CNS---MCQ questions

1. Which is the product of two distinct prime
   a. 189
   b. 355
   c. 31
   d. 27
2. The greatest common divisor of 63 and 81 is
   a. 9
   b. 7
   c. 3
   d. 1
3. If both 112 and 33 are factors of a number a.43.62.1311 then what is the smallest possible value of a?
   a. 131
   b. 1451
   c. 363
   d. 2019
4. Consider 36 students to be seated such that each row has the same number of students as the others. If at least 3 students are to be seated per row and at least 2 row have to be there, how many arrangement are possible?
   a. 6
   b. 7
   c. 5
   d. 4
5. The greatest comman divisor of 3x4y2z, 4xy3z2, 5x3yz is
   a. 3x4y2z
   b. 4xy3z2
   c. 5x3yz
   d. Xyz
6. The additive inverse of 2 in Z7 is
   a. 0
   b. 6
   c. 4
   d. 5
7. Multiplicative inverse of 3 in Z11 is
   a. 1
   b. 4
   c. 10
   d. 9
8. The solution of the equation $3x + 4 \equiv 6 (\text{mod} 13)$ is
   a. 5
   b. 0
   c. 1
   d. 2
9. 1. Use Caesar's Cipher to decipher the following
   HQFUBSWHG WHAW
   a) ABANDONED LOCK
   b) ENCRYPTED TEXT
   c) ABANDONED TEXT
   d) ENCRYPTED LOCK
10. Caesar Cipher is an example of
    a) Poly-alphabetic Cipher
    b) Mono-alphabetic Cipher

c) Multi-alphabetic Cipher
d) Bi-alphabetic Cipher

11. Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.
    a) True
    b) False
12. Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.
    a) Random Polyalphabetic, Plaintext, Playfair
    b) Random Polyalphabetic, Playfair, Vignere
    c) Random Polyalphabetic, Vignere, Playfair, Plaintext
    d) Random Polyalphabetic, Plaintext, Beaufort, Playfair
13. On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-
    a) abqdnwewuwjphfvrrtrfznsdokvl
    b) abqdvmwuwjphfvvyyrfznydokvl
    c) tbqyrvmwuwjphfvvyyrfznydokvl
    d) baiuvmwuwjphfoeiyrfznydokvl
14. On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
    a) nlazeiibljji
    b) nlazeiibljii
    c) olaaeiibljki
    d) mlaaeiibljki
15. Confusion hides the relationship between the ciphertext and the plaintext.
    a) True
    b) False
16. The S-Box is used to provide confusion, as it is dependent on the unknown key.
    a) True
    b) False
17. Which of the following slows the cryptographic algorithm –
    1) Increase in Number of rounds
    2) Decrease in Block size
    3) Decrease in Key Size
    4) Increase in Sub key Generation
18. DES follows
    a) Hash Algorithm
    b) Caesars Cipher
    c) Feistel Cipher Structure
    d) SP Networks
19. The DES Algorithm Cipher System consists of _____rounds (iterations) each with a round key
    a) 12
    b) 18
    c) 9
    d) 16
20. The DES algorithm has a key length of
    a) 128 Bits
    b) 32 Bits
    c) 64 Bits
    d) 16 Bits
21. In the DES algorithm the round key is _____ bit and the Round Input is _____bits.
    a) 48, 32
    b) 64,32
    c) 56, 24
    d) 32, 32

22. The Initial Permutation table/matrix is of size
    a) 16×8
    b) 12×8
    c) 8×8
    d) 4×8
23. In the DES algorithm the 64 bit key input is shortened to 56 bits by ignoring every 4th bit.
    a) True
    b) False
24. During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
    a) True
    b) False
25. The number of tests required to break the Double DES algorithm are
    a) 2112
    b) 2111
    c) 2128
    d) 2119