USN □□□□□□□□□□

RV COLLEGE OF ENGINEERING®

(An Autonomous Institution affiliated to VTU)

VI Semester B. E. Examinations September-2023

Information Science and Engineering

CRYPTOGRAPHY AND NETWORK SECURITY

Time: 03 Hours ***Maximum Marks: 100***

Instructions to candidates:

1. Answer all questions from Part A. Part A questions should be answered in first three pages of the answer book only.
2. Answer FIVE full questions from Part B. In Part B question number 2, 7 and 8 are compulsory. Answer any one full question from 3 and 4 & one full question from 5 and 6.

PART-A

1	1.1	Mention any four security services provided by $ITU-T$.	02
	1.2	Distinguish between a modern and traditional symmetric key cipher.	02
	1.3	Justify the statement “all block ciphers are polyalphabetic”.	02
	1.4	How many exclusive –or operations are used in the DES cipher, explain.	02
	1.5	Distinguish between cryptography and steganography.	02
	1.6	Define the elliptic curve digital signature scheme and compare it to the elliptic curve cryptosystem.	02
	1.7	Identify any two attacks on digital signatures.	02
	1.8	Can a PGP packet carrying the tag value of 6 contain another packet? Justify.	02
	1.9	When a session is resumed, which of the following cryptographic secrets need to be recalculated? a) Pre-master secret b) Master secret c) Authentic keys d) Encryption keys. e) IVs	02
	1.10	Discuss why IKE is needed in IPSec.	02

PART-B

2	a	Determine the key domain and the modulus when Alice often needs to encipher plaintext made of both letters(a to z) and digits (0 to 9). i) if she uses an additive cipher. ii) if she uses a multiplication cipher. iii) If she uses an affine cipher.	06
	b	Distinguish between active and passive security attacks. Identify some attacks under each category.	04
	c	Employ a Hill cipher to encipher the message “we live in a insecure world”. Use the following key: $K = \begin{bmatrix}3 & 2\\5 & 7\end{bmatrix}$	06

3	a	Consider a block cipher where $n = 64$, if there are 10 1's in the ciphertext, how many trail-error text does Eve need to do recover the plaintext from the intercepted ciphertext in each of the following cases? i) cipher is designed as a submission cipher. ii) The cipher is designed as a transposition cipher.	08
	b	Describe double DES. Identify and explain suitably what kind of attack on double DES makes it useless.	08
		OR	
4	a	Differentiate between block cipher and stream ciphers.	05
	b	Discuss a simple product cipher with two rounds with suitable diagram.	05
	c	Discuss briefly the weakness identified in the design of DES.	06
5	a	Illustrate and describe with suitable diagram encryption, decryption and key generation in Rabin cryptosystem. Write psuedocode for key generation.	10
	b	List and explain different kinds of attacks on digital signatures. List the types of forgery.	06
		OR	
6	a	Discuss the steps employed to sign and verify the message in DSS scheme.	08
	b	With taxonomy for potential attacks on RSA, discuss any two categories of potential attacks.	08
7	a	List the various types of messages and subtypes that are created from cryptographic message syntax in $S/MIME$. Discuss any one of the type listed above in detail that provides integrity of data/message.	08
	b	Describe the SSL Specific protocol-handshake action in detail by explaining the sequence of steps used in Secure Socket Layer handshake Protocol for establishing a new session.	08
8	a	Draw the IP security authentication header and describe the functions of each field.	08
	b	Explain the method of protecting IP datagram from replay attack using IPsec.	08