I A R E

EDUCATION FOR LIBERATION

# INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal - 500 043, Hyderabad, Telangana

## COURSE CONTENT

### CRYPTOGRAPHY AND NETWORK SECURITY

**II Semester:** ES

| Course Code | Category | Hours / Week | | | Credits | Maximum Marks | | |
|---|---|---|---|---|---|---|---|---|
| | | L | T | P | C | CIA | SEE | Total |
| BESE21 | Elective | 3 | 0 | 0 | 3 | 40 | 60 | 100 |
| Contact Classes: 45 | Tutorial Classes: Nil | Practical Classes: Nil | | | | Total Classes: 45 | | |

**Prerequisite: Wireless Sensor Networks.**

## I. COURSE OVERVIEW:

The aim of this course is to introduce the student to the areas of cryptography and cryptanalysis. it develops a basic understanding of the algorithms used to protect users online and to understand some of the design choices behind these algorithms. The course emphasizes to give a basic understanding of previous attacks on cryptosystems with theaim of preventing future attacks. A wide variety of basic cryptographic primitives will be discussed along with recent developments in some advanced topics like identity-based encryption, attribute- based encryption, functional encryption, two-party/multi-party computation, bitcoin and crypto-currency and postquantum cryptography. The cryptanalysis part will help us understanding challenges for cybersecurity that includes network security, data security, mobile security, cloud security and endpoint security.

## II. COURSES OBJECTIVES:

**The students will try to learn**

I. About attacks, services and mechanisms, security attacks, security services, a model for internetwork security.

II. The simplified DES, block cipher principles, data encryption standard, strength of DES, differential andlinearcryptanalysis, block cipher design principles and modes of operations.

III. The IP security overview, architecture, authentication, encapsulating security payload, combining securityassociations, key management.

## III. COURSE OUTCOMES:

**At the end of the course students should be able to:**

CO1 Understand principles and practice of network security and cryptography by gaining knowledge in cryptographic algorithms;

CO2 Design basic security architectures through selection and integration of relevant security components

CO3 Make use of advanced cryptographic algorithms in network protocols and network applications.

CO4 Analyze and apply system security concept to recognize malicious code.

CO5 Understand Key management using smart cards for authentication requires the use of a PKI.

CO6 Illustrate various public key cryptographic techniques in encryption/ decryption.

## IV. COURSE CONTENT:

**MODULE – I: INTRODUCTION TO CRYPTOGRAPHY AND BLOCK CIPHERS (9)**

Introduction to security attacks, services and mechanism, introduction to cryptography, conventional Encryption conventional encryption model, classical encryption techniques, substitution ciphers and transposition ciphers, cryptanalysis, steganography, stream and block ciphers, modern block ciphers: Block ciphers principals, Shannon’s theory of confusion and diffusion, fiesta structure, data encryption standard(DES), strength of DES, differential and linear crypt analysis of DES, block cipher modes of operations, triple DES, AES.

**MODULE – II: CONFIDENTIALITY AND MODULAR ARITHMETIC (9)**

Confidentiality using conventional encryption, traffic confidentiality, key distribution, random number generation-introduction to graph, ring and field, prime and relative prime numbers, modular arithmetic, Fermat’s and Euler’s theorem, primality testing, Euclid’s algorithm, Chinese remainder theorem, discrete algorithms.

**MODULE – III: PUBLIC KEY CRYPTOGRAPHY AND AUTHENTICATION REQUIREMENTS (9)**

Principles of public key crypto systems, RSA algorithm, security of RSA, key management, Duffle-Hellman key exchange algorithm, introductory idea of Elliptic curve cryptography, Elgamel encryption, message.

Authentication and hash function: authentication requirements, authentication functions, message authentication code,hash functions, birthday attacks, security of hash functions and MACS.

**MODULE –IV: INTEGRITY CHECKS AND AUTHENTICATION ALGORITHMS (9)**

MD5 message digest algorithm, secure hash algorithm (SHA) Digital Signatures: Digital Signatures, authentication protocols, digital signature standards (DSS), proof of digital signature algorithm, authentication applications: Kerberos and X.509, directory authentication service, electronic mail security-pretty good privacy (PGP) - S/MIME.

**MODULE – V: IP SECURITY AND WEB SECURITY (9)**

**IP SECURITY: Overview**: Architecture, authentication, encapsulating security payload, combining security associations, keyManagement.

**Web security**: Web security requirements, secure sockets layer and transport layer security, secure electronictransaction.

**Intruders, viruses and worms:** Intruders, viruses and related threats.

**Fire walls:** Fire wall design principles, trusted systems.

## V. TEXT BOOKS:

1. Cryptography and Network Security: Principles and Practice, William Stallings, person education.
2. Network Security Essentials (Applications and Standards) by William Stallings Pearson education.

## VI. REFERENCE BOOKS:

1. Fundamentals of Network Security by Eric Maiwald (Dramatic press)
2. Network Security, Private Communication in a Public World by Charlie Kaufman, Radia Perlman and Miken Speicher, person/PHI.
3. Principles of Information Security, Whitman, Thomson.
4. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH.

## VII. MATERIALS ONLINE

1. Course template
2. Tutorial question bank
3. Assignments
4. Model question paper - I
5. Model question paper - II
6. Lecture notes
7. Power point presentations
8. Early Lecture Readiness Videos