COURSE CODE	COURSE NAME	L-T-P-C	YEAR OF INTRODUCTION
EC468	SECURE COMMUNICATION	3-0-0 -3	2016

Prerequisite: EC407 COMPUTER COMMUNICATION

Course objectives:

•To impart the students about the theory and technology behind the secure communication.

Syllabus:

Introduction on Security, Security Goals, Types of Attacks, Modular arithmetic: Groups, Ring, Fields. The Euclidean algorithm, Finite fields of the form GF(p), Polynomial arithmetic, Symmetric Ciphers, Symmetric Cipher Model, Substitution Techniques, Transposition techniques, Block Ciphers, Data encryption Standards, Differential and Linear Crypt analysis Advanced Encryption standard, The AES Cipher, Public key cryptosystem, RSA algorithm, Intruders, Password management

Expected outcome:

The student will be

i. Exposed to the different approaches that handle security and the algorithms in use for maintaining data integrity and authenticity.

ii. Enabled student to appreciate the practical aspects of security features design and their implementation

Text Books:

1. Behrouz A. Forouzan , Cryptography and Network security Tata McGraw-Hill, 2008
2. William Stallings, Cryptography and Network security: principles and practice", 2nd Edition, Prentice Hall of India, New Delhi, 2002

References:

1. David S. Dummit & Richard M Foote, Abstract Algebra, 2nd Edition, Wiley India Pvt. Ltd., 2008.
2. Douglas A. Stinson, Cryptography, Theory and Practice, 2/e, Chapman & Hall, CRC Press Company, Washington, 2005.
3. Lawrence C. Washington, Elliptic Curves: Theory and Cryptography, Chapman & Hall, CRC Press Company, Washington, 2008.
4. N. Koeblitz: A course in Number theory and Cryptography, 2008
5. Thomas Koshy: Elementary Number Theory with Applications, 2/e, Academic Press, 2007
6. Tyagi and Yadav , Cryptography and network security, Dhanpatrai, 2012

Course Plan

Module	Course contents	Hours	End Sem. Exam Marks
I	Introduction on security, security goals and types of attacks: Passive attack, active attack, attacks on confidentiality, attacks on integrity and availability, Security services and mechanisms.	5	15%
II	Modular arithmetic: Groups, Ring, Fields. The Euclidean algorithm, Finite fields of the form GF(p)	4	15%
	Polynomial arithmetic: Finite fields of the form GF (2n).	4	
	FIRST INTERNAL EXAM		
III	Symmetric Ciphers, Symmetric Cipher Model	3	15%

	Substitution Techniques, Caesar Cipher, Mono alphabetic Cipher, Play fair cipher, Hill cipher, Poly alphabetic Cipher, one time pad	4	
IV	Transposition techniques ,Block Ciphers, Data encryption Standards, DES Encryption, DES decryption	3	**15%**
	Differential and Linear Crypt analysis Advanced Encryption standard	2	
	The AES Cipher, substitute bytes transformation, Shift row transformation, Mix Column transformation.	2	
SECOND INTERNAL EXAM			
V	Public key cryptosystem, Application for Public key cryptosystem requirements	2	**20%**
	RSA algorithm, Key management, Distribution of public key, public key certificates, Distribution of secret keys.	5	
VI	Intruders: Intrusion techniques, Intrusion detection, Statistical anomaly detection, Rule based intrusion detection, Distributed intrusion detection, Honey pot, Intrusion detection exchange format.	5	**20%**
	Password management: Password protection, password selection strategies.	2	
END SEMESTER EXAM			

Question Paper Pattern

The question paper shall consist of three parts. Part A covers modules I and II, Part B covers modules III and IV, and Part C covers modules V and VI. Each part has three questions uniformly covering the two modules and each question can have maximum four subdivisions. In each part, any two questions are to be answered. Mark patterns are as per the syllabus with 50% for theory and 50% for logical/numerical problems, derivation and proof.