20CA3E2: CRYPTOGRAPHY & NETWORK SECURITY

Course Name	Cryptography & Network Security		L	T	P	C	CIA	SEE	TM
Course Code	20CA3E2		4	0	0	4	30	70	100
Year of Introduction: 2005	**Year of Offering:** 2021	**Year of Revision**: 2022			**Percentage of Revision:** 30%				
L-Lecture, T-Tutorial, **P**-Practical, **C**-Credits, **CIA**-Internal Marks, **SEE**-External Marks, **TM**-Total Marks									

Course Description and Purpose: The course is intended to understand and gain knowledge on Computer & Network Security, Number Theory, Classical Encryption Techniques, Advanced Encryption Standard and Random Bit Generation and Stream Ciphers, Number Theory, Public Key Cryptography and RSA, Other Public-Key Crypto Systems and Message Authentication Codes, Digital Signatures, Key Management and Distribution and User Authentication, Transport Level Security, Electronic Mail Security and IP Security and Intruders and Firewalls.

Course Objective: The course aims to provide a comprehensive understanding of computer and network security, covering topics such as number theory, classical and advanced encryption techniques, public-key cryptography, digital signatures, key management, user authentication, transport level security, email and IP security, and intrusion detection, enabling students to secure digital communication and defend against cyber threats.

Specific Objectives include:

- To understand Basic Ideas about *Analysis of Algorithms* and the *Concept of Data Structures*.
- To know *Divide and Conquer*, *Greedy Methods* and *Solving Various Problems* by applying them.
- To apply *Dynamic Programming Method* and *Basic Traversal* and *Search Techniques* to solve various Problems.
- To understand *Backtracking and Branch and Bound* Techniques to Design Algorithms.
- To categorize *NP-Har*d and *NP-Complete* Problems.

Course Outcomes:

CO1: Upon completion of this course, students will master fundamental computer and network security concepts, classical encryption techniques (symmetric ciphers, substitutions, transpositions), Advanced Encryption Standard (AES) implementation, and random bit generation principles, equipping them with essential skills for securing digital systems and data against various threats.

CO2: Upon completion of this course, students will have a comprehensive understanding of fundamental number theory concepts, public key cryptography principles (including RSA, Diffie-Hellman, and elliptic curve cryptography), message authentication codes, and security protocols, enabling them to apply advanced cryptographic techniques in secure communication and data protection.

CO3: Upon completion of this course, students will possess in-depth knowledge of digital signatures, key management, and user authentication techniques, including the NIST Digital Signature Algorithm, symmetric key distribution using asymmetric encryption, distribution of public keys, Kerberos, and remote user authentication using asymmetric encryption, empowering them to design and implement robust security protocols for digital communication systems.

CO4: Upon completion of this course, students will be proficient in implementing Transport Layer Security, securing electronic mail using techniques like S/MIME and Pretty Good Privacy, and ensuring IP Security through comprehensive understanding of IP Security policy, Encapsulating Security Payload, and Combining Security Associations, enabling them to safeguard digital communication at the transport and network levels effectively.

CO5: Upon completion of this course, students will possess expertise in identifying and defending against intruders through intrusion detection techniques, implementing robust password management strategies, understanding the necessity of firewalls, grasping firewall characteristics and access policies, and recognizing different types of firewalls, enabling them to design and deploy effective security measures against unauthorized access and cyber threats.

Syllabus

UNIT-I (12 Hours)

Computer & Network Security Concepts: Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, A Model for Network Security.
Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques
Advanced Encryption Standard: AES Structure, An AES Example, AES Implementation.
Random Bit Generation and Stream Ciphers: Principles of Pseudo Random Number Generation, Pseudo Random Number Generators.

UNIT-II (12 Hours)

Introduction to Number Theory: Divisibility and the Division Algorithm, The Euclidean Algorithm, Modular Arithmetic, Prime Numbers, Fermat's and Euler's Theorems, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms.
Public Key Cryptography and RSA: Principles of Public Key Crypto Systems, The RSA Algorithm.
Other Public-Key Crypto Systems: Key Management, Diffie-Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.
Message Authentication Codes: Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs, MACs Based on Hash Functions: HMAC.

UNIT-III (12 Hours)

Digital Signatures: Digital Signatures, NIST Digital Signature Algorithm.
Key Management and Distribution: Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys.
User Authentication: Kerberos, Remote User-Authentication Using Asymmetric Encryption.

UNIT-IV (12 Hours)

Transport Level Security: Transport Layer Security.
Electronic Mail Security: S/MIME, Pretty Good Privacy.
IP Security: IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations.

UNIT-V (12 Hours)

Intruders: Intruders, Intrusion Detection, Password Management.
Firewalls: The Need for Firewalls, Firewall Characteristics and Access Policy, Types of Firewalls.

Prescribed Text Book			
	Author	Title	Publisher
1	William Stallings	Cryptography and Network Security	Pearson, Seventh Edition, 2017

Reference Text Book			
	Author	Title	Publisher
1	William Stallings	Cryptography and Network Security	Pearson, Sixth Edition, 2014
2	William Stallings	Network Essentials - Security Applications and Standards	Pearson Education (2007), Third Edition.

3	Chris McNab	Network Security Assessment	OReilly (2007), 2nd Edition
4	Jon Erickson	Hacking-The Art of Exploitation	Press (2006),SPD
5	Neal Krawety	Introduction to Network Security	Thomson (2007).
6	Ankit Fadia	Network Security-A Hackers Perspective	Macmillan (2008)
7	Behrouz A Forouzan, Debdeep Mukhopadhyay	Cryptography and Network Security	MCGraw-Hill, Indian Special Edition, Third Edition, 2015

Course has focus on : Employability

Websites of Interest :

3. https://www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighere d/preface/0132775069.pdf
4. http://faculty.mu.edu.sa/public/uploads/1360993259.0858Cryptography%20and%20Network%20Security%20Principles%20and%20Practice,%205th %20Edition.pd

Co-curricular Activities: Programming Contests, Hackathons & Quiz.

PARVATHANENI BRAHMAYYA SIDDHARTHA COLLEGE OF ARTS & SCIENCE

(An Autonomous College in the jurisdiction of Krishna University)

M.C.A, Third Semester

Course Name: Cryptography & Network Security

Course Code: 20CA3E2

(w.e.f admitted batch 2022-23)

Time: 3 Hours **Max Marks: 70**

SECTION-A

AnswerALLquestions **(5×4=20Marks)**

1. (a) Explain Caesar Cipher.(CO1,L2)

(or)

(b) Explain TRNGs, PRNGs. (CO1,L2)

2. (a) What is Modular Arithmetic? Explain. (CO2,L1)

(or)

(b) Explain RSA Algorithm. (CO2,L1)

3. (a) What is Digital Signatures? (CO3,L1)

(or)

(b) List the Distribution of Public Keys. (CO3,L1)

4. (a) Explain Handshake Protocol in TLS. (CO4,L2)

(or)

(b) Explain Pretty Good Privacy. (CO4,L2)

5. (a) Explain Password Management Briefly. (CO5,L2)

(or)

(b) Explain Firewall Characteristics? (CO5,L2)

SECTION-B

Answer Five Questions Choosing One Question from each unit.

All Questions Carry Equal Marks. **(5×10=50Marks)**

6. (a) Explain various Security Attacks and Security Services. (CO1,L2)

(or)

(b) Explain AES Encryption and Decryption Process. (CO1,L2)

7. (a) Illustrate Diffie-Hellman Key Exchange. (CO2,L2)

(or)

(b) Explain Internal and External Error Control in Message Authentication Functions. (CO2,L2)

8. (a) Explain NIST Digital Signature Algorithm with diagram. (CO3,L5)

(or)

(b) Explain Kerberos in detail. (CO3,L5)

9. (a) Explain Confidentiality and Authentication in S/MIME (CO5,L5)

(or)

(b) Illustrate Overview of IP Security. (CO4,L5)

10. (a) Discuss what are the problems that may intruder create and explain how to overcome those problem? (CO5,L6)

(or)

(b) Discuss Various Types of Firewalls. (CO5,L6)