**CNS Important Questions FOR CIE-1**

1.Illustrate a brief note on security goals.

2.Apply the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t.

1. 4 and 7
2. 291 and 42
3. 84 and 320

d) 400 and 60

3.Examine the term "congruence" in the context of modular arithmetic and its relevance to cryptographic algorithms.?

4.Difference Between DES And AES Algorithms.

5.explain DES Algorithm in details.

6.Different Type Of Security Attacks.

7. Find all solutions to the following sets of linear equations:

* 1. 3x + 5y ≡ 4 (mod 5) 2x + y ≡ 3 (mod 5)

8. List all additive inverse pairs in modulus 20.

9.List all multiplicative inverse pairs in modulus 20.

10 **Using Lagrange’s theorem, find the orders of all the potential subgroups of the following groups:**

**a. G =<Z₁₈,+>**

**b. G =<Z₂₉,+>**

**11.** Distinguish between a substitution cipher and a transposition cipher.

12. List four kinds of cryptanalysis attacks.

13. What is the block size in DES? What is the cipher key size in DES? What is the round-key size in DES?