CS 503 Discrete Mathematics for Cryptography Course Outcomes

Each course outcome is followed in parentheses by the Program Outcome to which it relates.

- State the definition of divisibility in the integers and the statement of the Division Algorithm. ()

- State the definitions of the algebraic notions semigroup, monoid, group, ring and field; the notion of an ideal in a ring and its application to the definitions of gcd and lcm. ()

- State the definition of the Euler Phi function and be competent in calculating its values. ()

- State the definition of a prime number and the statement of the Prime Number Theorem. ()

- State the definition of a finite cyclic group and the orders of a subgroup and an element in a finite group. ()

- State the definition of congruence mod n, the ring of integers mod n and the characterization of the units in this ring; be competent at mod n arithmetic. ()

- Determine when the group of units of the integers mod n is cyclic. ()

- Use the Chinese Remainder Theorem and Gauss' algorithm for finding a solution guaranteed by the theorem. ()

- State Fermat's Theorem and Euler's Theorem. ()

- State the definition of a quadratic residue mod n; the definitions and properties of the Legendre and Jacobi symbols and be competent at calculating them. ()

- Add and multiply polynomials with coefficients from a field (specifically Zp); know and apply the Division Algorithm for polynomials. ()

- State the definition of the gcd of a pair of polynomials and the development of the notion using the notion of an ideal in the ring of polynomials. ()

- State the definition of irreducibility and the factorization of a polynomial into irreducible factors. ()

- State the definitions of addition and multiplication in the ring of polynomials modulo a polynomial and when this ring is a field. ()

- State the definition of the characteristic of a finite field and the linear algebraic meaning of k in the expression p^k giving the number of elements in such a field. ()

- State the definition of the minimal polynomial of an element in a finite field and when such a polynomial is a primitive polynomial; be able to calculate it for the case of a "small" field. ()

- For small p^k, factorize x^(p^k) - x into irreducible factors with coefficients from Zp. ()

- Apply the factorization alluded to above to proving the existence of GF(p^k) using Mobius inversion. ()

- State the nature of the subfields of GF(p^k). ()