KADI SARVA VISHWAVIDYALAYA

B.E. Semester VI (NEW) EXAMINATION (APRIL – 2025)

Subject Code: CS602-N   Subject Name: Information Security And Ethical Hacking
Date: 7/4/25   Time: 12.30 to 3.30   Total Marks: 70 Marks

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Use of scientific calculator is permitted.
4. Indicate clearly, the options you attempt along with its respective question number.
5. Use the last page of main supplementary for rough work.

Section-I

Q:1 (A) Explain cryptanalysis & brute force attacks. [5]

(B) Define Euler's theorem and its applications. [5]

(C) Does Fermat's theorem hold true for prime number 11 with the integer 5? [5]

OR

(C) Prove Euler's theorem hold true for a =11 & n =33. [5]

Q:2 (A) Compare stream cipher with block cipher. [5]

(B) Draw a detailed block diagram of encryption process in DES. Add appropriate [5] description.

OR

Q:2 (A) Differentiate Conventional Encryption vs. Public Key Encryption. [5]

(B) Explain AES structure in detail. [5]

Q:3 (A) Calculate all the values of RSA assuming two primes p=7 and q=17. Assume other [5] values appropriately.

(B) Which are the properties of Digital Signature? Explain Digital Signature Standard in [5] detail.

OR

Q:3 (A) Calculate all the values for Diffie-Hellman key exchange, consider two primes q=19 [5] and a=10. Assume other values appropriately.

(B) Explain MD5 algorithm in brief. [5]

Section II

Q:4 **(A)** Difference between Hacker and Cracker.   **[5]**

      (B) What are the 5 phases in hacking? Explain it.   **[5]**

      (C) Define Foot Printing and Scanning. Explain both briefly.   **[5]**

OR

      (C) What is Threat? Describe types of threats in detail.   **[5]**

Q:5 **(A)** Explain DOS and DDOS attack with proper diagram.   **[5]**

      (B) Explain Cross-site Scripting Attack briefly.   **[5]**

OR

Q:5 **(A)** What is phishing? Explain it briefly.   **[5]**

      (B) Explain SQL Injection Attack briefly.   **[5]**

Q:6 **(A)** Define Firewalls. Also explain types of firewalls.   **[5]**

      (B) Briefly explain network security controls architecture. Also define authentication process in it.   **[5]**

OR

Q:6 **(A)** What is Kerberos? Explain it briefly.   **[5]**

      (B) Define Honeypots.   **[5]**