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

CYCLE TEST II

CSPC63 Principles of Cryptography

Time: 60 Mins

Date: 03/04/25

ANSWER ALL THE QUESTIONS

MAX: 20 Marks

1 With appropriate diagrams, explain how key expansion is done in AES - 128. (5)

2 Given the group $G = < Z_{16}^*, * >$, find the subgroups and the orders of the subgroups. Is G a cyclic group? (4)

3 Explain in brief about the following attacks on RSA:

(i) Factorization attack (2)
(ii) Chosen Ciphertext attack (2)

4. Given p =23 and P = 24; q , a prime number which is 2 more than the largest primitive root of Z_{14}^* . Using Rabin cryptosystem, find out the

(i) Private key (2)
(ii) Public key (1)
(iii) Plain texts after decryption (4)

---- ***** ----