Question Paper Code	13977

B.E. / B.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025
Seventh Semester

Computer Science and Engineering (Cyber Security)
20SCEL709 - NATIONAL SECURITY AND CYBER SECURITY
Regulations - 2020

Duration: 3 Hours   Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)
Answer ALL Questions

		Marks	K–Level	CO
1.	What is the primary objective of Cyber Security? a) Reduce software complexity b) Improve hardware performance c) Protect systems, networks, and data from cyber-attacks d) Speed up internet access	1	K1	CO1
2.	The CIA Triad in Cyber Security stands for: a) Central Intelligence Analysis b) Confidentiality, Integrity, Availability c) Cyber security, Intelligence, Assurance d) Control, Inspection, Authentication	1	K1	CO1
3.	A hash function is mainly used to: a) Encrypt data b) Digitally sign data c) Provide data integrity d) Compress data	1	K1	CO2
4.	Which of the following is a key principle of cryptography? a) Redundancy b) Confidentiality c) Modularity d) Accessibility	1	K1	CO2
5.	In the Secure SDLC, which phase involves identifying and mitigating potential threats early in the project? a) Requirement Analysis b) Testing Phase c) Deployment Phase d) Maintenance Phase	1	K1	CO3
6.	Which of the following best describes Penetration Testing? a) An automated process to check coding standards b) A simulation of real-world attacks to identify security weaknesses c) A debugging process to fix logical errors d) A forensic method for analyzing logs	1	K1	CO3
7.	The 2017 WannaCry attack was a case study in which type of cyber threat? a) Phishing attack b) Ransom ware attack c) SQL Injection d) DDoS attack	1	K1	CO4
8.	Which technology trend increases the risk of "shadow IT" security issues? a) Cloud computing b) Internet of Things c) Artificial Intelligence d) Block chain	1	K1	CO4
9.	The first step in developing a cyber security policy is: a) Deploying firewalls b) Risk assessment and requirement analysis c) Enforcing penalties d) Employee training	1	K1	CO5
10.	After containing a data breach, the next critical step is: a) Root cause analysis and eradication b) Employee promotion c) Business expansion d) Reducing system performance	1	K1	CO6

PART - B (12 × 2 = 24 Marks)
Answer ALL Questions

		Marks	K–Level	CO
11.	Outline the role of a firewall in Cyber Security.	2	K2	CO1
12.	Interpret about the Information Technology Act, 2000.	2	K2	CO1
13.	What is a digital signature?	2	K1	CO2
14.	Mention the difference between symmetric and asymmetric encryption.	2	K2	CO2
15.	What is meant by forensic investigation in cyber security?	2	K1	CO3
16.	Define software vulnerability. Name any two common software vulnerabilities.	2	K1	CO3
17.	Define adversarial attack in AI.	2	K1	CO4
18.	Illustrate the impact of the WannaCry ransom ware attack (2017).	2	K2	CO4
19.	State the ethical principle of "non-maleficence" mean in cyber security.	2	K1	CO5

K1 – Remember; K2 – Understand; K3 – Apply; K4 – Analyze; K5 – Evaluate; K6 – Create   **13977**

20. Interpret the main focus of the NIST Cyber security Framework.   2   K2   CO5

21. Define a data breach. Under GDPR, within how many hours must a breach be reported?   2   K2   CO6

22. Name two major international data protection regulations.   2   K1   CO6

PART - C (6 × 11 = 66 Marks)
Answer ALL Questions

23. a) i) Explain the importance of Cyber Security in today's digital world. How does it impact individuals, businesses, and governments?   5   K2   CO1

      ii) Elaborate on common types of malware (virus, worms, trojans, ransom ware, spyware). How do they operate and spread?   6   K2   CO1

OR

   b) i) Summarize CIA Triad in detail. How do confidentiality, integrity, and availability contribute to a secure cyber environment?   6   K2   CO1

      ii) Explain the various types of cyber threats. Illustrate your answer with real-world examples of recent cyber-attacks.   5   K2   CO1

24. a) Classify the different types of cryptographic techniques: symmetric, asymmetric, and hashing. Provide examples for each.   11   K2   CO2

OR

   b) Demonstrate the working of the SSL/TLS protocol. How does it provide confidentiality and integrity over the web?   11   K2   CO2

25. a) Summarize the phases of the Secure Software Development LifeCycle (SDLC) and highlight the security considerations in each phase.   11   K2   CO3

OR

   b) Explain the methodology and steps involved in conducting a penetration test on a web application.   11   K2   CO3

26. a) Examine the Case Study of 2017 Wanna Cry ransom ware attack. Explain how it spread, its global impact, and preventive strategies.   11   K4   CO4

OR

   b) Analyze the cyber security challenges that arise due to multi-tenancyin cloud computing. Provide real-world examples.   11   K4   CO4

27. a) Identify the importance of cyber security governance in an organization. How does it align with business objectives?   11   K3   CO5

OR

   b) Apply the objectives and applications of the NIST Cyber security Framework for critical infrastructure protection.   11   K3   CO5

28. a) Compare and contrast Privacy by Design and Privacy by Default with suitable illustrations.   11   K2   CO6

OR

   b) Explain the role of detection, containment, and recovery in managing a data breach.   11   K2   CO6