U.S.N | | | | | | | | | | |

P.E.S. College of Engineering, Mandya - 571 401

(An Autonomous Institution affiliated to VTU, Belagavi)

Eighth Semester, B.E. - Computer Science and Engineering

Semester End Examination; July - 2021

Cryptography and Network Security

Time: 3 hrs *Max. Marks: 100*

***Note**: Answer any **FIVE** full questions.*

1	a.	Explain structure of Feistel encryption and decryption with a neat diagram.	10
	b.	Encrypt the message "hello" with the key of (7, 2) using Affine cipher method. Also explain Affine cipher in brief.	10
2	a.	Explain Transposition cipher and solve the given problem using Transposition cipher "Begin operation at Noon".	10
	b.	Discuss DES structure in detail.	10
3	a.	In RSA system, given $p = 3$, $q = 11$, $e = 7$ and $m = 5$. Find the cipher text 'C' and also find message 'm' from decryption.	10
	b.	Discuss general idea of asymmetric key cryptosystem.	10
4	a.	Explain the working of Diffie-Hellman key exchange algorithm. Compute Diffie-Hellman practical key and secret key where $a = 24$, $b = 27$, $g = 2$, and $p = 131$.	10
	b.	Give a detailed note on Elgamal encryption. A block of plaintext message $m = 3$ has to be encrypted. Assume $p = 11$, $g = 2$, recipients private key = 5. Sender chooses random integer $r = 7$, perform encryption and decryption.	10
5	a.	With a neat diagram, explain the PKI architectural model.	10
	b.	Explain X.509 certificate format in detail.	10
6	a.	Explain the Kerberos message sequence with an example.	10
	b.	Explain mutual authentication and one-way authentication in remote user authentication using asymmetric encryption.	10
7	a.	Discuss ESP packet format with a neat diagram.	10
	b.	Write a note on; i) Security Association Database ii) Security Policy Database	10
8	a.	Explain transport and tunnel mode of IP security with a neat diagram.	10
	b.	Explain Anti replay service with an example.	10
9	a.	Explain IKE Phase-1 with a neat diagram.	10
	b.	Explain key exchange methods with an example.	10
10	a.	Along with a neat diagram, explain processing model for outbound packets and inbound packets.	10
	b.	Discuss ISAKMP general headder in detail.	10

* * * *