Exam Report: 2.4.3 Practice Questions

Date: 1/13/2020 12:27:15 pm
Time Spent: 3:37

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 83%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Incorrect

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

● ~~The data is protected from corruption or change~~

○ The data is available for access whenever authorized users need it

○ Transmitting the encrypted data is prohibited

➡ ○ Unauthorized users are prevented from viewing or accessing the resource

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

LabSim for Security Pro, Section 2.4.
[All Questions SecPro2017_v6.exm CRYPTO_BASICS_01||/]

Question 2: Correct

Which type of cipher changes the *position* of the characters in a plain text message?

○ Substitution

➡ ● Transposition

○ Steam

○ Block

Explanation

A *transposition* cipher changes the position of characters in the plain text message. It is also referred to as an *anagram*.

A substitution cipher replaces one set of characters with symbols or another character set. A block cipher takes a fixed-length number of bits, or block, and encrypts them all at once. A stream cipher creates a sequence of bits that are used as the key.

References

LabSim for Security Pro, Section 2.4.
[All Questions SecPro2017_v6.exm CRYPTO_BASICS_02]

Question 3: Correct

Which is the cryptography mechanism that hides secret communications within various forms of data?

○ Ciphertext

➡ ● Steganography

○ Cryptanalysis

○ Algorithm

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

LabSim for Security Pro, Section 2.4.
[All Questions SecPro2017_v6.exm CRYPTO_BASICS_05||/]

Question 4: Correct

Which of the following is **not** a valid example of steganography?

○ Microdots

➡ ● Encrypting a data file with an encryption key

○ Digital watermarking

○ Hiding text messages within graphical images

Explanation

Encrypting a data file with an encryption key is encryption, not steganography.

Digital watermarking, microdots, and hiding text messages within graphical images are all examples of steganography.

References

LabSim for Security Pro, Section 2.4.
[All Questions SecPro2017_v6.exm CRYPTO_BASICS_06]

Question 5: Correct

Which of the following algorithms combines a random value with plain text to produce cipher text?

○ Transposition

➡ ● One-time pad

○ Cryptanalysis

○ Steganography

Explanation

A *one-time pad* is a cryptography method in which plain text is converted to binary and combined with a string of randomly generated binary numbers, which is called the *pad*. A one-time pad is a form of substitution.

A *transposition cipher*, or *anagram*, changes the position of characters in the plain text message.

Steganography is a cryptography method that uses digital pictures, video clips, or audio clips to hide a message or some type of data. Steganography tools encode the message into the Least Significant Bit (LSB) of the binary coding.

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

References

LabSim for Security Pro, Section 2.4.
[All Questions SecPro2017_v6.exm CRYPTO_BASICS_07||/]

Question 6: Correct

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

○ Steganography

➡ ● Cryptanalysis

○ Algorithm

○ Ciphertext

Explanation

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

Steganography hides data or a message so that only the sender or the recipient suspects that the hidden data exists.

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

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

References

LabSim for Security Pro, Section 2.4.
[All Questions SecPro2017_v6.exm CRYPTO_BASICS_08||/]