Course code	Course Name	L-T-P - Credits	Year of Introduction
MA488	Cryptography	3-0-0-3	2016

Prerequisite : NIL

Course Objective:

1. To understand the fundamentals of Cryptography
2. To acquire knowledge on standard algorithms used to provide confidentiality, integrity and authenticity.

Syllabus: Number Theory - Divisibility, The Division algorithm, Euclidean Algorithm, GCD, Extended Euclidean Algorithm, Primes and properties, Fundamental theorem of arithmetic (statement and proof), Modular arithmetic, Euler function, Congruence in one unknown, Solution of congruences, Modular inverse. Algebra - Definition and examples of Groups, Rings and Fields and finite fields of the form $GF(p)$ and $GF(2^n)$, Euler's theorem, Fermat's little theorem, The Chinese reminder theorem. Asymmetric encryption: The discrete logarithm problem, Diffie–Hellman key exchange, The Elgamal public key cryptosystem, Elliptic Curve Cryptography. Integer Factorization and RSA: Euler's formula and roots modulo pq, The RSA public key cryptosystem, Implementation and security issues, man-in-the-middle Attack, Primality testing, Miller–Rabin test, Pollard' p − 1 factorization algorithm. Elliptic Curves: Elliptic curves over real numbers, Elliptic curve addition algorithm, Elliptic curves over finite fields, The group of an elliptic curve. The elliptic curve discrete logarithm problem, Elliptic curve cryptography, Elliptic Diffie–Hellman key exchange, Elliptic Elgamal public key cryptosystem.

Expected Outcome:

Students will be able to

1. Learn standard algorithms used to provide confidentiality
2. Understand how secure encryption techniques work
3. Design security applications in the field of information technology.

Textbook:

1. Jeffrey Hoffstein, Jill Pipher and Joseph H. Silverman, An Introduction to Mathematical Cryptography, Springer, 2008
2. William Stallings, Cryptography and Network Security, 5th Edition, Prentice Hall Press Upper Saddle River, NJ, USA, 2010

References:

1 Andreas Enge, Elliptic curves and their applications to cryptography: an introduction, 1st Edition Springer, 1999

2 D. R. Stinson, Cryptography, Theory and practice, Chapman & Hall (2006)

3 R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press.

4 Thomas Koshy, Elementary Number Theory with Applications, 2nd Edition, Academic Press, 2007

Module	Syllabus	Hours	End Sem. Exam Marks
I	**Number Theory:** Divisibility, The Division algorithm, Euclidean Algorithm, GCD, Extended Euclidean Algorithm, Primes and properties, Fundamental theorem of arithmetic (statement and proof), Modular arithmetic, Euler function, Congruence in one unknown, Solution of congruences, Modular inverse.	8	15%
II	**Algebra:** Definition and examples of Groups, Rings and Fields and finite fields of the form $GF(p)$ and $GF(2^n)$, Euler's theorem, Fermat's little theorem, The Chinese reminder theorem.	6	15%

FIRST INTERNAL EXAMINATION			
III	**Symmetric encryption:** Symmetric Cipher Model, Substitution Techniques, Transposition Techniques, Rotor Machines, AES cipher, Multiple Encryption and Triple DES,	6	15%
IV	**Asymmetric encryption:** The discrete logarithm problem, Diffie–Hellman key exchange, The Elgamal public key cryptosystem, Elliptic Curve Cryptography	7	15%
SECOND INTERNAL EXAMINATION			
V	**Integer Factorization and RSA:** Euler's formula and roots modulo *pq,* The RSA public key cryptosystem, Implementation and security issues, man-in-the-middle Attack, Primality testing, Miller–Rabin test, Pollard' $p - 1$ factorization algorithm	8	20%
VI	**Elliptic Curves:** Elliptic curves over real numbers, Elliptic curve addition algorithm, Elliptic curves over finite fields, The group of an elliptic curve. The elliptic curve discrete logarithm problem, Elliptic curve cryptography, Elliptic Diffie–Hellman key exchange, Elliptic Elgamal public key cryptosystem	7	20%
END SEMESTER EXAMINATION			

QUESTION PAPER PATTERN
(End semester examination)

The question paper shall consist of Part A, Part B and Part C.

Part A shall consist of three questions of 15 marks each uniformly covering Modules I and II. The student has to answer any two questions (15×2=30 marks).

Part B shall consist of three questions of 15 marks each uniformly covering Modules III and IV. The student has to answer any two questions (15×2=30 marks).

Part C shall consist of three questions of 20 marks each uniformly covering Modules V and VI. The student has to answer any two questions (20×2=40 marks)