Faculty of Science and Technology

Savitribai Phule Pune University

Maharashtra, India

http://unipune.ac.in

Honours* in Cyber Security

Board of Studies

(Computer Engineering)

(with effect from A.Y. 2020-21)

Savitribai Phule Pune University

Honours* in Cyber Security

With effect from 2020-21

Year & Semester	Course Code and Course Title	Teaching Scheme Hours / Week			Examination Scheme and Marks						Credit Scheme		
		Theory	Tutorial	Practical	Mid-Semester	End-Semester	Term work	Practical	Presentation	Total Marks	Theory / Tutorial	Practical	Total Credit
TE & V	Information and Cyber Security	04	--	--	30	70	--	--	--	100	04	--	04
	Information and Cyber Security Laboratory	--	--	02	--	--	50	--	--	50	--	01	01
	Total	04	-	02	100		50	-	-	150	04	01	05
									Total	**Credits =**		**05**	
TE & VI	Enterprise Architecture and Components	04	--	--	30	70	--	--	--	100	04	--	04
	Total	04	-	-	100		-	-	-	100	04	-	04
								Total	Credits =		04		
BE & VII	Internet of Things and Embedded Security	04	--	--	30	70	--	--	--	100	04	--	04
	Risk Assessment Laboratory	--	--	02	--	--	50	--	--	50	--	01	01
	Total	04	-	02	100		50	-	-	150	04	01	05
								Total	Credits =		05		
BE & VIII	Information Systems Management	04	-	--	30	70	--	--	--	100	04	--	04
	Seminar	--	02	--	--	--	-	--	50	50	02	--	02
	Total	04	-	02	100		-	--	50	150	06	-	06
								Total	**Credits =**		**06**		

Total Credit for Semester V+VI+VII+VIII = 20

*** <u>To be offered as Honours for Major Disciplines as–</u>**

1. Computer Engineering

2. Electronics and Telecommunication Engineering

3. Electronics Engineering

<u>For any other Major Disciplines which is not mentioned above, it may be offered as Minor Degree.</u>

Reference: https://www.aicte-india.org/sites/default/files/APH%202020_21.pdf / page 99-100

SavitribaiPhule Pune University
Honours* in Cyber Security
Third Year of Engineering (Semester V)
Information and Cyber Security

Teaching Scheme:	Credit:	Examination Scheme:
Theory: 04 Hours/Week	04	Mid_Semester(TH): 30 Marks End_Semester(TH): 70 Marks

Companion Course, if any: - Information and Cyber Security Laboratory

Course Objectives:

- To understand the basics of computer, network and information security.
- To study operating system security and malwares.
- To acquaint with security issues in internet protocols.
- To analyze the system for vulnerabilities.

Course Outcomes:

On completion of the course, learner will be able to–

- Use cryptographic techniques in secure application development.
- Apply methods for authentication, access control, intrusion detection and prevention.
- To apply the scientific method for security assessment
- To develop computer forensics awareness.

Course Contents

Unit I	Security Fundamentals	(06 Hours)

An Overview of Information Security: The Basic Components, Threats, Policy and Mechanism, Assumptions and Trust, Assurance, Operational Issues, Human Issues, Security nomenclature.
Access Control Matrix, Security Policies: Confidentiality, Integrity, Availability Policies and Hybrid Policies OS Security

Unit II	Modular Arithmetic and Cryptography Basics	(08 Hours)

Modular Arithmetic : Modular Arithmetic Notations, Modular Arithmetic Operations, Euclid's method of finding GCD, The extended Euclid's algorithm.
Cryptography : Classical encryption techniques, Block and Chain ciphers, Data Encryption Standard, Advanced Encryption Standard, RC5

Unit III	Advanced Cryptography	(08 Hours)

Chinese Remainder Theorem and its implication in Cryptography, Diffie-Hellman key exchange algorithm, RSA algorithm, Elgamal Arithmetic, Elliptic Curve Cryptography, Message Digest and Cryptographic Hash Functions, MD5 and SHA-1, Digital Signatures and Authentication.

Unit IV	Issues in Security Management and Cyber Laws	(08 Hours)

Overview, Risk identification, Risk Assessment, Risk Control Strategies, Quantitative vs. Qualitative Risk Control Practices. Risk Management. Laws and Ethics in Information Security, Codes of Ethics, Protecting programs and data
Cybercrime and Information security, Classification of Cybercrimes, The legal perspectives- Indian perspective, Global perspective, Categories of Cybercrime, Types of Attacks, a Social Engineering, Cyber stalking, Cloud Computing and Cybercrime.

Unit V	Key Management and Secure Communication	(08 Hours)

Public Key Infrastructure(PKI), X.509 Certificate, Needham Schroeder algorithm and Kerberos
IP Security: IPv6 and IPSec,
Web Security: SSL, HTTPS, Mail Security: PGP, S/MIME
Firewall : Different Types and Functionalities

Unit VI	Attacks, Malicious Logic and Countermeasures	(08 Hours)

Phishing, Password Cracking, Key-loggers and Spywares, Types of Virus, Worms, DoS and DDoS, SQL injection, Buffer Overflow, Spyware, Adware and Ransom ware. Antivirus and other security measures Intrusion Detection System: IDS fundamentals, Different types of IDS. Intrusion Prevention.

Learning Resources

Text Books:

1. William Stallings, "Computer Security: Principles and Practices", Pearson 6Ed, ISBN 978-0-13-335469-0
2. Nina Godbole, Sunit Belapure , "Cyber Security- Understanding Cyber Crimes", Computer Forensics and Legal Perspectives, Wiely India Pvt.Ltd, ISBN- 978-81-265-2179-1

Reference Books:

1. Bruice Schneier , "Applied Cryptography- Protocols, Algorithms and Source code in C", Algorithms, Wiely India Pvt Ltd, 2nd Edition, ISBN 978-81-265-1368-0.
3. CK Shyamala et el., "Cryptography and Security", Wiley India Pvt. Ltd, ISBN-978-81-265-2285-9.
4. Berouz Forouzan, "Cryptography and Network Security", TMH, 2 edition, ISBN -978-00-707-0208-0.
5. Mark Merkow, "Information Security-Principles and Practices", Pearson Ed., ISBN- 978-81-317-1288-7.

SavitribaiPhule Pune University
Honours* in Cyber Security
Third Year of Engineering (Semester V)
Information and Cyber Security Laboratory

Teaching Scheme	Credit Scheme	Examination Scheme and Marks
Practical:02 Hours/Week	01	Term work: 50 Marks

Guidelines for Laboratory Conduction

- **Lab Assignments:** Following is list of suggested laboratory assignments for reference. Laboratory Instructors may design suitable set of assignments for respective course at their level. Beyond curriculum assignments and mini-project may be included as a part of laboratory work. The instructor may set multiple sets of assignments and distribute among batches of students. It isappreciated if the assignments are based on real world problems/applications. The Inclusion of few optional assignments that are intricate and/or beyond the scope of curriculum will surely be the value addition for the students and it will satisfy the intellectuals within the group of the learners and will add to the perspective of the learners. For each laboratory assignment, it is essential for students to draw/write/generate flowchart, algorithm, test cases, mathematical model, Test data set and comparative/complexity analysis (as applicable). Batch size for practical and tutorial may be as per guidelines of authority.
- **Term Work–**Term work is continuous assessment that evaluates a student's progress throughout the semester. Term work assessment criteria specify the standards that must be met and the evidence that will be gathered to demonstrate the achievement of course outcomes. Categorical assessment criteria for the term work should establish unambiguous standards of achievement for each course outcome. They should describe what the learner is expected to perform in the laboratories or on the fields to show that the course outcomes have been achieved. It is recommended to conduct internal monthly practical examination as part of continuous assessment.
- **Assessment:**Students' work will be evaluated typically based on the criteria like attentiveness, proficiency in execution of the task, regularity, punctuality, use of referencing, accuracy of language, use of supporting evidence in drawing conclusions, quality of critical thinking and similar performance measuring criteria.
- **Laboratory Journal-** Program codes with sample output of all performed assignments are to be

submitted as softcopy. Use of DVD or similar media containing students programs maintained by Laboratory In-charge is highly encouraged. For reference one or two journals may be maintained with program prints in the Laboratory. As a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers as part of write-ups and program listing to journal may be avoided. Submission of journal/ term work in the form of softcopy is desirable and appreciated.

Suggested list of assignments
(Use suitable programming language/Tool for implementation)

Sr. No	Statement of Assignment
1	Implement Euclid's algorithm to find the GCD of two integers. Further implement extended Euclidean algorithm to find the multiplicative inverse of the given integer.
2	Develop the program to implement DES algorithm for encryption and decryption. Assume suitable key.
3	Develop the program to implement RSA algorithm for encryption and decryption. Assume suitable Private and Public Keys.
4	Write a program to implement SHA1 algorithm using libraries (API)
5	Configure and demonstrate use of vulnerability assessment tool like Wireshark or SNORT