Roll No. \_\_\_\_\_\_\_\_\_\_\_

**CLASS EVALUATION QUIZ**

**Information Security (20CP304T)**

**Sem V : Div 2**

**Section I (Each question carries 1 marks)**

1. Meera sent a mail to Rajat on Sunday. After few days she denied sending a mail to him. Which security service is violated?
2. Non-repudiation at origin
3. Non-repudiation at destintion
4. Peer entity authentication
5. Data origin authentication
6. Kunal wants to send private message to Ajay. Dev intervenes and does not allow this communication to happen. What type of attack is this?

a) Denial of service Attack

b) Masquerade Attack

c) Replay attack

d) None of the above

1. Decryption algorithm takes cipher text and \_\_\_\_\_\_ to produce the plain text.
2. Plain text
3. Cipher text
4. Key
5. None
6. As \_\_\_\_\_\_\_\_\_ is the science and art of creating secret codes, \_\_\_\_\_\_\_\_\_\_ is the science and art of breaking those codes.
7. \_\_\_\_\_\_\_\_ was used by the British army during World War I
8. Vernam Cipher
9. Hill cipher
10. Playfair Cipher
11. Vigenere Cipher
12. The order of columns becomes the key to the \_\_\_\_\_\_\_\_ algorithm
13. Playfair cipher
14. Rail fence cipher
15. Both a) and b)
16. Fiestel cipher
17. What is 216 mod 8?
18. 1
19. 3
20. 5
21. None
22. Identify the false statement.
23. GCD(7,-12)= GCD(-7,12)
24. HCF(a,b) = min [k, such that k|a and k|b]
25. There are n residue classes for mod n operation.
26. Multiplicative inverse modulo 7 of 2 exists
27. Euler totient function for a number n is
28. the number of positive integers that are relatively prime to n
29. the number of positive integers less than n
30. the number of positive integers less than n that are not relatively prime to n
31. None
32. \_\_\_\_\_\_\_\_\_ is used to solve a set of different congruent equations with one variable but different moduli
33. Eulers Theorem
34. Chinese Remainder Theorem
35. Miller-Rabin Algorithm
36. Euclidean Algorithm

**Section II (Each question carries 2 marks)**

1. State Fermat’s Theorem.
2. Mention two merits of Playfair cipher method.

**Section III (Each question carries 3 marks)**

1. Using the Vigenere cipher, encrypt the word “encryption” using the word “leg”
2. Using Hill cipher, decrypt the message “ZQGE” using the keyword “HILL”