K. S. INSTITUTE OF TECHNOLOGY

An Autonomous Institution under VTU, Approved by AICTE

Department of Computer Science & Engineering

M.Tech SECOND SEMESTER SYLLABUS

Course: Information & Network Security		Semester	II
Course Code	**25MSCS214B**	CIE Marks	50
Teaching Hours/Week (L:P:SDA)	3:0:0	SEE Marks	50
Total Hours of Pedagogy	40	Total Marks	100
Credits	03	Exam Hours	03
Examination type (SEE)	**Theory**		

Course Objectives (Course Skill Set)

1. Explain the basics of Cryptography and Network Security.
2. Secure a message over insecure channel by various means.
3. Maintain the Confidentiality, Integrity, Reliability and Availability of a data.

Module-1

Classical Encryption Techniques Symmetric Cipher Model, Cryptography, Cryptanalysis and BruteForce Attack, Substitution Techniques, Caesar Cipher, Mono-alphabetic Cipher, Playfair Cipher, Hill Cipher, Poly alphabetic Cipher, One Time Pad. Block Ciphers and the data encryption standard: Traditional block Cipher structure, stream Ciphers and block Ciphers, Motivation for the Feistel Cipher structure, the Feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key.

Module-2

Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. Public-key cryptanalysis. The RSA algorithm, description of the algorithm, computational aspects, the security of RSA. Other Public-Key Cryptosystems: Diffie-Hellman key exchange, The algorithm, key exchange protocols, man in the middle attack, Elgamal Cryptographic systems, Elliptic curve arithmetic, abelian groups, elliptic curves over real.

Module-3

Key Management and Distribution: Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory, public key authority, public keys certificates, X-509 certificates. Certificates, X-509 version 3, public key infrastructure. User Authentication: Remote user Authentication principles, Mutual Authentication, one way Authentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one way Authentication, Kerberos, Motivation , Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one way Authentication, federated identity

management, identity management, identity federation, personal identity verification.

Module-4

Wireless network security: Wireless security, Wireless network threats, Wireless network measures, mobile device security, security threats, mobile device security strategy, IEEE 802.11 Wireless LAN overview, the Wi-Fi alliance, IEEE 802 protocol architecture. Security, IEEE 802.11i services, IEEE 802.11i phases of operation, discovery phase, Authentication phase, key management phase, protected data transfer phase, the IEEE 802.11i pseudorandom function. Web Security Considerations: Web Security Threats, Web Traffic Security Approaches. Secure Sockets Layer: SSL Architecture, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, and shake Protocol, Cryptographic Computations. Transport Layer Security: Version Number, Message Authentication Code, Pseudorandom Functions, Alert Codes, Cipher Suites, Client Certificate Types, Certificate Verify and Finished Messages, Cryptographic Computations, and Padding. HTTPS Connection Initiation, Connection Closure. Secure Shell(SSH) Transport Layer Protocol, User Authentication Protocol, Connection Protocol

Module-5

Electronic Mail Security: Pretty good privacy, notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing, enhanced security services, Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow. IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service, transport and tunnel modes, combining security associations, authentication plus confidentiality, basic combinations of security associations, internet key exchange, key determinations protocol, header and payload formats, cryptographic suits.

Assessment Details (both CIE and SEE)

The weightage of Continuous Internal Evaluation (CIE) is 50% and for Semester End Exam (SEE) is 50%. The minimum passing mark for the CIE is 50% of the maximum marks. Minimum passing marks in SEE is 40% of the maximum marks of SEE. A student shall be deemed to have satisfied the academic requirements and earned the credits allotted to each subject/ course if the student secures not less than 50% (50 marks out of 100) in the sum total of the CIE (Continuous Internal Evaluation) and SEE (Semester End Examination) taken together.

Continuous Internal Evaluation:

1. Three Unit Tests each of **25 Marks**
2. Two assignments each of **25 Marks** or **one Skill Development Activity of 25 marks**
3. The sum of three tests, two assignments/skill Development Activities, will be scaled down to **50 marks.**

CIE methods /question paper is designed to attain the different levels of Bloom's taxonomy as per the outcome defined for the course.

Semester End Examination:

1. The SEE question paper will be set for 100 marks and the marks scored will be proportionately reduced to 50.
2. The question paper consists of Part A and Part B. Part A consists of 10 questions from 5 modules, each carrying 2 marks.
3. Part B consists of 10 questions. Each full question is for 16 marks. There will be two full questions (with a maximum of three sub-questions) from each module.
4. Each full question will have a sub-question covering all the topics under a module.
5. The students will have to answer five full questions, selecting one full question from each module.

Suggested Learning Resources:

Text Books:

1. Cryptography and Network Security,William Stallings, Pearson, 6thEdition
2. Cryptography and Information Security,V K Pachghare, PHI, 2nd Edition

Web links and Video Lectures (e-Resources):

- https://www.coursera.org/specializations/computer-network-security

Skill Development Activities Suggested:

The students with the help of the course teacher can take up relevant technical activities which will enhance their skill. The prepared report shall be evaluated for CIE marks.

Course outcome (Course Skill Set):

At the end of the course the student will be able to :

Sl. No.	Description	Blooms Level
CO1	Identify the vulnerabilities in any computing system and hence be able to design a security solution.	L2
CO2	Identify the security issues in the network and resolve it.	L2
CO3	Analyze security mechanisms using rigorous approaches, including theoretical.	L2
CO4	Apply various protocols for network security to protect against the threats in the networks	L3

Program Outcome of this course:

Sl. No.	Description	POs
1	**Engineering Knowledge:** Apply knowledge of mathematics, science, engineering fundamentals, and a specialization to the solution of complex engineering problems.	PO1
2	**Problem Analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles.	PO2
3	**Design/Development of Solutions:** Design solutions for complex engineering problems and design system components that meet specified needs with consideration for public health and safety, cultural, societal, and environmental concerns.	PO3

4	**Conduct Investigations of Complex Problems:** Use research-based knowledge and methods including design of experiments, analysis, and interpretation of data, and synthesis of information to provide valid conclusions.	PO4
5	**Modern Tool Usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools to complex engineering activities with an understanding of limitations.	PO5
6	**Engineer and Society / Project Management & Finance:** Demonstrate knowledge and understanding of engineering and management principles to manage projects, as well as societal, health, safety, legal, and cultural issues.	PO6

Mapping of COs and POs

	PO1	PO2	PO3	PO4	PO5	PO6
CO1		**x**		**x**		
CO2		**x**				**x**
CO3		**x**		**x**		
CO4			**x**			