S.No. : 38

BCACSN14222

No. of Printed Pages : 03

Following Paper ID and Roll No. to be filled in your Answer Book.

PAPER ID : 26422 Roll No. 1 2 3 0 2 6 4 0 2 8

BCA Examination 2024-25

(Even Semester)

CRYPTOGRAPHY & CYBER SECURITY

Time : Three Hours] *[Maximum Marks : 60*

Note :– Attempt all questions.

SECTION–A

1. Attempt all parts of the following : $1 \times 8 = 8$

   (a) Define the terms encryption and decryption.

   (b) Explain the concept of private key.

   (c) What are attacks?

   (d) How can we differentiate between confidentiality and integrity?

   (e) Which key is used symmetric and asymmetric cryptography respectively?

[P. T. O.

(f) Explain threats and attacks.

(g) Why do we need digital signature? Explain.

(h) Name two block cypher techinques.

SECTION–B

2. Attempt any two parts of the following: $2 \times 6 = 12$

(a) Explain DES algorithm for encryption in brief.

(b) What is Diffie Hellman Key Exchange Algorithm?

(c) Compare substitution and transposition techniques.

(d) Explain different types of intrusion detection system.

SECTION–C

Note:- Attempt all questions. Attempt two parts from each question. $8 \times 5 = 40$

3. (a) How does IDE algorithm work?

(b) Differentiate between RC5 and RC2 algorithm.

(c) What is CAST algorithm.

4. (a) Explain the RSA asymmetric encryption algorithm.

(b) Discuss about key exchange management.

(c) What are the principles of public key cryptography?

5. (a) Explain security policies and its types.

(b) What do you mean by threats and discuss its types?

(c) Explain CIA trait along with the diagram.

6. (a) Differentiate between spyware and ransomware.

(b) Explain antivirus and give any one example.

(c) What are the key concepts used for intrusion prevention?

⌘⌘⌘