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

COURSE CONTENT

FUNDAMENTALS OF CRYPTOGRAPHY								
VI Semester: CSE (CS)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACCD30	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:

The course provides the basic paradigm and principles of modern cryptography. The focus of this course will be on definitions and constructions of various cryptographic objects. We will try to understand what security properties are desirable in such objects, how to formally define these properties, and how to design objects that satisfy the definitions. The aim is that at the end of this course, the students are able to understand a significant portion of current cryptography research papers and standards.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The understanding of security concepts and the comprehension of classical encryption techniques
II. The symmetric cryptography approaches in information security
III. The study of different digital signature standards and message authentication techniques
VI. The applications of hash functions, codes and encryption and decryption keys

III. COURSE OUTCOMES:

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

CO1 Apply Security Concepts and Classical Encryption Techniques
CO2 Distinguish the working of symmetric encryption techniques
CO3 Identify the Difference between Cryptography and Cryptanalysis
CO4 Explain encryption techniques to secure data in transit across data networks
CO5 Analyze various algorithms
CO6 Apply various hash functions to generate digital signatures, message authentication codes (MACs), and key derivation functions

IV. COURSE CONTENT:

MODULE -I: INTRODUCTION (10)

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. Classical Encryption Techniques: Symmetric Cipher Model, Substitution Techniques, Transposition Techniques.

MODULE –II: SYMMETRIC KEY CRYPTOGRAPHY (10)

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: SECURITY SOFTWARE DESIGN (09)

Principles of Secure Software Development (Confidentiality, Integrity, Availability), Threat Modeling and Risk Assessment, Secure Coding Practices (Input Validation, Error Handling, Access Control), Authentication and Authorization Mechanisms, Cryptographic Techniques in Software (Encryption, Digital Signatures, Hashing),

Security Protocols and Secure Communication, Software Vulnerabilities and Mitigation (Buffer Overflow, SQL Injection, Cross-Site Scripting), Security Testing and Auditing (Static and Dynamic Analysis, Penetration Testing), Secure Software Development Life Cycle (SDLC) and Compliance Standards

MODULE-IV: STATISTICAL DATABASE PROTECTION AND INTRUSION DETECTION (09)

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: MODEL FOR PROTECTION OF NEW GENERATION DATABASE SYSTEMS (10)

Applications of Cryptographic Hash Functions, Two Simple Hash Functions, Message Authentication Requirements, Message Authentication Functions, MACs based on Hash functions: HMAC

V. TEXTBOOKS:

1. William Stallings, Cryptography and Network Security – Principles and Practice, Pearson Education, 8th Edition, 2020.
2. Atul Kahate, "Cryptography and Network Security", McGraw-Hill, 4th Edition, 2019.

3. REFERENCE BOOKS:

1. D. M. Burton, Elementary Number Theory, USA: McGraw-Hill, 7th edition, 2023.
2. Charles P1. Charles P. Pfleeger, Shari Lawrence Pfleeger, "Analyzing Computer Security", Pearson. 1st Edition, 2006.
3. C. Chou and D. Shoemaker**,** Information Assurance for the Enterprise, Tata McGraw-Hill (TMH), 1st Edition, 2006.

4. 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

VIII. MATERIAL ONLINE:

1. Course template
2. Tech-talk topics
3. Assignments
4. Definition and terminology
5. Tutorial question bank
6. Model question paper – I
7. Model question paper – II
8. Lecture notes
9. Early lecture readiness videos (ELRV)

10. Power point presentations