Roll No. | | | | | | | | | | |

ANNA UNIVERSITY (UNIVERSITY DEPARTMENTS)

B.E. /B. Tech / B. Arch (Full Time) - END SEMESTER EXAMINATIONS, APR / MAY 2024

INFORMATION TECHNOLOGY
VII Semester
IT5703 & Cryptography and Security
(Regulation 2019)

Time:3 hrs Max. Marks: 100

CO1	Apply the basic security algorithms and policies required for a computing system.
CO2	Predict the vulnerabilities across any computing system and hence be able to design security solution for any computing system.
CO3	To identify any network security issues and resolve the issues.
CO4	To manage the firewall and WLAN security.
CO5	Evaluate the system related vulnerabilities and mitigation.

BL – Bloom's Taxonomy Levels
(L1-Remembering, L2-Understanding, L3-Applying, L4-Analysing, L5-Evaluating, L6-Creating)

PART- A (10x2=20Marks)
(Answer all Questions)

Q. No.	Questions	Marks	CO	BL
1	Differentiate threat, vulnerabilities and attacks.	2	1	L2
2	Find the value of 6^{10} mod 11, using Fermat's little theorem.	2	1	L3
3	What are strong, weak and semi-weak keys with respect to DES.	2	2	L2
4	State the terms Confusion and Diffusion with respect to cryptography.	2	2	L2
5	Write about Replay attack and Man-in-the-middle attack.	2	3	L1
6	Define a cryptographic hash function.	2	3	L1
7	State the purpose of S/MIME and its message content types.	2	4	L1
8	What are the services provided by IPSec.	2	4	L1
9	State the differences between viruses and worms.	2	5	L2
10	List some Security protocols used for wireless LANs and its features.	2	5	L1

PART- B (5x 13=65Marks)
(Restrict to a maximum of 2 subdivisions)

Q. No.	Questions	Marks	CO	BL
11 (a)	Use the playfair cipher to encipher the message "The key is hidden inside the cupboard". The secret key can be made by filling the first and part of the second row with the word "CAUTIOUS" and filling the rest of the matrix with the rest of the alphabet.	13	1	L2,L3
	OR			
11 (b)	Solve the set of following linear congruences using Chinese Remainder Theorem : x=2 (mod 5), x=3 (mod 7), x=10 (mod 11)	13	1	L2,L3
12 (a)	Discuss about the general design rounds of operation	13	2	L2

12 (b)	(i) Explain about RC4 Algorithm (ii) Discuss the triple-DES encryption and decryption method.	7 6	2 2	L2 L2
13 (a)	Explain the processes involved in Secure Hash Algorithm.	13	3	L2
	OR			
13 (b)	(i) Describe the Diffie-Hellman Key Exchange algorithm. (ii) Alice and Bob use the Diffie-Hellman key Exchange technique with a common prime q = 23 and a primitive root α = 3. a. If Alice has a private key X_A = 97, find her public key Y_A. b. If Bob has a private key X_B = 233, find her public key Y_B. c. What is the shared secret key between Alice and Bob?	6 7	3 3	L2 L3
14 (a)	Elaborate on RSA Digital Signature Scheme and compare it with Elgammal Digital Signature Scheme	13	4	L2, L4
	OR			
14 (b)	Discuss in detail the Kerberos Authentication mechanism.	13	4	L2
15 (a)	Explain about the basic mechanisms of firewalls and its types along with the operational procedures.	13	5	L2
	OR			
15 (b)	Elaborate on the variety of functions performed by Intrusion Detection Systems and its types.	13	5	L2

PART- C (1x 15=15Marks)

(Q.No.16 is compulsory)

Q. No.	Questions	Marks	CO	BL
16.	(i) Elaborate on RSA algorithm, and possible approaches by which RSA can be attacked. (ii) Perform Encryption and Decryption using the RSA algorithm for the following inputs: two prime numbers, p = 17 and q = 31 whose public key, e = 7 for the message M = 2.	7 8	2 2	L2 L4 L3