Started on	Thursday, 20 March 2025, 12:14 PM
State	Finished
Completed on	Thursday, 20 March 2025, 12:23 PM
Time taken	9 mins 1 sec
Grade	**25.00** out of 25.00 (**100**%)

Question 1

Correct

Mark 1.00 out of 1.00

Which security service ensures that data cannot be modified in transit?

a. Authorization

b. Authentication

c. Confidentiality

d. Integrity ✓

Your answer is correct.

The correct answer is: Integrity

Question 2

Correct

Mark 1.00 out of 1.00

Which layer of the OSI model does the security service of "authentication" primarily operate within?

a. Data Link Layer

b. Application Layer ✓

c. Network Layer

d. Physical Layer

Your answer is correct.

The correct answer is: Application Layer

Question 3

Correct

Mark 1.00 out of 1.00

Which of the following is an example of a passive attack?

a. Denial of Service (DoS)

b. Man-in-the-Middle Attack

c. Traffic Analysis ✓

d. Replay Attack

Your answer is correct.

The correct answer is: Traffic Analysis

Question 4

Correct

Mark 1.00 out of 1.00

Which security mechanism involves the use of digital signatures?

a. Routing Control

b. Digital Signature ✓

c. Access Control

d. Encipherment

Your answer is correct.

The correct answer is: Digital Signature

Question 5

Correct

Mark 1.00 out of 1.00

In the network security model, what does the "trusted third party" provide?

a. Key distribution and certification ✓

b. Firewall configuration

c. Physical security

d. Network bandwidth

Your answer is correct.

The correct answer is: Key distribution and certification

Question 6

Correct

Mark 1.00 out of 1.00

Which classical encryption technique replaces characters with other characters or symbols?

a. Hashing

b. Steganography

c. Substitution ✓

d. Transposition

Your answer is correct.

The correct answer is: Substitution

Question 7

Correct

Mark 1.00 out of 1.00

The Caesar cipher is an example of which type of cipher

a. Stream cipher

b. Substitution cipher ✓

c. Block cipher

d. Transposition ciphe

Your answer is correct.

The correct answer is: Substitution cipher

Question 8

Correct

Mark 1.00 out of 1.00

Which classical encryption technique rearranges the order of characters in a message?

a. Steganography

b. Substitution

c. Transposition ✓

d. Hashing

Your answer is correct.

The correct answer is: Transposition

Question 9

Correct

Mark 1.00 out of 1.00

What is the primary goal of steganography?

a. To encrypt messages

b. To authenticate users

c. To ensure data integrity

d. To hide the existence of a message ✓

Your answer is correct.

The correct answer is: To hide the existence of a message

Question 10

Correct

Mark 1.00 out of 1.00

Which is a type of transposition cipher?

a. Polyalphabetic substitution

b. One-time pad

c. Monoalphabetic substitution

d. Rail fence cipher ✓

Your answer is correct.

The correct answer is: Rail fence cipher

Question 11

Correct

Mark 1.00 out of 1.00

What does "perfect security" mean in cryptography?

a. The key is very long.

b. The ciphertext is unbreakable.

c. The ciphertext reveals no information about the plaintext. ✓

d. The encryption algorithm is complex.

Your answer is correct.

The correct answer is: The ciphertext reveals no information about the plaintext.

Question 12

Correct

Mark 1.00 out of 1.00

Which mathematical theory provides a foundation for measuring information and entropy?

- a. Information Theory ✓
- b. Graph Theory
- c. Number Theory
- d. Set Theory

Your answer is correct.

The correct answer is: Information Theory

Question 13

Correct

Mark 1.00 out of 1.00

What is a "product cryptosystem"?

- a. A system that uses only software encryption.
- b. A system that combines multiple encryption methods. ✓
- c. A system that uses only one encryption method.
- d. A system that uses only hardware encryption.

Your answer is correct.

The correct answer is: A system that combines multiple encryption methods.

Question 14

Correct

Mark 1.00 out of 1.00

What is the goal of cryptanalysis?

- a. To distribute encryption keys.
- b. To design new encryption algorithms.
- c. To ensure data integrity.
- d. To break encryption algorithms. ✓

Your answer is correct.

The correct answer is: To break encryption algorithms.

Question 15

Correct

Mark 1.00 out of 1.00

What is a one-time pad an example of?

a. A perfectly secure cipher ✓

b. A substitution cipher

c. A weak cipher

d. A transposition cipher

Your answer is correct.

The correct answer is: A perfectly secure cipher

Question 16

Correct

Mark 1.00 out of 1.00

What is Entropy in the context of information theory?

a. The amount of data transmitted.

b. The randomness or unpredictability of data. ✓

c. The size of the encryption key.

d. The speed of encryption.

Your answer is correct.

The correct answer is: The randomness or unpredictability of data.

Question 17

Correct

Mark 1.00 out of 1.00

Frequency analysis is a form of:

a. Steganography.

b. Key generation.

c. Encryption.

d. Cryptanalysis. ✓

Your answer is correct.

The correct answer is: Cryptanalysis.

Question 18

Correct

Mark 1.00 out of 1.00

What makes a one time pad difficult to use in real world applications?

a. It is too complex to implement.

b. The key must be as long as the plaintext and used only once. ✓

c. It requires a very powerful computer.

d. It is too easy to break.

Your answer is correct.

The correct answer is: The key must be as long as the plaintext and used only once.

Question 19

Correct

Mark 1.00 out of 1.00

What is the purpose of confusion in a product cipher?

a. To compress the plaintext.

b. To generate a random key.

c. To hide the relationship between plaintext and ciphertext. ✓

d. To rearrange the order of the plaintext.

Your answer is correct.

The correct answer is: To hide the relationship between plaintext and ciphertext.

Question 20

Correct

Mark 1.00 out of 1.00

What is the purpose of diffusion in a product cipher?

a. To hide the relationship between plaintext and ciphertext.

b. To spread the influence of a single plaintext bit over many ciphertext bits. ✓

c. To generate a random key.

d. To compress the plaintext.

Your answer is correct.

The correct answer is: To spread the influence of a single plaintext bit over many ciphertext bits.

Question 21

Correct

Mark 1.00 out of 1.00

What is a known plaintext attack?

a. An attack where the attacker has no information.

b. An attack where the attacker guesses the key.

c. An attack where the attacker has both the plaintext and corresponding ciphertext. ✓

d. An attack where the attacker only has the ciphertext

Your answer is correct.

The correct answer is: An attack where the attacker has both the plaintext and corresponding ciphertext.

Question 22

Correct

Mark 1.00 out of 1.00

What is a ciphertext only attack?

a. An attack where the attacker has no information.

b. An attack where the attacker has both the plaintext and corresponding ciphertext.

c. An attack where the attacker guesses the key.

d. An attack where the attacker only has the ciphertext ✓

Your answer is correct.

The correct answer is: An attack where the attacker only has the ciphertext

Question 23

Correct

Mark 1.00 out of 1.00

What is a chosen plaintext attack?

a. An attack where the attacker can choose plaintext and receive the corresponding ciphertext. ✓

b. An attack where the attacker has both the plaintext and corresponding ciphertext.

c. An attack where the attacker guesses the key.

d. An attack where the attacker only has the ciphertext.

Your answer is correct.

The correct answer is: An attack where the attacker can choose plaintext and receive the corresponding ciphertext.

Question 24

Correct

Mark 1.00 out of 1.00

What is the main goal of a brute force attack?

a. To use statistical analysis.

b. To use frequency analysis.

c. To exploit a vulnerability in the algorithm.

d. To try every possible key. ✓

Your answer is correct.

The correct answer is: To try every possible key.

Question 25

Correct

Mark 1.00 out of 1.00

Which of the following is a key distribution problem in cryptography?

a. Securely exchanging the key between sender and receiver ✓

b. Decrypting the ciphertext

c. Encrypting the plaintext

d. Ensuring the key is complex

Your answer is correct.

The correct answer is: Securely exchanging the key between sender and receiver