

UG-491

BSCS-20

**B.Sc. DEGREE EXAMINATION –
DECEMBER, 2018.**

Third Year

NETWORK SECURITY

Time : 3 hours

Maximum marks : 75

PART A — (5 × 5 = 25 marks)

Answer any FIVE questions.

1. Explain passive attack with neat sketch.
2. Demonstrate steganography techniques with example.
3. Classify stream and block cipher.
4. Mention any five ingredients involved in public – key encryption and define each one of them.
5. Explain the types of attacks on encrypted messages.
6. State the reasons, why hash function can be used?
7. Enumerate the attack procedure of man-in-the-middle attack.

PART B — (5 × 10 = 50 marks)

Answer any FIVE questions.

8. Explain the techniques involved in substitution
 - (a) Ceaser cipher (5)
 - (b) One-Time pad (5)
 9. Elucidate DES encryption with diagrammatic representation.
 10. Illuminate RSA algorithm with example and diagram.
 11. Briefly explain Euler's theorem in number theory with example.
 12. Explain Diffie-Hellman key exchange algorithm.
 13. Give detailed explanation on security of hash function and MACs.
 14. Bring the substitution technique followed in
 - (a) Monoalphabetic cipher (5)
 - (b) Polyfair cipher. (5)
-