SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Department of Information Technology	LP: IT18603 Rev. No: 01
B.E/B.Tech/ME/M.Tech: B.Tech Regulation: 2018 PG Specialiasation: Sub. Code / Sub. Name : IT18603 Information Security Unit : I	Date: 28.02.2022

Unit Syllabus:

INTRODUCTION TO SECURITY AND CRYPTOGRAPHY

Introduction to Information security, Critical characteristics of information –Components of an information system –Balancing information security and access - The SDLC and Security SDLC- NIST – Need for Security. Foundations of Cryptography, Simple Substitution and Transposition Ciphers.

Objective: To give an insight into the key principles of information security and cipher methods.

Session No *	Topics to be covered	Ref	Teaching Aids
1	Introduction to Information security – History, Key information security concepts	1-Ch.1 Pg (1-32)	LCD/BB
2	Critical characteristics of information – CNSS model, Components of an information system, Balancing information security and access	1-Ch.1 Pg (1-32)	LCD/BB
3	The SDLC and Security SDLC –Methodology and Phases	1-Ch.1 Pg (1-32)	LCD/BB
4	NIST – Need for Security	1-Ch.1 Pg (1-32)	LCD/BB
5	Foundations of Cryptography – Encryption, Decryption, Plain Text, Cipher Text, Brute force attack	1-Ch.1 Pg (1-32)	LCD/BB
6	Simple Substitution - Caesar Cipher, Vigenere cipher using formula	1-Ch.1 Pg (1-32)	LCD/BB
7	Vigenere cipher using Tabula Recta	3-Ch.3 Pg (39-68)	LCD/BB
8	Playfair Cipher	3-Ch.3 Pg (39-68)	LCD/BB
9	Transposition Ciphers – Rail fence cipher- Single Columnar and Double Columnar Transposition cipher	3-Ch.3 Pg (39-68)	LCD/BB
10,11, 12	Tutorial		LCD/BB
Content Beyond Syllabus :			

* Session duration: 50 minutes

Sub. Code / Sub. Name: IT18603 Information Security
Unit : II

Unit Syllabus :

LEGAL ETHICAL & PROFESSIONAL ISSUES
Law and Ethics in Information Security- International law and legal bodies, Ethical differences across cultures, ethics and education, deterring unethical and illegal behavior- codes of ethics at professional organization.

Objective: To get insight about the Law and Ethics in Information Security

Session No *	Topics to be covered	Ref	Teaching Aids
13	Law and Ethics in Information Security – policy, law, code of conduct, Liability	1-Ch.2 Pg (89-115)	LCD/BB
14	International law and legal bodies – General computer crime laws, export and espionage laws, copyright law	1-Ch.2 Pg (89-115)	LCD/BB
15	Financial Reporting , Freedom of Information Act	1-Ch.2 Pg (89-115)	LCD/BB
16	State and local regulations	1-Ch.2 Pg (89-115)	LCD/BB
17	International laws and legal bodies	1-Ch.2 Pg (89-115)	LCD/BB
18	Digital millennium copyright Act	1-Ch.2 Pg (89-115)	LCD/BB
19	Ethical differences across cultures, ethics and education, deterring unethical and illegal behavior	1-Ch.2 Pg (89-115)	LCD/BB
20	Codes of ethics at professional organization, HIPAA principles	1-Ch.2 Pg (89-115)	LCD/BB
21	Summary		LCD/BB
22, 23, 24	Tutorial		LCD/BB

Content beyond syllabus covered (if any): HIPAA principles

- Session duration: 50 mins

Sub. Code / Sub. Name: IT18603 Information Security
Unit : III

Unit Syllabus :

CRYPTOGRAPHY AND DIGITAL SIGNATURES
Cryptographic Algorithms - Symmetric and Asymmetric encryption – Cryptographic tools – Digital Signature, Digital certificates, Hybrid cryptographic systems, Steganography, protocols for secure communication.
Objective: To gain knowledge about Cryptographic Algorithms, Digital certificates and Steganography .

Session No *	Topics to be covered	Ref	Teaching Aids
25	Cryptographic Algorithms - Stream Ciphers vs. Block Ciphers	3-Ch.3 Pg (39-68)	LCD/BB
26	Symmetric and Asymmetric encryption – DES	3-Ch.5 Pg(249-261)	LCD/BB
27	Symmetric and Asymmetric encryption - AES	3-Ch.6 Pg(267-277)	LCD/BB
28	Diffie Hellmen, RSA	3-Ch.7 Pg(287-317)	LCD/BB
29	Cryptographic tools - Public key Infrastructure	3-Ch.8 Pg(320-351)	LCD/BB
30,31	Cryptographic tools - Digital Signature – NIST DSA, Elliptic curve, Digital certificates	3-Ch.8 Pg(320-351)	LCD/BB
32	Hybrid cryptographic systems, Steganography	1-Ch.8 Pg (349-386)	LCD/BB
33	Protocols for secure communication.	1-Ch.8 Pg (349-386)	LCD/BB
34, 35 36	Summary & Tutorial		LCD/BB

Content beyond syllabus covered (if any):

- Session duration: 50 mins

SRI VENKATESWARA COLLEGE OF ENGINEERING

COURSE DELIVERY PLAN - THEORY

Sub. Code / Sub. Name: IT18603 Information Security
Unit : IV

Unit Syllabus :

SECURITY TECHNOLOGY
Introduction- Access control- firewall, protecting remote connections- Intrusion Detection and Prevention system –Honey pots, Honey Nets and Padded cell systems, scanning and analysis tools, Digital forensics.

Objective: To understand the importance of access control, firewall, honeypots and digital forensics.

Session No *	Topics to be covered	Ref	Teaching Aids
37	Introduction- Access control- firewall, protecting remote connections	1-Ch.7 Pg (291-346)	LCD/BB
38	Intrusion Detection and Prevention system – Terminology, need, method	1-Ch.7 Pg (291-346)	LCD/BB
39	Intrusion Detection and Prevention system –Deployment and implementation	1-Ch.7 Pg (291-346)	LCD/BB
40	Honey pots – Introduction, Trap and Trace	1-Ch.7 Pg (291-346)	LCD/BB
41	Honey Nets and Padded cell systems – Active Analysis tool	1-Ch.7 Pg (291-346)	LCD/BB
42,43	scanning and analysis tools – Port scanners, firewall analysis tools, OS detection tools	1-Ch.7 Pg (291-346)	LCD/BB
44.45	Digital forensics – Methodology, evidentiary procedure	1-Ch.12 Pg (563-573)	LCD/BB
46, 47, 48	Summary		LCD/BB
Content beyond syllabus covered (if any):			

- Session duration: 50 mins

Sub. Code / Sub. Name: IT18603 Information Security
Unit : V

Unit Syllabus:

Blockchain and beyond
Hashing – SHA – MD5 – Block chain: Basics – Contents of a Block – Hashchain to Blockchain - Digital Money to Distributed Ledgers , Design Primitives: Protocols, Security, Consensus, Permissions, Privacy - Basic consensus mechanisms Requirements for the consensus protocols, Proof of Work (PoW) – Crypto Currency
Objective: To understand the concept of blockchain and crypto currency

Session No *	Topics to be covered	Ref	Teaching Aids
49	Introduction to Hashing – simple hashing	4-Ch.15 Pg(305-320)	LCD/BB
50	SHA – characteristics, types,methodologies	4-Ch.15 Pg(305-320)	LCD/BB
51	MD5 – characteristics, types,methodologies	4-Ch.15 Pg(305-320)	LCD/BB
52	Block chain: Basics – Contents of a Block – Hashchain to Blockchain	3-Ch.1 Pg(1-6)	LCD/BB
53	Digital Money to Distributed Ledgers	3-Ch.2 Pg(9-24)	LCD/BB
54	Design Primitives: Protocols, Security, Consensus, Permissions, Privacy	3-Ch.1 Pg(9-24)	LCD/BB
55	Basic consensus mechanisms Requirements for the consensus protocols	3-Ch.1 Pg(9-24)	LCD/BB
56	Proof of Work (PoW) – Crypto Currency	3-Ch.1 Pg(9-24)	LCD/BB
57	Summary		LCD/BB
58,59, 60	Tutorial		LCD/BB
Content beyond syllabus covered (if any):			

* Session duration: 50 mins

Sub. Code / Sub. Name: **IT18603 Information Security**

References:

1. Michael E Whitman and Herbert J Mattord, "Principles of Information Security", Vikas Publishing House, New Delhi, fifth edition, Cengage learning , 2015.
2. Melanie Swa, "Block chain: Blueprint for a new economy", First edition, O'Reilly, 2015
3. William Stallings, "Cryptography and Network Security: Principles and Practices", Seventh Edition, Pearson Education, 2017.
4. Mark Rhodes- Ousley ,"Information Security: The complete Reference", Second Edition Mcgraw Hill, 2013.

	Prepared by	Approved by
Signature		
Name	Dr.G.Sumathi & Dr.T.Sukumar	Dr.V.Vidhya,
Designation	Prof/IT Assoc.Prof/IT	HOD/IT
Date	28/02/22	28/02/22
Remarks* :		
Remarks* :		

* If the same lesson plan is followed in the subsequent semester/year it should be mentioned and signed by the Faculty and the HOD