INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

CRYPTOGRAPHY AND NETWORK SECURITY								
VII Semester: CSE(DS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACDD27	Elective	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: There are no prerequisites to take this course								

I. COURSE OVERVIEW:
This course provides foundational knowledge of cryptographic techniques and network security principles. It covers classical and modern encryption algorithms, public key cryptography, hash functions, digital signatures, and authentication protocols. Students will explore security threats, network vulnerabilities, and defense mechanisms, focusing on secure communication, data integrity, and confidentiality in real-world networked systems.

II. COURSE OBJECTIVES:
The students will try to learn:

I. The principles of network security and OSI architecture, along with classical encryption techniques, form the basis of secure communication.
II. The concepts of finite fields and modular arithmetic, supported by key number theory theorems, underpin modern cryptography.
III. The fundamentals of block ciphers, symmetric algorithms, and public key cryptography, enable secure encryption and key exchange..
IV. The use of hash functions, MACs, digital signatures, and protocols, ensures integrity and authentication in secure systems.

III. COURSE OUTCOMES:
CO1 **Explain** the foundational principles of network security, classical encryption techniques, and the role of the OSI security architecture.
CO2 **Develop** the ability to formulate, analyze, and solve linear programming problems using techniques like the graphical method and simplex method.
CO3 **Explore** integer programming applications and solve problems using branch-and-bound and cutting- plane algorithms.
CO4 **Understand** and solve nonlinear optimization problems, including both unconstrained and constrained cases
CO5 **Learn** and **apply** advanced methods such as the Karush-Kuhn-Tucker (KKT) conditions, quadratic programming, and convex programming.
CO6 **Apply** optimization techniques to domains such as transportation, logistics, and resource management.

IV. COURSE CONTENT:

MODULE – I: INTRODUCTION & NUMBER THEORY (09)

Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography). FINITE FIELDS AND NUMBER THEORY: Groups, Rings, Fields-Modular arithmetic-Euclid's algorithm-Finite fields- Polynomial Arithmetic –Prime numbers-Fermat's and Euler's theorem-Testing for primality -The Chinese remainder theorem-Discrete logarithms.

MODULE – II: BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY (10)

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES)-Triple DES-Blowfish-RC5 algorithm. Public key cryptography: Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange- Elliptic curve arithmetic-Elliptic curve cryptography.

MODULE – III: HASH FUNCTIONS AND DIGITAL SIGNATURES (10)

Authentication requirement – Authentication function – MAC – Hash function–Security of hash function and MAC–MD5-SHA-HMAC–CMA.

Digital signature and authentication protocols–DSS–EI Gamal– Schnorr.

MODULE – IV: SECURITY PRACTICE & SYSTEM SECURITY (09)

Authentication applications–Kerberos–X.509 Authentication services-Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions. Intruder–Intrusion detection system–Virus and related threats–Countermeasures–Firewalls design principles –Trusted systems – Practical implementation of cryptography and security.

MODULE – V: E-MAIL, IP & WEB SECURITY (10)

E-mail Security: Security Services for E-mail-attacks possible through E-mail - establishing keys privacy-authentication of the source-Message Integrity-Non-repudiation-Pretty Good Privacy-S/MIME. IPSecurity: Overview of IP Sec - IP andIPv6-Authentication Header-Encapsulation Security Payload (ESP)-Internet Key Exchange (Phases of IKE, ISAKMP/IKE Encoding). Web Security: SSL/TLS Basic Protocol-computing the keys- client authentication-PKI as deployed by SSL Attacks fixed in v3- Exportability-Encoding-Secure Electronic Transaction (SET).

V. TEXTBOOKS:

1. William Stallings, Cryptography and Network Security, 6 th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security", 1st Edition, Prentice Hall of India, 2002

VI. REFERENCE BOOKS:

1. Behrouz A. Ferouzan, "Cryptography & Network Security", 1st Edition ,Tata Mc Graw Hill, 2007.
2. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", 1st Edition, Wiley Publications, 2003.
3. Charles Pfleeger, "Security in Computing", 4th Edition, Prentice Hall of India, 2006.
4. Ulysess Black, "Internet Security Protocols", 1st Edition , Pearson Education Asia, 2000.
5. Charlie Kaufman and Radia Perlman, Mike Speciner, "Network Security, 2nd Edition, Private Communication in Public World", PHI 2002.

VII. ELECTRONIC RESOURCES

1. https://www.geeksforgeeks.org/cryptography-introduction/
2. https://www.youtube.com/watch?v=JoeiLuFNBc4&list=PLBlnK6fEyqRgJU3EsOYDTW7m6SUmW6kII
3. https://www.javatpoint.com/cryptography-definition
4. https://www.youtube.com/watch?v=1plMO7ChXMU&list=PLJ5C_6qdAvBFAuGoLC2wFGruY_E2gYtev

VIII. MATERIALS ONLINE

1. Course template
2. Tutorial question bank
3. Tech talk topics
4. Definitions and terminology
5. Assignments
6. Model question paper – I
7. Model question paper – II
8. Lecture notes
9. PowerPoint presentation
10. E-Learning Readiness Videos (ELRV)