NETWORK SECURITY AND CRYPTOGRAPHY

II Semester: ES								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
		L	T	P	C	CIA	SEE	Total
BESB18	Elective	3	-	-	3	30	70	100
Contact Classes: 45	Tutorial Classes: Nil	Practical Classes: Nil				Total Classes: 45		

I. COURSE OVERVIEW:

The aim of this course is to introduce the student to the areas of cryptography and cryptanalysis. It develops a basic understanding of the algorithms used to protect users online and to understand some of the design choices behind these algorithms. The course emphasizes to give a basic understanding of previous attacks on cryptosystems with the aim of preventing future attacks. A wide variety of basic cryptographic primitives will be discussed along with recent developments in some advanced topics like identity-based encryption, attribute-based encryption, functional encryption, two-party/multi-party computation, bitcoin and crypto-currency and postquantum cryptography. The cryptanalysis part will help us understanding challenges for cybersecurity that includes network security, data security, mobile security, cloud security and endpoint security.

II. COURSE OBJECTIVES:

The students will try to learn:

I. About Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security

II. The simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operations.

III. The IP Security Overview, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations, Key Management.

III. COURSEOUTCOMES:

After successful completion of the course, students should be able to:

CO1	**Understand** principles and practice of network security and cryptography by gaining knowledge in cryptographic algorithms;	Understand
CO2	**Design** basic security architectures through selection and integration of relevant security components	Apply
CO3	**Make use** of advanced cryptographic algorithms in network protocols and network applications.	Apply
CO4	**Analyze and apply system security concept to recognize malicious code**	Analyze
CO5	**Understand** Key management using smart cards for authentication requires the use of a PKI.	Understand
CO6	**Illustrate** various Public key cryptographic techniques in encryption/ decryption.	Understand

IV. SYLLABUS:

UNIT-I	INTRODUCTION	Classes: 08
Attacks, Services and Mechanisms, Security attacks, Security services, A Model for Internetwork security. Classical Techniques: Conventional Encryption model, Steganography, Classical Encryption Techniques.		

UNIT-II MODERN TECHNIQUES Classes: 10

MODERN TECHNIQUES:
Simplified DES, Block Cipher Principles, Data Encryption standard, Strength of DES, Differential and Linear Cryptanalysis, Block Cipher Design Principles and Modes of operations.
Algorithms: Triple DES, International Data Encryption algorithm, Blowfish, RC5, CAST-128, RC2, Characteristics of Advanced Symmetric block cifers. **Conventional encryption:** Placement of Encryption function, Traffic confidentiality, Key distribution, Random Number Generation.
Public key cryptography: Principles, RSA Algorithm, Key Management, Diffie-Hellman Key exchange, Elliptic Curve Cryptography.

UNIT-III NUMBER THEORY Classes: 08

NUMBER THEORY:
Prime and Relatively prime numbers, Modular arithmetic, Fermat's and Euler'stheorems, Testing for primality, Euclid's Algorithm, the Chinese remainder theorem, Discrete logarithms.

Message authentication and hash functions:
Authentication requirements and functions, Message Authentication, Hash functions, Security of Hash functions and MACs.

UNIT-IV HASH AND MAC ALGORITHMS Classes: 10

HASH AND MAC ALGORITHMS:
MD File, Message digest Algorithm, Secure Hash Algorithm, RIPEMD-160, HMAC.
Digital signatures and authentication protocols: Digital signatures, Authentication Protocols, Digital signature standards.
Authentication applications: Kerberos, X.509 directory Authentication service. Electronic Mail Security: Pretty Good Privacy, S/MIME.

UNIT-V IP SECURITY AND WEB SECURITY Classes: 09

IP SECURITY:
Overview, Architecture, Authentication, Encapsulating Security Payload, Combining security Associations, Key Management.
Web security: Web Security requirements, Secure sockets layer and Transport layer security, Secure Electronic Transaction.
Intruders, viruses and worms: Intruders, Viruses and Related threats.
Fire walls: Fire wall Design Principles, Trusted systems.

TEXT BOOKS:

1. Cryptography and Network Security: Principles and Practice - William Stallings, Pearson Education.
2. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.

REFERENCE BOOKS:

1. Fundamentals of Network Security by Eric Maiwald (Dreamtech press)
2. Network Security - Private Communication in a Public World by Charlie Kaufman, Radia Perlman and Miken Speciner, Pearson/PHI.
3. Principles of Information Security, Whitman, Thomson.
4. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH
5. Introduction to Cryptography, Buchmann, Springer.