USN | | | | | | | | | | |

RV COLLEGE OF ENGINEERING®

(An Autonomous Institution Affiliated to VTU)

V Semester B. E. Examinations April/May -2024

Information Science and Engineering

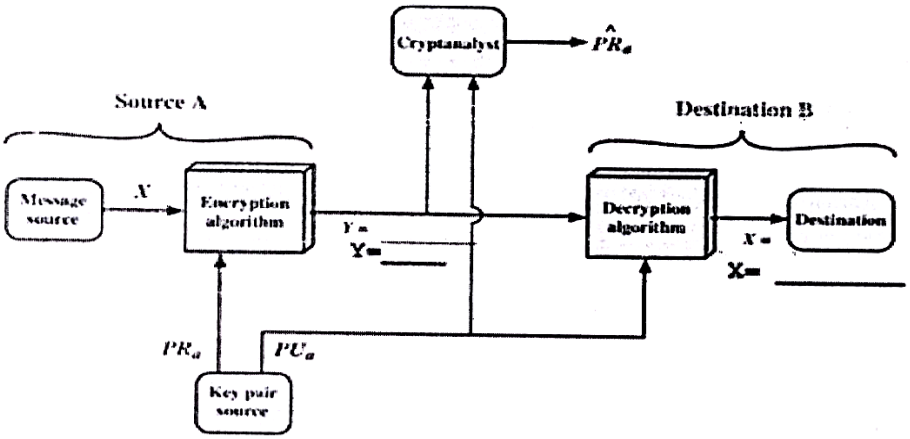
CRYPTOGRAPHY AND NETWORK SECURITY

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 is compulsory. Answer any one full question from 3 and 4, 5 and 6, 7 and 8, 9 and 10.

PART-A

			M	BT	CO
1	1.1	Use Caesar cipher with each letter replaced by 4 places down in the alphabetical order, for the following : $ATTACKATONCEINASIGHT$	02	3	2
	1.2	Vigenere cipher is also referred as	01	1	1
	1.3	Name any two techniques which conceal the existence of messages in communication.	02	2	1
	1.4	Show examples to illustrate nonsingular and singular transformation for $n = 2$ in a block cipher.	02	2	2
	1.5	A change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext which is referred to as _____.	01	1	2
	1.6	List any two techniques used for providing authentication in block cipher modes of operation.	02	2	3
	1.7	Fill in the blanks for the below values X and Y shown in fig 1.7.  Fig 1.7	02	3	3
	1.8	Key exchange is based on the use of the prime number $q = 353$ and a primitive root of 353, in this case $a = 3$. A and B select private keys $XA = 97$ and $XB = 233$, respectively. Compute public keys of A and B using Diffie-Hellman algorithm.	02	3	3
	1.9	Mention any two usages of hash functions in cryptography.	02	1	3
	1.10	Show the TCP segment used in error control code.	02	2	4
	1.11	_____ mode is designed to be parallelizable to provide high throughput with low cost and low latency and the message is encrypted in variant of _____ mode.	02	1	4

PART-B

2	a	i) Apply the playfair algorithm to encrypt the plaintext: INSPIRATION using the key: $JEOPARDITE$. Show all the steps to generate cipher text. ii) Using the railfence technique encipher the message "meet me after the toga party "of depth 2 and the following message using the row technique of same algorithm : "attack postponed until two am" of order 2 with Key:4312567.	10	3	1
	b	Write short notes on Rotor machines.	06	2	1
3	a	Design DES algorithm and explain the steps.	10	2	2
	b	Differentiate between the following : Electronic code Book(ECB), Output Feedback(OFB) and Counter(CTR)	6	2	2
		OR			
4	a	Differentiate double and triple DES algorithms	08	2	3
	b	Explain $XTS - AES$ mode for block oriented storage device.	08	2	1
5	a	i) Using 'RSA' algorithm, if $p = 13$, $q = 5$ and $e = 7$ and cipher value of '6' with(e, n).Find the value of d? ii) Use RSA algorithm with $p = 3$ and $q = 11$ and $d = 3$, find the values of public key e, plaintext and cipher text?	08	3	3
	b	List and explain the variety of ways in which a hash code can be used to provide message authentication with a neat diagram.	08	2	4
		OR			
6	a	Describe the Deffie-Hellman key exchange algorithm in detail.	06	1	3
	b	Illustrate with a neat figure $SHA - 512$ algorithm for general structure, message digest generation and round function.	10	2	3
7	a	Mention the purpose and functioning of Hash-Based message authentication code ($HMAC$) algorithm in detail with a neat figure.	10	1	3
	b	State the essence of the use of key hierarchy with a neat figure.	06	2	1
		OR			
8	a	List and explain the $MACs$ based on clock ciphers.	08	1	1
	b	Explain briefly $X.509$ certificates and $PKIX$.	08	1	4
9	a	Illustrate SSL protocol in detail.	10	2	4
	b	Explain encapsulation security payload in brief.	06	1	4
		OR			
10	a	Write Short notes on the following: i) Kerberos ii) Web Security iii) PGP iv) Tunnel modes in ESP for transfer of segment	16	2	1