Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Fourth Year Bachelor of Engineering (Computer/IT)

(To be Proposed For: Academic Year 2020-21)

Subject Code: CT703B-N	**Subject Title: Computational Number Theory**
Pre-requisite	Discrete Mathematics, Algorithms, Probability

Teaching Scheme (Credits and Hours)

Teaching scheme				**Total Credit**	**Evaluation Scheme**					
L	**T**	**P**	**Total**		**Theory**		**Mid Sem Exam**	**CIA**	**Pract.**	**Total**
Hrs	**Hrs**	**Hrs**	**Hrs**		**Hrs**	**Marks**	**Marks**	**Marks**	**Marks**	**Marks**
04	00	02	06	05	03	70	30	20	30	150

Course Objective:

- The emphasis of the course is on the application of the number theory in the design of cryptographic algorithms. Putting them together we will see how we can design several cryptographic algorithms.
- The course will start with the notion of time complexity and with several elementary number theoretic algorithms.
- Computational number theory is a very important area of mathematics that became more prominent in the 70's due to newly discovered applications to cryptography, coding theory, communications and other areas of applied science and technology. It is not an exaggeration that electronic commerce, for example, would be impossible without these recent advances.

Outline of the Course:

Sr. No	**Title of the Unit**	**Minimum Hour**
1	Algorithms for integer arithmetic	8
2	Representation of finite fields	9
3	Algorithms for polynomials	6
4	Elliptic curves	8
5	Primality testing algorithms	9
6	Integer factoring algorithms	8
7	Computing discrete logarithms over finite fields	9
8	Key Exchange and Applications of Number Theory	7

Total hours (Theory):64
Total hours (Lab): 32
Total hours: 96

Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Fourth Year Bachelor of Engineering (Computer/IT)

(To be Proposed For: Academic Year 2020-21)

Detailed Syllabus

Sr. No	Topic	Lecture Hours	Weightage (%)
1	**Algorithms for integer arithmetic:** Divisibility, GCD Computation: (Euclid's Algorithm, Extended Euclid's Algorithm), Modular Arithmetic (Groups, Solving Modular Linear Equations. Chinese Remainder Theorem. Modular Exponentiation, Discrete Logarithm Problem), Montgomery arithmetic, congruence, Hensel lifting, orders and primitive roots, integer and modular square roots, prime number theorem, continued fractions and rational approximations.	8	12
2	**Representation of finite fields:** Prime and extension fields, representation of extension fields, polynomial basis, primitive elements, normal basis, optimal normal basis, irreducible polynomials.	9	15
3	**Algorithms for polynomials:** Root-finding and factorization, Lenstra-Lenstra-Lovasz algorithm, polynomials over finite fields.	6	10
4	**Elliptic curves:** The elliptic curve group and method, elliptic curves over finite fields, Schoof's point counting algorithm.	8	12
5	**Primality testing algorithms:** Pseudo primality Testing, Quadratic Residues, Randomized Primality Test & Deterministic Polynomial Time Algorithm, Fermat test, Miller-Rabin test, Solovay-Strassen test, AKS test.	9	14
6	**Integer factoring algorithms:** Trial division, Pollard rho method, *p*-1 method, CFRAC method, quadratic sieve method.	8	12
7	**Computing discrete logarithms over finite fields:** Baby-step-giant-step method, Pohlig-Hellman method, index calculus methods, linear sieve method, Coppersmith's algorithm.	9	14
8	**Key Exchange and Applications of Number Theory:** Diffie Hellman, ElGamal, MasseyOmura. Computation of Generators of Primes, Algebraic coding theory, cryptography.	7	11
	Total	**64**	**100**

Instructional Method and Pedagogy:

- At the start of course, the course delivery pattern, prerequisite of the subject will be discussed.
- Lectures will be conducted with the aid of multi-media projector, black board, OHP etc.
- Attendance is compulsory in lecture and laboratory which carries 10 marks in overall evaluation.
- One internal exam will be conducted as a part of internal theory evaluation.
- Assignments based on the course content will be given to the students for each unit and will be evaluated at regular interval evaluation.
- Surprise tests/Quizzes/Seminar/tutorial will be conducted having a share of five marks in the overall internal evaluation.
- The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.

- Experiments shall be performed in the laboratory related to course contents.
- Instructor can use SAGE or any other relevant tool for implementation of all experiments.

Learning Outcome:

On successful completion of this course, the student should be able to:

- Understand different number theory algorithms used for design of various cryptographic algorithms.
- Understand different number theory algorithms used coding theory, communications and other areas of applied science and technology.

e-Resources:

- https://nptel.ac.in/courses/106/103/106103015/
- https://nptel.ac.in/courses/111103020/
- https://academic.csuohio.edu/fmartins/courses/mth493/
- http://doc.sagemath.org/html/en/tutorial/
- http://doc.sagemath.org/html/en/reference/

Reference Books:

1. V. Shoup, *A computational introduction to number theory and algebra*, Cambridge University Press.
2. M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag.
3. I. Niven, H. S. Zuckerman and H. L. Montgomery, *An introduction to the theory of numbers*, John Wiley.
4. J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press.
5. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press.
6. A. J. Menezes, editor, *Applications of finite fields*, Kluwer Academic Publishers.
7. J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer International Edition.
8. D. R. Hankerson, A. J. Menezes and S. A. Vanstone, *Guide to elliptic curve cryptography*, Springer-Verlag.
9. A. Das and C. E. Veni Madhavan, *Public-key cryptography: Theory and practice, Pearson Education Asia.*
10. H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag.
11. Introduction to Algorithms: T. H. Cormen, C. E. Leiserson, R. Rivest and C. Stein Prentice Hall India, 2 nd Edition,
12. A Course in Number Theory and Cryptography: Neal Koblitz, SpringerVerlag, New York Inc. May 2001.
13. Cryptography and Network security: Principles and Practice, William Stallings, Pearson Education, 2002.
14. Introduction to Cryptography with Coding Theory, Second Edition, W. Trappe and L. C. Washington, Pearson Education 2007.
15. Cryptography: Theory and Practice, Douglas R. Stinson, CRC Press.
16. Randomized Algorithms, R. Motwani and P. Raghavan, Cambridge University Press, 1995

Kadi Sarva Vishwavidyalaya

Faculty of Engineering & Technology

Fourth Year Bachelor of Engineering (Computer/IT)

(To be Proposed For: Academic Year 2020-21)

List of experiments

No	Name of Experiment
1	Practical based on Rings, Groups and Fields.
2	Program for Chinese Remainder Theorem.
3	Program for Euclid's Algorithm, Extended Euclid's Algorithm.
4	Program based on Integer Arithmetic.
5	Define Hensel lifting for roots and factorizations of polynomials over Henselian rings
6	Write a function that lifts a root of a polynomial (defined to sufficient precision) up one precision or upto two precision.
7	Write a function that lifts a coprime factorization up one precision precision or upto two
8	Program to implement Lenstra-Lenstra-Lovasz algorithm.
9	Program to implement Coppersmith's algorithm
10	Program to implement various elliptic curve algorithms.
11	Program to implement various primality testing.
12	Program to implement Baby-step-giant-step, Pollard rho and Pohlig-Hellman method.
13	Write a program to compute the n-th cyclotomic polynomial on input n
14	Using the CRT to Speed Up RSA Decryption