

OD-102

October-2019

B.C.A., Sem.-V

**SEC-301(B) : Information Security
(New Course)**

[Max. Marks : 70]

Time : 2:30 Hours]

1. (A) Answer the following :

- (i) What is Intellectual Property Law ? Also, discuss Patents law, Trademarks and Trade Secrets. 7
- (ii) Discuss : Legislative Branch, Administrative Branch and Judicial Branch of legal systems. 7

OR

- (i) Discuss: The Information Security Principles of Success.
- (ii) Discuss : The information security common body of knowledge (CBK). 4

(B) Answer any 4 :

- (1) Security through _____ means that hiding the details of security mechanisms is sufficient to Secure the system.
 - (a) Layers
 - (b) Networks
 - (c) Obscurity
 - (d) None of the above
- (2) _____ is the enemy of security.
 - (a) Fear
 - (b) Complexity
 - (c) Doubt
 - (d) Uncertainty
- (3) _____ grants an inventor the right to exclude others from producing or using the inventor's discovery or invention for a limited period of time.
 - (a) Trade Marks
 - (b) Patents
 - (c) Intellectual Property Right
 - (d) All of above
- (4) Which of the following definition best describes "Computer Forensics"?
 - (a) Using computers to investigate crime
 - (b) Probing the operating system for signs of malfeasance
 - (c) Predicting behaviours of cyber criminals
 - (d) Investigating crimes committed using computers.

(5) Copying or downloading software and using it without permission is known as _____.

- (a) Software Piracy (b) Dumpster Diving
(c) Social Engineering (d) None of the above

(6) The computer criminal who calls a help desk trying to obtain other users password is most likely a _____.

- (a) Dumpster diver (b) Black-hat hacker
(c) Social engineer (d) Spammer

(A) Answer the following :

(i) What are the Physical security threats ? What are the administrative control for providing physical security ? 7

(ii) Discuss the technical controls for providing physical security in detail. 7

OR

(i) Write a detailed note on Operations Security controls in Action.

(ii) Discuss the principles of operation security and Operations Security Process Controls. 4

(B) Answer any 4 :

(1) What is the main objective of separation of duties ?

- (a) To prevent employees from disclosing sensitive information
(b) To ensure access controls are in place
(c) To ensure that no single individual can compromise a system.
(d) To ensure that audit trails are not tampered with

(2) _____ Processes refers to how long transactions and other types of computerised or process records should be retained.

- (a) Preventive (b) Resource Protection
(c) Monitoring (d) Record Retention

(3) _____ controls are needed for proper marking and handling of assets.

- (a) Monitoring (b) Detective
(c) Preventive (d) Media viability

(4) Which of the following does not pertain to physical security ?

- (a) Site selection
(b) Securing a site against unauthorized access
(c) Protecting people and property
(d) Installing firewalls on all computer.

(5) _____ devices detects an unusual movements within well-defined interior space.

- (a) Intrusion detectors (b) Alarm system
- (c) Motion Detectors (d) Biometrics.

(6) What is an audit trail ?

- (a) A history of transactions indicating data that has been changed or modified.
- (b) A sound recording of conversation taped through perimeter devices.
- (c) Both (a) and (b)
- (d) None of above

(A) Answer the following :

(i) What are the principles of Authentication ? Also, discuss Biometrics in Information Security. 7

(ii) Discuss the following terms :
Identification, Authentication, Least Privilege, Information Owner. 7

OR

(i) Encrypt and decrypt the following message using transposition method with keyword : **Caution**.

Message is : MARCH FORWARD INTO THE NIGHT TUESDAY NEXT.

(ii) Explain the concept of Hashing functions and Block ciphers.

(b) Answer any 3 :

3

(1) When you use the same key to both encrypt and decrypt a message, its called _____ cryptography.

- (a) Asymmetric key (b) Symmetric key
- (c) Public private key (d) None of above

(2) _____ is a network authentication protocol named from the three headed dog in Greek mythology.

- (a) Kerberos (b) Single Sign on
- (c) Federated Identities (d) VPN

(3) What are the two types of ciphers ?

- (a) Transposition and substitution
- (b) Substitution and replacement
- (c) Transposition and shift
- (d) None of above

- (4) _____ methods of Identification work by measuring unique human characteristic as a way to conform identity.
- (a) Biometrics (b) Micrometrics
(c) Macro biometrics (d) Macro metrics
- (5) A _____ disguises messages, allowing only selected people to see through the disguise.
- (a) Cryptosystem (b) Cryptography
(c) Cryptanalysis (d) Cryptology.

4. (A) Answer the following :

- (i) Write a detailed note on Intrusion Detection System. 7
(ii) Discuss : OSI Reference Model. 7

OR

- (i) How can we improve security across the SDLC ? What are the different subgroups recommended to increase the software security throughout the SDLC ?
(ii) Write a detailed note on Malware and Antivirus softwares.

(B) Answer any 3 :

3

- (1) _____ is a miniature Java application embedded in a web page and downloaded to the users machine for execution.
- (a) ActiveX (b) Distributed object
(c) Applet (d) None of Above
- (2) Which of the following is risk with distributed environment ?
- (a) Software Agents (b) Java Applets
(c) ActiveX Control (d) All of Above
- (3) Which of the following occurs when the system classifies an action as anomalous, when it is a legitimate action ?
- (a) False negative (b) Subversion Error
(c) False Positive (d) None of the above
- (4) _____ translates the hardware interface (MAC) addresses to IP protocol addresses.
- (a) Address Resolution protocol
(b) Reverse Address Resolution protocol
(c) Internet Control Message Protocol
(d) File transfer protocol
- (5) Another name for a VPN
- (a) tunnel (b) firewalls
(c) pipeline (d) bypass