Semester: VII	Department of ISE & CSE(AI)	AY: 2026-27
Course Code: BIS703	Course Name: Information and Network Security	

Question Bank

Q.	Module-01	M	L	C
1.	Explain the basic terminology of crypto along with its black box?	6	L2	CO1
2.	Explain simple substitution cipher with an example?	8	L3	CO1
3.	Discuss double transposition cipher with an example?	8	L3	CO1
4.	Explain modern crypto history?	6	L2	CO1
5.	Describe the taxonomy of cryptography	7	L2	CO1
6.	Describe the taxonomy of cryptanalysis.	7	L2	CO1
7	Write short notes on (i) Project VENONA, (ii) Codebook Cipher	10	L2	CO1
8	Define one- time pad and apply one time pad to encrypt and decrypt the data given, "heilhitler" e = 000, h=001, i=010, k=011,l=100, r=101,s=110, t=111 and key : 110 101 110 101 111 100 000 101 110 000	10	L3	CO1
9	Compute the Encryption and Decryption of plain text **VSRQJHEREVTXDUHSDQWU** using CAESAR cipher. Assume shift position k=4?	8	L3	CO1
10	Define one time pad with example?	6	L2	CO1
	Module-02			
11	Discuss the requirements of a cryptographic has function	6	L2	CO2
12	Explain Cryptographic Tiger Hash Algorithm	10	L3	CO2
13	Explain the uses of hash function	6	L2	CO2
14	Define secret sharing. Explain the concept of secret sharing using key escrow.	10	L3	CO2
15	Discuss the usage of random numbers with unpredictability.	6	L2	CO2
16	With an example, explain HMAC function in detail.	8	L3	CO2
17	Demonstrate birthday problem with example	8	L3	CO2
18	What is cryptographic has function. What are the needs that cryptographic hash function must provide?	8	L2	CO2
19	Write short notes on (i) Information Hiding , (ii) Secret sharing	10	L2	CO2
20	Explain tiger hash outer round with neat diagram.	8	L3	CO2
	Module-03			

Aditya College of Engineering and Technology

21.	Define randomness. Differentiate between deterministic and non-deterministic generators.	10	L2	CO3
22.	Explain the freshness mechanism in detail.	10	L2	CO3
23.	Explain the problem related to passwords.	6	L2	CO3
24.	Describe the dynamic password schemes based on challenge-response.	8	L2	CO3
25.	Explain the Diffie-Hellman key agreement protocol.	8	L2	CO3
26.	With a neat diagram, explain the reflection attack against protocol-3.	8	L3	CO3
27.	Explain zero knowledge analogy with example.	8	L2	CO3
28.	What are the typical AKE protocol goals? Explain	8	L2	CO3
29.	Explain cryptographic password protection with neat diagram.	8	L2	CO3
30.	Describe various categories of identification information used for entity authentication. Illustrate each with examples.	10	L2	CO3
	Module-04			
31.	Explain the key life cycle with a neat diagram.	6	L2	CO4
32.	Discuss key distribution approaches to acquiring shared keys from a KC	10	L2	CO4
33.	Explain the key storage risk factor.	6	L2	CO4
34.	Explain the fields of X.509 version 3 public key certificate.	8	L2	CO4
35.	Explain the public key certificate management models	10	L2	CO4
36.	With a neat diagram, explain the unique key per transaction (UKPT) scheme in key establishment process.	8	L3	CO4
37.	Explain governing key management. Discuss key-management policies, practices and procedures.	10	L2	CO4
38.	Explain tamper resistance techniques	8	L2	CO4
39.	Explain alternative approaches to public-key management	8	L2	CO4
40.	Explain certification of public keys. Why is certification required	8	L2	CO4
	Module-05			
41.	Explain simple SSL handshake protocol.	10	L2	CO5
42.	Discuss the SSL Key management in detail.	10	L2	CO5
43.	Discuss WLAN design issues.	6	L2	CO5
44.	Explain GSM and UMTS key management.	10	L2	CO5
45.	Discuss the usage of cryptography in video broadcasting.	6	L2	CO5
46.	Explain the application of cryptography for securing the Internet.	8	L2	CO5
47.	Explain the problems/attacks associated with WEP	8	L2	CO5
48.	Explain cryptography for secure payment card transactions.	8	L2	CO5
49.	Explain cryptography for identity cards/eID cards.	8	L2	CO5
50.	Explain cryptography for mobile telecommunications.	8	L2	CO5

Aditya College of Engineering and Technology

Aditya College of Engineering and Technology