Sub Committee for Curriculum Development
COMPUTER SCIENCE AND INFORMATION TECNOLOGY

Format to submit syllabus

Course Name: Cyber Security

(UG/PG): UG & PG

Number of Credits: 02

Level: 4

Learning Objective(s):

1. Analyze and illustrate threat models
2. Examine the different cyber laws and their importance
3. Compare and contrast the implemented management practices in the cyber world
4. Illustrate Symmetric and Asymmetric Encryption mechanisms

Pre-requisites:

1. Knowledge of Computer Networks
2. Knowledge of Operating system

Course Outline

Sr. No.	Topic	Hours
1.	**Introduction:** Common Security Goals, Threat Modeling, Security Analysis; Cyber Attack Trends, Threats, and Homeland Security: Cyber Crime and Botnets, DDoS Attacks, Estonia, and Hacktivism, Cyber Espionage and the Athens Affair, Critical Infrastructure and Cyber Security	9
2.	**Cyber Laws:** Introduction about the cyber space, Regulation of cyber space, Scope of Cyber Laws- ecommerce, online contract; IPRs (copyright, trademarks and software patenting); e-taxation; e-governance and cyber crimes, cyber law in India with special reference to information technology Act, 2000.	9
3.	**Management and Protection:** Management of malicious intent, threat scenarios, critical infrastructures, security targets and policies, security mechanisms, examples of applications and their different security requirements, multi-lateral security, privacy and data protection, computer misuse legislation, Operating system and network security.	9
4	**Security Mechanism and Algorithms** End-end security (COMSEC), link encryption (TRANSEC), compartments. Privacy, Authentication, Denial of service. Non-repudiation. Types of encryption, classical encryption mechanisms: ceaser cipher, mono alphabetic cipher, play fair cipher. Symmetric ciphers: fiestel cipher structure, DES. Integrity and authentication in symmetric mechanism. Asymmetric Encryption: public key encryption mechanism	

Books Recommended:

Text Books:

1. Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives", First Edition, Wiley India Pvt Ltd.
2. Schneier, B., "Applied Cryptography - Protocols, Algorithms, and Source Code in C", Second Edition. John Wiley and Sons, 1995

Reference Books:

1. Stinson D., "Cryptography - Theory and Practice", CRC Press, Boca Raton, FA, 1995
2. Stein L., "Web Security: A Step-by-Step Reference Guide", Addison Wesley Longman,
3. Inc., 1998
4. Gollmann, D., "Computer Security", Wiley, 1999
5. Anderson R., "Security Engineering: A Guide to Building Dependable Distributed Systems", Wiley
6. Cheswick W., Bellovin S., "Firewalls and Internet Security: Repelling the Wily Hacker", 2nd ed., Addison-Wesley
7. Garfinkel S., Spafford G., "Practical Unix and Internet Security", O'Reilly
8. Amoroso E., "Fundamentals of Computer Security Technology", Prentice-Hall

Research Papers/Articles recommended for reading :

1. http://www.techrepublic.com/resource-library/topic/security/
2. http://www.csc.com/cybersecurity/insights/53094-csc_security_stack_an_integrated_security_service

Suggested Evaluation Methods:

Continuous Assessment – 2 credits	Test, Assignment

Sub-specialization Committee:

Name of Member	Prof. Maya Shelke	Prof. Praveen Gubbala		
Designation	Asst. Prof	Asst. Prof		
Org. / Inst.	SIT	SIT		
Signature				

Name of the Expert:

Signature:

Date: