

Total No. of Questions : 8]

[Total No. of Printed Pages : 2

Roll No

IT-801 (GS)
B.E. VIII Semester
 Examination, May 2018
Grading System (GS)
Information Security
Time : Three Hours

Maximum Marks : 70

- Note :* i) Attempt any five questions.
 ii) All questions carry equal marks.

1. a) Differentiate substitution and transposition ciphers with suitable examples.
 b) Define the term cryptanalysis. Explain linear and differential cryptanalysis.
2. a) What is the purpose of the S-boxes in DES? Explain the avalanche effect. rgpvonline.com
 b) What is steganography? How is it differs from cryptography?
3. a) Briefly discuss Diffie-Hellman key exchange scheme.
 b) What is hash function? Give the basic uses of hash function.
4. a) Explain digital signature with arbitrated and direct approaches.
 b) What was kerberos designed for? Explain the architecture of kerberos.

IT-801 (GS)

PTO

5. Define following attacks in detail.

- a) SQL injection attack
- b) Phishing attack
- c) Ransomware attack

6. a) Define virus, intruders, worms. Also write the basic principle of intrusion detection system.

- b) What is the use of firewall? Explain firewall design principles. rgpvonline.com

7. a) Define the terms Integrity, Confidentiality, Denial of Service and Authentication.

- b) Explain architecture of Secure Socket Layer.

8. Write short notes on any two

- a) IP spoofing
- b) Brutte force attack
- c) Strength of DES
- d) RSA encryption algorithm

IT-801 (GS)