St. Vincent Pallotti College of Engineering & Technology, Nagpur
Department of Computer Engineering
Session 2024-25
CNS Practical Details
7th Semester (A & B)

Practical 8:

Problem Statement: To implement Asymmetric Key Algorithms and its related mathematical theorems.

Theory:

8.1. To implement Euler's Theorem with Euler's Totient Function and Fermat's Little Theorem.

8.2. To implement Chinese Remainder Theorem (CRT).

8.3. To implement RSA Cryptosystems.

8.4. Summarize the attacks on RSA in your words.

8.5. Compare EEA, Fermat's Little and Euler's theorem for calculating inverse of a number based on the following:

- Concept
- Steps
- Applicability
- Efficiency

(Reference: "Cryptography & Network Security" e-book, by Forouzan, Pg no. 280 onwards).

Note the following regarding practical record:

1. **For Theory, only related Algorithms or Pseudocodes should be written for the same.**
2. **Code printout should be attached.**
3. **Flowchart for the same should be drawn.**
4. **Minimum 3 outputs should be attached.**
5. **Conclusion.**

Prof. Reema Roychaudhary
Practical In-charge