D.K.M.COLLEGE FOR WOMEN (AUTONOMOUS),VELLORE-1.

SKILL BASED NUMBER THEORY

Unit – I SECTION-A 2 MARKS

1. Define well ordering principles.
2. Define perfect number.
3. State Fermat's last theorem.
4. Define Fibonacci number.
5. Define Division Algorithm.

SECTION-B 5 MARKS

1. Let S be a subset of N with the following two properties
   (i) $1 \in S$
   (ii) If $n \in S$ then $n + 1 \in S$ then $S = N$.
2. Let $S_n = 1 + 2 + 3 \ldots n$. Prove that $S_n = \frac{1}{2} n (n + 1)$
3. $2^n > n$ for every natural number N.
4. $n \geq 3$, then P.T $2^{n-1} > n$.

UNIT – II SECTION-B 2 MARKS

1. Define primes.
2. Define GCD.
3. Define Euclid algorithm.
4. Define proper divisor.
5. Define Sieve Eratosthenes.
6. Define Canonical Factorization.
7. State Fundamental theorem of Arithmatic.
8. Find 480.

SECTION-C 10 MARKS

1. Write properties of divisibility.
2. Find the GCD of (87, 27)
3. Prove that properties of LCM.

UNIT – III SECTION-A 2 MARKS

1. Define Congruences.
2. Define Equivalence Relation.
3. State Chinese Remainder Theorem.
4. Define linear congruence.
5. Define Equivalence class.
6. Solve Congruent equations $455 x = 204 \pmod{469}$

SECTION-C 10 Marks

1. Solve the system of Linearcongruences.
   $x \equiv 3 \pmod 5$
   $x \equiv 2 \pmod 6$
   $x \equiv 4 \pmod 7$
2. Prove that properties of congruences.

UNIT – IV SECTION-A 2 Marks

1. State Euler's Theorem.
2. Define Order
3. Define Index
4. Find the order of $2 \pmod 7$
5. Define integers.

SECTION-B 10 MARKS

1. 5 is a primitive root of (mod 7)
2. Prove properties of indices.
3. Solve $3x^5 \equiv 5 \pmod 7$.

UNIT – V SECTION-A 2 MARKS

1. Define Decoding.
2. Define Character ciphers.
3. Define one – time pads – Exponential ciphers.
4. Define Block ciphers

SECTION-B 10 MARKS

1. Explain public – key cryptography.
2. Write the shoot notes on cryptology.