RollNo. | | | | | | | | | | |

ANNA UNIVERSITY (UNIVERSITY DEPARTMENTS)

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

INFORMATION TECHNOLOGY
VII Semester
IT5703 & Cryptography and Security
(Regulation2019)

Time:3hrs

Max.Marks: 100

CO1	To apply the basic security algorithms and policies required for a computing system.
CO2	To 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	To evaluate the system related vulnerabilities and mitigation and to design secured web applications in real-time.

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	State the importance of Non-Repudiation in Security service.	2	1	L2
2	Using Euclidean algorithm, find the greatest common divisor of the following pair of integers: 300 and 42.	2	1	L3
3	Why does DES function need an expansion permutation?	2	2	L2
4	Which of the transformations of AES change the content of bytes and which do not?	2	2	L1
5	Define Pre-image resistance and Second pre-image resistance properties of cryptographic hash functions.	2	3	L1
6	What are the key advantages of Quantum Key Distribution over classical key exchange methods?	2	3	L2
7	State the importance of certificate authority in X.509.	2	4	L1
8	What is the procedure for developing Digital Signature?	2	4	L1
9	List the two schemes of 802.11i for protecting data in the transfer phase.	2	5	L1
10	On what criteria a security system is evaluated?	2	5	L2

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

Q.No.	Questions	Marks	CO	BL
11 (a)	(i) Solve the following simultaneous congruences using the same: $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$, $x \equiv 10 \pmod{11}$	8	1	L3

	(ii) Write the pseudocode for Miller-Rabin primality testing.	5	1	L2
	OR			
11 (b)	(i) If P = (18,20) and Q = (6,4) are two points in the elliptic curve E23(1,1), find P+Q and 2P. (ii) Discuss about the various categories of transpositional ciphers with examples.	8 5	1 1	L3 L2
12 (a)	(i) Describe the structure and operations involved in Fiestel Cipher used in DES. (ii) Write about the importance of Linear and differential cryptanalysis.	8 5	2 2	L2 L2
	OR			
12 (b)	(i) Explain about the RC4 cipher along with pseudocode. (ii) Elaborate the key expansion process of AES with neat diagram.	8 5	2 2	L2 L2
13 (a)	Explain the processes involved in SHA algorithm for the maintaining integrity.	13	3	L2
	OR			
13 (b)	(i) Write about the Elgammal Digital signature Scheme. (ii) Users A and B use the Diffie-Hellman key exchange technique with a common prime, q = 71 and a primitive root, α = 7. If the user has a private key, X_A = 5, What is A's public key Y_A ?	8 5	3 3	L2 L3
14 (a)	(i) Explain the IP security protocol and its modes of operation. (ii) Differentiate SSL and TLS protocols.	8 5	4 4	L2 L2
	OR			
14 (b)	(i) Describe the fields involved in X.509 certificate and the revocation list. (ii) Write a note on the importance of Blockchain in current digital security with respect to any application of your choice.	8 5	4 4	L2 L3
15 (a)	Discuss about the different types of Firewalls.	13	5	L2
	OR			
15 (b)	Explain about the different malicious softwares and suggest various measures to overcome the malwares.	13	5	L2

PART- C(1x 15=15Marks)

(Q.No.16 is compulsory)

Q.No.	Questions	Marks	CO	BL
16.	(i) Elaborate on OWASP top ten vulnerabilities of recent years that prevail in various computing systems, with case studies. Also suggest suitable measures to overcome those.	15	5	L4, L6