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

COURSE CONTENT

INFORMATION SECURITY AND MANAGEMENT								
V Semester: CSE / IT/ CSE (CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
ACCD04	Core	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		3	0	0	3	40	60	100
Contact Classes:48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: Network security								

I. COURSE OVERVIEW:

This course introduces a variety of network security concepts. A fundamental grasp of objectives, dangers, assaults, and methods, as well as algorithms and their design decisions, is developed in this course. Additionally, the course introduces students to a few mathematical ideas that are relevant to cryptology. The focus of the course is on providing students with a fundamental grasp of cryptosystem assaults and information protection techniques. Moreover, information security and Security Management, digital signatures, and message authentication is covered.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The fundamental concepts of computer and network security, including security threats, services, and mechanisms.
II. The cryptographic algorithms and techniques, including symmetric and asymmetric encryption, digital signatures, and authentication protocols.
III. The security solutions and management practices for securing web applications, IP communications, and enterprise-level information systems.

III. COURSE OUTCOMES:

After successful completion of the course, students should be able to:

CO1 Describe the concepts of security architecture, including attacks, services, and mechanisms.
CO2 Apply classical and modern encryption techniques such as DES, AES, and RC4 for data confidentiality.
CO3 Analyze and implement authentication protocols and digital signatures to ensure secure identity verification.
CO4 Evaluate and implement IP security protocols such as IPsec and Internet Key Exchange (IKE).
CO5 Demonstrate the use of web security protocols, including SSL/TLS and SET, for secure online communication.
CO6 Develop security policies and risk management strategies, and apply digital forensic methods for maintaining and investigating system security.

IV. COURSE CONTENT:

MODULE-I: INTRODUCTION (09)

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.

MODULE-II: SYMMETRIC KEY CRYPTOGRAPHY (09)

Block Ciphers and the Data Encryption Standard (DES) algorithm. Differential and linear cryptanalysis, triple DES.Block cipher design principles, Block cipher modes of operation, Advanced Encryption Standard (AES), Stream Ciphers: RC4.

MODULE-III: CRYPTOGRAPHY AND CRYPTANALYSIS (10)

Digital Signatures, Digital signature Standard, Authentication Applications, Kerberos, X.509.

Directory Authentication Service. Email Security: Pretty Good Privacy (PGP) and S/MIME.

MODULE-IV: IP SECURITY AND WEB SECURITY (10)

IP Security: Overview, IP Security Architecture, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange. Web Security: Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

MODULE-V: MANAGEMENT AND INFORMATION SECURITY (10)

Security Policy, Developing Security Programs, Risk Management, Security Management Models, Security Management Practices, Contingency Planning: Disasters/Business Continuity, Security Maintenance and Digital Forensics Protection Mechanism

V. TEXT BOOKS:

1. W. Stallings, "Cryptography and Network Security – Principles and Practice", 8th edition. Pearson Education, 2020.
2. M. E. Whitman and H. J. Mattord, Management of Information Security, 6th edition. Boston, MA: Cengage Learning, 2018.

VI. REFERENCE BOOKS:

1. N. Godbole and S. Belapure, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives,1st edition. New Delhi, India: Wiley India, 2011.
2. C. P. Pfleeger and S. L. Pfleeger, Analyzing Computer Security, 1st edition. Pearson Education, 2012.
3. C. Schou and D. Shoemaker, Information Assurance for the Enterprise, 1st edition. New Delhi, India: McGraw-Hill (TMH), 2007.

VII, ELECTRONIC RESOURCES:

1. http://www.hashcash.org/hashcash.pdf
2. https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.
3. https://www.coursera.org/learn/crypto
4. https://www.coursera.org/learn/crypto2

VII. 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)