INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

NETWORK SECURITY AND CRYPTOGRAPHY								
VII Semester: ECE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
AECD48	**Elective**	3	-	-	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisite: VLSI Design								

I. COURSE OVERVIEW:

Understand the fundamentals of networks security, security architecture, threats and vulnerabilities & apply the different cryptographic operations of symmetric cryptographic algorithms.

II. COURSES OBJECTIVES:

The students will try to learn

1. To understand the fundamentals of network security and security architecture.
2. To learn the different symmetric key cryptographic algorithms.
3. To study the various asymmetric key cryptographic algorithms and techniques.
4. To know the importance of message authentication and integrity.
5. To learn the various security practices and system security mechanisms.

III. COURSE OUTCOMES:

At the end of this course, the students will be able to:

CO1: Understand the fundamentals of networks security, security architecture, threats and vulnerabilities
CO2: Apply the different cryptographic operations of symmetric cryptographic algorithms
CO3: Apply the different cryptographic operations of public key cryptography **CO4**: Apply the various Authentication schemes to simulate different applications. **CO5:** Understand various Security practices and System security standards

IV. COURSE CONTENT:

UNIT I: INTRODUCTION (10)
Security trends - Need for Security at Multiple levels, Security Policies, Model of network security, Security attacks, services and mechanisms, OSI security architecture, Classical encryption techniques: substitution techniques, transposition techniques, steganography

UNIT II: SYMMETRIC KEY CRYPTOGRAPHY (10)
Mathematics Of Symmetric Key Cryptography: Algebraic structures, Modular arithmetic- Euclid‟s algorithm-Congruence and matrices. Symmetric Key Ciphers: SDES, Block cipher Principles of DES, Strength of DES, Differential and linear cryptanalysis, Block cipher design principles, Block cipher mode of operation, Evaluation criteria for AES, Advanced Encryption Standard.

UNIT III: PUBLIC KEY CRYPTOGRAPHY (09)
Mathematics Of Asymmetric Key Cryptography: Primes, Primality Testing, Factorization, Euler‘s totient function, Chinese Remainder Theorem, Exponentiation and Algorithm, Asymmetric Key Ciphers:

RSA cryptosystem, Key distribution, Key management, Diffie Hellman key exchange, ElGamal cryptosystem, Elliptic curve arithmetic. Elliptic curve cryptography.

UNIT IV: RUN-TIM ENVIRONMENT AND CODE GENERTION (10)
Authentication requirement, Authentication function, MAC, Hash function, Security of hash function and MAC, SHA, Digital signature and authentication protocols, DSS- Entity Authentication: Biometrics, Passwords, Challenge Response protocols- Authentication applications.

UNIT V: SECURITY PRACTICE AND SYSTEM SECURITY (09)
Electronic Mail security, PGP IP security, Web Security System Security: Intruders, Malicious software, viruses, Firewalls

V. TEXT BOOKS:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson education 8th Edition, 2020

VI. REFERENCE BOOKS:

1. C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security,Wiley India Pvt.Ltd 1st Edition,2011
2. Behrouz A.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.
3. Wade Trappe, Lawrence C. Washington: Introduction to Cryptography with Coding Theory, 3rd Edition, 2020

VIII. MATERIALS ONLINE

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