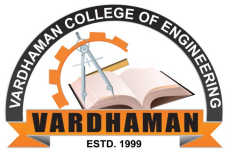

VARDHAMAN COLLEGE OF ENGINEERING

(AUTONOMOUS)

Affiliated to **JNTUH,** Approved by **AICTE,** Accredited by **NAAC** with **A++** Grade, **ISO 9001:2015** Certified

Kacharam, Shamshabad, Hyderabad - 501218, Telangana, India

www.vardhaman.org

CURRICULUM

For

Bachelor of Technology (Minors)

In

Cyber Security

Department of Information Technology

Programme Curriculum Structure
B.Tech Minors in Cyber Security

S. No.	Yr/ Sem	Course Code	Course Name	Type	Credits
1	III/I	M1507	Number Theory and Cryptography	Theory	3
2	III/I	M1508	Number Theory and Cryptography Lab	Practice	2
3	III/II	M1509	Foundations of Cyber Security	Theory	3
		Elective			
4	III/II	M1510	Ethical Hacking Fundamentals	Theory	3
		M1511	Web and Mobile Application Security		
		Elective			
5	IV/I	M1512	Ethical Hacking Fundamentals Lab	Practice	2
		M1513	Web and Mobile Application Security Lab		
		Elective			
6	IV/I	M1514	Block Chain and its Applications	Theory	3
		M1515	Cloud Security		
		M1516	Security Incident & Response Management		
7	IV/II	M1542	Mini Project for Cyber Security	Project Work	2
Total Credits					18

VARDHAMAN COLLEGE OF ENGINEERING, HYDERABAD

An Autonomous Institute, Affiliated to JNTUH

Course Structure

M1507 - Number theory and Cryptography

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	**T**	**P**	**L**	**T**	**P**	**C**	**CIE**	**SEE**	**Total**
3	0	0	42	0	0	3	30	70	100

1. Course Description

Course Overview

This is an introductory undergraduate level course of number theory and cryptography. Roughly speaking, on the one hand, number theory is the mathematical branch that studies relations between integers. On the other hand, cryptography is the science of concealing messages and is one very active domain nowadays. All you need here is high school algebra and scientific maturity.

Course Pre/co-requisites

The course has no specific prerequisite and co requisite.

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1507.1 Implementation of Number System, Modular arithmetic, GCD computation, Prime Numbers and Multiplicative Inverse computation

M1507.2 Implementation of key exchange algorithms, cryptography algorithms and digital signature algorithms.

3. Course Syllabus

Number System: The number system, Divisibility, GCD Computation: Euclid's Algorithm, Extended Euclid's Algorithm

Modular Arithmetic: Groups, Solving Modular, Linear Equations. Chinese Remainder Theorem. Modular Exponentiation, Discrete Logarithm Problem.

Key Exchange: Diffie-Hellman, ElGamal, Massey Omura. Computation of Generators of Primes

Elliptic Curve Cryptosystem: Theory of Elliptic Curves, Elliptic Curve Encryption & Decryption Algorithms, Security of Elliptic Curves Cryptography, Elliptic Curve Factorization.

Digital Signatures: Authentication Protocols, Digital Signature Standards (DSS). Proxy Signatures.

4. Books and Materials

Text Books:

1. Introduction to Algorithms: T. H. Cormen, C. E. Leiserson, R. Rivest and C. Stein Prentice Hall India, 2nd Edition, 2002.

2. A Course in Number Theory and Cryptography: Neal Koblitz, Springer Verlag, New York Inc. May 2001.
3. Cryptography and Network security: Principles and Practice, William Stallings, Pearson Education, 2002.
4. Introduction to Cryptography with Coding Theory, Second Edition, W. Trappe and L. C. Washington, Pearson Education 2007.
5. Cryptography: Theory and Practice, Douglas R. Stinson, CRC Press.
6. Randomized Algorithms, R. Motwani and P. Raghavan, Cambridge University Press, 1995.

Course Structure
M1508 - Number theory and Cryptography Lab

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
0	0	4	0	0	56	2	30	70	100

1. Course Description

Course Overview

This is an introductory undergraduate level course of number theory and cryptography. Roughly speaking, on the one hand, number theory is the mathematical branch that studies relations between integers. On the other hand, cryptography is the science of concealing messages and is one very active domain nowadays. All you need here is high school algebra and scientific maturity

Course Pre/co-requisites

The course has no specific prerequisite and co requisite.

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1508.1 Demonstrate the knowledge of Number System, Modular arithmetic, GCD computation, Prime Numbers and Multiplicative Inverse computation.

M1508.2 Apply the basic of Number system to implement key exchange algorithms, cryptography algorithms and digital signature algorithms.

3. Course Syllabus

Practice

1. Tile-a-Rectangle-with-Squares
   Given an n × m grid (where n,mn,m are integers), we would like to tile it with the minimal number of same size squares. Clearly, it can always be tiled with nm squares of size 1 × 1, but it is not always optimal. For example, a 6 × 10 grid can be tiled by 15 squares of size 2 × 2.
   My goal in this problem is to implement a function squares(n, m) that returns the minimum number of same size squares required to tile a grid of size n × m.

2. Diophantine-Equations
   Solving two unknown parameter equations (Diophantine Equations) This solution is taken from "http://new.math.uiuc.edu/public348/python/jimcarlsonpy.pdf" and the following paragraphs are taken from the same site.

   We will use the recursive implementation of the Euclidean algorithm to design a function isolve for solving the Diophantine equation ax + by = c. (1) Such equations are solvable if and only if the gcd(a, b) divides c. First note that if b divides a then we can write down a solution: x = 0, y = c/b. If b does not divide a, write a = bq + r as in the (long) divsion algorithm and then substitute into (1): (bq + r)x + by = c. Rearrange as b(qx + y) + rx = c. Set u = qx + y, v = x and substitute again to obtain the equation bu + rv = c. (2) We have reduced the equation (1) to the

equivalent equation (2) with smaller coefficients. If we can solve the new equation, then we recover a solution of the old equation by the formulas x = v, y = u - qv. 11 The process eventually terminates (by the theory of the Euclidean algorithm) with an equaiton where the second coefficient divides the first. These ideas are embodied in the Python code below. Note the use of the divmod operation to compute the quotient and remainder at the same time. The function divmod returns a pair of numbers, the quotient and remainder, which we store in q, r. Note also the use of lists for the return value.

3. Modular Division
   Now that we know how to use extended Euclid's algorithm for finding modular inverses, implement an efficient algorithm for dividing b by a modulo n.
   Given three integers a, b, and n, such that gcd(a,n)=1 and n > 1, the algorithm should return an integer x such that 0 <= x <= n - 1, and b / a = x (modn) (that is, b = a x (modn)).
4. Chinese Remainder Theorem

   Implement the algorithm to construct the number from the Chinese Remainder Theorem. You need to implement the function Chinese Remainder Theorem(n-1, r-1, n-2, r-2) which takes two coprime numbers n-1 and n-2 and the respective remainders 0 <= r-1 < n-1 and 0 <= r-2 < n-2, and must return the number r such that 0 < r < n-1 n-2 <r r=r1modn1 and r=r2modn2.
   You have access to the function ExtendedEuclid(a, b)ExtendedEuclid(a,b) which returns pair of numbers (x, y)(x,y) such that ax + by = GCD(a, b)ax+by=GCD(a,b).

   Implement the algorithm explained in the lectures.
5. Modular Exponentiation
   How to compute b^e mod? There is no need to compute the giant number b^e and divide by m. We can start with 1, then multiply by b and immediately take the result modulo m, repeat e times.

6. Fast Modular Exponentiation
   (1) Implement the function Fast Modular Exponentiation (b, k, m) which computes (b^2k) modm using only around 2k modular multiplications. You are not allowed to use Python built-in exponentiation functions.
   (2) Implement the function FastModularExponentiation(b, e, m) which computes (b^e) modm using around 2log2(e) modular multiplications. You are not allowed to use Python built-in exponentiation functions.
7. RSA Quiz: Code Question 1 (Encryption)
   Implement RSA encryption with the given public key modulo, exponent modulo, exponent.

   You have access to the function PowMod(a, n, modulo) which computes anmodmodulo using the fast modular exponentiation algorithm from the previous module. You also have access to the function ConvertToInt(message) which converts a text message to an integer.

   You need to fix the implementation of the function Encrypt(message, modulo, exponent) to return the integer ciphertext according to RSA encryption algorithm

8. RSA Quiz: Code Question 2 (Decryption)
   Implement RSA decryption with the given private key p, q, exponent.You have access to the function ConvertToStr(m) which converts from integer mm to the plain text message message. You also have access to the function Invert Modulo(a, n) which takes coprime integers a and n as inputs and returns integer b such that ab=1modn. You also have access to the function PowMod(a, n, modulo) which computes anmod(modulo) using fast modular exponentiation

   You need to fix the implementation of the function Decrypt(ciphertext, p, q, exponent) to decrypt the message which was encrypted using the public key (n=p q,e=exponent)

9. RSA Quiz: Code Question 3 (Ciphertext Attack)
   Secret agent Alice has sent one of the following messages to the center: attack don't attack wait Alice has ciphered her message using public key modulo, exponent that is available to you, and you have intercepted her ciphertext. You want to know what was the content of her message. You have access to the function Encrypt(message, modulo, exponent) which takes in a message as a string and returns a big integer as a ciphertext. It uses RSA encryption with public key modulo, exponent. In the starter code, you have an example usage of the function Encrypt. You also have function DecipherSimple (ciphertext, modulo, exponent, potential-messages) implemented in the starter code. You need to fix this implementation to solve the problem. It should take the ciphertext sent from Alice to the center, the public key modulo, exponent and the set of potential messages that Alice could have sent, and return the message that Alice encrypted and sent as a string. For example, if Alice took message "wait", encrypted it with the given modulo and exponent, and got number 139763215 as the ciphertext, you will need to return the string "wait" given the ciphertext = 139763215, modulo, exponent and potential-messages ="attack","don't attack","wait"

10. RSA Quiz: Code Question 4 (Small Prime Attack)
    Alice is using RSA encryption with a public key modulo, exponent such that modulo=pq with one of the primes p and q being less than 1000000, and you know about it. You want to break the cipher and decrypt her message.

    You can use the functionDecrypt(ciphertext,p,q,e) which decrypts the ciphertext given the private key p, q and the public exponent e.

    You are also given the function DecipherSmallPrime(ciphertext,modulo,exponent), and you need to fix its implementation so that it can decipher the ciphertext in case when one of the prime factors of the public modulo is smaller than 1000000

4. Books and Materials

Text Books:

1. Introduction to Algorithms: T. H. Cormen, C. E. Leiserson, R. Rivest and C. Stein Prentice Hall India, 2nd Edition, 2002.
2. A Course in Number Theory and Cryptography: Neal Koblitz, Springer Verlag, New York Inc. May 2001.

3. Cryptography and Network security: Principles and Practice, William Stallings, Pearson Education, 2002.
4. Introduction to Cryptography with Coding Theory, Second Edition, W. Trappe and L. C. Washington, Pearson Education 2007.
5. Cryptography: Theory and Practice, Douglas R. Stinson, CRC Press.
6. Randomized Algorithms, R. Motwani and P. Raghavan, Cambridge University Press, 1995.

Course Structure
M1509 - Foundations of Cyber Security

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
3	0	0	42	0	0	3	30	70	100X

1. Course Description

Course Overview

This course introduces the concept of cyber security, its interdisciplinary nature and its relation to nation, businesses, society and people. Students would gain knowledge of various cyber security terminologies, technologies, protocols, threat analysis, and forensics.

Course Pre/co-requisites

The course has no specific prerequisite and co requisite.
A7XXX - Cryptography and Network Security

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1509.1 Adequate level of cross-disciplinary knowledge of design, implementation, evaluation and testing of secure protocols, systems or applications.
M1509.2 Foundational skills for developing expertise in one or more sub-domains of cyber-security.
M1509.3 Foundational skills and knowledge of impact of security on economics, legal, business, warfare and social domains .

3. Course Syllabus

Introduction: Psychology and Usability: Introduction, Insights from psychology research, Deception in practice, Passwords, CAPTCHAs.

CIA Triad; Protocols: Password eavesdropping risks, Who goes there? – simple authentication, Manipulating the message, Changing the environment, Chosen protocol attacks, Managing encryption keys.

Banking and Bookkeeping: Bookkeeping systems, Interbank payment systems, Automatic teller machines, Credit cards, EMV payment cards, Online banking, Nonbank payments.

Biometrics: Handwritten signatures, Face recognition, Fingerprints, Iris codes, Voice recognition and morphing, What goes wrong.

Electronic and Information Warfare: Communications systems, Surveillance and target acquisition, IFF systems, Improvised explosive devices, Directed energy weapons, Information warfare ; Legal Issues and Ethics.

4. Books and Materials

Text Books:

1. Ross Anderson, Security Engineering. 2nd Edition. John Wiley and Sons. 2008, ISBN-13: 978-0470068526.

Reference Books:

1. Charles P. Pfleeger, Security in Computing, 5th Edition, Prentice Hall, 2015, ISBN-10: 0134085043.

Course Structure
M1510 - Ethical Hacking Fundamentals

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
3	0	0	42	0	0	3	30	70	100

1. Course Description

Course Overview

Ethical hacking is a subject that has become very important in present-day context, and can help individuals and organizations to adopt safe practices and usage of their IT infrastructure. Starting from the basic topics like networking, network security and cryptography, the course will cover various attacks and vulnerabilities and ways to secure them.

Course Pre/co-requisites

The course has no specific prerequisite and co requisite.

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1510.1 Demonstrate the knowledge of Computer Networks, Cryptography, Information security concepts and its applications.
M1510.2 Ability to apply threats identification principles.

3. Course Syllabus

Introduction: to Computer Networks, OSI and TCP/IP Reference models, types of attacks, Security Services.

Information gatherings: basics of e-hacking, network security, open ports, URL extraction.

Web security problems: vulnerable WP, user enumeration, brute forcing user password, basics of network packet capture.

ARP and TCP analysis, OSINT, network extraction, URL extraction, mail server, name server

Message Authentication Code (MAC), SHA-512, Digital Signatures and TCP layer security.

4. Books and Materials

Text Books:

1. "The Basics of hacking and penetration testing" by Patrick engebreston, elsevier.

Reference Books:

1. Network Security Essentials (Applications and Standards), William Stallings Pearson Education.

Course Structure
M1511 - Web and Mobile Application Security

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
3	0	0	42	0	0	3	30	70	100

1. Course Description

Course Overview
The course has been designed to equip students with the relevant skills, tools and techniques to identify vulnerabilities and flaws within web and mobile applications.

Course Pre/co-requisites
Interactive Web Development
Ethical Hacking & Systems Defense

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1511.1 To understand the knowledge of Web application hacking and attack for evasion techniques
M1511.2 To apply the different techniques for hijacking and fixation
M1511.3 To discover and exploit through techniques for Web services vulnerabilities
M1511.4 To To analyze the android and iOS for mobile application security.

3. Course Syllabus

Web applications: Introduction to web applications, Web application hacking, Overview of browsers, extensions, and platforms, Attacks, detection evasion techniques, and countermeasures for the most popular web platforms, including IIS, Apache, PHP, and ASP.NET Attacks and countermeasures for common web authentication mechanisms, including password-based, multifactor (e.g., CAPTCHA), and online authentication services like Windows Live ID.

Advanced session analysis, hijacking, and fixation techniques, cross-site scripting, SQL injection, classic categories of malicious input, Overlong input (like buffer overflows), canonicalization attacks (like the infamous dot-dot-slash), and meta characters (including angle brackets, quotes, single quote, double dashes, percent, asterisk, underscore, newline, ampersand, pipe, and semicolon), beginner-to-advanced SQL injection tools and techniques, stealth-encoding techniques and input validation/ output-encoding countermeasures.

Web services vulnerabilities discovery and exploited through techniques including WSDL disclosure, input injection, external entity injection, and XPath injection. Web application management attacks against remote server management, web content management/authoring, admin misconfigurations, and developer-driven mistakes. Web browser exploits.

Android Architectures, Setting up a Testing Environment, Android Build Process, Reversing APKs, Device Rooting, Android Application Fundamentals, Network Traffic,

Device and Data Security, Tapjacking, Static Code Analysis, Dynamic Code Analysis

iOS Architecture, Device Jailbreaking, Setting up a Testing Environment, iOS Build Process, Reversing iOS Apps, iOS Application Fundamentals, iOS Testing Fundamentals, Network Traffic, Device Administration, iOS: Dynamic Analysis.

4. Books and Materials

Text Books:

1. Hacking Exposed Web Applications, 3rdEdition, JOEL SCAMBRAY, VINCENT LIU, CALEB SIMA
2. The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws By Dafydd Stuttard, Marcus Pinto
3. Rich Bowen, Ken Coar, "Apache Cookbook", O'Reilly
4. "Mobile Application Security" by David Thiel, Chris Clark, Himanshu Dwivedi Released February 2010 Publisher(s): McGraw-Hill ISBN: 9780071633574

Reference Books:

1. Open Web Application Security Project. A Guide to Building Secure Web Applications and Web Services. http://www.owasp.org/index.php/Category:OWASP Guide Project.
2. https://www.udemy.com/course/web-application-security/
3. https://www.udemy.com/course/mobile-application-hacking-and-penetration-testing-android-security/
4. https://legacy.elearnsecurity.com/course/mobile application security and penetration testing/
5. https://krademy.com/mobile-application-security
6. https://www.oreilly.com/library/view/mobile-application-security/9780071633567/

Course Structure
M1512 - Ethical Hacking Fundamentals Lab

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
0	0	4	0	0	56	2	30	70	100

1. Course Description

Course Overview

Ethical hacking is a subject that has become very important in present-day context, and can help individuals and organizations to adopt safe practices and usage of their IT infrastructure. Starting from the basic topics like networking, network security and cryptography, the course will cover various attacks and vulnerabilities and ways to secure them.

Course Pre/co-requisites

Computer Networks

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1512.1 Demonstrate the knowledge of Computer Networks, Cryptography, Information security concepts and its applications.
M1512.2 Ability to apply threats identification principles.

3. Laboratory Equipment/Software/Tools Required

1. Working with open ports scanning (Nmap).
2. Working with wordpress security scan (WPSCAN)
3. Working with sniffers for monitoring network communication (Wireshark).
4. Using maltego, extract foot print of URL
5. Using shodan, get the information about of wireless devices.
6. Working with hydra for finding user name and password
7. Working with masscan for finding IP address of URL
8. Write a program to implement the DES algorithm
9. Write a program to implement RSA algorithm
10. Calculate the message digest of a text using the SHA-1 algorithm

4. Books and Materials

Text Books:

1. "The Basics of hacking and penetration testing" by Patrick engebreston, elsevier
2. "Applied Cryptography" by Bruce Schneier

Reference Books:

1. "Cryptography and Network Security" by William Stallings 3rd Edition, Pearson Education

Course Structure
M1513 - Web and Mobile Application Security Lab

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
0	0	4	28	0	0	2	30	70	100

1. Course Description

Course Overview

The course has been designed to equip students with the relevant skills, tools and techniques to identify vulnerabilities and flaws within web and mobile applications.

Course Pre/co-requisites

Interactive Web Development
Ethical Hacking and Systems Defense

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1513.1 To understand the knowledge of Web application hacking and attack for evasion techniques
M1513.2 To apply the different techniques for hijacking and fixation
M1513.3 To discover and exploit through techniques for Web services vulnerabilities
M1513.4 To analyze the android and iOS for mobile application security.

3. Laboratory Equipment/Software/Tools Required

1. Lab 1 – Enumeration Responses
2. Lab 2 – Security Misconfiguration Responses
3. Lab 3 – Using Components with Known Vulnerabilities Responses
4. Lab 4 – Broken Authentication Responses
5. Lab 5 – Broken Access Control Responses
6. Lab 6 – Injections Responses
7. Lab 7 – XXE and XSS Responses
8. Lab 8 – Insecure Deserialization Responses
9. Lab 9 – Sensitive Data Exposure Responses
10. Lab 10 – Bypass Security Controls
11. Lab 11 – Tapjacking
12. Lab 12 – eLS_LogIn (Reverse Engineering Lab)
13. Lab 13 – eLS_LogIn (Dynamic Analysis Lab)
14. Lab 14 – Secure OTP generator

4. Books and Materials

Text Books:

1. Hacking Exposed Web Applications, 3rd edition, JOEL SCAMBRAY, VINCENT LIU, CALEB SIMA

2. The Web Application Hacker's Handbook Discovering and Exploiting Security Flaws By Dafydd Stuttard, Marcus Pinto
3. Rich Bowen, Ken Coar, "Apache Cookbook", O'Reilly
4. "Mobile Application Security" by David Thiel, Chris Clark, Himanshu Dwivedi Released February 2010 Publisher(s): McGraw-Hill ISBN: 9780071633574

Reference Books:

1. Open Web Application Security Project. A Guide to Building Secure Web Applications and Web Services. http://www.owasp.org/index.php/Category:OWASP_Guide _Project
2. https://www.udemy.com/course/web-application-security/
3. https://www.udemy.com/course/mobile-application-hacking-and-penetration-testing-android-security/
4. https://legacy.elearnsecurity.com/course/mobile_application_security_and _penetration_testing/
5. https://krademy.com/mobile-application-security
6. https://www.oreilly.com/library/view/mobile-application-security/9780071633567/

Course Structure
M1514 - Blockchain and its Applications

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
3	0	0	42	0	0	3	30	70	100

1. Course Description

Course Overview

TheIn the last few years, Blockchain technology has generated massive interest among governments, enterprises, and academics, because of its capability of providing a transparent, secured, tamper-proof solution for interconnecting different stakeholders in a trustless setup. This subject will cover the basic design principles of Blockchain technology and its applications over different sectors.

Course Pre/co-requisites

Computer Networks
Operating Systems
Cryptography and Network Security

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1514.1 Describe the basic concepts and technology used for blockchain
M1514.2 Describe the primitives of the distributed computing and cryptography related to blockchain.
M1514.3 Illustrate the concepts of Bitcoin and their usage.
M1514.4 Implement Ethereum block chain contract.
M1514.5 Apply security features in blockchain technologies.
M1514.6 Use smart contract in real world applications.

3. Course Syllabus

Introduction: Need for Distributed Record Keeping, Modeling faults and adversaries, Byzantine Generals problem, Consensus algorithms and their scalability problems, Nakamoto's concept with Blockchain based cryptocurrency, Technologies Borrowed in Blockchain – hash pointers, consensus, byzantine fault-tolerant distributed computing, digital cash etc.

Basic Distributed Computing & Crypto primitives: Atomic Broadcast, Consensus, Byzantine Models of fault tolerance, Hash functions, Puzzle friendly Hash, Collison resistant hash, digital signatures, public key crypto, verifiable random functions, Zero-knowledge systems.

Bitcoin basics: Bitcoin blockchain, Challenges and solutions, proof of work, Proof of stake, alternatives to Bitcoin consensus, Bitcoin scripting language and their use

Ethereum basics: Ethereum and Smart Contracts, The Turing Completeness of Smart Contract Languages and verification challenges, Using smart contracts to enforce legal contracts, comparing Bitcoin scripting vs. Ethereum Smart Contracts, Writing smart

contracts using Solidity & JavaScript

Privacy, Security issues in Blockchain: Pseudo-anonymity vs. anonymity, Zcash and Zk-SNARKS for anonymity preservation, attacks on Blockchains: Sybil attacks, selfish mining, 51% attacks advent of algorand; Sharding based consensus algorithms to prevent these attacks, Blockchain Applications

4. Books and Materials

Text Books:

1. Narayanan, Bonneau, Felten, Miller and Goldfeder, "Bitcoin and Cryptocurrency Technologies – A Comprehensive Introduction", Princeton University Press.
2. Imran Bashir, "Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained", Packt Publishing

Reference Books:

1. Josh Thompson, 'Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming', Create Space Independent Publishing Platform, 2017.
2. Merunas Grincalaitis, "Mastering Ethereum: Implement Advanced Blockchain Applications Using Ethereum-supported Tools, Services, and Protocols", Packt Publishing.
3. Prof. Sandip Chakraborty, Dr. Praveen Jayachandran, "Blockchain Architecture Design And Use Cases"[MOOC], NPTEL: https://nptel.ac.in/courses/106/105/106105184/

Course Structure
M1515 - Cloud Security

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
3	0	0	42	0	0	3	30	70	100

1. Course Description

Course Overview
This course covers cloud security, addressing known risks and vulnerabilities and focuses on sound architectural design for secure computing.

Course Pre/co-requisites
Web application development.

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1515.1 Understand the architecture and infrastructure of cloud computing along with the hands-on experience in various cloud computing platforms.
M1515.2 Identify the known threats, risks, vulnerabilities, and privacy issues in the various layers of cloud computing

3. Course Syllabus

Introduction: Need for Distributed Record Keeping, Modeling faults and adversaries, Byzantine Generals problem, Consensus algorithms and their scalability problems, Nakamoto's concept with Blockchain based cryptocurrency, Technologies Borrowed in Blockchain – hash pointers, consensus, byzantine fault-tolerant distributed computing, digital cash etc.

Basic Security Design and Architecture for Cloud Computing Infrastructure and host threats, service provider threats, generic threats, threats assessment, Authentication and authorization techniques for cloud solutions, Protection of application infrastructure, Data Protection Strategies.

Data Protection for Cloud Infrastructure and Services Understand the Cloud based Information Life Cycle, Data protection for Confidentiality and Integrity, Common attack vectors and threats, Encryption, Data Redaction, Tokenization, Management, assuring data deletion, Data retention, deletion and archiving procedures for tenant data.

Cloud infrastructure: Understand the access control requirements for Cloud infrastructure, Enforcing Access Control Strategies, Compute, Network and Storage, Authentication and Authorization, Roles-based Access Control, Multi-factor authentication, Host, storage and network access control options, Firewalls, IDS, IPS and honeypots.

Security Patterns for Cloud Computing: Trusted Platform, Geo-tagging, Cloud VM Platform Encryption, Trusted Cloud Resource Pools, Secure Cloud Interfaces, Cloud Resource Access Control, Cloud Data Breach Protection, Permanent Data Loss Protection,

Cloud Denial-of-Service Protection, Cloud Traffic Hijacking Protection, Cloud Authentication Gateway, Cloud Key Management.

4. Books and Materials

Text Books:

1. John R. Vacca, "Cloud Computing Security – Foundations and Challenges" CRC Press, 2017
2. Cloud Computing Design Patterns by Thomas Erl (Prentice Hall) - 978-0133858563

Reference Books:

1. Ronald L. Krutz and Russell Dean Vines, "Cloud Security- A Comprehensive Guide to Secure Cloud Computing", Wiley, 2010
2. Tim Mather, S. Kumaraswamy and S. Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'Reilly Media, 2009.

Course Structure
M1516 - Security Incident & Response Management

Hours Per Week			Hours Per Semester			Credits	Assessment Marks		
L	T	P	L	T	P	C	CIE	SEE	Total
3	0	0	42	0	0	3	30	70	100

1. Course Description

Course Overview

This course provides Security incident & response management knowledge required to analyze problem encountered in engineering. This course covers network security, incidence, operations, dynamic malwares analysis, restoration, attacks, detection techniques, recovery process, backup with identification, policies, procedures and guidelines for handling incident. Further, this course can be applied in many areas of engineering such as network security, networking, big data analytics and cryptography.

Course Pre/co-requisites

The course has no specific prerequisite and co requisite.

2. Course Outcomes (COs)

After the completion of the course, the student will be able to:

M1516.1. Understand network security, security incidence response and relation with security operations.
M1516.2. Evaluate about malwares, dynamic malware analysis and restoration of affected systems & attacks.
M1516.3. Analyze the malwares detection techniques using signatures and recovery process with response tools.
M1516.4. Apply techniques for information security Incident Management & data backup with identification and detection.
M1516.5. Remembers the policies, procedures and guidelines for handling incident and troubleshooting of network security.

3. Course Syllabus

Introduction: Definition of network security, Application of Security, Evaluation of network security, principles, Information Security Services, characteristics of network security, definitions of security incident response, IP addressing, relation of incident response to the rest of security operations,incident response phases - preparation, identification, recovery, follow-up, Identifying Unauthorized Devices.

Introduction to malware: OS security concepts, malware threats, evolution of malware, malware types viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis. Eradication: Actual removal and restoration of affected systems, removal of attack artifacts, scanning of other systems to ensure complete eradication, use of IOCs on other systems and local networks, understand the attack.

Malware Detection Techniques: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences. Recovery: Test and validate systems before putting back into production, monitoring of system behavior, ensuring that another incident will not be created by the recovery process, response Management, incident response tool, support investigations.

Information Security Incident Management & Data Backup: Information Security Incident Management overview- Handling-Response, Incident Response Roles and Responsibilities, Incident Response Process etc. Data Back introduction, Types of Data Backup and its techniques, Developing an Effective Data Backup Strategy and Plan, Security Policy for Back Procedures. Identification: Detection, incident triage, information gathering and reporting, incident classification.

Policies and procedures incident workflows, guidelines, incident handling forms, principles of malware analysis, log analysis,threat intelligence, vulnerability management, penetration testing, Troubleshooting Network Devices and Services: Introduction & Methodology of Troubleshooting, Troubleshooting of Network security, Connectivity-Network Devices- Network Slowdowns-Systems-Modems.

4. Books and Materials

Text Books:

1. Managing Information Security Risks, The Octave Approach by Christopher Alberts, and Audrey Dorofee.
2. 'Cryptography and Network Security (4th Edition) by (Author) William Stallings.
3. "Incident Response & Computer Forensics, Third Edition" by Jason T. Luttgens and Matthew Pepe.

Reference Books:

1. Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder", by Don Murdoch.
2. Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012 2
3. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006.
4. https://www.sans.org/reading-room/whitepapers/incident/security-incident-handling-small-organizations-32979