GUJARAT TECHNOLOGICAL UNIVERSITY

CYBER SECURITY (59)
MATHEMATICAL FOUNDATION FOR CYBER SECURITY
SUBJECT CODE: 3715901
SEMESTER: I

Type of course: Master of Engineering

Prerequisite: Basic knowledge of Computer Networks and Basic mathematics

Rationale: The course focuses on mathematical foundation. It highlights the basics of number theory like, GCD, Divisibility, Prime number etc. This course includes algebraic structure for Groups, Discrete logarithms and Classification. Probability theory is important to understand the concept of probability and conditional probability. Coding theory is important for liner code, hamming code and syndrome decoding. Pseudorandom number is used for next bit predictor and Blum-Blum-Shub Generator. All mathematical concepts are highly important for the mathematical foundation and calculation of Cyber Security.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE(E)	PA (M)	PA (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Sr. No.	Content	Total Hrs	% Weightage
1	**Introduction to Number Theory** Introduction-Divisibility - Greatest common divisor – Primes- Prime numbers – Cardinality of Primes, Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers, Fermat's and Euler's Theorem, Testing for Primality, Factorization, The Chinese Reminder Theorem, Quadratic Congruence, Exponentiation and Logarithms, Discrete Logarithms	08	20
2	**Algebraic Structures and Finite Fields** Groups – Cyclic groups, Co sets, Modulo groups - Primitive roots – Discrete logarithms The Euclidean Algorithm, Modular Arithmetic, Algebraic Structures-Groups, Rings and Fields, Future Fields of the Form GF(2"), Polynomial Arithmetic, Finite Fields of the Form GF(2^n)	08	15
3	**Pseudorandom Number Generation and Stream Ciphers** Principles of Pseudorandom Number Generation, Principles of Pseudorandom Number Generation using a Block Cipher, Stream Ciphers, RC4 , True Random Number Generators	06	15

4	**Discrete Mathematics for Cryptography** Cryptography and Modular Arithmetic, Inverses & GCDs, The RSA Cryptosystems, Mathematical Induction, Recursion, Recurrences and Induction, Recurrences and Selection	06	10
5	**Coding Theory**	06	15
	Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes - Hadamard Code - Goppa codes.		
6	**Probability Theory** Introduction – Concepts of Probability - Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous- central Limit Theorem-Stochastic Process- Markov Chain.	06	15
7	**Cryptographic Hash Functions** Application of Cryptographic Hash Functions, Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Functions (SHA), SHA-512	06	10

Reference Books:

- Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
- Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.
- Cryptography and Network Security by William Stallings 5th Edition Pearson Education
- Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
- C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
- Cryptography and Network Security by Behrouz A. Forouzan TMH Publication

Course Outcome:

After learning the course the students should be able to:

1. To learn about Number theory including Divisibility, Greatest common divisor and Prime numbers.
2. To understand and apply Euclidean algorithm, Fermat's theorem and Euler's theorem.
3. To understand the concept of Algebraic structure including Groups, Rings, Fields and Classifications.
4. To calculate probability based on Baye's theorem.
5. To calculate probability for discrete random variables and continuous random variables.
6. To apply the concept of Coding.
7. To use Pseudorandom number generation for Next Bit Predictors and Blum-Blum-Shub Generator.

List of Experiments / Tutorials:

1. Find greatest common divisor for following:
    a. gcd (2, 4)
    b. gcd (6, 9)
    c. gcd (7, 5)
    d. gcd (8, 9)
    e. gcd (124, 72)
    f. gcd (748, 2024)

2. Find x,y ∈ Z such that ax + by = gcd (a,b)?
3. Explain Fundamental theorem of arithmetic.
4. Find integer x, y such that 5*x + 7*y = 1
5. Find integer x, y such that 12*x + 8*y = 4
6. Find integer x, y such that

   27*x + 42*y = gcd (27, 42)
7. Using CRT (Chinese Remainder Theorem) to Simplify Modulo Computations Calculate 3299 mod 24
8. Using CRT to Simplify Modulo Computations Calculate 12345*12345 mod 35
9. Using Fermat's little theorem Solve 11^{17} mod 3
10. Using Fermat's little theorem Solve 11^{2016} mod 15
11. Explain properties of Group.
12. Check for the Closure, Identity, Inverse and Associativity properties for following:

    a. $Z_3 = (\{0,1,2\}, +_{mod3})$

    b. $Z_7 = (\{0,1,\ldots,6\}, +_{mod7})$

    c. $_{3 = (\{1,2\}, *mod3)}$

    d. $_{7 = (\{1,\ldots,6\}, *mod7)}$
13. Which integers belong to ?
14. Explain Conditional probability.
15. What is the expected outcome of rolling a dice?
16. Rolling a fair dice, what is the expectation of the square of the outcomes?
17. What is the expected output about rolling a dice Twice?
18. What are the application of Cryptographic Hash Functions?