Course Code: ITC502	**Course Title :Computer Network Security**	**Credit**
Currently same	(Subject name)	3
1)Prerequisite: Basic concepts of Computer Networks & Network Design, Operating System		
2)Course Objectives: The course aims:		
1	Explain the fundamentals concepts of computer security and network security.	
2	Identify the basic cryptographic techniques using classical and block encryption methods.	
3	Study and describe the system security malicious software.	
4	Describe the Network layer security, Transport layer security and application layer security.	
5	Explain the need of network management security and illustrate the need for NAC.	
6	Identify the function of an IDS and firewall for the system security.	
3)Course Outcomes: On successful completion, of course, learner/student will be able to:		
1	Explain the fundamentals concepts of computer security and network security.	
2	Identify the basic cryptographic techniques using classical and block encryption methods.	

3	Study and describe the system security malicious software.
4	Describe the Network layer security, Transport layer security and application layer security.
5	Explain the need of network management security and illustrate the need for NAC.
6	Identify the function of an IDS and firewall for the system security.

4) Syllabus

Module		**Content**	**Hrs**
Module 1	**Introduction to Network Security & cryptography**	Computer security and Network Security(Definition), CIA, Services, Mechanisms and attacks, The OSI security architecture, Network security model. Classical Encryption techniques (mono-alphabetic and poly-alphabetic substitution techniques: Vigenere cipher, playfair cipher, transposition techniques: keyed and keyless transposition ciphers). Introduction to steganography. **Self-learning Topics:** Study some more classical encryption techniques and solve more problems on all techniques. Homomorphic encryption in cloud computing	07

Module 2	**Cryptography: Key management, distribution and user authentication**	Block cipher modes of operation,Data Encryption Standard, Advanced Encryption Standard (AES). RC5 algorithm. Public key cryptography: RSA algorithm. Hashing Techniques: SHA256, SHA-512, HMAC and CMAC, Digital Signature Schemes – RSA, DSS. Remote user Authentication Protocols, Kerberos, Digital Certificate: X.509, PKI **Self-learning Topics:** Study working of elliptical curve digital signature and its benefits over RSA digital signature.	09
Module 3	**Malicious Software**	SPAM, Trojan horse, Viruses, Worms, System Corruption, Attack Agents, Information Theft, Trapdoor, Keyloggers, Phishing, Backdoors, Rootkits, Denial of Service Attacks, Zombie **Self-learning Topics:** Study the recent malicious software and their effects.	04
Module 4	**IP Security, Transport level security and Email Security**	IP level Security: Introduction to IPSec, IPSec Architecture, Protection Mechanism (AH and ESP), Transport level security: VPN. Need Web Security considerations, Secure Sockets Layer (SSL)Architecture, Transport Layer Security (TLS), HTTPS,	07

		Secure Shell (SSH) Protocol Stack. Email Security: Secure Email S/MIME Screen reader support enabled. **Self-learning Topics:** Study Gmail security and privacy from Gmail help	
Module 5	**Network Management Security and Network Access Control**	Network Management Security:SNMPv3, NAC:Principle elements of NAC,Principle NAC enforcement methods, How to implement NAC Solutions, Use cases for network access control **Self-learning Topics:** Explore any open source network management security tool	06
Module 6	**System Security**	IDS,Classification of Intrusion Detection Systems,Detection Method of IDS Deployment, Firewall Design Principles, Characteristics of Firewalls, Types of Firewalls,IDS vs Firewalls **Self-learning Topics:** Study firewall rules table	06
		Total	**39**

5) Textbooks:	
1	William Stallings, Cryptography and Network Security, Principles and Practice, 6th Edition, Pearson Education, March 2013.
2	Behrouz A. Ferouzan, “Cryptography & Network Security”, Tata Mc Graw Hill.
3	Mark Stamp’s Information Security Principles and Practice, Wiley
4	Bernard Menezes, “Cryptography & Network Security”, Cengage Learning.
6) Reference Books:	
1	Applied Cryptography, Protocols, Algorithms and Source Code in C, Bruce Schneier, Wiley.
2	Cryptography and Network Security, Atul Kahate, Tata Mc Graw Hill.
3	www.rsa.com

7) Internal Assessment:

Assessment consists of one)Mid Term Test of 20 marks and Continuous Assessment of 20 marks.(Total 40

Mid Term test is to be conducted when approx. 50% syllabus is completed Duration of the midterm test shall be one hour.

8) Continuous Assessment:-

Continuous Assessment **is of 20 marks.** The rubrics for assessment will be considered on approval by the subject teachers. The rubrics can be any 2 or max 4 of the following:-

Sr.no	**Rubrics**	**Marks**
1.	*Certificate course for 4 weeks or more:- NPTEL/ Coursera/ Udemy/any MOOC	10 marks
2	Mini Project / Extra Experiments/ Virtual Lab	10 marks
3.	GATE Based Assignment test/Tutorials etc	10 marks
4.	Multiple Choice Questions (Quiz)	5 marks

*****For sr.no.1, the date of the certification exam should be within the term and in case a student is unable to complete the certification , the grading has to be done accordingly.

9)Rubrics for slow learners:-

1.) Case study, Presentation, group discussion, technical debate on recent trends in the said course (10 marks)

2. Project based Learning and evaluation / Extra assignment / Question paper solution (10 marks)

3) Multiple Choice Questions (Quiz) (5marks)

4) Literature review of papers/journals (5 marks)

5) Library related work (5 marks)

10)Rubrics for Indirect Assessment :-

1. Mock Viva/Practical
2. Skill Enhancement Lecture
3. Extra Assignments/lab/lecture

11)End Semester Theory Examination:	
1	Question paper will be of 60 marks
2	Question paper will comprise a total of five questions
3	All question carry 20 marks
4	Any three questions out of five need to be solved.