Silver Oak University
Silver Oak College of Computer Application
Master of Computer Application

Semester:	3	**Academic Year:**	2024-25
Course Name:	Information Security	**Course Code:**	2040237202

Question Bank

Sr. No.	Question Text	Marks	CO
1 : Introduction to IS & Symmetric Cipher Model			
1	Define Cryptography and Crypt-analysis.	3	CO-1
2	Draw and explain conventional cryptosystem.	5	CO-1
3	Differentiate Symmetric and Asymmetric key cryptography.-	4	CO-1
4	what are challenges of symmetric key cryptography? List out various symmetric key algorithms	3	CO-1
5	Explain the Conventional security model used for Information security.	5	CO-1
6	List and briefly define categories of securityattacks.	4	CO-1
7	List and briefly define the security services.	3	CO-1
8	What is security Services? Explain any three types of security services.	5	CO-1

9	Define the terms: Confidentiality, Data integrity, Non-repudiation	3	CO-1
10	What is Security mechanism?	2	CO-1
11	List and explain various security mechanisms.	5	CO-1
12	Explain Various types of Attack.	5	CO-1
13	Let the keyword in playfail cipher is “keyword”. Encrypt a message “come to thewindow” using playfair cipher.	5	
14	Construct a playfair matrix with the key “occurrence”. Generate the cipher text for theplaintext “Tall trees” **OR** Construct 5 X 5 playfair matrix for the keyword “OCCURANCE”.	5	
15	Using playfair cipher encrypt the plaintext “Why, don’t you?”. Use the key “keyword”.	5	
16	Explain rail fence Cipher technique	4	
17	difference between substitution and transposition technique	3	
18	What is the purpose of S-boxes in DES?	3	
19	Draw and explain the single round of DES algorithm. Explain single round function of DES with suitable diagram. Explain single round of DES algorithm.	5	
20	Explain various steps of AES in short.	5	
21	Explain the key generation in DES algorithm	5	
22	Explain the key generation in AES algorithm	5	
23	Differentiate DES and AES.	4	
2 : Cipher Feedback mode			
24	List various modes of operations of block cipher. Explain any three of them briefly. List and explain various block cipher modes of operation with the help of diagram.	5	CO-2
25	Explain cipher feedback mode of operation.	4	CO-2
26	Explain working of ECB.Why ECB (Electronic code book) is rarely used to encryptmessage?	4	CO-2
27	Why CFB(Cipher feedback mode) encrypted messages are less	5	CO-2

	subject to tampering thanOFB(Output feedback mode)?		
28	Explain Cipher Feedback (CFB) and Output Feedback mode (OFB) block cipher modes ofoperation with the help of diagram.	5	CO-2
29	Explain Cipher Block Chaining (CBC) and Electronic Code Book (ECB) block cipher modes ofoperation with the help of diagram.	5	CO-2
30	Explain Counter (CTR) algorithm mode with diagram.	4	CO-2
31	Explain CFB algorithm mode with diagram.	4	
3 : Public Key Infrastructure			
32	What is public key cryptography?	3	CO-3
33	Compare public with conventionalcryptography	4	CO-3
34	Write the differences between conventional encryption and public keyencryption	3	CO-3
35	Compare public and Private key Cryptography.	4	CO-3
36	Give the steps of RSA algorithm	4	CO-3
37	Explain RSA algorithm with Example.	5	CO-3
38	In a public key system using RSA, the cipher text intercepted is C=10 which is sent tothe user whose public key is e=5, n=35. What is the plaintext M?	4	CO-3
39	Calculate ciphertext in case of RSA if p=3,q=11,e=3,M=5	5	CO-3
40	Perform encryption and decryption using the RSA algorithm for p=3, q=11, e=7,M=5	5	CO-3
41	The encryption algorithm to be used is RSA. Given two prime numbers 11 and 3 and public key (e) is 3. Calculate the decryption key and Calculate the ciphertext if the givenplaintext is 7	5	CO-3
42	P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm?	5	CO-3
43	Explain process of encryption in RSA Algorithm with suitable example. (Prime Number P,Q and Encryption Key E is given for reference) P=7, Q=17, E=7	5	CO-3
44	Briefly explain Diffie-Hellman key exchage with example - (	5	CO-3

	Write and explain the Diffie-Hellman key exchange algorithm.- Explain Deffie Hellman key exchange scheme in detail What is primitive root? Explain Diffi-Hellman key exchange algorithm with proper example.- Explain Diffie – Hellman key exchange.		
45	Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middleattack? Justify	5	CO-3
46	Briefly explain the Diffie-Hellman key exchange.	4	CO-3
47	Write Diffie Hellman key exchange algorithm.	3	CO-3
4 : Cryptographic Hash Functions			
48	Explain different characteristics of hash function	4	CO-4
49	Explain Following properties of hash function. 1)one way property 2) Weak collision resistance 3) Compression Function in hash algorithm	5	CO-4
50	What is the difference between weak and strong collision resistance?	3	CO-4
51	Write the properties of hash functions	4	CO-4
52	Differentiate between hashing and encryption.	3	CO-4
53	Explain basic Hash code generation	3	CO-4
54	What are the practical applications ofhashing?	2	CO-4
55	Write requirement of hash function and briefly explain simple hash function?	5	CO-4
56	Explain the general structure of secure hash functions	3	CO-4
57	What characteristics are needed in a secure hash function?	4	CO-4
58	What is the need for message authentication? List various techniques used forAuthentication. Explain anyone	5	CO-4
59	How message authentication code can be used to achieve message authentication andconfidentiality?	5	CO-4
60	How following can be achieved with message authentication code (MAC)? a) Message authentication b) Message authentication and confidentiality	4	CO-4

61	What is MAC?	2	CO-4
5 : Key Infrastructure			
62	Write the key distribution scenario in which each user shares a unique master key withkey distribution center	3	CO-5
63	Explain the key distribution scenario and write how does decentralized key control work?	5	CO-5
64	What is KDC?	3	CO-5
65	What is a nonce in key distribution scenario?	2	CO-5
66	Explain different key distribution techniques?	5	CO-5
67	Discus the ways in which public keys can be distributed to two communicationparties	5	CO-5
68	List and Explain Various Key management techniques.	5	CO-5
69	Explain Key Distribution Methods	4	CO-5
70	List and explain four general categories of schemes for the distribution of publickeys	5	CO-5
71	How public keys can be distributed	4	CO-5
72	Explain Public key Infrastructure	4	CO-5

Ms. Hiral Shastri
Course Coordinator

Ms. Risha Tiwari
Head of Department