length block.

~~Cipher Block Chaining Mode~~ Block Cipher Mode

Sender and recipient access a reliable counter that computes a new shared value each time a cipher text block is exchanged.

~~Output Feedback Mode~~ Counter Mode

Feeds the output blocks back to the block cipher.

~~Counter Mode~~ Output Feedback Mode

Explanation

Advanced cryptography includes the following modes of operation:

- **Block Cipher Mode**: This mode provides confidentiality and authenticity services. It can encrypt or decrypt one fixed-length block. It works on large chunks of data at a time, often combining blocks for additional security. Block ciphers are more useful when the amount of data is known.
- **Cipher Block Chaining Mode**: Each plaintext block is added to the previous cipher text block, and then the result is encrypted with the key.
- **Cipher Feedback Mode**: Each cipher text block is fed back into the encryption to then encrypt the next plaintext block.
- **Output Feedback Mode**: This mode feeds the output blocks back to the block cipher. These blocks then make strings of bits to feed the encryption algorithm, acting as the key generator.
- **Counter Mode**: Both the sender and recipient will access a reliable counter that computes a new shared value each time a cipher text block is exchanged. The counter needs to be synchronized between both parties.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_03]

Question 2: Incorrect

At the end of the cryptographic process, output is generated. With one type of output, simple character changes in the plaintext will cause several characters to change in the cipher text.

What type of output is this?

○ Collision

○ Encryption

● ~~Hashing~~

➡ ○ Diffusion

Explanation

At the end of the cryptographic process, output is generated:

- Simple character changes in the plaintext will cause several characters to change in the cipher text. This is called a diffusion.
- When two different inputs to a function produce the same output, it is called a collision. They are not common, but can occur.
- A digital signature is a mathematical scheme for demonstrating the authenticity of digital message or document. A valid digital signature gives a message credibility, guaranteeing the recipient that the message has not been tampered with in transit.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_05]

▼ Question 3: Correct

If a message sender encrypts a message with a key and a message receiver decrypts it using the same key, which type of key exchange is taking place?

➡ ● Symmetric

○ Digital signature

○ Counter mode

○ Asymmetric

Explanation

A symmetric key is when the sender uses a public key to encrypt a message and the recipient uses that same public key to decrypt it.

An asymmetric key is where the sender's and the receiver's keys are different for the encrypting and decrypting processes. Using counter mode, both the sender and recipient access a reliable counter that computes a new shared value each time a cipher text block is exchanged. A digital signature is a mathematical scheme for demonstrating the authenticity of digital message or document.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_02]

▼ Question 4: Incorrect

You want email sent from users in your organization to be encrypted to make messages more secure.

Which of the following is an option you can use to enhance the encryption of email messages?

➡ ○ A cryptographic service provider

● ~~An asymmetric key exchange~~

○ A symmetric key exchange

○ A hashing service provider

Explanation

Cryptographic service providers (CSPs) are software libraries that can be used to enhance encryption. Applications can use these to help secure email and provide strong user authentication.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_01]

Question 5: Incorrect

Drag the cryptographic algorithm on the left to the appropriate explanation on the right. (Each algorithm may be used once, more than once, or not at all.)

Generates two different yet mathematically related keys.

✓ Asymmetric

Only the private key can be used to decrypt information.

✓ Asymmetric

Generates a single key that is used for both encryption and decryption.

✓ Symmetric

Algorithm used for signature verification and data integrity checking.

✓ Hashing

The public key can only be used to encrypt information.

~~Symmetric~~ Asymmetric

Explanation

Cryptographic algorithms are as follows:

- **Symmetric**: Generates a single key that is used for both encryption and decryption. If the key were to fall in the wrong hands, messages encrypted with the key both past and future can be decrypted.
- **Asymmetric**: Generates two different yet mathematically related keys. The encryption key can be shared publicly. This is because the public key is used only to encrypt information; it cannot decrypt information at all. The only key that can decrypt the information is the private key.
- **Hashing**: Instead of being used to encrypt information, keys are used for signature verification and data integrity checking. They take a string of characters of an undetermined length and convert it into a string of characters that has a specific length. This output is known as a digest. Hashes should not be able to be reconstructed from the output of the hash function.

References

LabSim for Security Pro, Section 9.2.
[All Questions SecPro2017_v6.exm ADV_CRY_04]