

Course: B. Tech.

Branch : AI & DS & Allied

Semester : VI

Subject Code & Name: BTAIOE604B Cryptography and Network Security

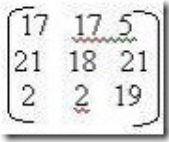
Max Marks: 60

Date: 21/06/2024

Duration: 3 Hr.

Instructions to the Students:

1. All the questions are compulsory.
2. The level of question/expected answer as per OBE or the Course Outcome (CO) on which the question is based is mentioned in () in front of the question.
3. Use of non-programmable scientific calculators is allowed.
4. Assume suitable data wherever necessary and mention it clearly.

	(Level/CO)	Marks
Q. 1 Solve Any Two of the following.		12
A) Explain the substitution encryption techniques in detail?	L1/CO1	6
B) Describe the various security mechanisms.	L1/CO1	6
C) Convert "MEET ME" using Hill cipher with the key matrix  Convert the cipher text back to plaintext .	L1/CO1	6
Q.2 Solve Any Two of the following.		12
A) Describe the working principles of simple DES with an example.	L2/CO2	6
B) Discuss in detail the encryption and decryption process of AES.	L2/CO2	6
C) Briefly explain Daffier- Hellman Key Exchange.	L2/CO2	6
Q. 3 Solve Any Two of the following.		12
A) Write and explain the digital signature.	L3/CO3	6
B) Describe HMAC Algorithm.	L3/CO3	6
C) Describe X.509 Authentication Service in detail.	L3/CO3	6
Q.4 Solve Any Two of the following.		12
A) Describe IP Security architecture.	L4/CO4	6
B) Explain Encapsulating security payload.	L4/CO4	6
C) Explain Authentication Header.	L4/CO4	6
Q. 5 Solve Any Two of the following.		12
A) Describe SSL Record Protocol.	L5/CO5	6
B) Explain Transport Layer Security.	L5/CO5	6
C) Describe SET with it's requirements and SET Key Features.	L5/CO5	6