Semester: **VII**	DEPARTMENT OF AIML	AY: 2026-27
Course Code: **BAD703**	Course Name: Data Security and Privacy	

Question Bank

Q.	Module-01	M	L	C
1.	Draw the simplified model of symmetric encryption and explain it.	4	L2	CO1
2.	list the three independent dimensions of cryptographic systems	6	L1	CO1
3.	Define following terms: i) Cryptography ii) Ciphertext iii) Encryption iv) Decryption	6	L1	CO1
4.	Explain Caesar cipher with example OR Interpret ceasar cipher substitution for below message: meet me after toga party and explain the mathematical equations with key =3.	10	L3	CO1
5.	Apply play fair cipher algorithm. Find the cipher text for plain text =“instruments” with key =MONARCHY. OR Encrypt the plain text “electronics” using a play fair cipher with a key= INDIA OR Explain the Playfair cipher and its rules for the following example Plain text =cryptography key =MONARCHY OR A message is received at an Australian wireless station in Playfair code: KXJEY UREBE. The key used was ROYAL NEW ZEALAND NAVY. Decrypt the message.	10	L3	CO1
6.	Demonstrate and Explain the plain text = ‘cryptography’ using Hill cipher technique with key matrix $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and decrypt the same. OR	10	L3	CO1

Aditya College of Engineering and Technology

	Using Hill Cipher technique, encrypt the plain text "Paymoremoney" using the key K= $\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ [Hint : a = 0, b = 1, ..., z = 25]. OR Encrypt the message "MAM" using Hill cipher with key K= $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$ Further show the calculations for corresponding decryption of Cipher text. OR Encrypt the message "Meet me at the usual place at ten rather than eight O'clock". Hill cipher with key $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ Show your calculation and result.			
7.	In the One – time pad version of a Vigenere Cipher, Key stream is 9 0 7 23 15 21 14 11 11 2 8 9. In this scheme, encryption is done by shifting with number mentioned in the key. Modify and Encrypt the plain text "sendmoremoney" and using the Cipher text obtained, find a key such that Cipher text decrypts to "cashnotneeded".	10	L3	CO1
8.	Distinguish between: i) Confusion and Diffusion ciphers ii) Block cipher and stream ciphers	6	L2	CO1
9.	Infer Feistel encryption and decryption algorithm with neat diagram Differentiate confusion and diffusion, explain the working of Feistel structure of DES method	8	L2	CO1
10.	Summarize DES encryption algorithm with need diagram OR With a neat schematic ,explain the DES encryption algorithm	10	L2	CO1
11.	Given data = 208 and IP = [4 1 8 2 3 5 6 7] (IP means Initial Permutation). Find the permutation of the data and its inverse by applying suitable algorithm.	6	L3	CO1
12.	Define substitution and transposition techniques.	4	L1	CO1
	Module-02			
13.	Explain about pseudorandom number generators based on asymmetric cipher			CO2

Aditya College of Engineering and Technology

14.	With a neat diagram, explain the six ingredients of a public-key cryptography. OR Explain Public-Key Cryptosystems. OR Differentiate Public Key Encryption and Conventional Encryption. Classify and explain Public Key Cryptosystems.	6	L2	C02
15.	With relevant diagram, explain Authentication and secrecy in public-key cryptosystem.	8	L2	C02
16.	What requirements must a public-key cryptosystems fulfill to be a secure algorithm?	8	L2	C02
17.	Explain the requirements and applications for public key cryptography.(3+4)	10	L2	C02
18.	Explain RSA algorithm operation in detail. Perform an encryption of plain text and decryption of cipher text using RSA algorithm for P = 3, q = 11, e = 7 and M = 5.(R) OR Explain the description of the RSA algorithm. OR Explain RSA algorithm. Using RSA algorithm perform encryption and decryption using p = 17, q = 11, e = 7 and M = 88. OR In a Public key system using RSA, you intercept the ciphertext C = 10 sent to a user where n = 221. What is the plaintext	10	L3	C02
19.	Infer about the security of RAS	4	L2	C02
20.	Explain Diffie-Hellman key exchange algorithm. Apply Diffie-Hellman key exchange algorithm for q = 71, as primitive root α = 7. A's private key is 5, B's private key is 12. Find: i) A's public key ii) B's public key iii) Shared secret key. OR Explain the Diffie-Hellman key exchange algorithm. OR Explain Diffie-Hellman key exchange algorithm and also show that the calculations produce the identical results. OR Consider a Diffie-Hellman scheme with common prime, q = 11 and primitive root α = 2.	10	L3	C02

Aditya College of Engineering and Technology

	i. Show that 2 is a primitive root of 11. ii. If user1 has public key YA = 9, what is A's private key XA. iii. If user B has public key YB = 3, what is secret key K shared with A. OR Evaluate a Diffie-Hellman key exchange concept for prime number q = 71 and primitive root α = 7. i) If user A has private key XA = 5, what is A's public key YA= ? ii) If user B has private key XB = 12, what is B's public key YB = ? iii) What is shared key?			
21.	Diffie-Hellman Key exchange is vulnerable to Man-in-the-middle attack. Substantiate with a sequence diagram. OR Compare how Diffie-Hellman key exchange algorithm useful in evaluating man-in-the-middle attack concept.	8	L2	C02
22.	Explain Symmetric Key Distribution using Asymmetric Encryption with a solution for Man-in-the-Middle attack.	10	L2	C02
23.	"Diffie -Hellman Key Exchange is vulnerable to Man-in-the- middle attack" sustainable with a sequence diagram.	10	L2	C02
24.	Explain about the elliptic curve cryptography	6	L2	C02
25.	Discuss elliptic curve cryptography for analog of Diffie -Hellman key exchange and explain with neat steps	10	L2	C02
	Module-03			
26.	Explain the key principles of key management in a cryptographic system. Why is it considered a critical part of cybersecurity?	8	L2	CO3
27.	Discuss the importance of key lengths and lifetimes. How do they affect the strength and security of cryptographic systems?	8	L2	CO3
28.	Describe the key generation process. What are the requirements for generating strong cryptographic keys?	8	L2	CO3
29.	Differentiate between key agreement and key transport. How are they used in key establishment protocols?	8	L2	CO3
30.	Explain various techniques for key establishment. Support your answer with examples like Diffie-Hellman or RSA key transport.	8	L2	CO3
31.	What are the different options available for secure key storage? Compare hardware and software-based methods.	8	L2	CO3
32.	Explain how keys are used differently in symmetric and asymmetric cryptography. Provide examples.	8	L2	CO3
33.	What are the primary goals of governing key management? How do governance policies help prevent security breaches?	8	L2	CO3
34.	What is a digital certificate? Explain the process of certification of public keys using a Certificate Authority (CA).	8	L2	CO3

Aditya College of Engineering and Technology

35.	Describe the certificate lifecycle. Include stages like issuance, validation, renewal, revocation, and expiration.	8	L2	CO3
36.	Discuss different public-key management models such as hierarchical, mesh, and bridge CA models.	8	L2	CO3
37.	Compare traditional certificate-based key management with Identity-Based Public Key Cryptography (IDPKC).	8	L2	CO3
	Module-04			
38.	Explain the major threats to web security and describe how they affect modern web applications.	10	L2	CO4
39.	Explain web security considerations and common web-based attacks.	10	L2	CO4
40.	Describe the architecture of TLS and explain how it ensures confidentiality, integrity, and authentication.	10	L2	CO4
41	Discuss the architecture of IPsec and explain its main components.	10	L2	CO4
42	Demonstrate how organizations create and enforce IPsec policies to protect network traffic.	10	L2	CO4
43	Discuss the Encapsulating Security Payload (ESP) protocol and explain how it provides confidentiality, integrity, and authentication.	10	L2	CO4
44	Explain the challenges in managing and maintaining multiple Security Association (SAs) in large networks	10	L2	CO4
45	Describe the purpose of Internet Key Exchange (IKE) in IPsec.	10	L2	CO4
46	Compare TLS and IPsec in terms of purpose, operation layer, use cases, and security characteristics.	10	L2	CO4
	Module-05			
47	Describe the IP security overview and the need for IP security policies.	10	L2	CO5
48	Explain the LSB (Least Significant Bit) encoding technique with a suitable example. LSB (Least	10	L2	C05
49	Explain watermarking and its intuitive and digital methods.	10	L2	CO5
50	Illustrate the process of data hiding in text using innocuous text techniques.	10	L2	CO5
51	Briefly explain about BPCS steganography? Explain its working principle and advantages.	10	L2	CO5
52	Explain the different techniques of data hiding in images, including LSB encoding.	10	L2	CO5
53	Explain the concept of lossless data hiding in images and discuss its working procedure	10	L2	CO5
54	Explain text-based data hiding techniques, including intuitive methods, simple digital methods, innocuous text, and mimic functions.	10	L2	CO5
55	Explain the concept of data hiding and discuss its important applications in data security.	10	L2	CO5

Aditya College of Engineering and Technology

56	Explain mimic functions in text-based data hiding with suitable examples.	10	L2	CO5

Aditya College of Engineering and Technology