Syllabus

Honours Programme in
Cyber Security & Forensics
(Offered by Department of Computer Engineering)

From
Academic Year 2021-22
Revision 1

(Approved in Academic Council meeting dated)

K J Somaiya College of Engineering, Mumbai-77
(A Constituent College of Somaiya Vidyavihar University)

Honours' Degree Programme in Cyber Security and Forensics

Offered by Department of Computer Engineering

Introduction:

Security is a critical issue in all the computing systems due to increasing number of security related breaches and incidents. The need of security professionals is ever increasing due to most of the services being made available online.

With the information sharing and processing going from centralized to distributed to the entire internet and due to inherent vulnerabilities and weaknesses of hardware, software and protocols there are constant risks and threats on compromising of data and information. This led to the need of Security in the form of controls, algorithms, procedures, policies and laws for securing information in the cyber space.

This programme will focus on basics of security starting security goals, vulnerabilities, threats & controls to advanced topics like blockchain, cyber forensics and cyber laws etc. There will be topics on applied cryptography, cyber security, forensics, secure coding and vulnerability assessment & penetrative testing.

Objectives: The offered programme aims to give the understanding of:

(1) Security goals, vulnerabilities, threats & controls.

(2) Implementation of various control mechanisms related to various security services.

(3) Understand cybercrime, its prevention and cyber laws.

(4) Carrying out the various information security-related tasks such as Penetration Testing and Vulnerability Analysis.

(5) Understand Digital forensics and Advanced Offensive Security techniques.

Learning Outcomes of the Honours' Degree Programme:

At the successful completion of this programme, an Engineering Graduate will be able to:

- Design and develop secure applications and systems.
- Classify the types of cybercrimes their prevention and applicability of various cyber laws.
- Implement penetration testing, vulnerability analysis and offensive security techniques for applications and systems.
- Apply and use various digital forensic tools for cybercrime investigation.

Assessment Methods: Evaluation will done by a variety of tools including Open book tests, MCQs (multiple choice questions), Study of research papers, Internal Assessment tools and End Semester Examinations etc. Mini-Projects are offered in courses also to encourage project based learning among students.

Acronyms used in syllabus document	
Acronym	**Definition**
CA	Continuous Assessment
ESE	End Semester Exam
IA	Internal Assessment
O	Oral
P	Practical
P&O	Practical and Oral
TH	Theory
TUT	Tutorial
TW	Term work
ISE	In-semester Examination
CO	Course Outcome

Acronyms used in Course code e.g. 116h55C301

Position of Digit	Acronym	Definition
1	**1**	First revision SUV KJSCE 2020
2	**16**	KJSCE
3	**h**	**Honour Degree Program**
4	**55**	**Cyber Security & Forensics**
5	**C**	Core Course
	L	Laboratory Course
	T	Tutorial
	P	Project Based Course
6	**1/2/3/4**	Semester Number
7	**01/02/03--**	Course Number

Credit Scheme

Course Code	Course Name	Teaching Scheme (Hrs.) TH – P – TUT	Total (Hrs.)	Credits Assigned TH – P – TUT	Total Credits	Suggested semester of Major degree
116h55C301	Applied Cryptography	3 – 0 – 0	03	3 –0 – 0	03	III
116h55L301	Applied Cryptography	0 – 2 – 0	02	0 –1 – 0	01	III
116h55C401	Cyber Security, Forensics and Cyber Law	3 – 0 – 0	03	3 – 0 – 0	03	IV
116h55C501	Block Chain Technology	3 – 0 – 0	03	3 –0 – 0	03	V
116h55L501	Block Chain Technology	0 – 2 – 0	02	0 –1 – 0	01	V
116h55C601	Vulnerability Assessment and Penetrative Testing	3 – 0 – 0	03	3 –0 – 0	03	VI
116h55L601	Vulnerability Assessment and Penetrative Testing	0 – 2 – 0	02	0 –1 – 0	01	VI
116h55C701	Secure Coding	3 – 0 – 0	03	3 – 0 – 0	03	VII
116h55P801	Applied Project / Internship	0 – 4 – 0	04	0 – 2 – 0	02	VII or VIII
	Total	15 – 10 – 0	25	15 – 5 – 0	20	

Examination Scheme

Course Code	Course Name	Examination Scheme							
		Marks							
		CA		ESE	TW	O*	P	P& O	Total
		ISE	IA						
116h55C301	Applied Cryptography	30	20	50	-	-	-	-	100
116h55L301	Applied Cryptography	-	-	-	25	25	-	-	50
116h55C401	Cyber Security, Forensics and Cyber Law	30	20	50	-	-	-	-	100
116h55C501	Block Chain Technology	30	20	50	-	-	-	-	100
116h55L501	Block Chain Technology	-	-	-	25	25	-	-	50
116h55C601	Vulnerability Assessment and Penetrative Testing	30	20	50	-	-	-	-	100
116h55L601	Vulnerability Assessment and Penetrative Testing	-	-	-	25	25	-	-	50
116h55C701	Secure Coding	30	20	50	-	-	-	-	100
116h55P801	Applied Project / Internship	-	-	-	50	50	-	-	100
Total		**150**	**100**	**250**	**125**	**125**			**750**

Course Code	Course Title							
116h55C301	Applied Cryptography							
	TH		P			TUT		Total
Teaching Scheme(Hrs.)	03		--			--		03
Credits Assigned	03		--			--		03
Examination Scheme	Marks							
	CA		ESE	TW	O	P	P&O	Total
	ISE	IA						
	30	20	50	--	--	--	--	100

Course prerequisites (if any):
Some mathematical maturity, in terms of understanding and working with mathematical definitions, concepts, and proofs, and elementary notions of logic, set theory, number theory, probability and statistics;

Course Objectives
In the era of Digital Computers and internet ensuring confidentiality, authentication, integrity of data during communication is very critical. This course impart students the knowledge of cryptographic algorithms and techniques to achieve same. It also introduces students to the advances in the area of cryptography

Course Outcomes
At the end of successful completion of the course the student will be able to

CO1	Explain fundamentals of Information Security and cryptography
CO2	Demonstrate various Cryptographic Algorithms for securing systems
CO3	Comprehend cryptographic hash functions, Message Authentication Codes and Digital Signatures for Authentication
CO4	Realize advances in the field of cryptography

Module No.	Unit No.	Details	Hrs.	CO
1	**Introduction to Information Security & Cryptography**		05	CO 1
	1.1	Information Security and its goals, Vulnerability Threats and Attacks		
	1.2	Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Cryptanalysis		
	1.3	Substitution Techniques, Transposition Techniques		
2	**Symmetric Key Cryptography**		09	CO2
	2.1	DES Structure, DES Analysis: Properties, Design Criteria, DES Weaknesses, DES Security, Multiple DES, 3DES		
	2.2	AES Structure, Key Expansion, Analysis of AES: Security, Implementation, Simplicity and Cost		
		IDEA, RC4		
		#Self Learning - RC5, Block Cipher Modes		
3	**Asymmetric Key Cryptography**		10	CO3
	3.1	Public key cryptography: Principles of public key cryptosystems, The RSA algorithm, attacks on RSA		
	3.2	Key management: Diffie Hellman Key exchange, Man-in Middle attack		
	3.3	Elliptic Curve Cryptography: Elliptic curves, The Addition Law, Elliptic curve Mod p, Factoring with Elliptic Curves, Elliptic Curve Cryptosystems		
		#Self Learning : Rabin Cryptosystem		
4	**Message Authentication and Digital Signatures**		11	CO3
	4.1	Message Authentication Approaches. Hash Function, Cryptographic Hash Function Requirements, Cryptographic Hash Function Security, Cryptographic Hash Function Structure, SHA, HMAC, MD5.		
	4.2	Using Symmetric Encryption for Message Authentication, Message Authentication Code (MAC), Digital Authentication Algorithm (DAA)		
	4.3	Using Public Key for Authentication, Digital Signatures, Properties of Digital Signatures beyond Message Authentication, DSS, Authentication Applications: Kerberos, X.509 Authentication Service		
		#Self Learning : RSA and Schnorr Digital Signature		
5	**Introduction to Advances in Cryptography**		10	CO4
	5.1	Quantum Cryptography, Quantum key distribution-QKD		
	5.2	Homomorphic Encryption		
	5.3	Secure Multi-Party Computation (MPC) In particular, Zero-Knowledge Proofs		
	5.4	Cryptographic Obfuscation		
		Total	45	

 # Students should prepare all Self Learning topics on their own. Self-learning topics will enable students to gain extended knowledge of the topic. Assessment of these topics may be included in IA and Laboratory Experiments.

Recommended Books:

Sr. No.	Name/s of Author/s	Title of Book	Name of Publisher with country	Edition and Year of Publication
1.	Behrouz A. Forouzan	Cryptography and Network Security	Mc Graw Hill	3rd Edition, 2017
2.	William Stallings	Computer Security Principles and Practice	Pearson Education	2016. 5th Edition
3.	Mark stamp	Information Security Principal and Practice	Wiley	2008, 3rd Edition
4.	Bruce Schneier	Applied Cryptography	Wiley	2015, Second Edition
5.	Jaydip Sen	Theory and practice of cryptography and network security protocols and technologies	Intech Publishers, Croatia, Europe	2013. First Edition
6.	Oded Goldreich	Foundations of Cryptography – A Primer	Foundations and Trends® in Theoretical Computer Science: Vol. 1: No. 1, pp 1-116	2005

<table>
<tr><th>Course Code</th><th colspan="8">Course Title</th></tr>
<tr><td>116h55L301</td><td colspan="8">Applied Cryptography</td></tr>
<tr><td></td><td colspan="3">TH</td><td colspan="2">P</td><td colspan="2">TUT</td><td>Total</td></tr>
<tr><td>Teaching Scheme(Hrs.)</td><td colspan="3">-</td><td colspan="2">02</td><td colspan="2">--</td><td>02</td></tr>
<tr><td>Credits Assigned</td><td colspan="3">-</td><td colspan="2">01</td><td colspan="2">--</td><td>01</td></tr>
<tr><td rowspan="3">Examination Scheme</td><td colspan="8">Marks</td></tr>
<tr><td colspan="2">CA</td><td rowspan="2">ESE</td><td rowspan="2">TW</td><td rowspan="2">O</td><td rowspan="2">P</td><td rowspan="2">P&O</td><td rowspan="2">Total</td></tr>
<tr><td>ISE</td><td>IA</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>25</td><td>25</td><td>--</td><td>--</td><td>50</td></tr>
</table>

Term-Work:

Term work will consist of experiments/ tutorials covering entire syllabus of the course ‘Applied Cryptography’. Students will be graded based on continuous assessment of their term work.

Course Code	Course Title						
116h55C401	Cyber Security, Forensics & Cyber Law						
	TH		P		TUT		Total
Teaching Scheme(Hrs.)	03		--		--		03
Credits Assigned	03		--		--		03
Examination Scheme	Marks						
	CA		ESE	TW	O	P	P&O	Total
	ISE	IA						
	30	20	50	--	--	--	--	100

Course prerequisites (if any): Computer Organization & Architecture, Cryptography & System Security, Computer Networks.

Course Objectives: The objective of the course is to enable students to understand the basic principles of information security, computer crimes and methods of defence. The course introduces the process of digital forensic investigation, extraction of evidence using appropriate tools. It covers the techniques of data hiding, recovery, disk analysis, volatile data extraction. Further, it explores different network based attacks, tools to monitor/mitigate such attacks. Tools such as metasploit, interfaces to dark web and deep web explore the conducive environment for attackers. Cyber laws, IT Acts enable the student to understand the legal aspects of various cyber-crimes.

Course Outcomes:
At the end of successful completion of the course the student will be able to:

CO1	Identify various security goals, computer crimes & methods of defence.
CO2	Understand the fundamentals of digital forensics.
CO3	Analyze and interprete the results of disk forensic operations.
CO4	Apply forensic tools to extract and investigate the evidences from network.
CO5	Relate the corresponding computer security acts with the crimes.

Module No.	Unit No.	Details	Hrs.	CO
1	**Introduction to Security Architecture**		03	CO
	1.1	Introduction to information security, security goals, security services, attacks & its types, security mechanism.		
	1.2	Introduction to cyber security, cyber crimes, its origins, classification of cyber crimes, cyberspace and cyber profiling.		
2	**Data Privacy and Theft**		10	CO
	2.1	Data theft - Adwares, malwares, ransomwares, trojans, spywares, keyloggers, phishing & its types, SQL injection attacks.		
		#Self Learning - Data privacy law in India.		
	2.2	Identity theft, its types, prevention techniques, software piracy.		
		#Self Learning – Case study on identity theft.		
	2.3	Data privacy, issues surrounding data privacy, guidelines for data privacy, data privacy vs data security, data privacy mechanisms, legislations on data privacy - local and global.		
		#Self Learning - GDPR Compliance		
3	**Digital Forensics Fundamentals**		10	CO
	3.1	Introduction, six A's of digital forensics, digital evidence, digital investigations, incident response, incident response methodology.		
	3.2	Classification of digital evidence - volatile and non-volatile, rules and guidelines for extraction of digital evidence, forensic duplicates, establishing chain of custody, admissibility of evidence in the court of law.		
		#Self Learning – CERT and its role in digital investigation.		
	3.3	Information retrieval and recovery, cloning techniques, password cracking, data recovery from file systems and mobile devices, forensics audit, tools for forensic investigation, anti-forensics.		
4	**Network Forensics**		12	CO
	4.1	Network based attacks – MITM, OWASP, ARP spoofing, IP and MAC spoofing, DNS attacks, SYN flooding attacks, port scanning, DOS, DDOS.		
	4.2	Sources of Digital Evidence from Emails, Web usage, Network Traffic, Email forensic and investigations.		
		Network Forensic Tools & Applications – Browser forensics, Nmap, Nessus, Wireshark, Metasploit, Kali-Linux, Deep-Web, Dark-Web.		
		#Self Learning : Criminal cases strongly based on digital evidences		

5	**Cyber Law**		**10**	**CO**
	5.1	Fundamentals of Cyber Law-Legislative, Judicial, Quasi-judicial, Investigative and International Cyber Law Framework.		
		#Self learning : Cyber crime cases studies- sample list but not limited to: Shreya Singhal v Union Of India, Syed Asifuddin v The State of Andhra Pradesh, Chambers v. Director of Public Prosecutions (UK), Riley v California (US), US v Ross William Ulbricht Carpenter v US, Packingham v North Carolina, Reno v ACLU, In Re: Nickelodeon Consumer Privacy Litigation, In Re: Google Inc. Cookie Placement Consumer Privacy Litigation, Memorandum of Decision - Google warrant case		
	5.2	Intellectual Property Issues & Cyberspace - Computer Software & Copyright Law, Software Licenses, Computer Databases & the Law, Domain Names & the Law, Trademark issues in Cyberspace and Semiconductor Layout & Design Law.		
	5.3	Cyber Crime Law in India- Cyber Frauds, Computer Source Code, Cyber Pornography, Cyber Terrorism, Data Privacy & confidentiality, Digital Signature, Freedom of speech, Information & Traffic Data, Intermediaries, Malware, Unauthorised Access and Violation of privacy.		
		#Self Learning- A Global Protocol on Cybersecurity and Cybercrime		
		Total	**45**	

 # Students should prepare all Self Learning topics on their own. Self-learning topics will enable students to gain extended knowledge of the topic. Assessment of these topics may be included in IA and Laboratory Experiments.

Recommended Books:

Sr. No.	Name/s of Author/s	Title of Book	Name of Publisher with country	Edition and Year of Publication
1.	Bill Nelson, Amelia Phillips, Christopher Steuart.	Guide to Computer Forensics and Investigations.	Cengage Learning, USA.	3rd Edition paperback, 2002.
2.	Jason T. Luttgens, Mathew Pepe, Kevin Mandia	Incident Response and Computer Forensics.	Tata McGraw Hill Education	3rd Edition, 2014.
3.	Marie-Helen Maras	Computer Forensics: Cybercriminals, Laws and Evidences	Jones and Bartlett Learning	2nd Edition, 2014
4.	Davidoff Ham	Network Forensics Tracking Hackers through Cyberspace	Pearson India	1st Edition, 2013.
5.	Adv. Prashant Mali	Cyber Law and Cyber Crimes Simplified	Cyber Infomedia	January 2017.
6.	Asian School of Cyber	https://www.asianlaws.org/		

Course Code	Course Title						
116h55C501	Block Chain Technology						
	TH		P	TUT			Total
Teaching Scheme(Hrs.)	03		--	--			03
Credits Assigned	03		--	--			03
Examination Scheme	Marks						
	CA		ESE	TW	O	P	P&O	Total
	ISE	IA						
	30	20	50	--	--	--	--	100

Course prerequisites (if any):
Networking Concepts, Object Oriented Programming Skills, Cryptography and Network Security Concepts.

Course Objectives
The objective of the Course is to explore the Bitcoin protocol followed by the Ethereum protocol – to lay the foundation necessary for developing applications and programming. Course will give the idea about the decentralized peer-to-peer network, an immutable distributed ledger and the trust model that defines a blockchain.
This course explains basic components of a blockchain (transaction, block, block header, and the chain) its operations (verification, validation, and consensus model) underlying algorithms, and essentials of trust (hard fork and soft fork).
.

Course Outcomes
At the end of successful completion of the course the student will be able to

CO1	Build your own Blockchain businesses with acquired knowledge
CO2	Learn Solidity language & Multiple Technology-based developments.
CO3	Apply the algorithm and techniques used in Blockchain.
CO4	Grasp the in-depth understanding of Blockchain, Smart Contracts & how it works.
CO5	Describe the methods of mining.

Module No.	Unit No.	Details	Hrs.	CO
1	**Blockchain Basics**		09	CO 1
	1.1	Introduction to Blockchain, what is Block? Registry of Transaction, Blockchain Structure, Basic Operations, Blockchain & Distributed Ledger Technology (DLT), Elements of Distributed Computing.		
	1.2	Elements of Cryptography, Elements of Game Theory, Cryptocurrencies, Tokens, and ICOs.		
	1.3	Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain.		
2	**Mining and Distributed Consensus**		12	CO 5
	2.1	Decentralized Consensus, Mining Node, The Coinbase Transaction, Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate		
	2.2	Mining the Block, Validating New Block, Blockchain Forks, and Mining Pool,Changing the consensus Rules, Hard Fork and Soft Fork,		
3	**Building Smart Contracts : Using Ethereum, Solidity**		10	CO 4
	3.1	Smart Contract Basics: Why Smart Contracts? Smart Contracts Defined, Processing Smart Contracts, Deploying Smart Contracts.		
	3.2	Solidity: Structure, Basic Data Types & Statements (Bidder Data & Functions Demos), Specific Data Types , Data Structures, Access Modifiers & Applications		
		#Self Learning – write your first Smart Contract?		
4	**Cryptocurrency and Cryptocurrency Regulation:**		7	CO 3
	4.1	History, Distributed Ledger, Bitcoin protocols - Mining strategy and rewards, Ethereum - Construction, DAO, Smart Contract, GHOST, Vulnerability, Attacks, Sidechain, Namecoin.		
	4.2	Stakeholders, Roots of Bit coin, Legal Aspects-Crypto currency Exchange, Black Market and Global Economy		
5	**Applications and Case studies**		8	CO 2
	5.1	Developing Smart Contracts, Time Elements, Validation & Test, Client Application. **#Self Learning – Limitations of Blockchain Technology.**		
	5.2	Case Studies: Government, Energy supply, Supply Chain, Insurance, Border Control, Waste Management, Shipping, Land Registry, HealthCare, Music, Real Estate, Fishing, Tourism, National Security etc….		
		Total	**45**	

 # Students should prepare all Self Learning topics on their own. Self-learning topics will enable students to gain extended knowledge of the topic. Assessment of these topics may be included in IA and Laboratory Experiments.

Recommended Books:

Sr. No.	Name/s of Author/s	Title of Book	Name of Publisher with country	Edition and Year of Publication
1.	*Andreas M. Antonopoulos*	*Mastering the Bitcoin: Programming the Open Blockchain*	O' Reilly	2nd Edition, 2017
2.	*Melanie Swan*	*BlockChian*	O'Reilly	2015
3.	*Nitin Gaur, Luc Desrosiers, Petr Novotny, Venkatraman Ramakrishna*	*Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer*	Packt	Kindle Edition, 2018
4.	Stephen Fleming business ecosystems	*Blockchain Technology: Introduction to Blockchain Technology and its impact on*	Stephen Fleming	2017
5.	Zeeshan-ul- hassan Usmani	*Introduction to lockchain with Case Studies*	Guhftgu Publication	2018

Course Code	Course Title							
116h55L501	Block Chain Technology							
	TH			P		TUT		Total
Teaching Scheme(Hrs.)	-			02		--		02
Credits Assigned	-			01		--		01
Examination Scheme	Marks							
	CA		ESE	TW	O	P	P&O	Total
	ISE	IA						
	-	-	-	25	25	--	--	50

Term-Work:

Term work will consist of experiments/ tutorials covering entire syllabus of the course 'Block Chain Technology'. Students will be graded based on continuous assessment of their term work.

Course Code	Course Title							
116h55C601	Vulnerability Analysis and Penetration Testing							
	TH			P		TUT		Total
Teaching Scheme(Hrs.)	03			--		--		03
Credits Assigned	03			--		--		03
Examination Scheme	Marks							
	CA		ESE	TW	O	P	P&O	Total
	ISE	IA						
	30	20	50	--	--	--	--	100

Course prerequisites (if any): Knowledge of Networking and System Programming

Course Objectives: The objective of this course is to impart knowledge about the principles and techniques associated with the information and cybersecurity practice known as penetration testing or ethical hacking. The topics covered in the course are the entire penetration testing process including planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting.

Course Outcomes:
At the end of successful completion of the course the student will be able to

CO1	Understand penetration testing with scope of its ethical implications, documentation and reporting.
CO2	Perform Penetration testing and vulnerability assessment on various systems.
CO3	Comprehend post exploitation phase of penetration testing.
CO4	Apply unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies.

Module No.	Unit No.	Details	Hrs.	CO
1	**Penetration Testing**		**04**	**CO**
	1.1	Introduction to Penetration testing, Ethics , Laws.		
	1.2	Types of Penetration Testing, Phases of Penetration Testing.		
	1.3	Setting up a Penetration Lab.		
2	**Collecting Information**		**12**	**CO**
	2.1	Reconnaissance Passive Information gathering with Foot printing Active Information Gathering Open Service Information Gathering		
	2.2	Network Scan Passive and active Network Scan, Port Scanning, ARP Spoofing, Network Traffic Scanning.		
		#Self Learning: NMAP Network Mapper tool		
3	**Identification of Vulnerability and Exploits**		**12**	**CO**
	3.1	Understanding Vulnerabilities		
	3.2	Buffer Overflow Exploitation		
	3.3	Fuzzing		
	3.4	Searching for Exploits		
	3.5	Privilege Escalation Exploits		
	3.6	System Hacking		
	3.7	Port Redirection and Tunneling		
		#Self Study : Tools viz. QualysGuard vulnerability management		
4	**Exploitation and Professional Reporting**		**9**	**CO**
	4.1	MITM and Session Hijacking		
	4.2	Shell Script Exploitation		
	4.3	Metasploit Framework Metasploit User Interfaces, Setting up Metasploit Framework, Exploring the Metasploit Framework		
	4.4	Preparing Report		
	4.5	Presenting Findings		
5	**Security Landscape, Red Team and Blue Team**		**8**	**CO**
	5.1	Incident Response Process		
	5.2	Red Team and Blue Team		
	5.3	Red Team Operations		
	5.4	Blue Team Defense		
		Total	**45**	

 # Students should prepare all Self Learning topics on their own. Self-learning topics will enable students to gain extended knowledge of the topic. Assessment of these topics may be included in IA and Laboratory Experiments.

Recommended Books:

Sr. No.	Name/s of Author/s	Title of Book	Name of Publisher with country	Edition and Year of Publication
1.	Joseph Muniz Aamir Lakhani	*Web Penetration Testing with Kali Linux*	Packt Publishing	2013
2.	George Kurtz, Joel Scambray, and Stuart McClure	*Hacking Exposed 7: Network Security Secrets and Solutions*	McGraw Hill	2012
3.	Sagar Rahalkar	*Network Vulnerability Assessment*	Packt Publishing	2018
4.	Micah Zenko	*Red Team How to Succeed By Thinking Like The Enemy*	Basic Books	2015
5.	Don Murdoch Gse	*Blue Team Handbook: A Condensed Field Guide for the Cyber Security Incident Responder*	Createspace Independent Publishing Platform	2014

Course Code	Course Title							
116h55L601	Vulnerability Analysis and Penetration Testing							
	TH			P		TUT		Total
Teaching Scheme(Hrs.)	-			02		--		02
Credits Assigned	-			01		--		01
Examination Scheme	Marks							
	CA		ESE	TW	O	P	P&O	Total
	ISE	IA						
	-	-	-	25	25	--	--	50

Term-Work:

Term work will consist of experiments/ tutorials covering entire syllabus of the course 'Vulnerability Analysis and Penetration Testing'. Students will be graded based on continuous assessment of their term work.

Course Code	Course Title							
116h55C701	Secure Coding							
	TH			P		TUT		Total
Teaching Scheme(Hrs.)	03			--		--		03
Credits Assigned	03			--		--		03
Examination Scheme	Marks							
	CA		ESE	TW	O	P	P&O	Total
	ISE	IA						
	30	20	50	--	--	--	--	100

Course prerequisites (if any): Knowledge of programming languages

Course Objectives:
Understanding the Application Security, Threats and attacks. Learning the security coding practices, and architecture.

Course Outcomes:
At the end of successful completion of the course the student will be able to

CO1	Incorporate S-SDLC
CO2	Fix software security bugs using secure coding techniques
CO3	Use appropriate techniques and tools to analyze and test software applications for weaknesses and vulnerabilities
CO4	Implement secure coding practices for cryptography
CO5	Design and implement software applications using secure architecture

Module No.	Unit No.	Details	Hrs.	CO
1	**Introduction**		**8**	**CO**
	1.1	Understanding secure SDLC model, Methodologies for developing secure code: Risk analysis, threat modeling, and guidelines for secure coding practice. SAST (Static application security testing tools) Web application security, Mobile Application security.		
2	**Secure programming techniques**		**14**	**CO**
	2.1	Worms and Other Malware, Buffer Overflows, Client-State Manipulation		
	2.2	SQL Injection, Password Security		
		#Self Learning secure coding practices for c, c++, java and php		
3	Cross-Domain Security in Web Applications.		**8**	**CO**
	3.1	Interaction Between Web Pages from Different Domains, Introduction to session management in web applications, secure coding practices for error handling		
	3.2	Attack patterns, preventing XSRF attack, preventing XSSI		
4	**Secure coding practices for Cryptography**		**5**	**CO**
	4.1	Introduction to cryptography and guidelines for using encryption		
	4.2	Symmetric cryptography, Asymmetric cryptography, Hashing algorithms, verification test		
5	**Secure architecture concepts and Principles and secure designing**		**10**	**CO**
	5.1	What is security architecture?		
	5.2	Principles of security architecture, case study: Java sandbox		
	5.3	Secure design steps		
	5.4	Secure deployment and maintenance		
		Total	**45**	

 # Students should prepare all Self Learning topics on their own. Self-learning topics will enable students to gain extended knowledge of the topic. Assessment of these topics may be included in IA and Laboratory Experiments.

Recommended Books:

Sr. No.	Name/s of Author/s	Title of Book	Name of Publisher with country	Edition and Year of Publication
1.	Robert seacord	Secure coding in C c++	Pearson	Second Edition
2.	Micheal Howard, David LeBlanc	Writing secure code		Second edition
3.	Neil Daswani, Christoph Kern, and Anita Kesavan.	Foundations of Security		2007,First Edition

Course Code	Course Title								
116h55P801	Applied Project / Internship								
	TH			P		TUT		Total	
Teaching Scheme (Hrs./Week)	-			04		-		04	
Credits Assigned	-			02		-		02	
Examination Scheme	Marks								
	CA			ESE	TW	O	P	P&O	Total
	ISE		IA						
	-	-	-	-	50	50	-	-	100

Course prerequisites: Conceptual knowledge of Cyber Security & Forensics

Course Objectives: The objectives are to address a real-world problem, which includes identify and solve the problem by implementing the solution using the courses learned in earlier semesters. Recognize various hardware and software requirements for solving the problem. It will also inculcate qualities such as working in team, meeting deadlines, making and following work plan. The Project may include some software or techniques not covered in the courses taught to provide solution of the chosen problem.

Course Outcomes:
At the end of successful completion of the course the student will be able to

CO1	Define the problem statement and scope of problem.
CO2	Identify various hardware and software requirements for problem solution
CO3	Describe the design with the help of flowchart/block diagrams or any design Tool.
CO4	Implement and test the design to meet the desired specifications.
CO5	Analyze, interpret results and correspondingly modify the designed system to get the desired results.
CO6	Prepare a technical report and technical paper based on the project.

Term Work and Oral : This is an activity to be undertaken by the group of 2 or 3 students. Each group will be assigned one faculty member as a supervisor. There will be continuous assessment of the project and progress report of the project needs to be maintained by students. The final oral will be a presentation based on a demonstration of the project in front of a committee of examiners. Students are expected to publish technical paper based on the project.