14CMU29

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BSc DEGREE EXAMINATION DECEMBER 2018
(Fifth Semester)

Branch - **COMPUTER SCIENCE**

CORE ELECTIVE -1 CRYTOGRAPHY & 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 masquerade?
2 Define preoutput.
3 What are multiple encryptions?
4 Give four possible approaches for attacking the RSA algorithm.
5 Write any four properties of hash function H.
6 Define message authentication.
7 What is a symmetric encryption?
8 Define public keys.
9 Write applications of IPSec.
10 What are security associations ?

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

11 a Sketch a model for network security.
OR
b Discuss the strength of DES.

12 a Explain any two block cipher modes of operation.
OR
b Give details about Diffie-Hellman key exchange.

13 a Write a note on two simple hash functions.
OR
b Explain HMAC.

14 a Explain digital signatures.
OR
b Detailed note on distribution of public keys.

15 a Enumerate the overview of IP security.
OR
b Explain internet key exchange.

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

16 Explain data encryptions standard (DES).

17 Explain principles of public - key cryptosystems.

18 Give detailed note about secure Hash algorithm (SHA).

19 Discuss X.509 certificates.

20 Explain the concept of encapsulating security payload.