YESHWANTRAO CHAVAN COLLEGE OF ENGINEERING
(An Autonomous Institution affiliated to R T M Nagpur University Nagpur)
Accredited by NAAC (1st Cycle) with 'A' Grade (Score 3.25 on 4 Point Scale)

Wanadongri, Hingna Road, Nagpur-441110

Department of Information Technology
(Honors in CS)

B.E. Honors in Cyber Security
SoE & Syllabus 2021-22

B.E. Honor in Cyber Security

Information Brochure of Honor / Minor Program

1. Title of Program: **Honors in Cyber Security**
2. Type of Program : **Honor**
3. Department offering the program**: Information Technology**
4. Industry Association; **Crypto Forensic**

   https://www.cryptoforensic.in/.
5. Department/s eligible to opt for the program: **Students of Department of Information Technology are only eligible to opt for this program.**

6. General information about courses in program:

   In regard to the changing trends and demands in cyberspace, cyber security will continue to grow as obligatory technologies as the world becomes digitally connected. This program of B.E. Honor in Cyber Security- is intended to mould students into well prepared cyber security professionals and has been designed with a good balance between theoretical & practical aspects, analytical and architectural methods complemented by academic research and industry best practices. The curriculum is specially prepared by experts covering all the needs and aspects a cyber security engineer needs. Through this program, the students will learn and acquire the necessary theoretical background with concept clarity and insights into hands-on technical aspects of cyber security, a good understanding of analytical methods and industry practices in the field. They cultivate an proficiency into the growing threats and vulnerabilities in cyber era.

7. Advance knowledge or research orientation of Program:

   The program will deliver an opportunity for the students to acquire the needed soft skills, technical skills, implementation applied cyber security skills and also IT management skills. It serves as a hybrid blend of cyber perception and industrial practice. In near future, the number of unfilled cyber security jobs is expected to grow by 350 percent (source: MIT Technology Review) creating massive skills gap over copious cyber security industries in India and abroad, Antivirus companies, Banking/Finance/Insurance sectors, IT companies and government (defense and non-defense) organizations need security analyst to protect their digital assets as not surprisingly, they all deal with sensitive information, which is commonly targeted by attackers.

8. Employability potential of program:

The program is designed specially keeping in mind the demand and skill requirement for coming decade for satisfying the 3.5 million unfilled cyber security jobs globally by 2025 (Source: NY Times). Opportunities for our graduates are easy to fit into the core job roles of Cyber Security Analyst, Security Engineer, Security Architect, Security Administrator, Security Software Developer, Cryptanalyst, Digital Forensic Analyst, Vulnerability Assessor, Cloud Security Architect, Intrusion Detection Specialist, Cybercrime Investigator, Malware Analyst, Data Privacy Officer, Computer Security Incident Responder, Governance Compliance & Risk (GRC) Manager and Security Consultant. There is a wide range of placements for these cyber security job roles program and some includes and not limited to: ABB Corp, Cisco, IBM, VMware, EY, Paladion Networks, Bosch, Nokia, Philips, Amazon, IndusFace, Deloitte, SBI-Infosec Wing, Symantec, CloudByte and so on. There is wide range of opportunities available in India and abroad for Cyber Security Research.

9. Departmental Steering committee:

SN	Name of the Faculty Member	Post	Designation	e-mail ID	Contact Number
1.	Dr. R. C. Dharmik	HOD, IT & Chairman	Asstt. Prof.	raj_dharmik@yahoo.com	9158003335
2.	Dr. K. K. Bhoyar	Member	Professor	kkbhoyar@yahoo.com	9764996487
3.	Prof. S.W. Shende	Member	Asso. Prof.	Shailendra.shende@gmail.com	9766698600
4.	Prof. R.A. Fadnavis	Member	Asst.prof	rafatycce@gmail.com	9923465898
5.	Prof. A.D. Gaikwad	Member	Asst.prof	amolgaikwad.ag@gmail.com	9970743434

10. Program Coordinator:

SN	Name of the Faculty Member	Post	Designation	e-mail ID	Contact Number
1	Prof. A.D. Gaikwad	Program Coordinator	Asst.prof	amolgaikwad.ag@gmail.com	9970743434

Scheme of Examinations
Honors in Cyber Security (Industry Associated-Crypto Forensic)

SN	Sem	Sub. Code	Course Name	T/P	L	P	Hrs	Credits	MSEs	TA	ESE	ESE-Hr
1	V	ITH141	Introduction to Cyber Security	**T**	3	0	3	3	30	30	40	3
2	V	ITH142	Introduction to Cyber Security Lab.	**P**	0	2	2	1		60	40	3
3	VI	ITH151	Cryptrography and Network Security	**T**	3	0	3	3	30	30	40	3
4	VI	ITH152	Cryptrography and Network Security Lab.	**P**	0	2	2	1		60	40	
5	VII	ITH161	Ethical Hacking	**T**	3	0	3	3	30	30	40	3
6	VIII	ITH171	Cyber Crime Invenstigation and Digital Forensics	**T**	3	0	3	3	30	30	40	3
7	VIII	ITH172	Introduction to Blockchain Technology	**T**	3	0	3	3	30	30	40	3
8	VIII	ITH173	Introduction to Blockchain Technology Lab.	**P**	0	2	2	1		60	40	
Total					**15**	**6**	**21**	**18**				

MSEs* = Three MSEs of 15 Marks each will conducted and marks of better 2 of these 3 MSEs will be considered for Continuous Assessment

TA ** = for Theory : 20 marks on lecture quizzes, 8 marks on assignments, 2 marks on class performance
TA = for Practical : MSPA will be 15 marks each**

V Semester

ITH141	**Introduction to Cyber Security**			L= 3	T = 0	P = 0	Credits = 3
Evaluation Scheme *Best Two out of three MSE's would be considered	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
	15	15	15	30	40	100	3 Hrs
Prerequisites							

Course Objective

Students should be able to

To Create cyber security awareness and to understand principles of web security

- To understand key terms and concepts in cyber law, intellectual property and cyber crimes, trademarks and domain theft.
- To make attentive to students about possible hacking and threats in this communication era.
- Discuss Issues for creating Security Policy for a Large Organization.

Course Outcome

Students will be able to

- Students will be able to acknowledge about the cybercrime, cyber criminal, and intellectual property rights.
- Encouraging Open Standards.
- Protection and resilience of Critical Information Infrastructure.
- To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

UNIT I : Cyber **Security Fundamentals** [06 Hrs.]

Security Concepts: Authentication, Authorization, Non-repudiation, Confidentiality, Integrity, availability. Cyber Crimes and Criminals: Definition of cyber-crime, types of cyber-crimes and types of cyber-criminals.

UNIT II : Cyber attacker Techniques and Motivations

Anti-forensics: Use of proxies, use of tunneling techniques. Fraud techniques: Phishing and malicious mobile code,Rogue antivirus, Click fraud. Threat Infrastructure: Botnets, Fast Flux and advanced fast flux.

UNIT III : Exploitation

Techniques to gain foothold: Shell code, Buffer overflows, SQL Injection, Race Conditions, DoS Conditions, Brute force and dictionary attacks. Misdirection, Reconnaissance, and Disruption. Methods: Cross-Site Scripting (XSS), Social Engineering, WarXing, DNS Amplification Attacks.

UNIT IV : Information Technology Act 2000

Overview of IT Act 2000, Amendments and Limitations of IT Act, Electronic Governance, Legal Recognition of Electronic Records, Legal Recognition of Digital Signature, Certifying Authorities, Cyber Crime and Offenses, Network Service Providers Liability, Cyber Regulations Appellate Tribunal, Penalties and Adjudication

UNIT V: Firewall And Intrusion

Introduction, Computer Intrusions. Firewall Introduction, Characteristics and types, Benefits and limitations. Firewall architecture, Trusted Systems, Access Control. Intrusion detection, IDS: Need, Methods, Types of IDS, Password Management, Limitations and Challenges.

UNIT VI: Cyber Law and Related Legislation

Patent Law, Trademark Law, Copyright, Software Copyright or Patented, Domain Names and Copyright disputes, Electronic Data Base and its Protection, IT Act and Civil Procedure Code, IT Act and Criminal Procedural Code, Relevant Sections of Indian Evidence Act, Relevant Sections of Bankers Book Evidence Act, Relevant Sections of Indian Penal Code, Relevant Sections of Reserve Bank of India Act, Law Relating To Employees And Internet, Alternative Dispute Resolution, Online Dispute Resolution (ODR).

Text Books:

	Title	Edition	Author	Publisher
1	Cyber Security Essentials,	**1st**	James Graham (Editor), Ryan Olson (Editor), Rick Howard (Editor)	**Auerbach Publications**
2	Cyber Laws: Intellectual property & E Commerce Security,	**1st**	Krishna Kumar.	**Dominant Publishers & Distributors**
3	"Network Security and Cryptography"	2014	Bernard Menezes	Cengage Learning India, 2014, ISBN No.: 8131513491
4	"Cyber Security"	2014	Nina Godbole, Sunit Belapure	Wiley India, 2014, ISBN No.: 978-81- 345-2179-1

Reference Book:

	Title	Edition	Author	Publisher
1	Cyber Law Text & Cases, ,	**1st**	Gerald R. Ferrera, Margo E. K. Reder	CENGAGE LEARNING Publication.
2	Ethics in Information Technology,	**1st**	George W. Reynolds,	CENGAGE LEARNING Publication

V Semester

ITH142	**Introduction to Cyber Security Lab.**			L= 0	T = 0	P = 1	Credits = 1
Evaluation Scheme *Best Two out of three MSE's would be considered	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
	--	--	--	60	40	100	3 Hrs
Prerequisites							

Course Objective	**Course Outcome**
Students should be able to To make attentive to students about possible hacking and threats in this communication era.	Students will be able to To enable effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

1. Implement the following SUBSTITUTION & TRANSPOSITION TECHNIQUES concepts:
   a) Caesar Cipher
   b) Playfair Cipher

2. Implement the following algorithms
   a) DES
   b) RSA Algorithm

3. Implement the Signature Scheme - Digital Signature Standard

4. Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG).

5. Study of steps to protect your personal computer system by creating User Accounts with Passwords and types of User Accounts for safety and security.

6. Study the steps to protect a Microsoft Word Document of different version with different operating system.

7. Study the steps to remove Passwords from Microsoft Word

8. Study various methods of protecting and securing databases.

9. Study "How to make strong passwords" and "passwords cracking techniques".

10 Study the steps to hack a strong password.

VI Semester

ITH151	**Cryptography and Network Security**			L= 3	T = 0	P = 0	Credits = 3
Evaluation Scheme *Best Two out of three MSE's would be considered	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
	15	15	15	30	40	100	3 Hrs
Prerequisites							

Course Objective
Students should be able to

1. To understand basics of Cryptography and network Security.
2. To be able to secure a message over insecure channel by various means.
3. To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
4. To understand various protocols for network security to protect against the threats in the networks.

Course Outcome
Students will be able to

1. Provide security of the data over the network.
2. Do research in the emerging areas of cryptography and network security.
3. Implement various networking protocols.
4. Protect any network from the threats

UNIT I : **[06 Hrs.]**
An overview of computer security ,Goals of information security, confidentiality, integrity, Availability, Security policies: Types of access control, Basic cryptography, OSI security architecture , Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.

UNIT II :
Authentication: Authentication basics, Passwords, Key management , Diffie Hellman key exchange , Elliptic curve architecture and cryptography , Introduction to number theory , Confidentiality using symmetric encryption , Public key cryptography and RSA.

UNIT III :
Authentication: Authentication basics, Passwords, Key management , Diffie Hellman key exchange , Elliptic curve architecture and cryptography , Introduction to number theory , Confidentiality using symmetric encryption , Public key cryptography and RSA.

UNIT IV : Basics of Cryptography Symmetric Cipher Model, Substitution Techniques, Transportation Techniques, Other Cipher Properties Confusion, Diffusion, Block and Stream Ciphers.
UNIT V: SQL injection and cross-site scripting, symmetric encryption, SSL and TLS, PKI,and Certificate Systems, Passwords and Secure Cookies, IPsec, Ingress filtering, and Firewalls, Digital signatures, Digital Signature Schemes, Authentication Protocols, Digital Signature Standards, files and devices, Program security,
UNIT VI: Intrusion Detection ,Firewalls and proxy, Image Security-Biometrics, Web Security: Web Security Considerations, Secure Sockets Layer and Transport Layer ,Security, Electronic Payment Combining security Associations, Internet Key Exchange, Virus and worms

Text Books:				
	Title	**Edition**	**Author**	**Publisher**
1	Introduction to Computer Security	**1st**	Matt Bishop	Addison-Wesley
2	Cryptography and Network Security	**1st**	Atul Kahate	**McGraw Hill Education**
Reference Book:				
	Title	**Edition**	**Author**	**Publisher**
1	Cryptography and Network Security: Principles and Practice	4th	William Stallings	**Pearson**
2	Network Security Essentials: Applications and Standards	1st	William Stallings	Pearson

VI Semester

ITH152	**Cryptrography and Network Security Lab.**			L= 0	T = 0	P = 1	Credits = 1
Evaluation Scheme	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
*Best Two out of three MSE's would be considered	--	--	--	60	40	100	3 Hrs
Prerequisites							

Course Objective	**Course Outcome**
Students should be able to To understand various protocols for network security to protect against the threats in the networks.	Students will be able to Protect any network from the threats

1. Learn to install wine / virtual box or any other equivalent Software on the host os.
2. Perform an experiment to grab a banner with telnet and perform The task using netcat utility
3. Perform an experiment for port scanning with nmap, superscan Or any other software
4. Using nmap
   a) find open ports on a system
   b) find the machines Which are active
   c) find the version of remote os on other systems
   d) find the version of s/w installed on other system
5. Perform an experiment on active and passive finger Printing using xprobe2 and nmap.
6. Performa an experiment to demonstrate how to sniff for router Traffic by using the tool wireshark.
7. Perform an experiment how to use dumpsec.
8. Perform an wireless audit of an access point / router and Decrypt wep and wpa.
9. Perform an experiment to sniff traffic using arp poisoning.
10. Install jcrypt tool (or any other equivalent) and demonstrate Asymmetric, symmetric crypto algorithm, hash and digital/pki Signatures

Text Books:				
	Title	**Edition**	**Author**	**Publisher**
1	Introduction to Computer Security	**1st**	Matt Bishop	Addison-Wesley
2	Cryptography and Network Security	**1st**	Atul Kahate	**McGraw Hill Education**
Reference Book:				
	Title	**Edition**	**Author**	**Publisher**
1	Cryptography and Network Security: Principles and Practice	4th	William Stallings	**Pearson**
2	Network Security Essentials: Applications and Standards	1st	William Stallings	Pearson

VII Semester

ITH161	Ethical Hacking			L= 3	T = 0	P = 0	Credits = 3
Evaluation Scheme	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
*Best Two out of three MSE's would be considered	15	15	15	30	40	100	3 Hrs
Prerequisites							

Course Objective

Students should be able to

1. Understanding the basics of networking with the introduction on the system attacks
2. Describes attacks in terms of industry, society and information systems
3. Describes various types of securities and vulnerabilities
4. Demonstration of the ethical hacking tools

Course Outcome

Students will be able to

1. Explain basics of networking with the introduction on the system attacks
2. Explain attacks in terms of industry, society and information systems
3. Elaborate various types of securities and vulnerabilities
4. Demonstrate various ethical hacking tools

UNIT I :

Ethical Hacking: Introduction, Networking & Basics, Foot Printing, Google Hacking, Scanning, Windows Hacking, Linux Hacking, Trojans & Backdoors, Virus & Worms, Proxy & Packet Filtering, Denial of Service, Sniffer, Social Engineering

UNIT II :

Introduction to Computer Systems and Networks , information systems and networks (including wireless networks) and their role in industry business and society, System and Network Vulnerability and Threats to Security , various types of attack and the various types of attackers in the context of the vulnerabilities associated with computer and information systems and networks

UNIT III :

Physical Security, Steganography, Cryptography, Wireless Hacking, Firewall & Honeypots,IDS & IPS, Vulnerability, Penetration Testing, Session Hijacking, Hacking Web Servers,SQL Injection, Cross Site Scripting, Exploit Writing, Buffer Overflow, Reverse Engineering, Email Hacking, Incident Handling & Response, Bluetooth Hacking, Mobile Phone Hacking

UNIT IV : An introduction to the particular legal, professional and ethical issues likely to face the domain of ethical hacking. Ethical responsibilities, professional integrity and making appropriate use of the tools and techniques associated with ethical hacking.
UNIT V: Understanding the password hacking techniques-Rootkits-Trojans-Backdoors-Viruses and wormssniffers-denial of service-Session hijacking.
UNIT VI: CASE STUDY Latest Study Topics on Cyber Crime and Investigations - Recent Cyber Crime Cases –Recent Digital Forensics Cases – Bridging the Gaps in Cyber Crime Investigations between the cyber security stake holders

Text Books:

	Title	Edition	Author	Publisher
1	Hands-On Ethical Hacking and Network Defense	Second	James Corley (Author), Kent Backman (Author), Michael Simpson (Author)	**Delmar Cengage Learning**
2	Official Certified Ethical Hacker Review Guide –	**1st**	By Steven DeFino, Barry Kaufman, Nick Valenteen.	**Delmar Cengage Learning**

Reference Book:

	Title	Edition	Author	Publisher
1	The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy	first	Patrick Engebretson	**Syngress**

VIII Semester

ITH171	Cyber Crime Investigation and Digital Forensics			L= 3	T = 0	P = 0	Credits = 3
Evaluation Scheme	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
*Best Two out of three MSE's would be considered	15	15	15	30	40	100	3 Hrs
Prerequisites							

Course Objective

Students should be able to

1. To understand underlying principles and many of the techniques associated with the digital forensic practices and cyber crime
2. To explore practical knowledge about ethical hacking Methodology.
3. To learn the importance of evidence handling and storage for various devices
4. To develop an excellent understanding of current cyber security issues (Computer Security Incident) and analyzed the ways that exploits in securities.

Course Outcome

Students will be able to

1. Define the concept of ethical hacking and its associated applications in Information Communication Technology (ICT) world.
2. Underline the need of digital forensic and role of digital evidences .
3. Explain the methodology of incident response and various security issues in ICT world, and identify digital forensic tools for data collection .
4. Recognize the importance of digital forensic duplication and various tools for analysis to achieve adequate perspectives of digital forensic investigation in various applications /devices like Windows/Unix system.

UNIT I :

Introduction of Cybercrime: Types of cybercrime ,categories of cybercrime , Computers' roles in crimes, Prevention from Cyber crime, Hackers, Crackers, Phreakers Ethical Hacking :Difference between Hacking and Ethical hacking : Steps of Ethical Hacking, Exploring some tools for ethical hacking: reconnaisance tools, scanning tools

UNIT II :

Digital Forensic ,Rules for Digital Forensic The Need for Digital Forensics, Types of Digital Forensics, Ethics in Digital Forensics, Digital Evidences : Types and characteristics and challenges for Evidence Handling

UNIT III :

Introduction to Computer Security Incident Goals of Incident response, Incident Response Methodology, Formulating Response Strategy, IR Process – Initial Response, Investigation, Remediation, Tracking of Significant, Investigative Information, Reporting Pre Incident Preparation, Incident Detection and Characterization. Live Data Collection : Live Data Collection on Microsoft Windows Systems: Live Data, Collection on Unix-Based Systems

UNIT IV :

Forensic Duplication Forensic Image Formats, Traditional Duplication, Live System Duplication, Forensic Duplication tools Disk and File System Analysis: Media Analysis Concepts, File System Abstraction Model The Sleuth Kit : Installing the Sleuth Kit , Sleuth Kit Tools Partitioning and Disk Layouts : Partition Identification and Recovery, Redundant Array of Inexpensive Disks Special Containers : Virtual Machine Disk Images , Forensic Containers Hashing, Carving : Foremost , Forensic Imaging : Deleted Data , File Slack , dd , dcfldd , dc3dd Data Analysis Analysis Methodology Investigating Windows systems , Investigating UNIX systems , Investigating Applications, Web Browsers, Email, Malware Handling: Static and Dynamic Analysis

UNIT V:

Network Forensics: Technical Exploits and Password Cracking , Introduction to Intrusion Detection systems, Types of IDS Understanding Network intrusion and attacks , Analyzing Network Traffic, Collecting Network based evidence, Evidence Handling. Investigating Routers, Handling Router Table Manipulation Incidents, Using Routers as Response Tools.

UNIT VI:

Forensic Investigation :Goals of Report, Layout of an Forensic Investigation VI University of Mumbai, B. E. (Information Technology), Rev 2016 162 CO6 7 Investigative Report, Guidelines for Writing a Report, sample for writing a forensic report . Computer Forensic Tools : need and types of computer forensic tools, task performed by computer forensic tools . Study of open source Tools like SFIT, Autopsy etc. to acquire, search, analyze and store digital evidence

Text Books:

	Title	Edition	Author	Publisher
1	"Incident Response and computer forensics",	3rd Edition Tata	Jason Luttgens, Matthew Pepe, Kevin Mandia,	McGraw Hill, 2014
2	"Digital Forensic : The fascinating world of Digital Evidences "	first	Nilakshi Jain, Dhananjay Kalbande,	Wiley India Pvt Ltd 2017.
3	"Digital forensics with open source tools "	first	Cory Altheide, Harlan Carvey	Syngress Publishing,Inc. 2011

Reference Book:				
	Title	**Edition**	**Author**	**Publisher**
1	"Digital Forensics for Network, Internet, and Cloud Computing A forensic evidence guide for moving targets and data ,	1st	Clint P Garrison	Syngress Publishing, Inc. 2010
2	Guide to Computer Forensics and Investigations" .	1st	Bill Nelson,Amelia Phillips,Christopher Steuart, "	Cengage Learning, 2014

VIII Semester

ITH172	**Introduction to Blockchain Technology**			L= 3	T = 0	P = 0	Credits = 3
Evaluation Scheme	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
*Best Two out of three MSE's would be considered	15	15	15	30	40	100	3 Hrs
Prerequisites							

Course Objective

Students should be able to

1. Understand how blockchain systems (mainly Bitcoin and Ethereum) work,
2. To securely interact with them,
3. Design, build, and deploy smart contracts and distributed applications
4. Integrate ideas from blockchain technology into their own projects.

Course Outcome

Students will be able to

1. Explain design principles of Bitcoin and Ethereum.
2. Explain Nakamoto consensus.
3. Explain the Simplified Payment Verification protocol.
4. List and describe differences between proof-of-work and proof-of-stake consensus.

UNIT I : Basics:

Distributed Database, Two General Problem, Byzantine General problem and FaultTolerance, Hadoop Distributed File System, Distributed Hash Table, ASIC resistance, Turing Complete. Cryptography: Hash function, Digital Signature - ECDSA, Memory Hard Algorithm, Zero Knowledge Proof.

UNIT II : Blockchain:

Introduction, Advantage over conventional distributed database, Blockchain Network,Mining Mechanism, Distributed Consensus, Merkle Patricia Tree, Gas Limit, Transactions and Fee, Anonymity, Reward, Chain Policy, Life of Blockchain application, Soft & Hard Fork, Private and Public blockchain.

UNIT III : : Distributed Consensus: [07Hrs.]

Nakamoto consensus, Proof of Work, Proof of Stake, Proof of Burn, Difficulty Level, Sybil Attack, Energy utilization and alternate .

UNIT IV : **Cryptocurrency**: [07Hrs.]

History, Distributed Ledger, Bitcoin protocols - Mining strategy and rewards, Ethereum - Construction, DAO, Smart Contract, GHOST, Vulnerability, Attacks, Sidechain, Namecoin **.**

		May 2021	1.00	Applicable for AY2021-22 Onwards
Chairperson	Dean (Acad. Matters)	Date of Release	Version	

UNIT V:

Cryptocurrency Regulation: Stakeholders, Roots of Bit coin, Legal Aspects-Crypto currency Exchange, Black Market and Global Economy.

UNIT VI:

Applications: Internet of Things, Medical Record Management System,Domain Name Service and future of Blockchain.

Text Books:

	Title	Edition	Author	Publisher
1	Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction	1st 19 July 2016	Arvind Narayanan (Author), Joseph Bonneau (Author), Edward Felten (Author),,	**Princeton University Press**
2	Mastering Bitcoin: Unlocking Digital Cryptocurrencies	1st Edition	Andreas M. Antonopoulos	**Syngress**

Reference Book:

	Title	Edition	Author	Publisher
1	Advanced Blockchain Development: Build highly secure, decentralized applications and conduct secure transactions	1st	Imran Bashir (Author), Narayan Prusty (Author)	**Packt Publishing**

VIII Semester

ITH173	Lab :Introduction to Blockchain Technology			L= 0	T = 0	P = 2	Credits = 1
Evaluation Scheme	MSE-I*	MSE-II*	MSE-III*	TA	ESE	Total	ESE Duration
*Best Two out of three MSE's would be considered	--	--	--	60	40	100	3 Hrs
Prerequisites							

Course Objective	**Course Outcome**
Students should be able to 1. Design, build, and deploy smart contracts and distributed applications.	Students will be able to 1.Explain design principles of Bitcoin and Ethereum

Practical List

1. Create a Simple Blockchain in any suitable programming language.
2. Use Geth to Implement Private Ethereum Block Chain.
3. Build Hyperledger Fabric Client Application.
4. Build Hyperledger Fabric with Smart Contract.
5. Create Case study of Block Chain being used in illegal activities in real world.
6. Using Python Libraries to develop Block Chain Application.

Text Books:

	Title	Edition	Author	Publisher
1	Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction	1st 19 July 2016	Arvind Narayanan (Author), Joseph Bonneau (Author), Edward Felten (Author),,	**Princeton University Press**
2	Mastering Bitcoin: Unlocking Digital Cryptocurrencies	1st Edition	Andreas M. Antonopoulos	**Syngress**

Reference Book:

	Title	Edition	Author	Publisher
1	Advanced Blockchain Development: Build highly secure, decentralized applications and conduct secure transactions	1st	Imran Bashir (Author), Narayan Prusty (Author)	**Packt Publishing**

		May 2021	1.00	Applicable for AY2021-22 Onwards
Chairperson	Dean (Acad. Matters)	Date of Release	Version	