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

COURSE CONTENT

INFORMATION SECURITY								
VI Semester: CSE(DS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACDD16	Elective	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: Basic knowledge of computer networks, operating systems, and programming fundamentals.								

I. COURSE OVERVIEW:

This course provides a foundational understanding of information security principles, including threats, vulnerabilities, cryptographic techniques, access control mechanisms, network security protocols, and risk management. It aims to equip students with the skills to identify security risks and implement appropriate protection mechanisms to safeguard digital assets in modern computing environments.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The fundamental concepts of information security, including confidentiality, integrity, and availability.
II. The various types of threats, attacks, and vulnerabilities in computing systems and networks.
III. The principles and techniques of cryptography and secure communication.
IV. Risk assessment, access control, and mechanisms for enforcing security policies in real-world systems.

III. COURSE OUTCOMES:

CO1 Explain the core principles and goals of information security.
CO2 Identify different types of threats, attacks, and system vulnerabilities.
CO3 Apply cryptographic algorithms to ensure data confidentiality and integrity.
CO4 Describe various authentication and access control mechanisms.
CO5 Analyze security issues in network communication and propose appropriate solutions.
CO6 Assess risks and develop security policies for managing information systems securely.

IV. COURSE CONTENT:

MODULE – I: ATTACKS ON COMPUTERS AND COMPUTER SECURITY (09)
Attacks on computers and computer security: Introduction, the need for security, security approaches, principles of security, types of security attacks, security services, security mechanism, a model for network security; Cryptography concepts and techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, steganography, key range and key size, possible types of attacks.

MODULE – II: SYMMETRIC KEY CIPHERS (10)
Symmetric key ciphers: Block cipher principles and algorithms (DES, AES, Blowfish), differential and linear cryptanalysis, block cipher modes of operation, stream ciphers, RC4 location, and placement of encryption function, key distribution; Asymmetric key ciphers: Principles of public key cryptosystems, algorithms (RSA Diffie Hellman, ECC) key distribution.

MODULE – III: MESSAGE AUTHENTICATION ALGORITHM AND HASH FUNCTIONS (10)
Message authentication algorithm and hash functions: Authentication requirements, functions, message, authentication codes, hash functions, secure hash algorithm, whirlpool, HMAC, CMAC, digital signatures, knapsack algorithm.

Authentication application: Kerberos, X.509 authentication service, public – key infrastructure, biometric authentication.

MODULE – IV: E-MAIL SECURITY (10)
E-mail Security: Pretty Good Privacy; S/MIMI IP Security: IP security overview, IP security architecture, authentication header, encapsulating security payload, combining security associations, key management.

MODULE – V: WEB SECURITY (09)
Web security: Web security considerations, secure socket layer and transport layer security, secure electronic transaction intruders; Virus and firewalls: Intruders, intrusion detection password management, virus and related threats, countermeasures, firewall design principles; Types of firewalls Case Studies on Cryptography and security: Secure inter-branch payment transactions, cross site scripting vulnerability, virtual electronics.

V. TEXTBOOKS:

1. William Stallings, “Cryptography and Network Security: Principles and Practice,” Pearson, 8th Edition, 2023.
2. Behrouz A. Forouzan, “Cryptography and Network Security,” McGraw-Hill Education, 3rd Edition, 2022.
3. William Stallings, “Network Security Essentials: Applications and Standards,” Pearson, 7th Edition, 2022.
4. Michael E. Whitman and Herbert J. Mattord, “Principles of Information Security,” Cengage Learning, 7th Edition, 2021

VI. REFERENCE BOOKS:

1. Shon Harris, Allen Harper, Jonathan Ness, Chris Eagle, Daniel Regalado, Gray Hat Hacking: The Ethical Hacker's Handbook, McGraw-Hill Education, 6th Edition, 2022.
2. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 3rd Edition, 2020

VII. ELECTRONICS RESOURCES:

1. www.coursera.org
2. www.edx.org
3. www.udemy.com
4. www.linkedin.com/learning
5. http://bookboon.com/en/search?q=INFORMATION+SECURITY

6. https://books.google.co.in/books/about/Cryptography_Network_Security_Sie_2E.html?id=Kokjwdf0E7QC
7. https://books.google.co.in/books/about/Information_Security.html?id=Bh45pU0_E_4C

VIII. MATERIALS ONLINE

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