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: BCA 5
Name of the Paper: Cryptography
Paper Code: TBC 504
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) The total mark for each question is 20 (twenty).
(iv) Each sub-question carries 10 marks.
(v) Please specify COs against each question.

(2X10=20 Marks)

Q1.
a. Define the necessary features of the data security and why is it necessary? (CO1)
b. Discuss various types of cryptographic attacks and provide an example of each. (CO1)
c. using a 3×3 Hill cipher matrix encrypt and decrypt the following message.
Key matrix: Key: 17 17 5 ,21 18 21,2 2 19
Plaintext:P: paymoremoney. (CO1)

(2X10=20 Marks)

Q2.
a. Explain the structure and functioning of the Data Encryption Standard (DES). (CO2)
b. **Explain the following:**
(i) Confusion and diffusion
(ii)Permutation
(iii)stream cipher
(iv)cryptanalysis
(v)Role of totient function (CO2)
c. Describe the principles of Feistel Design? Explain its application in modern block ciphers? Also Implement simple Feistel cipher with 3 rounds. The following parameters are provided:
Plaintext: P=10101101. Split the plaintext into two halves:
Key for round 1: K1=0110
Key for round 2: K2=1001
Perform Round function FFF is a simple XOR operation between the right half and the key. (CO2)

(2X10=20 Marks)

Q3.
a. Describe the Blowfish encryption algorithm and its significance in modern encryption systems. (CO3)
b. Explain major concerns any network will feel after "man in the middle attack" and "meet in the middle attack". Differentiate between both. (CO3)
c. Discuss brief notes on IDEA algorithm and explain single round of IDEA algorithm also explain how to generate subkeys in IDEA algorithm with proper diagram. (CO3)

(2X10=20 Marks)

Q4.
a. Discuss the difference between symmetric and asymmetric key cryptosystems with suitable examples. Also Explain Euler's Theorem with Property of Euler Totient Function and verify Euler's theorem where P=4, q=10. (CO4)
b. If a message to be send is M=4 and N=77 find out the value of d that one will use to decrypt this message using RSA algorithm if encryption is first performed by assuming values according to N. (CO4)
c. sender chooses p = 23 and e1 = 7. Receiver chooses random integer k = 3 calculate C1 and C2 for the

End Term (Odd) Semester Examination December 2024

plaintext 20 using elgamal algorithm. Also Explain Elgamal encryption components. (CO4)

Q5. (2X10=20 Marks)

a. Explain the MD-5 Message Digest Algorithm and its application in message integrity. (CO5)

b. Discuss the working of the Digital Signature Algorithm (DSA) and its importance in secure transactions. (CO5)

c. Explain message authentication code. What kind of encryption techniques are being used to generate them. (CO5)