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

**CLASS EVALUATION QUIZ**

**Information Security (20CP304T)**

**Sem V : Div 1**

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

1. Which is not a security service?
2. Authentication
3. Non-repudiation
4. Loss of data
5. Access control
6. Kunal wants to send private message to Ajay. Before he could do so, his ID is hacked by Dev who sends another message to Ajay. What type of attack is this?

a) Denial of service Attack

b) Masquerade Attack

c) Replay attack

d) None of the above

1. \_\_\_\_\_\_\_\_ is the scrambled message produced after encryption.
2. Plain text
3. Cipher text
4. Key
5. None
6. Based on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, one should always assume that the adversary, Eve, knows the encryption/ decryption algorithm.
7. The key matrix in the Hill cipher needs to have a \_\_\_\_\_\_\_\_
8. Multiplicative inverse
9. Additive inverse
10. Both
11. None
12. The transposition cipher can be made significantly more secure by performing more than one stage of transposition.
13. True
14. False
15. What is 138 mod 10?
16. 1
17. 3
18. 7
19. 9
20. Identify the false statement.
21. Any non-zero number divides 0
22. Two numbers are relatively prime if their HCF is 1
23. There are (n-1) residue classes for modulo n operation.
24. 22 is congruence modulo 7 to -6
25. Euler totient function for 77 is

a) 60

b) 66

c) 70

d) 76

1. \_\_\_\_\_\_\_\_\_\_\_ determines whether the given number is prime
2. Euclidean Algorithm
3. Fermat Theorem
4. Chinese Remainder Theorem
5. Miller Rabin Algorithm

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

1. Write two merits of Hill cipher.
2. State Euler’s Theorem.

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

1. Determine the inverse mod 26 of
2. Using Playfair cipher, encrypt the message “DO IT TOMORROW” using the keyword “AUSTRALIA”