DD Nitin Gupta

8/5/2023

176

Name of the Student _____ **Roll No**_____

NATIONAL INSTITUTE OF TECHNOLOGY HAMIRPUR
Department of Computer Science and Engineering (CSE)
END- TERM EXAMINATION

09th May 2023

Course — B.TECH./Dual Degree **Semester-VIII** **Branch — CSE**
Subject Name- Information Security **Subject Code: CS-422**
Time- 03 Hours **Max.Marks-50**
Note:

- **Answer all questions. Write precise answers only. Assume suitable data.**
- **Parts of a question should be answered at the same place.**

Q.No	Questions	Marks
Q1(a)	Encrypt and decrypt "pay more money" using Hill cipher with key $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$	6
(b)	Difference between (i) Diffusion and Confusion with a suitable example. (ii) Modular arithmetic and Ordinary arithmetic	4
Q2(a)	How could we use the Rail Fence Technique for encryption? By using the Rail Fence Technique encrypt message = 'ABCDEFGHIJ' with depth = 4 and then decrypt the obtained ciphertext.	3
(b)	Explain the Playfair Cipher technique in detail, and encrypt the message "Hide the gold under the carpet" by using the key "Neso Academy".	4
(c)	How could we use the Columnar Transposition Cipher for encryption? By using the Columnar Transposition Cipher encrypt message = 'THANK YOU EVERYONE' with Key = HACK and then decrypt the obtained ciphertext.	3
Q3(a)	Differentiate between (i) Group, cyclic group and abelian group with suitable examples and their utility in cryptography. Is (Z*,+) a group or not? Explain with a suitable example. (i) Ring, commutative ring, field and finite Field suitable examples and their utility in cryptography. Set Z%2 and Z%5 are classified in which Group, Ring, Field and Finite Field?	8
(b)	What is the last two digits of 29^5 (By using a relevant approach)? Solve 88^7 mod 187 (By using a relevant approach).	2
Q4(a)	Is there any relationship between the hash function and the birthday attack? If yes, then explain it in detail. Is there any difference between Wired Equivalent Privacy (WEP) and IEEE 802.11? If yes, then explain the difference in detail.	4

(b) With a neat diagram, explain the steps involved in HMAC algorithm for encrypting a message with maximum length of less than 2^128 bits and produces as output a 512-bit message digest. 3

(c) How the following elements affect the efficiency (computing speed) and safety of the AES algorithm? 3

(i) Number of rounds
(ii) Block size
(iii) Key Size
(iv) Sub key Generation
(v) Size of Plaintext

Q5(a) How a message is converted into a block or stream? Differentiate between both with a suitable example. 2

(b) Determine the value of x 3

x=3(mod 5)
x=1(mod 7)
x=6(mod 8)
by using Chines Remainder Theorem.

(c) Explain Euler's Totient function and its properties with suitable examples. And By using the Miller Rabin Primality Test, can we determine whether 29 is a prime number or not? 5