Graphic Era
HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

End Term (Odd) Semester Examination December 2024

Roll no.....

Name of the Course and semester: B.Tech/7th Semester
Name of the Paper: Cryptography and Network Security
Paper Code: TIT 704
Time: 3 hour *Maximum Marks: 100*

Note:

(i) All the questions are compulsory.
(ii) Answer any two sub questions from a, b and c in each main question.
(iii) Total marks for each question is 20 (twenty).
(iv) Each sub-question carries 10 marks.

Q1. (2X10=20 Marks)

a. Explain the role of encryption and decryption in cryptography. How do symmetric and asymmetric encryption differ from one another?
b. Discuss the various types of cryptographic algorithms and categorize them based on their functionality. Provide examples for each category.
c. Explain transposition ciphers and their working principle. Compare them to substitution ciphers, highlighting their strengths and weaknesses. CO-1

Q2. (2X10=20 Marks)

a. You are using a substitution cipher with a key that shifts each letter by 4 positions in the alphabet. If the ciphertext is "XLI PMR XLIEX", what is the original plaintext? Show the decryption process.
b. Compare the different modes of operation of block ciphers: ECB (Electronic Codebook) and CBC (Cipher Block Chaining). Highlight their advantages, disadvantages, and typical use cases. Explain how these modes work and analyze their security implications.
c. Explain the Blum Blum Shub (BBS) algorithm for generating cryptographically secure pseudo-random numbers. How does BBS ensure security compared to other PRNGs? Discuss the mathematical properties that make BBS secure. CO-2

Q3. (2X10=20 Marks)

a. Given a=84 and b=65, use Euclid's Algorithm to find GCD(a,b). Show all steps.
b. Using the Extended Euclidean Algorithm, find the multiplicative inverse of 17 modulo 43.
c. Explain why the security of RSA depends on the difficulty of factoring large numbers. How does choosing very large primes for p and q enhance security? CO-3

Q4. (2X10=20 Marks)

a. Describe the role of the Key Distribution Center (KDC) in Kerberos authentication. Why are ticket-granting tickets (TGTs) used, and how do they enhance security?
b. Describe the role of the Internet Key Exchange (IKE) protocol in IPsec. How does IKE Phase 1 and Phase 2 facilitate secure key exchange and negotiation?
c. Explain how S/MIME ensures confidentiality, authentication, message integrity, and non-repudiation in electronic mail security. CO-4

Q5. (2X10=20 Marks)

a. Explain the key components of the IEEE 802.11 network architecture. How does the architectural model support secure communication in a wireless LAN?
b. Explain how TLS works to provide secure communication over the web. How is it implemented in HTTPS to ensure data integrity and confidentiality?
c. Explain the role of encryption in protecting data stored in the cloud. What is the significance of "encryption at rest" and "encryption in transit"? CO-5