B.E. COMPUTER SCIENCE AND ENGINEERING FOURTH YEAR SECOND SEMESTER - 2022

INFORMATION SECURITY

Time: 4 hours Full Marks: 70

Group A (Total Marks: 20) [CO1]
Answer Question No. 1 AND
Answer Question No. 2 OR Question no. 3.

1. What is integrity? What are the types of integrity? Why is availability considered to be an aspect of security? What is the difference between security policy and security mechanism? [8]

2. a) How is disruption differentiated from *userpation*? Give a suitable example.
   b) How does *private key cryptosystem* work? What are its disadvantages? In what circumstances will it be beneficial than *public key cryptosystem*?
   c) What is *integrity policy*? Where is it required?
   d) What role does *assumption* play? [3+4+3+2=12]

3. a) What is *threat*?
   b) What is the *property of confidentiality*? When is information I said to possess the *property of integrity*?
   c) What is *repudiation of origin*? What is *denial of receipt?* You may provide suitable examples for both. [2+4+6=12]

Group B (Total Marks: 10) [CO2]
Answer any ONE Question.

4. a) What are the different types of *malware*? In what category do the following malware belong: *Trojan horse, Botnet, rootkit*
   b) What is *ransomware*? How does *worm* spread and in what ways does it cause damage? [4+6=10]

5. a) How does virus and worm differ? In what category do the following malware belong: *scareware, spyware, botnets*
   b) How does *spyware* work? How does *trojan horse* work? [5+5=10]

6. Why are security best practices required? What does ISO/IEC 27000 series refer to? What are the components of Information Security framework? What is COBIT? [10]

(Contd. From previous page)

Group C (Total Marks: 25) [CO3]
Answer Question No. 7 AND
Answer Question No. 8 OR Question no. 9.

7. What is *cryptographic hash function?* Explain its properties briefly. [3+6=9]

8. a) How is *hash-message authentication code* computed? Why is it used?
   b) What is meant by *access control*? What are the *access control* mechanisms? Briefly explain any two of them. Which access control mechanism may be suitable for hospital management system? Justify your answer. [5+(2+2+3+4)=16]

9. a) How can cryptographic hash function detect duplicate data? What property is this? What may be the size of the message digests produced, say for a single word vis-à-vis a sentence with multiple words? Justify your answer.
   b) What are the *access control* mechanisms? Briefly explain any two of them. Which access control mechanism may be suitable for a user working under different environments with different devices? Justify your answer. [7+(2+3+4)=16]

Group D (Total Marks: 15) [CO4]

10. Answer ANY ONE question: 1X15=15

a) What is *differential privacy*? What are the types of security controls? Mention any one from each type with appropriate example.
How is *k-anonymity* achieved? Obtain *k-anonymity* (k=3) for the following:

Name	Age	Gender	Area of residence	Disease	Hospital
N1	47	F	Kol-67	D1	H1
N2	36	M	Kol-69	D2	H1
N3	56	F	Kol-56	D3	H1
N4	49	F	Kol-56	D3	H2
N5	45	M	Kol-67	D1	H2
N6	38	F	Kol-67	D1	H2
N7	46	F	Kol-69	D2	H3
N8	39	M	Kol-69	D2	H3
N9	38	F	Kol-67	D1	H3

Name any two threat sources.

b) What is ϵ-*differential privacy*? How is *security risk* assessed? How can *threat-vulnerability* pair be identified?
What are the qualitative risk components for a project? What may be the risk impact categories? Identify any two risks and their impact categories with mitigation plan/s for a website development project.

--- --- --- --- --- --- --- --- --- --- --- --- --- --- -- --- --- --- --- ---