SHREE SATHYAM COLLEGE OF ENGINEERINGAND TECHNOLOGY

(Approved by AICTE, NewDelhi and Affiliated To AnnaUniversity, Chennai)

Question Bank for the Units – I to V

IIIrd Year / Vth Semester–B.Tech.,

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

CW3551 DATA AND INFORMATION SECURITY

No	Question	Level	Mark
UNIT - I			
1.	Name he multiple layers of security that a successful organization should have in its place to protect its operations	L1	2
2.	Information Security is which of the following: An Art or Science or both? Justify your answer.	L4	2
3.	Classify the three components of the C.I.A Triangle.What are they used for?	L2	2
4.	Compare Vulnerability and Exposure	L4	2
5.	What is the use of methodology in the implementation of Information Security?	L3	2
6.	Describe a Security Team in an organization. Should the approach to security be technical or managerial?	L3	2
7.	Examine if the C.I.A. triangle is incomplete, why is it so commonly used in security?	L4	2
8.	State the responsibilities of Data Owners, Data custodians and Data users.	L2	2
9.	Create a diagram for Information Security Implementation.	L3	2
10.	Assess the importance of a C.I.A triangle	L5	2
11.	How shall you design the computer as the subject and object of the attack?	L6	2
12.	Show with the help of a diagram about the components of information Security	L3	2
13.	What are the measures required to protect confidentiality of information?	L3	2
14.	Give a short note on E-mail spoofing.	L2	2
15.	How shall you interpret Information Security?	L2	2
16.	Differentiate direct and indirect attacks.	L4	2
17.	Discuss the bottom up approach and top down approach.	L4	2
18.	Define Information Security.	L1	2
19.	List the characteristics of CIA triangle	L1	2
20.	Give the critical characteristics of Information.	L2	2
PART – B – 16 MARKS			
21.	Discuss the steps common to both the systems development life cycle and the security systems life cycle.	L5	16
22.	Analyze the critical characteristics of information. How are they used in the study of computer security?	L4	16
23.	i).Infer about Information Security Project Team. ii) Analyze the methodology important in the implementation of information security? How does a methodology improve the process?	L4	16

24.	What are the six components of an information system? Which are most directly affected by the study of computer security?	L4	16
25.	i)Illustrate the different types of instruction set architecture in detail. ii)Examine the basic instruction types with examples	L2	16
26.	Describe the Security Systems Development Life Cycle.	L3	16
27.	i) Compose the roles of Information Security Project Team. ii) Design the steps unique to the security systems development life cycle in all the phases of SSDLC model.	L2	
28.	Illustrate briefly about SDLC waterfall methodology and its relation in respect to information security.	L6	16
29.	Evaluate the various components of Information Security that a successful organization must have.	L6	16
30.	i) List the various components of an information system and tell about them. ii) List the history of Information Security.	L4	
31.	i).What is NSTISSC Security Model? ii).Describe in detail about the top down approach and the bottom up approach with the help of a diagram.	L5	16
UNIT – II – PART – A – 2 MARKS			
32.	Construct with the help of a table any 4 threats with its examples.	L1	2
33.	What is the difference between a denial-of-service attack and a distributed denial-of-service attack? Which is more dangerous? Why?	L4	2
34.	Examine the meaning of the sentence “data in motion and data at rest”.	L2	2
35.	List any five attacks that is used against controlled systems.	L4	2
36.	Analyse about commonplace security principles.	L3	2
37.	Interpret the following terms: Macro Virus & Boot Virus	L3	2
38.	Evaluate the measures that individuals can take to protect themselves from shoulder surfing	L4	2
39.	Formulate which management groups are responsible for implementing information security to protect the organization’s ability to function.	L2	2
40.	Name the most common methods of virus transmission.	L6	2
41.	Discuss about malware.	L5	2
42.	State the various types of malware? How do worms differ from viruses? Do Trojan horses carry viruses or worms?	L6	2
43.	Express about the password attacks.	L3	2
44.	Define the meaning of the term ‘Electronic Theft’.	L3	2
45.	Express the logic behind using a licence agreement window and the use of online registration process to combat piracy	L2	2
46.	Analyze the major differences between a Threat and an Attack.	L2	2
47.	Illustrate the technical mechanisms that have been used to enforce copyright laws.	L4	2
48.	Give the definition of software piracy.	L4	2
49.	What is meant by the term “Information Extortion”?	L1	2
50.	Show with the help of points the 4 important functions for an organization based on the information security	L1	2
PART – B – 16 MARKS			
51.	How has the perception of the hacker changed over recent years? Compose the profile of a hacker today.	L1	16
52.	i) Explain Integrity Policies. ii) Assess the Secure Software Development.	L2	16
53.	i) List the Computer Security Hybrid Policies. ii) Describe the types of Computer Security.	L2	16
54.	i) State the types of password attacks. ii) Tell the three ways in which an authorization can be handled.	L2	16

55.	Illustrate the methods does a social engineering hacker use to gain information about a user’s login id and password? How would this method differ if it were targeted towards an administrator’s assistant versus a data-entry clerk?	L2	16
56.	How will you develop management groups that are responsible for implementing information security to protect the organization’s ability to function ?	L3	16
57.	Analyze whether information security a management problem? What can management do that technology cannot?	L6	16
58.	Point out why data the most important asset an organization possesses? What other assets in the organization require protection?	L4	16
UNIT – III – TWO MARKS			
59.	List the properties of digital signature	L1	2
60.	Explain the types of attacks.	L2	2
61.	List the forgeries done by attacker to break the break the digital signature	L1	2
62.	What is meant by primitive root?	L1	2
63.	Given two integers A=3 and M=11, identify the modular multiplicative inverse of A under modulo M.	L3	2
64.	Identify the primitive roots of a prime number q=7.	L3	2
65.	Compare RSA approach and DSA approach	L4	2
66.	Explain Kerberos TGS.	L2	2
67.	List the characteristics of user certificate generated by CA.	L1	2
68.	Explain different authentication mechanisms.	L2	2
69.	Discuss the three threats that may occur in a workstation.	L4	2
70.	List the requirements for Kerberos.	L1	2
71.	Explain the Key distribution center.	L2	2
72.	Explain the principles of Kerberos.	L2	2
73.	List the requirements that are not satisfied by version 2 of X.509 certificate.	L1	2
74.	List the categories of certificate extensions.	L1	2
UNIT-III – 16 MARKS			
75.	Explain Elgamal Digital Encryption Scheme.	L2	
76.	Explain the categories of certificate extensions in X.509 certificates.	L2	
77.	Explain briefly about Kerberos.	L2	
78.	Outline the working of X.509 certificate along with its format.	L3	
79.	Outline RSA-PSS Digital signature algorithm.	L3	
80.	Explain Schnorr Digital Encryption Scheme.	L2	
81.	Explain NIST Digital Signature Algorithm.	L2	
UNIT-IV – TWO MARKS			
82.	Discuss about the purpose of padding field in ESP.	L2	2
83.	Explain the steps for preparing signed Data.	L3	2
84.	Explain the two additional fields in payload of ESP.	L2	2

85.	What is PGP?	L1	2
86.	List the IPsec services.	L1	2
87.	What is POP3?	L1	2
88.	Explain the applications of IPV6.	L2	2
89.	Explain the advantages of using Authentication header?	L2	2
90.	Describe replay attack.	L2	2
91.	Explain the usage of Mail Submission Agent.	L2	2
92.	Explain the usage of usage of Message Transfer Agent.	L2	2
93.	List the IPsec services.	L1	2
94.	Explain “must” and “should” terminology in S/MIME.	L2	2
UNIT-IV – 16 MARKS			
95.	Explain S/MIME operational descriptions, message content types and enhanced security services.	L2	16
96.	Explain AH protocol with its format and modes.	L2	16
97.	Illustrate the ESP along with its modes.	L2	16
98.	Explain all the fields in Authentication Header with its two modes.	L2	16
99.	Explain the various IPsec components with a neat architecture diagram. Also explain the IPsec modes.	L2	16
100.	Illustrate email architecture and explain its protocols.	L2	16
UNIT-V – TWO MARKS			
101.	Compare Passive and Active web security attacks.	L2	2
102.	List the parameters of connection state in TLS.	L2	2
103.	Outline the final step of TLS Record protocol.	L2	2
104.	Explain the purpose of alert protocol.	L2	2
105.	List any 5 alert messages.	L2	2
106.	What is chosen-plaintext attack?	L2	2
107.	Explain S-HTTP.	L2	2
108.	Explain the ways of classifying web security threats	L2	2
109.	Explain change cipher spec protocol.	L2	2
110.	Compare TLS connection and TLS Session.	L2	2
111.	Discuss how the TLSV1.3 differs from its previous version?	L2	2
112.	Explain SET protocol.	L2	2
113.	List the parameters of session state in TLS.	L2	2
UNIT – V – 16 MARKS			
114.	Explain the following protocols i) TLS record protocol ii) Heartbeat protocol	L3	16
115.	i) Explain the secure socket layer and working of SSL protocol. ii) Explain the categories of web security threats that affects the integrity, authenticity, confidentiality and availability and explain its consequences and countermeasures.	L3	16

116.	Outline Transport level security architecture and explain its protocols.	L3	16
117.	Explain the protocols for securing internet communication, email and web transactions.	L3	16
118.	Explain the working of Handshake protocol.	L3	16
119.	You are developing a mobile application where users can chat securely with one another. The application will send messages over the internet, and you want to ensure that these messages remain private and unaltered during transit. Describe how you would apply Transport Level Security (TLS) in your application to protect the messages. Discuss how the two layers of protocols in TLS architecture would participate in establishing and maintaining this secure communication.	L3	16

1: Knowledge, L2: Comprehension, L3: Application, L4: Analysis, L5: Evaluation, L6: Synthesis