14CMU29A

PSG COLLEGE OF ARTS & SCIENCE

(AUTONOMOUS) *U £ ^ 4*

BSc DEGREE EXAMINATION MAY 2017

(Fifth Semester)

Branch - **COMPUTER SCIENCE**

CORE ELECTIVE-I: CRYPTOGRAPHY & NETWORK SECURITY

Time : Three Hours Maximum : 75 Marks

SECTION-A (20 Marks)

Answer **ALL** questions

ALL questions carry **EQUAL** marks (1 0 x 2 = 20)

1 Define availability.
2• Give the types of security attacks.
3 List out the stages of multiple encryption.
4 Specify the encryption and decryption forms of RSA.
5 Mention the first two objectives of acceptability of HMAC.
6 What are the requirements to be satisfied by any candidate for SHA - 3?
7 Mention the steps to establish session key.
8 What is meant by backward compatibility?
9 Define Internet key exchange.
10 Define replay attack.

SECTION - B (25 Marks)

, Answer **ALL** Questions

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

11 a Explain the security services provided by protocol layer.

OR

b Discuss on the strength of DES.

12 a Elucidate the cipher block chain mode operations. '

OR .

b Describe the Diffie-Hellman key exchange algorithm.

13 a Discuss on the algorithm SHA - 3.

OR

b Describe the requirements of message authentication.

14 a Explain the symmetric key distribution using asymmetric encryption. .

OR

b Exemplify the distribution of public keys.

15a Elucidate the IP security policy.

OR

b Describe the combining the security associations.

SECTION - C (30 Marks)

Answer any **THREE** Questions '

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

16 Discuss on the network security mechanism, and model.

17 Describe the multiple encryption method and triple DES. •

18 Elucidate the MACs based on hash functions.

19 Exemplify the symmetric key distribution using symmetric encryption.

20 Explain the Internet key exchange methods.

Z-Z-Z END