VIT-AP UNIVERSITY

Programme: MTSE Semester: Winter 2020-21

Subject: Information and System Security Subject Code: SWE3003

PRACTICAL ASSIGNMENT-3

Points (Weightage): 30 (12%) Submission Due Date: 20-May-2021

Use Java programming language to implement the following:

1. Find the GCD using Euclidian algorithm and multiplicative inverse modulo n using Extended-Euclidian algorithm.
2. Design a menu based modular arithmetic calculator [addition, subtraction, multiplication, division, inverse of a number (additive and multiplicative)].
3. Implement Caesar cipher and multiplicative substitution cipher and try cryptanalysis.
4. Implement Affine cipher and try cryptanalysis.
5. Implement Autokey and Playfair ciphers.
6. Implement Vigenère cipher and try cryptanalysis.
7. Implement Hill cipher and One-time-pad cipher.
8. Implement deterministic and probabilistic Primality testing algorithms.
9. Implement Chinese Remainder Theorem.
10. Implement RSA cryptosystem.
11. Implement Rabin cryptosystem.
12. Implement ElGamal cryptosystem.

---$---