Department	General Studies		**Major**								
Course Name	Applied Mathematics		**Course Code**	MATH 304							
Prerequisites			**Credit Hours CRH**	4			CTH		6		
				L	3	P	2	T	1		

CRH**: Credit Hours** L**: Lecture** P**: Practical** T**: Tutorial** CTH**: Contact Hours**

Course Description:

This course introduces students to basics of mathematical principles and functions from discrete mathematics that form the foundation for cryptographic and cryptanalysis methods. The course covers five important themes; Mathematical reasoning and mathematical logic and Structures, algorithmic thinking, the concepts and techniques of number theory, modular arithmetic and finite fields. These principles and functions will be helpful in understanding symmetric and asymmetric cryptographic methods examined in (Applied Cryptography) Course.

Topics:

- The Foundations of logic and Proofs
- Basics of discrete structures that include sets, permutations, relations, graphs, trees and finite state machines.
- Algorithms.
- The concepts and techniques of Number Theory.
- Finite fields.

Experiments:

References:

- M. Huth and M. Ryan, Logic in Computer Science, 2nd ed, Cambridge university Press, Cambridge, England, 2004
- Handbook of Proof Theory (Studies in Logic and the Foundations of Mathematics 137) 1st Edition, Kindle Edition by S. R. Buss (Editor) 1998
- R. A. Brualdi, Introductory Combinatorics, 5th ed., Prentice-Hall, Englewood Cliffs, NJ,2009
- Kenneth H. Rosen, 7th ed., Discrete Mathematics and its Applications, MC Graw Hill, 2012
- S. Baase and A. Van Gelder, Computer Algorithms: Introduction to Design and Analysis, 3rd ed., Adisson-Wesley, Reading, MA, 1999
- DECODE, Design & Analysis of Algorithms 2015 A Guide for Engineering Students
- Richard Crandall and Carl Pomerance, 2nd ed., Prime Numbers: A Computational Perspective, Springer-Verlag, New York, 2010
- Richard A. Mollin, Fundamental Number Theory with Application 2nd Edition 2008
- Gary L. Mullen, Daniel Panario, Handbook of Finite Fields, 1st Edition 2013
- Rudolf Lidl, Harald Niederreiter, Introduction to Finite Fields and Their Applications 1986

Detailed of Theoretical Contents		
No.	**Contents**	**Hours**
1	**The Foundations: Logic and Proofs:** • Propositional Logic • Applications of Propositional Logic • Predicates and Quantifiers • Introduction to Proofs • Proof Methods and Strategy	2
2	**Basic Structures: Sets, Functions, Sequences, Sums, and Matrices** • Sets • Cardinality of Sets • Set Operations • Functions • Sequences and Summations • Matrices	4
3	**Algorithms:** • Algorithms • The Growth of Functions • Complexity of Algorithms	4
4	**Number Theory:** • Divisibility and Modular Arithmetic • Integer Representations and Algorithms • Primes and Greatest Common Divisors • Tool to compute Bezout coefficients • Solving Congruencies and Applications	8
5	**Finite fields:** • Groups • Rings • Fields • Finite Fields of the Form GF(p) • Polynomial Arithmetic • Finite Fields of the Form GF(2^n)	8

Detailed of Practical Contents		
No.	**Contents**	**Hours**
1	**The Foundations: Logic and Proofs:** • Propositional logic • Predicates and quantifiers • Rules of inference and introduction to proofs	2
2	**Basic Structures: Sets, Functions, Sequences, Sums, and Matrices** • Sets, set operations and cardinality of sets • Functions, sequences and summations • Matrices	2
3	**Algorithms:** • Algorithms and complexity of algorithms • The Growth of Functions	4
4	**Number Theory:** • Divisibility and Modular Arithmetic • Integer Representations and Algorithms • Primes and Greatest Common Divisors • Bezout coefficients • Solving Congruencies and Applications	6
5	**Finite fields:** • Groups • Rings • Fields • Finite Fields of the Form GF(p) • Polynomial Arithmetic • Finite Fields of the Form GF(2^n)	6

Textbooks	1	M. Huth and M. Ryan, Logic in Computer Science, 2nd ed, Cambridge university Press, Cambridge, England, 2004
	2	Handbook of Proof Theory (Studies in Logic and the Foundations of Mathematics 137) 1st Edition, Kindle Edition by S. R. Buss (Editor) 1998
	3	R. A. Brualdi, Introductory Combinatorics, 5th ed., Prentice-Hall, Englewood Cliffs, NJ,2009
	4	Kenneth H. Rosen, 7th ed., Discrete Mathematics and its Applications, MC Graw Hill, 2012
	5	S. Baase and A. Van Gelder, Computer Algorithms: Introduction to Design and Analysis, 3rd ed., Adisson-Wesley, Reading, MA, 1999
	6	DECODE, Design & Analysis of Algorithms 2015 A Guide for Engineering Students
	7	Richard Crandall and Carl Pomerance, 2nd ed., Prime Numbers: A Computational Perspective, Springer-Verlag, New York, 2010
	8	Richard A. Mollin, Fundamental Number Theory with Application 2nd Edition 2008
	9	Gary L. Mullen, Daniel Panario, Handbook of Finite Fields, 1st Edition 2013
	10	Rudolf Lidl, Harald Niederreiter, Introduction to Finite Fields and Their Applications 1986