SOUTHERN UNIVERSITY COLLEGE

ACADEMIC YEAR 2021

MID TERM EXAM

**BTIS 2703 INFORMATION SECURITY AND ASSURANCE**

DATE : TIME :

## BACHELOR OF SOFTWARE ENGINEERING

YEAR THREE

**Instruction to Candidates :**

1. Answer **ALL** questions. All questions carry equal marks.
2. Please rename your answer file with the following format (your name\_ID.pdf)

**SECTION A**

Choose the right answer.

1. Which of the following is not one of the components for C.I.A triad?
2. Availability
3. Configuration
4. Confidentiality
5. Integrity
6. The elements in C.N.S.S model of information security has evolved from which concept?
7. The C.I.A triad
8. Information security and assurance
9. Cybersecurity model
10. Network security
11. What is the definition of access?
12. An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it.
13. A subject or object’s ability to use, manipulate, modify, or affect another subject or object.
14. The organisational resource that is being protected.
15. A technique used to compromise a system.

*“Enable authorised users-people or computer systems- to access information without interference or obstruction and to receive it in the required format.”*

1. Question number 4 is based on the above excerpt. Which of the following best describes about the above excerpt?
2. Availability
3. Confidentiality
4. Integrity
5. Nonrepudiation
6. Which of the following are the components for information systems?
7. Hardware
8. Software
9. People
10. Networks
11. i and ii only
12. i, ii and iii only
13. i, and iii only
14. i, ii, iii and iv
15. The information security is the protection of information assets that use, store, or transmit information through the application of policy, education, and technology.
16. True
17. False
18. A worm sends a copy of itself to other systems.
19. True
20. False
21. Data security means protecting data in \_\_\_, in processing, and at rest (storage) is a critical aspect of information security.
22. Deletion
23. Addition
24. Transmission
25. Diversion
26. Which of the following is not an example of software attacks?
27. Viruses
28. Worms
29. Bugs
30. Denial of service
31. The types of threats to the security of a computer system or network are?
32. Interruption
33. Interception
34. Interconnection
35. Integration
36. I and ii only
37. I, ii and iii only
38. I and iii only
39. All the above
40. Which of the following best describes about confidentiality?
41. Active computer systems can only be modified by authorized users.
42. Information contained in a computer system can only be read by authorized users.
43. The users who can assesses the system and information without authorization and often illegally.
44. Unauthorized entry into the real or virtual property of another party.
45. An asymmetric key cipher uses \_\_ .
46. Public key
47. Private key
48. Public and private key
49. Public key infrastructure
50. We use cryptography term to transforming messages to make them \_\_\_.
51. Secure and immune to change.
52. Secure and immune to idle.
53. Secure and immune to defend.
54. Secure and immune to attack.
55. In cryptography, the original message before being transformed is called \_\_.
56. Filled text
57. Plain text
58. Empty text
59. Encrypted text
60. In symmetric key cryptography, the key used by the sender and the receiver is \_\_.
61. Same keys are used
62. Two keys are used
63. Shared
64. Different
65. The cryptography can provide \_\_\_.
66. Authentication
67. Confidentiality
68. Nonrepudiation of messages
69. Entity authentication
70. The process of transforming plaint text to unreadable text is known as \_\_\_.
71. Network security
72. Cryptography
73. Encryption
74. Data hiding
75. An attack in which the site is not capable of answering valid request is known as \_\_.
76. Email bombing
77. Ping storm
78. Denial of service
79. Smurfing
80. A unique piece of information that is used in encryption:
81. Plain text
82. Encode
83. Decode
84. Key
85. Attack in which a user creates a packet that appears to be something else:
86. Falsification
87. Fabrication
88. Spoofing
89. Rainbow table

[Total marks: 40 marks]

**SECTION B [60 MARKS]**

Answer all questions.

**Question 1**

1. There are three characteristics of information that gives value to the organisation: confidentiality, integrity, and availability. How would these information characteristics protect your organisation data? (6 marks)
2. Physical security policies deal with hardware components of an information system. Provide two examples of physical security. (4 marks)
3. People always have been a threat to information security. As a security personnel in your organisation, please suggest what are the solution you would like to propose to the management so that at least this threat will not remain as the weakest link in your organisation. (6 marks)
4. The implementation of information security in an organisation must begin somewhere, and it can not happen in overnight. In your organisation, the management board really take information security as one of the crucial elements in your software development project. Which type of information security implementation is applicable for this situation? Justify your answer. (4 marks)

[Total marks: 20 marks]

**Question 2**

1. Why an antiqued or obsolesce technology can lead to unreliable and untrustworthy systems? (4 marks)
2. Explain what is meant by a social engineering attack on a password. Please provide one example to illustrate your answer. (4 marks)
3. One of the functions information security is to protect data that organisation collects and use. How an information security can ensure the data is secured? (6 marks)
4. Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. What is espionage? Provide one example of espionage and state one suggestion how to overcome this problem. (6 marks)

[Total marks: 20 marks]

**Question 3**

1. Explain how public key cryptography may be used for identification? (4 marks)
2. Describe two primary functions of cryptography in the context of data security. (4 marks)
3. Encrypt the message ISA MID TERM EXAM with the Caesar cipher with the 6 as the key. (6 marks)
4. How an IDPS would help the organisation to examine the causes of the intrusion? (6 marks)

[Total marks: 20 marks]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_