DEPARTMENT OF COMPUTER SCIENCE AND ENGG.
NATIONAL INSTITUTE OF TECHNOLOGY
TIRUCHIRAPPALLI.

CYCLE TEST I

CSPC63 Principles of Cryptography

Date: 22/02/22 **Time:** 60 Mins

ANSWER ALL THE QUESTIONS

MAX: 20 Marks

1. With examples, explain in brief about the various Cryptographic attacks. (4)
2. Find all common divisors of 252 and 180 using the Euclidean algorithm. (2)
3. Find the multiplicative inverse of 24140 in Z^*_{40902} (2)
4. Use the Extended Euclidean Algorithm to find integers x and y such that $300 \cdot x + 222 \cdot y = 6$. (2)
5. Consider the group Z_{53}.
    a. What are the possible element orders? (1)
    b. How many elements exist for each order? (1)
    c. How many elements does each of the multiplicative groups have? (1)
    d. Do all orders from this divide the number of elements in the corresponding multiplicative group? (1)
6. Find all the subgroups of $G = <Z_{16}^*, * >$ (2)
7. Generate the multiplication table for the extension field $GF(2^3)$ using the irreducible polynomial is $P(x) = x^3 + x + 1$. Show the steps in the computation. (4)

******