VIT Vidyalankar Institute of Technology
Accredited A+ by NAAC

Version 05/22-8

Consolidated Academic Administration Plan for the Course

Cryptography and System Security (Core) Sem. VI– Program Computer Engineering 2023-2024 –Even Semester
Faculty - Prof.Amit K.Nerurkar, Prof. Amit Ayalani (Cluster Mentor) & Dr Dilip Motwani

The academic resources available in VIT –

VMIS (ERP)	V-Refer and V-Live	VIT Library	VAC & MOOC Courses
Institute & Department Vision and Mission	Former IA question papers and solutions (prepared by faculty)	Former IA question papers solutions - hardcopy	Value Added Courses (VAC) are conducted throughout the semester & in the semester break - Enrol for the VACs
Program Educational Objectives (PEO)	MU end semester examination question papers and solutions (prepared by faculty)	MU end semester exam question paper & solutions - by faculty, hardcopy	
Program Specific Outcome (PSO)	Class notes and Digital Content for the subject (scanned / typed by faculty)	All text books, reference books, e -books mentioned in the syllabus & AAP	Online courses from NPTEL, Coursera etc. are pursued throughout the semester - Register for the course & get certified
Program Outcome (PO)	Comprehensive question bank, EQ, GQ, PPT, Class Test papers	Technical journals and magazines for reference	
Departmental Knowledge Map	Academic Administration Plan & Beyond Syllabus Activity report	VIT library is member of IIT Bombay Library	Watch former lectures captured in LMS at VIT

1.a Course Objectives (Write in detail – as per NBA guidelines)

Cognitive	What do you want students to know?	To know the basic concepts of networking and its topological design and mathematical functions like modulo arithmetic.	
Affective	What do you want students to think / care about?	To understand how various supporting tools in providing assurance concerning privacy and integrity of information.	
Behavioural	What do you want students to be able to do?	To provide skills to design security protocols for recognizing security problems and use of various cryptographic & security algorithms for real time applications.	

Advice to Students:

Attend every class!!! Missing even one class can have a substantial effect on your ability to understand the course. Be prepared to think and concentrate, in the class and outside. I will try to make the class very interactive. Participate in the class discussions. Ask questions when you don't understand something. Keep up with the class readings. Start assignments and homework early. Meet me in office hour to discuss ideas, solutions or to check if what you understand is correct. The v-Refer Link http://vidyalankarlive.com/vrefer/index.php/apps/files/?dir=/vRefer/CMPN/SEM%20VI&fileid=27331

Collaboration Policy:

We encourage discussion between students regarding the course material. However, no discussion of any sort is allowed with anyone on the assignment and homework for the class. If you find solution to some problems in a book or on the internet, you may use their idea for the solution; provided you acknowledge the source (name and page in the book or the website, if the idea is found on the internet). Even though you are allowed to use ideas from another source, you must write the solution in your own words. If you are unsure whether or not certain kinds of collaboration is possible please ask the teacher.

1.b Course Outcome (CO) Statements and Module-Wise Mapping (follow NBA guideline)

CO No.	Statements	Related Module/s
CO1	Understand system security goals and concepts, classical encryption techniques and acquire fundamental knowledge on the concepts of modular arithmetic and number theory.	I
CO2	Understand, compare and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication.	I, II
CO3	Apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.	III
CO4	Apply different digital signature algorithms to achieve authentication and design secure applications.	IV
CO5	Understand network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols like SSL, IPSec, and PGP.	V
CO6	Analyze and apply system security concept to recognize malicious code.	VI

1.c Mapping of COs with POs (mark 3: Strong, 2: Moderate, 1: Weak, Dash '–': not mapped)

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12
CO 1	3	3	2			2						
CO 2	2		2									
CO 3	2	2				2						
CO 4	2		3									
CO 5		2			3							
CO6			2		2							

1.d Mapping of COs with PSOs (mark 3: Strong, 2: Moderate, 1: Weak, Dash '–': not mapped)

	PSO 1	PSO 2	PSO 3
CO 1	3	1	-
CO 2	2	-	-
CO 3	2	1	-
CO 4	2	-	-
CO 5	1	1	-
CO6	1	1	-

1.e Teaching and Examination Scheme (As specified by the University) for the Course

Categories	Mathematics	Basic Science & General Engg.	Humanities & Soft Skill	Core Engg./ Technology - Design & Analysis	Multidisciplinary
Tick suitable category	✓	-	-	✓	-

Subject Code	Subject Name	Teaching Scheme			Credits Assigned			
		Theory	Practical	Tutorial	Theory	TW/Practical	Tutorial	Total
CSC604	Cryptography & System Security	3	2	-	3	1	-	4

Subject Code	Subject Name	Examination Scheme							
		Theory Marks IA Test			End Sem. Exam Marks	ISA lab	Practical	Oral	Total
		ISA	MSE						
CSC604	Cryptography & System Security	20	30		80	25	-	-	125

1.f Faculty-Wise Distribution of all Lecture-Practical-Tutorial Hours for the Course

Divisions	Lecture (Hrs.)	Practical (Hrs.)				Tutorial (Hrs.)			
		Batch 1	Batch 2	Batch 3	Batch 4	Batch 1	Batch 2	Batch 3	Batch 4
A	AKN	AKN	ATA	ATA	AKN	-	-	-	-
B	AKN	ATA	ATA	ATA	ATA	-	-	-	-

1.g Office Hours (Faculty will be available in office in this duration for solving students' query)

Division	Day	Time (at least 1 Hr. / Division)	Venue (Office Room No.)
ALL	Monday	3pm	M 209

2.a Syllabus : Module Wise Teaching Hours and % Weightage in University Question Paper

Module No.	Module Title and Brief Details	Teaching Hrs. for each module	% Weightage in University Question Papers
1	Security Goals, Attacks, Services and Mechanisms, Techniques. Modular Arithmetic: Euclidean Algorithm, Fermat's and Euler's theorem. Classical Encryption techniques, Symmetric cipher model, mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, playfair cipher, Hill cipher, transposition techniques: keyed and keyless transposition ciphers	8hrs	10%
2	Symmetric and Asymmetric key Cryptography and key Management Block cipher principles, block cipher modes of operation, DES, Double DES, Triple DES, Advanced Encryption Standard (AES), Stream Ciphers: RC4 algorithm. Public key cryptography: Principles of public key cryptosystems- The RSA Cryptosystem, The knapsack cryptosystem. Symmetric Key Distribution: KDC, Needham-schroeder protocol. Kerberos: Kerberos Authentication protocol, Symmetric key agreement: Diffie Hellman, Public key Distribution: Digital Certificate: X.509, PKI	11hrs	20%
3	Cryptographic Hash Functions Cryptographic hash functions, Properties of secure hash function, MD5, SHA-1, MAC, HMAC, CMAC.	3hrs	20%
4	Authentication Protocols & Digital Signature Schemes User Authentication, Entity Authentication: Password Base, Challenge Response Based Digital Signature, Attacks on Digital Signature, Digital Signature Scheme: RSA	5hrs	20%
5	Network Security and Applications Network security basics: TCP/IP vulnerabilities (Layer wise), Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing. Denial of Service: DOS attacks, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service Internet Security Protocols: PGP, SSL, IPSEC. Network security: IDS, Firewalls	9hrs	20%
6	System Security Buffer Overflow, malicious Programs: Worms and Viruses, SQL injection	3hrs	10%
* Insert rows for more modules in the Course	**Total**	**39hrs**	100%

2.b Prerequisite Courses

No.	Semester	Name of the Course	Topic/s
1	I	Structured Programming and Approach (SPA)	C Programming
2	III	Object Oriented Programming and Methodology (OOPM)	Java Programming
3	V	Computer Network (CN)	Network Layer, Transport Layer, Networking concepts

2.c Relevance to Future Courses

No.	Semester	Name of the Course
1	VII	Project I
2	VIII	Project II
3	VIII	Digital Forensic

2.d Identify real life scenarios / examples which use the knowledge of the subject

Real Life Scenario	Concept Used
End to End Encryption : Encryption is widely used to protect data stored on devices such as computers, smartphones, and external drives. For example, full disk encryption ensures that all data on a device is encrypted, preventing unauthorized access even if the device is lost or stolen. File-level encryption is also used to protect specific files or folders containing sensitive information.	Symmetric and Asymmetric key Cryptography
Password Storage: When you create an account on a website or application, your password is often not stored in plaintext but is instead encrypted using cryptographic hashing algorithms such as SHA-256 or bcrypt. This ensures that even if a database containing user passwords is compromised, the passwords are not easily retrievable by attackers.	Hashing
Digital Signatures: Digital signatures are used to verify the authenticity and integrity of digital documents and messages. For example, when you digitally sign a contract or an email, cryptographic algorithms are used to generate a unique digital signature that can be verified by the recipient to ensure that the document has not been altered and was indeed sent by you.	Digital Signature Schemes
Secure Communication: Secure communication over the internet relies heavily on cryptography. When you make a purchase online, access your bank account, or send sensitive information via email, cryptography ensures that the data transmitted is encrypted, making it unreadable to unauthorized parties. Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols are commonly used to secure communication between web browsers and servers during online transactions.	Network Security and Applications

3. Past Results – Division-Wise

Details	Target – May 2024	May 2023	May 2022	May 2021
Course Passing % – Average of 3 Divisions	100%	100%	100 %	100 %
Marks Obtained by Course Topper (mark/100)	77/80	75/80	80/80	79

	Division A		Division B	
Year	Initials of Teacher	% Result	Initials of Teacher	% Result
May 2023	AKN	100 %	AKN	100 %
May 2022	AKN	100 %	AKN	100 %
May 2021	AKN	100%	AKN	100%

4 All the Learning Resources – Books and E-Resources

4.a List of Text Books (T – Symbol for Text Books) to be Referred by Students

Sr. No	Text Book Titles	Author/s	Publisher	Edition	Module Nos.
1	"Cryptography and Network Security, Principles and Practice",	William Stallings	Pearson Education, March 2013	6th Edition,	I, II, III, IV, V,VI
2	"Cryptography & Network Security",	Behrouz A. Ferouzan	Tata McGraw Hill	2nd Edition	I, II, III, IV
3	"Cryptography and Network Security"	Behrouz A. Forouzan & Debdeep Mukhopadhyay,	McGraw Hill	3rd Edition,	IV,V, VI

4.b List of Reference Books (R – Symbol for Reference Books) to be Referred by Students

Sr. No	Reference Book Titles	Author/s	Publisher	Edition	Module Nos.
1	Applied Cryptography, Protocols Algorithms and Source Code in C	Bruce Schneier	Wiley	2nd	I, II, II
2	Cryptography & Network Security	Atul Kahate	Tata McGraw Hill	2nd	I, II, III, IV, V, VI
3	"Network Security Bible",	Eric Cole	Wiley, 2011.	Second Edition,	V, VI

4.c List of E - Books (E – Symbol for E-Books) to be Referred by Students

Sr. No	E- Book Titles	Author/s	Publisher	Edition	Module Nos.
1	Cryptography and Network Security https://books.google.co.in/books?id=YMcenO0rpFoC&printsec=frontcover&source=gbs_atb#	V.S. Bagad , I. A. Dhotre	Technical Publications	2rd	I-VIII

	v=onepage&q&f=false				
2	Handbook of Applied Cryptography http://cacr.uwaterloo.ca/hac/	Alfred J.Menezes, Paul C. Van Oorschot and Sc	CRC Press	5th	I-VI
3	Introduction to Cryptography Principles and Applications https://books.google.co.in/books?id=KwmkCgAAQBAJ&pg=PA1&lpg=PA1&dq=journals+on+introduction+to+cryptography&source=bl&ots=Jvyu9494hn&sig=ylU7JoKILZmH2qM6pyo6a1dr0mA&hl=en&sa=X&ved=0ahUKEwi_tZWqxLzUAhUBvY8KHWofBuMQ6AEISjAG#v=onepage&q&f=false	Hans Delfs, Helmut Knebl	Springer	3rd	I-V
4	Cryptography and Network Security https://books.google.co.in/books?id=OYiwCgAAQBAJ&printsec=frontcover&dq=ebook+on+cryptography+and+network+security&hl=ta&sa=X&ved=0ahUKEwjxj_L3mb3UAhULMY8KHWHSCdQ6AEIKTAB#v=onepage&q&f=false	Behrouz A Forouzan, Debdeep Mukhopadhyay	Special Indian Edition	3rd	I-V
5	Information Security https://books.google.co.in/books?id=Ux7gMy-f6DEC&printsec=frontcover&dq=ebook+on+cryptography+and+network+security&hl=ta&sa=X&ved=0ahUKEwjxj_L3mb3UAhULMY8KHWHSCdUQ6AEIMjAC#v=onepage&q&f=false	A Forouzan, Debdeep Mukhopadhyay	Technical Publications	1st	I-VIII
6	Cryptography and Network Security Principles and Practices https://books.google.co.in/books?id=qKcrce0x_2YC&printsec=frontcover&dq=ebook+on+cryptography+and+network+security&hl=ta&sa=X&ved=0ahUKEwjxj_L3mb3UAhULMY8KHWHSCdUQ6AEIOjAD#v=onepage&q&f=false	William Stallings	Pearson Education	4th	I-VIII
7	Cryptography and Network Security https://books.google.co.in/books?id=7ohHBQAAQBAJ&printsec=frontcover&dq=ebook+on+cryptography+and+network+security&hl=ta&sa=X&ved=0ahUKEwjxj_L3mb3UAhULMY8KHWHSCdUQ6AEIQjAE#v=onepage&q&f=false	Prakash C. Gupta	PHI Learning private Limited	1st	I-VII

4.d Reading latest / top rated research papers (at least 5 papers)

Name of Paper	Authors with Background	Published in		Problem Statement
		Date	Journal	
Offensive Security: Ethical Hacking Methodology on the Web	Fabián Cuzme-Rodríguez1, Marcelo León-Gudiño2 , Luis	2019	SPRINGER	The objective of this research is to generate policies, protocols and an information assurance plan based on methodologies controlled

	Suárez-Zambrano1 , and Mauricio Domínguez-Limaico1			in terms of security; As well as standards
Analysis of TCP/IP Header Attack and How to Prevent	Hirushan Sajindra Sri Lanka Institute of Information Technology | SLIIT · Department of Information Technology	15 July 2022	International Journal of Scientific Research in Computer Science	Security in TCP/IP Header
TCP/IP Protocol Security Problems and Defenses	Zhi Kanmai School of Engineering and Technology, Xi'an Fanyi University, Xi'an, China	10 May 2021	2020 International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI)	TCP/IP Protocol Security and Defence
A Survey of Research on CAPTCHA Designing and Breaking Techniques	Yang Zhang; Haichang Gao; Ge Pei; Sainan Luo Xidian University, Xian, China ; Guoqin Chang; Nuo Cheng	2022	18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)	How CAPTCA works for authentication on networks
Intelligent robotic process automation that shall make captcha security ineffective	Amit K. Nerurkar; G. T. Thampi; Dilip Motwani; Krutik Chaudhari; Pragati Panhale	2023	INTERNATIONAL CONFERENCE ON WIRELESS TECHNOLOGIES, NETWORKS, AND SCIENCE	The future of CAPTCHAs depends on exploring new directions to break CAPTCHAs
Understanding the /etc/shadow file in Linux	Aybala Sevinc	2022	https://medium.com/@aybala.sevinc/understanding-the-etc-shadow-file-in-linux-674555ab345e	As a Linux super user understanding the /etc/shadow file is very crucial for managing Linux users. /etc/shadow is a plain text file that stores information about the passwords of the system's users. It

				has 640 permissions and is owned by user root and group shadow. This file is only readable by the root user, so you must be root or have root privileges to view its contents.

4.e **Based on research paper an identify the current Problem statement**

Problem Statement	Used in					
	Quiz	Assignment	Lab	Mini Project	Poster Presentation	Test
As a Linux super user understanding the /etc/shadow file is very crucial for managing Linux users. /etc/shadow is a plain text file that stores information about the passwords of the system's users. It has 640 permissions and is owned by user root and group shadow. This file is only readable by the root user, so you must be root or have root privileges to view its contents.	√	√				
Security in TCP/IP Header			√			√

4.f **Identify Companies / Industries which use the knowledge of the subject and thus may provide Internships and final Placements**

Name of the Company	To be / Contacted for		
	Student Internship	Student Final Placement	Faculty Internship
DigiSec 360	√	√	
Cyberfrat	√	√	√
COE Security		√	

4.g **Identify suitable relevant TOP Guest Speakers from Industry (CS50 Lecture by Mark Zuckerberg - 7 December 2005 - YouTube)**

Name of the Identified Guest Speaker	Designation	Name of the Company
Christof Paar (https://www.youtube.com/@introductiontocryptography4223)	Professor of mathematics	University of Massachusetts Amherst.
Prof. Shafi Goldwasser (https://www.youtube.com/watch?v=jDsfV2ohFPs&list=PL6ogFv-ieghe8MOIcpD6UDtdK-UMHG8oH)	Professor	University of California, Berkeley, Carnegie Mellon University

4.h **Identify relevant Technical competitions to participate [Competitions -Paper Presentations, Projects, Hackathons, IVs etc..]**

Name of the Relevant Technical Competition Identified to participate	Organized by	Date of the Event
Alan Turing Cryptography Competition (https://www.maths.manchester.ac.uk/cryptography/)	The Department of Mathematics at The University of Manchester	Jan 2024
https://www.hackerhalted.com/	EC Council	Dates to be announced

4.i **Identify faculty in TOP schools / Universities who are teaching same / similar subject and develop rapport e.g. Exchange Lecture Material (Assignments / Tests / Project etc..), Joint Paper Publication**

University	Name of the Course	Name of Faculty	Type of Collaboration		
			Exchange of Lecture Material	Joint Publication/ Research	Other
IIT Kharagpur	Ethical Hacking	Prof. Indranil Sen Gupta			√(Publication)
MIT	Computer Systems Security	Prof. Nickolai Zeldovich	https://ocw.mit.edu/courses/6-858-computer-systems-security-fall-2014/		
MIT	Network And Computer	Prof. Ronald Rivest	https://ocw.mit.edu/courses/6-857-		

	Security		network-and-computer-security-spring-2014/		

4.j Web Links and Names of Magazines, Journals, E-journals – [VIT is member of IIT Bombay Library]

Refer online journals subscribed in VIT library. You can also access IIT Bombay online library for journals from IITB campus.

Sr. No.	Web-Links and Names of Journals and E-Journals Recommended to Students for this Course	Web-Links and Names of Magazines Recommended to Students for this Course	Module Nos.
1	Network Security Attacks: Volume 2017, Issue 5, Pages 1-20 (May 2017) https://www.sciencedirect.com/journal/network-security	Cryptography https://www.pcmag.com/encyclopedia/term/40522/cryptography	V, VI
2	Network Security: Volume 2017, Issue 4, Pages 1-20 (April 2017) https://www.sciencedirect.com/journal/network-security/vol/2017/issue/4	Backpack algorithms and Public-key cryptography made easy, Smashing Magazine https://www.smashingmagazine.com/2012/05/backpack-algorithms-and-public-key-cryptography-made-easy/	V, VI
3	Network Security with Cryptography, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 1, January 2015, pg 201-204, ISSN 2320-088X. https://www.ijarcsse.com/docs/papers/Volume_6/9_September2016/V6I9-0177.pdf	Cash and Credit in a cryptocurrency Economy, Cryptobiz magazine http://cryptobizmagazine.com/?p=1992	I, II, III, IV
4	Technical Survey on Cryptography algorithms for network security International Journal of Advanced Research in Computer Science and Software Engineering, volume 6, issue 9, September 2016, ISSN 2277 128X. https://www.ijarcsse.com/docs/papers/Volume_6/9_September2016/V6I9-0177.pdf	DoS, Cryptobiz magazine http://cryptobizmagazine.com/?p=2119	IV, V
5	Technical Review on Symmetric and Asymmetric Cryptography Algorithms		I, II

	International Journal of Advanced Research in Computer Science, volume 8, no.4, may 2017, ISSN No. 0976-5697 *http://ijarcs.info/index.php/Ijarcs/article/viewFile/3728/3215*		
6	A Review on Symmetric Key Encryption Techniques in Cryptography International Journal of Science, Engineering and Technology Research, Volume 3, Issue 3, March 2014, ISSN: 2278-7798. http://ijsetr.org/wp-content/uploads/2014/03/IJSETR-VOL-3-ISSUE-3-539-544.pdf		II, III
7	A study on Asymmetric key cryptography algorithms International Journals of Computer Science and Mobile Applications, volume 3, issue. 4, April 2015, pg. 8-13,ISSN 2321-8363. http://ijcsma.com/publications/april2015/V3I405.pdf		II, III
8	DES, AES, and Blowfish: Symmetric key Cryptography algorithms simulation based performance analysis International Journal of Emerging Technology and Advanced Engineering, volume 1, issue 2, December 2011, ISSN 2250-2459. https://pdfs.semanticscholar.org/d6b7/0f25e74e6ec069b1f44169171511b0f6b4aa.pdf		II, III, IV
9	Broad view of Cryptographic Hash functions International Journal of Computer Science Issues, volume. 10, issue 4, No. 1, July 2013, ISSN: 1694-0814. https://ijcsi.org/papers/IJCSI-10-4-1-239-246.pdf		III, IV

10	Security of network using IDs and Firewall International Journal of Scientific and Research Publications, volume 3, Issue 6, June 2013 ISSN 2250 – 3153. http://www.ijsrp.org/research-paper-0613/ijsrp-p18150.pdf		V, VI
11	Database Security – Attacks and Control Methods International Journal of Information Sciences and Techniques, Volume 6, No. 1 /2 , March 2016, DOI: 10.5121/ijist.2016.6218. http://aircconline.com/ijist/V6N2/6216ijist18.pdf		VI
12	Security survey of famous operating systems International Journal of computer science and information technology, volume 3, Issue 10, October 2014, Pg 106-113, ISSN 2320-088X. http://www.academia.edu/8740473/SECURITY_SURVEY_OF_FAMOUS_OPERATING_SYSTEMS		IV, V, VI
13	Kerberos: A strong authentication protocol International Journal of computer science & communication networks, vol 5(2), 103-106, ISSN 2249-5789. http://www.ijcscn.com/Documents/Volumes/vol5issue2/ijcscn2015050213.pdf		III, IV
14	Detecting of session hijacking and IP spoofing using sensor nodes and cryptography, IOSR Journal of Computer Engineering, e-ISSN 22780661, ISSN 2278-8727, Volume 13, Issue 2 (Jul – August 2013), PP 66-73 http://www.iosrjournals.org/iosr-jce/papers/Vol13-Qissue2/K01326673.pdf?id=4013		IV, V

15	A Review: DoS and DDoS Attacks International journal of computer science and mobile computing, Vol.4, Issue. 6, June 2015, pg. 260-265, ISBN 2320-088X. https://www.ijcsmc.com/docs/papers/June2015/V4I6201515.pdf		V, VI
16	Security through SSL International Journal of advanced research in computer science and software engineering, volume 2, issue 12, December 2012, ISSN: 2277 128X. https://www.ijarcsse.com/docs/papers/12_December2012/Volume_2_issue_12_December2012/V2I10-0067.pdf		V, VI
17	Securing Email applications from various cyber issues International Journal of Emerging technology and advanced engineering, ISSN: 2250-2459, Volume 3, Issue 4, April 2013. https://pdfs.semanticscholar.org/f372/99b5066ffc7f559891beb067ffe3a37103a1.pdf		IV, V, VI

4.k **Module Best Available in - Tick ONE best resource [from *4.a* to *4.d* in this AAP] & give details**

Module No.	Category (Please Tick Mark) - √						Available In VIT Library?		Details of the Resource (i.e. Name, Chapter no.etc.)
	Book			Maga-zine	Journals				
	Text	Reference	E-Book		Regular	E-Journal	Y	N	
1	√	-	-	-	-	-	√	-	4. a). Book 1, Chapter 1, Page No. 8 – 34, Chapter 7, Page No. 220-237
2	√	-	-	-	-	-	√	-	4. a). Book 1, Chapter 4 Page No. 112 – 140, Chapter 6 Page No. 205-209, chapter 8 Page No. 242-265, Chapter 9 Page No. 277-284
3	√	-	-	-	-	-	√	-	4. a). Book 1, Chapter 10, Page No. 305 – 311,319-340, 349-369,389-398
4	√	-	-	-	-	-	√	-	4. a). Book 1, Chapter 14, Page No. 447 – 460, Chapter 12, Page No. 392-394
5	√	-	-	-	-	-	√	-	4. b). Book 3, Chapter 13, Page No. 429 – 439 4. b) Book 2 Chapter 1, Page No. 30-33, Chapter 6, Page No. 265-282 Chapter 10 Page No. 496-500

6	√	-	-	-	-	-	√	-	4. b). Book 2, Chapter 1, Page No. 28-33 Chapter 6, Page No. 283 – 284, Chapter 10, Page No. 499-500

4.l **Referred to any top-rated university in that subject for content**

University	Name of the Course	Name of Faculty	Date of Delivery of the Course	Remarks
Massachusetts Institute of Technology Cambridge	Computer Systems Security	Nickolai Zeldovich	March 2020	It will present abstractions and implementation techniques for cyber security.
IBM	Cybersecurity Trends for 2023	Jeff Crume	January 2023	Ransomware and MFA will continue to play key roles in IT security, but what role will AI, deep fakes, and quantum computing play going forward into the New Year

4.m **Faculty received any certification related to their subject. List of Certifications Identified / Done**

Course	Certifying Agency	Certification		Remarks
		Done on	Proposed to be on	
Cybersecurity and the Internet of Things	COURSERA	July 2020	July 2020	"Cybersecurity and the Internet of Things (IoT)" is designed to address the unique security challenges posed by the proliferation of connected devices in the IoT ecosystem
CompTIA Security+ (SY0-501) Cert Prep: 2 Technologies and Tools	LINKEDIN LEARNING	June 2020	June 2020	CompTIA Security+ (SY0-501) is a certification exam designed to validate the baseline skills required to perform core security functions and pursue an IT security career. The "Technologies and Tools" domain of the exam covers various technologies, tools, and techniques commonly used in the field of cybersecurity.
Introduction to cyber security	GREAT LEARNING	January 2022	January 2022	"Introduction to Cybersecurity" course provides foundational knowledge and skills necessary to understand the principles, concepts, and practices of securing information and information systems in the digital

				age.
Information security	UPGRAD	January 2023	January 2023	Information security, often referred to as InfoSec, is the practice of protecting information by mitigating information risks. It involves the preservation of confidentiality, integrity, and availability (CIA) of information, ensuring that it remains accessible only to authorized users, accurate and reliable, and available when needed.
Fundamentals of Cyber Security	UpGrad	January 2024	March 2024	The outcome of a Fundamentals of Cybersecurity course is to provide students with the knowledge, skills, and awareness necessary to understand the basics of cybersecurity and contribute to the protection of information and information systems in various contexts.

4.n **Completed subject wise/cluster wise training with cluster mentor.**
List of relevant Refresher Course Identified / Done

Course	Certifying Agency (As suggested by DAB/Cluster Mentor/Industry/ University other than MU)	Certification		Remarks
		Done on	Proposed to be on	
Pedagogy	Information security	UPGRAD	January 2023	January 2023
PBL	Virtual Lab Execution		March 2023	Nice Simulations
Sub. Content Training	Bits and Bytes of Networking	July 2020		A good practical approach to understand how networks work.

4.o **Best Practices Identified and adopted**

No.	Item	Best Practices Identified		
		Univ. 1	Univ. 2	Univ. 3
1	Microsite	University of Cambridge https://www.cam.ac.uk/research/news/honour-among-thieves-the-study-of-a-cybercrime-marketplace-in-action	MIT https://ocw.mit.edu/courses/6-857-network-and-computer-security-spring-2014/	
2	Video Lectures	Prof. Saurav IIT Kharagpur https://www.youtube.com/watch?v=1plMO7ChXMU&list=PLJ5C_6qdAvBFAuGoLC2wFGruY_E2gYtev	Prof. Shafi Goldwasser, MIT https://www.youtube.com/watch?v=jDsfV2ohFPs&list=PL6ogFv-ieghe8MOIcpD6UDtdK-UMHG8oH	

3	Assignments			
4	Mini Project			
5	Assessment Metric			
6	Quizzes	Coursera Complete Certification | Cryptography https://www.youtube.com/watch?v=0pglUy-9ZPA		
7	Labs/ Practical (PBL)	IITb Vlabs (Virtual Lab IITH https://cse29-iiith.vlabs.ac.in/)		
8	Tests			
9	Etc			
10	Peer Assessment etc.			

4.p Web Links for Online Notes/YouTube/VIT Digital Content/VIT Lecture Capture/NPTEL Videos

Students can view lectures by VIT professors, captured through LMS 'Lecture Capture' in VIT campus for previous years.

No.	Websites / Links	Module Nos.
1	Introduction to Number Theory https://nptel.ac.in/courses/106105031/3	1
2	Data Encryption Standard, Triple Data Encryption Standard, Advanced Encryption Standard, Stream Cipher https://nptel.ac.in/courses/106105162/6	2
3	Message Digest and Digital Signature Cryptographic Hash Function https://www.youtube.com/watch?v=PcsalunvXSk	3
4	Denial of Service Attack **https://www.youtube.com/watch?v=MKkax564_CE**	5

4.q Recommended MOOC Courses like Coursera / NPTEL / MIT-OCW / edX/VAC etc.

Sr. No.	MOOC Course Link	Course conducted by – Person / University / Institute / Industry	Course Duration	Certificate (Y / N)
1	Cryptography and Network Security https://swayam.gov.in/nd1_noc20_cs21/preview	NPTEL Course by Dr. Sourav Mukhopadhyay, Associate Professor, Indian Institute of Technology, Kharagpur.	12 Weeks	Yes
2	Secure Networked System with Firewall and IDS https://www.coursera.org/learn/secure-networked-system-with-firewall-ids/home/welcome	Edward Chow University of Colorado, Colorado Springs	3 Weeks	Yes
3	IT Fundamentals for Cybersecurity Specialization (Coursera) https://www.coursera.org/specializations/it-fundamentals-cybersecurity	IBM Security Learning Services Certification	16 Weeks	Yes

5 Consolidated Course Lesson Plan

	From (date/month/year)	From (date/month/year)	Total Number of Weeks
Semester Duration	08/01/24	29/04/24	15

Week	Lecture no.	Module No.	Lecture Topics MSE/ BSA planned to be covered	Actual date of Completion (Hand written)	COs Mapped	Recommended Prior Viewing / Reading	
						Lecture No. (on LMS)	Chapter No./ Books/ Web Site
1	1	1	Security Goals, Attacks, Services and Mechanisms, Techniques.		CO1	--	4.a) Book 1, Chapter 1, Page No. 8-13
	2	1	Modular Arithmetic: Euclidean Algorithm, Fermat's and Euler's theorem Classical Encryption techniques, Symmetric cipher model		CO1	--	4.a) Book 1, Chapter 7, Page No. 220-228 4.a) Book 1, Chapter 1, Page No. 8-13
	3	1	mono-alphabetic and polyalphabetic substitution techniques: Vigenere cipher, playfair cipher,		CO1, CO2	--	4.a) Book 1, Chapter 1, Page No. 16-27
2	4	1	Hill cipher, transposition techniques: keyed and keyless transposition ciphers		CO2	--	4.a) Book 1, Chapter 1, Page No. 12-15, 21-34
	5	2	Block cipher principles, block cipher modes of operation, DES		CO2	--	4.a) Book 1, Chapter 2, Page No. 42-60
3	6	2	Double DES, Triple DES, Advanced Encryption Standard (AES),		CO2	--	4.a) Book 1, Chapter 4, Page No. 112-140,

Week	Lecture no.	Module No.	Lecture Topics MSE/ BSA planned to be covered	Actual date of Completion (Hand written)	COs Mapped	Recommended Prior Viewing / Reading	
						Lecture No. (on LMS)	Chapter No./ Books/ Web Site
							159-164
	7	2	Ciphers: RC4 algorithm. Public key cryptography: Principles of public key cryptosystems- The RSA Cryptosystem,		CO2	--	4.a) Book 1, Chapter 6, Page No. 205-209 4.a) Book 1, Chapter 8, Page No. 242-265
4	8	2	The knapsack cryptosystem Symmetric Key Distribution: KDC, Needham-schroeder protocol		CO2, CO4	--	4.a) Book 1, Chapter 9, Page No. 282-284 4.a) Book 1, Chapter 14, Page No. 454-460
	9	2	Kerberos: Kerberos Authentication protocol, Symmetric key agreement: Diffie Hellman,		CO4, CO2	--	4.a) Book 1, Chapter 14, Page No. 454-460 4.a) Book 1, Chapter 9, Page No. 277-281
	10	2,3	Public key Distribution: Digital Certificate: X.509, PKI Cryptographic hash functions, Properties of secure hash function, MD5		CO3	--	4.a) Book 1, Chapter 12, Page No. 389-398 4.a) Book 1, Chapter 10, Page No. 319-340, Chapter 11, Page No.

Week	Lecture no.	Module No.	Lecture Topics MSE/ BSA planned to be covered	Actual date of Completion (Hand written)	COs Mapped	Recommended Prior Viewing / Reading	
						Lecture No. (on LMS)	Chapter No./ Books/ Web Site
							349-369
6	11	3	SHA-1, MAC, HMAC, CMAC.		CO3	--	4.a) Book 1, Chapter 10, Page No. 319-340, Chapter 11, Page No. 349-369
	12	4	User Authentication, Entity Authentication: Password Base, Challenge Response Based				4.a) Book 1, Chapter 10, Page No. 319-340, Chapter 11, Page No. 349-369
7	13	4	Digital Signature, Attacks on Digital Signature				4.a) Book 1, Chapter 10, Page No. 319-340, Chapter 11, Page No. 349-369
	14	4	Digital Signature, Attacks on Digital Signature			--	4.a) Book 1, Chapter 12, Page No. 401-406
8	15	4	Digital Signature Scheme: RSA		CO4	--	4.a) Book 4, Chapter 13, Page No. 429-439
	16	4	Digital Signature Scheme: RSA		CO4	--	4.b). Book 2, Chapter 10, Page No. 498-500, Chapter 1, 17Page No. 1830-33

Week	Lecture no.	Module No.	Lecture Topics MSE/ BSA planned to be covered	Actual date of Completion (Hand written)	COs Mapped	Recommended Prior Viewing / Reading	
						Lecture No. (on LMS)	Chapter No./ Books/ Web Site
9	17		Guest lecture, video assignment, quiz				
	18						
10	19		Debate, minute paper				
	20		OBT				
11	21	5	Network security basics: TCP/IP vulnerabilities (Layer wise)		CO5	--	4.b) Book 2, Chapter 10, Page No. 496-497, Chapter 1, Page No. 28-31
	22	5	Network Attacks: Packet Sniffing, ARP spoofing, port scanning, IP spoofing		CO5	--	
12	23		Video Lecture			--	
	24		Video Lecture			--	
13	25	5	Denial of Service: DOS attacks, ICMP flood, SYN flood, UDP flood, Distributed Denial of Service		CO5	--	4.b) Book 2, Chapter 6, Page No. 265-282
	26	5	Internet Security Protocols: PGP, SSL, IPSEC.		CO5		4.b) Book 2, Chapter 6, Page No. 265-282
14	27	5	Network security: IDS, Firewalls		CO5		4.b) Book 2, Chapter 6, Page No. 283-284, Chapter 10, Page 499-

Week	Lecture no.	Module No.	Lecture Topics MSE/ BSA planned to be covered	Actual date of Completion (Hand written)	COs Mapped	Recommended Prior Viewing / Reading	
						Lecture No. (on LMS)	Chapter No./ Books/ Web Site
							500
	28	6	Buffer Overflow		CO6		4.b) Book 2, Chapter 6, Page No. 283-284, Chapter 10, 26Page 499-500 4.b) Book 2, Chapter 1, Page No. 28-33
15	29	6	Malicious Programs: Worms and Viruses, SQL injection		CO6		4.b) Book 2, Chapter 1, Page No. 28-33
	30		Revision				

6 Rubric for Grading and Marking of ISA (inform students at the beginning of semester)

CSS ISA

Task 1 (Quiz)	Task 2 Sums	Task 3 /etc/shadow	Task 4 Quiz	Task 5 Cryptography & Hashing	Task 6 BSE Visit	Task 7 Minute Paper	Task 8 Video Assignment	Task 9 Kahoot	Task 10 Guest e	Task 11 Course	Task 12 Video Assignment
20	20	20	20	20	--	--	20	--	--	20	20

CSS LAB ISA

Lab Journal	PBLE	Case Studies	Mini Project	Average/25
10	10	10	10	(25/10*)M1+M2+M3+M4/4

7 Assignments / Tutorials Details

Assignment/ Tutorial No.	Title of the Assignments / Tutorials	CO Map	Assignment/ Tutorials given to Students on	Week of Submission
Assignment #1	Quiz on Chapter 1	CO1	8/1/24	1
Assignment #2	Sums on Modular Arithmetic	CO1	8/1/24	2
Assignment #3	Analysis of/etc/shadow & /etc/passwd File systems	CO2	8/1/24	3
Assignment #4	Quiz on /etc/shadow & /etc/passwd File systems	CO2	8/1/24	4
Assignment #5	Hashing Case Study	CO4	8/1/24	5
Assignment #6	BSE Visit	CO5	8/1/24	6
Assignment #7	Minute Paper	CO6	8/1/24	7
Assignment #8	Video Assignment (https://www.youtube.com/watch?v=r10AAYB8Q60&t=176s)	CO5	8/1/24	8
Assignment #9	Quiz on guest lecture	CO3	8/1/24	9
Assignment #10	Kahoot Quiz	CO3	8/1/24	10
Assignment #11	Course on Network Defense Essentials (NDE) (https://codered.eccouncil.org/course/network-defense-essentials?logged=true)	CO1, CO3, CO6	8/1/24	11
Assignment #12	Video Assignment on ISUW 2020 | Faruk Kazi, VJTI | SPECIAL PLENARY 2: Power Systems Security in the Era of Cyber Wars https://www.youtube.com/watch?v=olYP-7Mm6k8&t=655s Watch the video and write summary.	CO1-CO6	8/1/24	12

Analysis of Assignment / Tutorial Questions and Related Resources

Assignment / Tutorial No.	Week No.	Type* (√)			Module No.	Based on #			Question Type (√)	
		R	PQ	OBT		Text Book	Reference Book	Other Learning Resource	MU EQ	Thought Provoking
Assignment #1	1	√			1	1 ,2, 3	1 ,2			√
Assignment #2	2	√			1	1, 2, 3	1 ,2		√	√
Assignment #3	3				1	1 ,2, 3	1, 2,3		√	√
Assignment #4	4				2	1 ,2, 3	1 ,2,3			√
Assignment #5	5				3	1 ,2, 3	1 ,2,3			√
Assignment #6	6				4	1, 2, 3	1 ,2,3			√
Assignment #7	7				5	1 ,2, 3	1 ,2,3			√
Assignment #8	8				6	1 ,2, 3	1 ,2,3			√
Assignment #9	9				ALL					√
Assignment #10	10				1	1, 2, 3				√
Assignment #11	11				1,3,6					√
Assignment #12	12				ALL					√

* Tick (√) the Type of the Assignment: Regular (R); Pop Quiz (PQ) ; Open Book Test for TE/BE/ME (OBT)
# Write number for text book, reference book, other learning resource from this AAP – *from Points 4.a to 4.d*

8 Internal Assessment / Other Class Test / Open Book Test (OBT)/Take Home Test (THT) Details

Tests	Test Dates	Module No.	CO Map	MSE Question Paper Pattern	Policy
3 MSE		1,2,3,4,5	CO1-CO2-CO3-CO4-CO5	Q. 1. Attempt any Five (2 Marks Each) Q2. Attempt any one (10 Marks each) Q3. Attempt any one (10 Marks each)	

*** Failures of shall appear for test in the next semester. There is no provision for re-test in the same semester.**

9.a Practical Activities – Regular Experiments

Practical No.	Module No.	Title of the **Regular Experiments**	Topics to be highlighted	CO Map
1	1	Design and Implementation of Ceaser Cipher Technique	Cipher Algorithm	CO1
2	1	Design and Implementation of Monoalphabetic Cipher	Cipher Algorithm	CO1
3	4	Design and Implementation of Digital Signature	Hashing	CO4
4	2	Design and Implementation of RSA algorithm for generating public and private key	Public Key Cryptography	CO2
5	2	Design and Implementation of DES (Symmetric Key Encryption)	Advance encryption	CO2
6	6	Special Topic Seminar	Applications	CO6
7	2	Design and Implementation of Diffie Hellman Key Establishment	Key Exchange	CO2
8	3	Design and Implementation of HMAC	HMAC	CO3
9	5	Design and Implementation of DOS using Hping 3	DOS & DDOS	CO5
10	4	Simulation of SQL Injection (PBLE-1)	SQL injection	CO6
11	5	One of the most famous intrusion detection system and has been known for its flexibility with different environments. You can even integrate it with Kibana and elastic cloud.	IDS	CO5
12	5	Mini Project	Applications	CO5

9.b Practical Activities – Newly Added Experiments

Practical No.	Module No.	Title of the **Newly Added Experiments**	Concepts to be highlighted	CO Map
3	4	Design and Implementation of Digital Signature	Hashing	CO4
5	2	Design and Implementation of DES (Symmetric Key	Advance encryption	CO2

		Encryption)		

9.c Practical Activities – PBL Experiments

Practical No.	Module No.	Title of the **PBL Experiments**	Concepts to be highlighted	CO Map
4	6	One of the most famous intrusion detection system and has been known for its flexibility with different environments. You can even integrate it with Kibana and elastic cloud.	IDS	CO6
10	4	Simulation of SQL Injection (PBLE-1)	SQL injection	CO6

10 Beyond Syllabus Activities for Gap Mitigation

No.	Type of the Activity	Activities	Details – no of attendees, guest, feedback, mark sheet, report
1	Interaction with Outside World	Guest Lecture / Workshops	Ms. Manisha C., Founder & Director of DIGISEC 360, "Latest trends and challenges in security"
2		Industrial Visit	01 BSE
3	Collaborative and Group Activity	Poster Presentation	--
4		Minute Papers	1 Minute Paper for LMR (Last Minute Revision)
5		Students Seminars	--
6		Students Debates	Debate on different attacks
7		Panel Discussion / Mock GD	--
8		Mock Interview	--
9	Co-curricular Courses	MOOC-NPTEL/Coursera Videos	NPTEL Videos on Cryptography and Network Security
10		Value Added Courses	-
11		Lecture Capture Usage	01 (ALL Divisions)
12	Test and Assessments	Class Tests / Weekly Tests	--
13		Mini Projects	01
14		Pop Quiz	01
15		Mobile App Based Quiz	01
16		Open Book and Take-Home Test	00

11.1 One-on-One Academic Mentoring Meetings done

No.	Name of Mentee	Date of One-On-One Meeting		
		Beginning of Sem.	After Mid Term Results	Before End Sem.
1	Omkar Shitole			
2	Atharv Deshmukh			
3	Shrutika Mandhare			
4	Jatin Talekar			
5	Sunpreet Huda			
6	Kshitij Tripathi			
7	Bashar Kharbe			
8	Bhargavaram Krishnapur			
9	Vedika Desai			
10	Aditi Kakade			
11	Rajdutt Kangutkar			
12	Mayank Lad			
13	Parth Sase			
14	Vinayakash Thevar			
15	Srushti Patil			
16	Aryaman Jain			
17	Priyanka Kamble			
18	Sarthak Gaikwad			

11.2 Identify Financial Concerns and refer appropriately

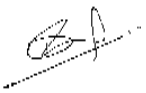
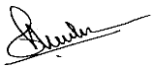
No.	Name of Mentee			
		Individual Goals Identified	Any Financial Concern which needs to be referred to	Any Emotional Concern to be referred to

*** Do not delete any activity. Give details for planned events. Write 'NA' for activity Not Planned.**

Consolidated Academic Administration Plan Prepared by (mention all theory teaching faculty names with signature)

Please write below your name and sign with date of the external cluster mentor meeting

Faculty 1	Faculty 2	Faculty 3

			
External Industry Mentor	External Academic Mentor	VIT Cluster Mentor	Program HOD