

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BSc DEGREE EXAMINATION MAY 2019
(Fifth Semester)

Branch - **COMPUTER TECHNOLOGY**

CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours

Maximum : 75 Marks

SECTION-A (20 Marks!)

Answer ALL questions

ALL questions carry **EQUAL** marks

(10 x 2 = 20)

- 1 Comment on injection of commands.
- 2 How does brute force attack works?
- 3 State the use of random delay.
- 4 What is birthday paradox?
- 5 Write about Kerberos.
- 6 Give your view on IP sec documents.
- 7 Define authentication.
- 8 What is TLS?
- 9 Define Firewall.
- 10 What is an intrusion?

SECTION - B (25 Marks)

Answer **ALL** Questions

ALL Questions Carry **EQUAL** Marks (5 x 5 = 25)

- 11 a Discuss about one - Time Pad in detail.
OR
b Write in detail on OSI security architecture.
- 12 a Explain about Cipher based message Authentication code.
OR
b Give necessary theory about key wrapping algorithm.
- 13 a Discuss about X.509 public key certificate format.
OR
b Give the applications of IPsec.
- 14 a Write about the services provided by TLS Record protocol.
OR
b Discuss about HTTPS.
- 15 a How the firewall blocks the usage? Explain.
OR
b Explain about the virus attack and its consequences.

SECTION - C (30 Marks)

Answer any **THREE** Questions

ALL Questions Carry **EQUAL** Marks (3 x 10 = 30)

- 16 Write in detail about conventional encryption algorithm.
- 17 Discuss about the Secure Hash Algorithm(SHA).
- 18 Explain in detail about Pretty Good Privacy Protocol.
- 19 Discuss in detail about handshake protocol.
- 20 How intrusion can be managed? Explain.