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

Practical 6:

Problem Statement: To implement the core components of the 128-bit Advanced Encryption Standard (AES), specifically focusing on the AES round structure and the key expansion process.

Aim: Show the Implementation of the following:

1. AES Round Structure. (a single program)
2. AES Key Expansion process.

Execute the following and add the output screenshot for the following:

1. Example No 7.6.
2. Example No. 7.9.
3. Example No. 7.10.
4. Example No. 7.13.
5. Example No. 7.14.

(Reference: "Cryptography & Network Security" e-book, by Forouzan, Pg no. 236 onwards).

Note the following regarding practical record:

1. **For Theory, only related Algorithms or Pseudocodes should be written for the same.**
2. **SubBytes table is to be feed in the program.**
3. **Code printout should be attached.**
4. **Flowchart for the same should be drawn.**
5. **Only Pre-round and Round 1 of the AES Round Structure (Ex. 7.9) & Key Expansion process (Ex. 7.10) should be solved manually to match with the output screenshot.**
6. **Analysis of AES should be summarized in your own words.**
7. **Conclusion.**

Prof. Reema Roychaudhary
Practical In-charge