



44733/E0230

Reg. No.

--	--	--	--	--	--	--	--

V Semester B.C.A. (CBCS) Degree Examination, March/April - 2023

**NETWORK SECURITY****(Regular)****Time : 3 Hours****Maximum Marks : 80****Instructions to Candidates :**

- 1) All sections are compulsory.
- 2) Draw neat diagrams wherever necessary.

**Section - A**Answer any **ten** of the following.**(10×2=20)**

1.
  - a) List the motives for cyber attacks
  - b) Define authentication. Give the types of authentication.
  - c) Define groups and rings.
  - d) What is meant by firewall?
  - e) Define Hash function. List the properties of Hash function.
  - f) Define Digital signature.
  - g) List the types of PKI Architecture.
  - h) Define intrusion. Give 2 examples.
  - i) Define
    - a) Certifying authority.
    - b) Affixing digital signature.
  - j) What are the scopes of the IT act 2000.
  - k) Define
    - a) Pushing
    - b) Phishing
  - l) Define kerberos.

**P.T.O.**



(2)

44733/E0230

**Section - B**

Answer any **four** of the following questions.

(4×5=20)

2. Calculate the value of  $x$  using Chinese remainder theorem from the given data  $N = 210, n_1 = 5, n_2 = 6, n_3 = 7, x_1 = 3, x_2 = 5, x_3 = 2$ .
3. Explain x.509 digital certificate format.
4. Write the steps of RSA algorithm.
5. Explain authentication and master session key exchange in 802.11 i.
6. Explain the importance of securing electronic records and digital signature.
7. Explain Euclidean's algorithm with an example.

**Section - C**

Answer any **four** of the following questions.

(4×10=40)

8. Explain Mono alphabetic and polyalphabetic ciphers with example.
9. Define Dictionary attacks. Explain in detail the types of Dictionary attacks.
10. What is SSL? Explain SSL Handshake protocol.
11. Who is a controller? Outline its functions and power.
12. Explain the working of diffie Hellman key exchange protocol.