



**PARVATHANENI BRAHMAYYA  
SIDDHARTHA COLLEGE OF ARTS &  
SCIENCE**  
*Autonomous*  
**Siddhartha Nagar, Vijayawada-520010**  
*Re-accredited at 'A+' by the NAAC*

**Offered to: M.Sc. (Computational Data Science)**

<b>Course Name</b>	Cryptography & Network Security	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>	<b>CIA</b>	<b>SEE</b>	<b>TM</b>
<b>Course Code</b>	22DS4E6	4	0	0	4	30	70	100
<b>Year of Introduction:</b>	<b>Year of Offering:</b>	<b>Year of Revision:</b>		<b>Percentage of Revision:</b>				
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.

**Course Outcomes:**

Upon completion of this course students should be able to

**CO1:** Name Encryption Algorithms and MAC

**CO2:** Utilize Number Theory, Encryption Techniques, Symmetric and Asymmetric keys and Firewalls for IP security.

**CO3:** Apply Digital Signatures, Random Bit Generation and Stream Ciphers.

**CO4:** Analyse Key Management and Distribution, S/MIME and Pretty Good Privacy.

**CO5:** Identify intruders, User Authentication and Computer & Network Security Concepts

CO-PO MATRIX								
COURSE CODE	CO-PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7
22DS4E6	CO1	M			M			
	CO2		M			M		
	CO3			H	M			
	CO4				H	M		
	CO5			M		H		

**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 Books			
	Author	Title	Publisher
1	William Stallings	Cryptography and Network Security	Pearson, Sixth Edition, 2014
2	William Stallings	Network Essentials - Applications and Security Standards	Pearson Education (2007), Third Edition.
3	Chris McNab	Network Security Assessment	OReilly(2007), 2 <sup>nd</sup> 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 :**

1. [https://www.pearsonhighered.com/assets/hip/us/hip\\_us\\_pearsonhighered/preface/0132775069.pdf](https://www.pearsonhighered.com/assets/hip/us/hip_us_pearsonhighered/preface/0132775069.pdf)
2. <http://faculty.mu.edu.sa/public/uploads/1360993259.0858Cryptography%20and%20Network%20Security%20Principles%20and%20Practice,%205th%20Edition.pdf>

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



**PARVATHANENI BRAHMAYYA  
SIDDHARTHA COLLEGE OF ARTS &  
SCIENCE**

*Autonomous*

**Siddhartha Nagar, Vijayawada-520010**

*Re-accredited at 'A+' by the NAAC*

**M.Sc.(Computational Data Science)**

**Semester :IV**

**Course Code: 22DS4E6 Course Name: Cryptography & Network Security**

**Time: 3 Hours**

**Max Marks: 70**

**SECTION-A**

**Answer the following questions. (5×4=20Marks)**

1. (a) Explain Caesar Cipher.(CO1,L2)  
(or)  
(b) Explain TRNGs, PRNGs. (CO3,L2)
2. (a) What is Modular Arithmetic? Explain. (CO2,L1)  
(or)  
(b) Explain RSA Algorithm. (CO1,L2)
3. (a) What is Digital Signatures? (CO3,L1)  
(or)  
(b) List the Distribution of Public Keys. (CO4,L1)
4. (a) Explain Handshake Protocol in TLS. (CO2,L2)  
(or)  
(b) Explain Pretty Good Privacy. (CO4,L2)
5. (a) Explain Password Management Briefly. (CO5,L2)  
(or)  
(b) Explain Firewall Characteristics? (CO2,L2)

**SECTION-B**

**Answer the following questions**

**(5×10=50Marks)**

6. (a) Explain various Security Attacks and Security Services. (CO5,L2)  
(or)  
(b) Explain AES Encryption and Decryption Process. (CO2,L2)
7. (a) Illustrate Diffie-Hellman Key Exchange. (CO2,L2)  
(or)  
(b) Explain Internal and External Error Control in Message Authentication Functions. (CO1,L2)
8. (a) Explain NIST Digital Signature Algorithm with diagram. (CO3,L5)  
(or)  
(b) Explain Kerberos in detail. (CO5,L5)
9. (a) Explain Confidentiality and Authentication in S/MIME (CO4,L5)  
(or)  
(b) Illustrate Overview of IP Security. (CO2,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. (CO2,L6)

