Hall Ticket Number:

Code No. : 13110 AENTC

VASAVI COLLEGE OF ENGINEERING *(Autonomous)*, HYDERABAD

B.E. (CBCS) III-Semester Main Examinations, December-2017

Applications of Elementary Number Theory in Cryptology

Time: 3 hours Max. Marks: 70

*Note: i) Answer **ALL** questions in **Part-A** and any **FIVE** from **Part-B***
ii) Scientific calculators are permitted. iii) Assume missing data if any.

Part-A (10 × 2 = 20 Marks)

1. Show that $a^2 \equiv b^2 \pmod m$ if $a \equiv b \pmod m$ where a, b, m are integers.
2. Convert 451 in to binary system.
3. Define inverse of a modulo m where a and m are integers.
4. Define ciphertext.
5. Write deciphering formula for block cipher.
6. Encipher **NICE** using Caesar cipher.
7. Write deciphering formula in public key cryptography.
8. Write the enciphering formula in knapsack cipher system.
9. Discuss whether the sequence (3, 13, 17, 19, 25, 89) is super-increasing or not
10. Compute ei = Mi.yi, Mi = M/mi, m*i* = {11, 13, 17, 19}, yi are inverses of Mi modulo mi and M = product of mi's.

Part-B (5 × 10 = 50 Marks)

(All sub-questions carry equal marks)

11. a) If a, b, c, m are integers with m > 0 such that a≡ b(mod m) then show that
    i) a + c ≡ b + c (mod m) ii) ac ≡ bc (mod m).
    b) If $13 \equiv 8 \ (mod\ 5)$, $7 \equiv 2 \ (mod\ 5)$ then show that the addition and subtraction of congruence is true.
12. a) Solve the linear congruences 3x + 4y ≡ 5 (mod 13) ; 2x + 5y ≡ 7 (mod 13).
    b) If B1 and B2 are inverses of A then show that B1 ≡ B2 (mod m).
13. a) Encipher the message GOOD DAY by Caesar cipher.
    b) Decipher LFDP VLDZL using Caesar cipher.
14. a) Using the prime 101 and enciphering key e = 3, encipher the message GOOD using modular exponentiation.
    b) Encipher the message EXPONENTIATION when p = 2633, e = 29.
15. a) Find p and q if n = pq = 4386607 and $\emptyset(n)$ = 4382136.
    b) What is the ciphertext that is prodiced when RSA cipher with key (e,n) = (3, 2669) is used to encipher the message BEST WISHES?
16. a) Decide whether the sequence (11,21,41,81,151) is super–increasing with explanation.
    b) Encipher the message BUY NOW using the knapsack cipher based on the sequence obtained from the super-increasing sequence (17,19,37,81,160) by performing modular multiplication with multiplier w = 29 and modulus m = 331.
17. Answer any ***two*** of the following:
    a) Find the inverse of $\begin{pmatrix} 2 & 5 & 6 \\ 1 & 0 & 5 \\ 2 & 4 & 2 \end{pmatrix}$
    b) Encipher the message STO PPA YME NTE by block cipher system
    c) Briefly explain secrete sharing system.