BR23 B.Tech CSE III YEAR II SEMESTER SYLLABUS

		L	T	P	C
III Year II Semester	**CRYPTOGRAPHY & NETWORK SECURITY (23CS6T03)** **(Common to CSE, IT branches)**	3	0	0	3

Course Objectives:

The main objectives of this course are to explore the working principles and utilities of various cryptographic algorithms including secret key cryptography, hashes and message digests, public key algorithms, design issues and working principles of various authentication protocols and various secure communication standards including Kerberos, IPsec, and SSL/TLS.

Course Outcomes:

- **CO1:** Understand security goals, cryptographic primitives, and mathematical foundations.
- CO2: Apply symmetric encryption algorithms.
- CO3: Apply asymmetric encryption algorithms.
- CO4: Analyze hash functions, message authentication, digital signatures and Kerberos.
- CO5: Evaluate security protocols such as SSL, IPsec.

UNIT I:

Basic Principles : Security Goals, Cryptographic Attacks, Services and Mechanisms, Mathematics of Cryptography- integer arithmetic, modular arithmetic, matrices, linear conguence.

UNIT II:

Symmetric Encryption: Mathematics of Symmetric Key Cryptography-algebraic structures, GF(2^n) Fields, Introduction to Modern Symmetric Key Ciphers-modern block ciphers, modern stream ciphers, Data Encryption Standard- DES structure, DES analysis, Security of DES, Multiple DES, Advanced Encryption Standard-transformations, key expansions, AES ciphers, Analysis of AES.

UNIT III:

Asymmetric Encryption: Mathematics of Asymmetric Key Cryptography-primes, primality testing, factorization, CRT, Asymmetric Key Cryptography- RSA crypto system, Rabin cryptosystem, Elgamal Crypto system, ECC

Dr.N.Rama Krishnaiah, Professor of CSE,UCEK & Control of Examination JNTUK, kakinada.	Dr.C.Krishna Mohan, Professor of CSE,IIT, Kandi, Hyderabad.	Dr.P.Radha Krishna, Professor of CSE,NIT, Warangal	Mr.Rajesh Bobburi Chief Operating Officer, HighQ Labs Private Limited, Rajahmundry	Dr.Lakshmi Haritha Medida, Associate Professor, R.M.K.Engineering College,Kavaraipettai,Tamilnadu	Dr.K.Srinivas, Professor & HoD Department of CSE, B.V.C.I.T.S, Batlapalem

UNIT IV:

Data Integrity, Digital Signature Schemes & Key Management : Message Integrity and Message Authentication-message integrity, Random Oracle model, Message authentication, Cryptographic Hash Functions-whirlpool, SHA-512, Digital Signature- process, services, attacks, schemes, applications, Key Management-symmetric key distribution, Kerberos.

UNIT V:

Network Security-I: Security at application layer: PGP and S/MIME, Security at the Transport Layer: SSL and TLS, **Network Security-II :** Security at the Network Layer: IPSec-two modes, two security protocols, security association, IKE, ISAKMP, System Security-users, trust, trusted systems, buffer overflow, malicious software, worms, viruses, IDS, Firewalls.

Text Books:

1. Cryptography and Network Security, 3rd Edition Behrouz A Forouzan, Deb deep Mukhopadhyay, McGraw Hill,2015
2. Cryptography and Network Security,4th Edition, William Stallings, (6e) Pearson,2006
3. Everyday Cryptography, 1st Edition, Keith M.Martin, Oxford,2016

Reference Books:

1. Network Security and Cryptography, 1st Edition, Bernard Meneges, Cengage Learning,2018

			Rajesh		
Dr.N.Rama Krishnaiah, Professor of CSE,UCEK & Control of Examination JNTUK, kakinada.	Dr.C.Krishna Mohan, Professor of CSE,IIT, Kandi, Hyderabad.	Dr.P.Radha Krishna, Professor of CSE,NIT, Warangal	Mr.Rajesh Bobburi Chief Operating Officer, HighQ Labs Private Limited, Rajahmundry	Dr.Lakshmi Haritha Medida, Associate Professor, R.M.K.Engineering College,Kavarai pettai,Tamilnadu	Dr.K.Srinivas, Professor & HoD Department of CSE, B.V.C.I.T.S, Batlapalem