ADDITIONAL CONTROLLER OF EXAMINATIONS ★
AU
CHENNAI
600 025

Roll No.

ANNA UNIVERSITY (UNIVERSITY DEPARTMENTS)

B. TECH (IT) ARREAR EXAMINATIONS – APR/MAY 2025

INFORMATION SCIENCE AND TECHNOLOGY

IT5703-CRYPTOGRAPHY AND SECURITY

(REGULATIONS 2019)

Time: 3 Hours Answer ALL Questions Max. Marks 100

PART- A (10 x 2 = 20 Marks)

Q.No	Questions	Marks
1.	Define Caesar cipher in cryptosystem.	2
2.	State Fermat's theorem. Find 349 mod 7 using Fermat's theorem	2
3.	What is the purpose of S-Box & P-Box in DES?	2
4.	How elliptic curve cryptography is considered to be better than RSA?	2
5.	What is the block size of MD5 and how many bits are produced as the message digest?	2
6.	What are the possible attacks on digital signature?	2
7.	Differentiate Transport and Tunnel mode in IPsec?	2
8.	What are the fields present in IP Header for Authentication?	2
9.	List the most dangerous threats in cyber world. Brief any two.	2
10.	Mention the Roles of IDS in network security.	2

PART- B (5 x 13 = 65 Marks)

(Restrict to a maximum of 2 subdivisions)

Q.No	Questions	Marks
11.	a) i) Encrypt the message "A GOOD TONGUE IS A GOOD WEAPON" using rail fence cipher and decrypt the same. (8) ii) Define Euler's theorem and solve 6^{24} mod 35 using Euler's theorem (5)	13
	OR	
	b) State and explain the Chinese Remainder Theorem. Using this theorem find a single congruence equivalent to the following congruence's: $x \equiv 2(mod\ 3) \quad x \equiv 3(mod\ 5) \quad x \equiv 2(mod\ 7)$	13
12	a) i) Write in detail about how security established by using RSA algorithm in cryptosystem? Sign and verify a message '6' using RSA cryptosystem as p = 11, q=3; Choose a valid alpha. If the private key is 7, find the public key.	13
	OR	
	b)i) Explain the Kerberos protocol for key distribution? Explain the functionality of each step. Also write about Kerberos Realms. Compare version 4 and version 5.	13

13.	a) With DSS, because the value of 'K' is generated for each signature, even if the same message is signed twice on different occasions, the signature will differ. When using RSA signatures this does not happen. What is the practical implication of this difference?	**13**
	OR	
	b) Describe in detail about MD5 Algorithm with neat diagram and also compare the upgraded features of MD5 with SHA algorithm.	**13**
14.	a) i) Explain the various operation of Pretty Good Privacy with necessary diagrams to enhance your email service (8) ii) what is the need for Multipurpose Internet Mail Extensions service in SMTP protocol towards email communication? (5)	**13**
	OR	
	b) i) Explain briefly about IP Security. What services are provided by IP Security? (8) ii) Explain in detail about Internet Key exchange protocol (5)	**13**
15.	a) i) Explain briefly about Intrusion Detection System (8) ii) Why does a web server need to know the address, browser type, and cookies for a requesting client? (5)	**13**
	OR	
	a) i) Describe how the various types of firewalls interact with the network traffic at various levels of the OSI model. (8) ii) List the five generations of firewall technology. Which generations are still in common use? (5)	**13**

PART- C (1 x 15 = 15 Marks)

(Q. No 16 is Compulsory)

Q.No	**Questions**	**Marks**
16.	i) Users Alice and Bob use the Diffie-Hellman key exchange technique with a common Prime A=11 and a primitive root g=2. If Alice chooses the private key a=4 and Bob chooses the Private Key b=3, explain how do they compute the shared secret key k? Explain the algorithm. (10) ii) Solve using Play fair cipher. Encrypt the word **"Semester Result"** with the keyword **"ARREAR".** List the rules used (5)	**15**

ADDITIONAL CONTROLLER OF EXAMINATIONS ★
AU
CHENNAI
600 025