15CTU30

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BSc DEGREE EXAMINATION DECEMBER 2018
(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 What is an attack surface?
2 Write about cryptanalysis.
3 Comment on digital signature.
4 How timing attack is working?
5 What is web of trust?
6 Write about Internet Key Exchange(IKE).
7 What is Cipher suite?
8 State the use of session - ID.
9 How does virus affect the network?
10 Is firewall necessary? Justify.

SECTION - B (25 Marks)
Answer **ALL** Questions
ALL Questions Carry **EQUAL** Marks (5 x 5 = 25)

11 a Discuss about casear cipher in details.
OR
b Comment on denial of service.

12 a Explain about Data Authentication Algorithm.
OR
b Write notes on HMAC design objectives.

13 a Give the requirements of Kerberos.
OR
b Write about S/MIME message content types.

14 a Discuss about heart beat protocol.
OR
b Explain about SSH protocol stack.

15 a How intrusion detection can be done? Explain.
OR
b Write about virus related threats.

SECTION - C (30 Marks)
Answer any **THREE** Questions
ALL Questions Carry **EQUAL** Marks (3 x 10 = 30)

16 Discuss about symmetric cipher model elaborately.

17 Explain the RSA algorithm with necessary theory.

18 Elaborately explain about IP security services.

19 Discuss about SSH transport layer cryptographic algorithms.

20 pYnlnin ot\nn* ...—