BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI
(END SEMESTER EXAMINATION)

CLASS: BE **SEMESTER : VI**
BRANCH: IT **SESSION : SP/19**

SUBJECT: IT6023 COMPUTER NETWORK AND SECURITY

TIME: 3 Hours **FULL MARKS: 60**

INSTRUCTIONS:
1. The question paper contains 7 questions each of 12 marks and total 84 marks.
2. Candidates may attempt any 5 questions maximum of 60 marks.
3. The missing data, if any, may be assumed suitably.
***4*. Before attempting the question paper, be sure that you have got the correct question paper.**
5. Tables/Data hand book/Graph paper etc. to be supplied to the candidates in the examination hall.

Q.1(a)	What do you understand by secure communication?	[2]
Q.1(b)	List and briefly define categories of security services.	[4]
Q.1(c)	Use the Playfair Cipher to encipher the message "The key is hidden under the door pad." The secret key can be made by filling the first & the part of the second row with the word GUIDANCE" & filling the rest of the matrix with the rest of the alphabet.	[6]
Q.2(a)	Define traffic confidentiality.	[2]
Q.2(b)	Mention the strength and weakness of DES. What is the purpose of S-Box in DES?	[4]
Q.2(c)	Explain the Advance Encryption Standard Algorithm (AES).	[6]
Q.3(a)	Define confusion and diffusion.	[2]
Q.3(b)	In a public key system using RSA, you intercepted the ciphertext C=8 sent to a user whose public key is e=13, n=33. What is the plaintext?	[4]
Q.3(c)	Discuss the security aspects of RSA.	[6]
Q.4(a)	Differentiate between Message Authentication Code and Message Digest.	[2]
Q.4(b)	Why is SHA more secure than MD5?	[4]
Q.4(c)	Explain the steps involved in digital certificate. How can we verify the digital certificate?	[6]
Q.5(a)	What is the difference between a CRC check and hashing function?	[2]
Q.5(b)	What key management issues are involved in Public Key Cryptography?	[4]
Q.5(c)	Explain the RSA scheme of digital signature through an Example.	[6]
Q.6(a)	Differentiate between conventional and digital signature.	[2]
Q.6(b)	Consider a situation: an attacker(A)creates a certificate, puts a genuine organizations name (say Bank B), and puts the attacker's own public key. You get this certificate from the attacker, without knowing that the attacker is sending it. You think it is from bank(B). How can this be prevented/resolved?	[4]
Q.6(c)	Explain Pretty Good Privacy algorithm.	[6]
Q.7(a)	Define trusted systems.	[2]
Q.7(b)	With the help of suitable block diagram explain firewall design principles.	[4]
Q.7(c)	Write a note on IP security.	[6]

:::::29/04/2019 E:::::