## SEMESTER S8

## SECURE COMMUNICATION

| | | | |
|---|---|---|---|
| **Course Code** | **OEEVT 834** | **CIE Marks** | 40 |
| **Teaching Hours/Week (L: T:P: R)** | 3:0:0:0 | **ESE Marks** | 60 |
| **Credits** | 3 | **Exam Hours** | 2 Hrs. 30 Min. |
| **Prerequisites (if any)** | None | **Course Type** | Theory |

**Course Objectives:**

1. To understand network security services and mechanisms and the types of attacks

## SYLLABUS

| Module No. | Syllabus Description | Contact Hours |
|---|---|---|
| **1** | OSI security architecture, Security attacks – Passive attacks, Active attacks, Security services- Authentication, Access Control, Data Confidentiality, Data integrity, Nonrepudiation, Availability service. Model for network security. Symmetric cipher model, Cryptography, Crypto analysis, Substitution techniques- Hill Cipher, One time pad, Transposition Techniques | **9** |
| **2** | Finite Fields Groups, Rings and Fields, Modular arithmetic, Euclidian algorithm, Finite Fields of the form GF(p), Polynomial arithmetic | **8** |
| **3** | Block Cipher Principles – Stream Ciphers and Block Ciphers, Feistel Cipher, Feistel Decryption algorithm, The Data encryption standard, DES Decryption - Avalanche effect, The AES Cipher, substitute bytes transformation, Shift row transformation, Mix Column transformation | **9** |
| **4** | Public Key Cryptography, RSA and Key Management Principles of public key cryptosystems-Public key cryptosystems, Application for Public key cryptosystem requirements, Fermat's theorem, Euler's Totient Function, Euler's theorem, RSA algorithm, Key management, Distribution of public keys, Publicly available directory, Public key authority, public key certificates, Distribution of secret keys using public key cryptography, Public Key Encryption, Message Authentication Code, Hash function | **10** |

**Course Assessment Method**
**(CIE: 40 marks, ESE: 60 marks)**

**Continuous Internal Evaluation Marks (CIE):**

| Attendance | Assignment/ Microproject | Internal Examination-1 (Written) | Internal Examination- 2 (Written ) | Total |
|---|---|---|---|---|
| 5 | 15 | 10 | 10 | 40 |

**End Semester Examination Marks (ESE)**

*In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions*

| Part A | Part B | Total |
|---|---|---|
| • 2 Questions from each module.<br>• Total of 8 Questions, each carrying 3 marks<br>**(8x3 =24marks)** | • Each question carries 9 marks.<br>• Two questions will be given from each module, out of which 1 question should be answered.<br>• Each question can have a maximum of 3 sub divisions.<br>**(4x9 = 36 marks)** | **60** |

**Course Outcomes (COs)**

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

| Course Outcome | | Bloom's Knowledge Level (KL) |
|---|---|---|
| **CO1** | Illustrate network security services, mechanisms and the types of attacks and also to understand symmetric encryption process and different encryption techniques | **K2** |
| **CO2** | Apply the concepts of group, ring, field, modular arithmetic, Euclidean algorithm, Finite fields and polynomial arithmetic | **K3** |
| **CO3** | Outline the principles of modern symmetric ciphers like the Data Encryption Standard and Advanced Encryption Standard | **K2** |
| **CO4** | Describe the concepts of public key cryptography, RSA algorithm, key distribution and management for public key systems | **K2** |

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

**CO-PO Mapping Table (Mapping od Course Outcomes to Program Outcomes)**

| | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PO8 | PO9 | PO10 | PO11 | PO12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **CO1** | **3** | **2** | | | | | | | | | | **2** |
| **CO2** | **3** | **3** | | | | | | | | | | **2** |
| **CO3** | **3** | **2** | | | | | | | | | | **2** |
| **CO4** | **3** | **2** | | | | | | | | | | **2** |

Note: *1: Slight (Low), 2: Moderate (Medium), 3: Substantial (High), -: No Correlation*

| **Text Books** | | | | |
|---|---|---|---|---|
| **Sl. No** | **Title of the Book** | **Name of the Author/s** | **Name of the Publisher** | **Edition and Year** |
| 1 | Cryptography and Network security: principles and practice | William Stallings | Prentice Hall of India | 4th Edition, 2006 |

| **Reference Books** | | | | |
|---|---|---|---|---|
| **Sl. No** | **Title of the Book** | **Name of the Author/s** | **Name of the Publisher** | **Edition and Year** |
| 1 | Cryptography and Network security Tata McGraw-Hill, | Behrouz A. Forouzan | Tata McGraw-Hill | 2008 |
| 2 | Abstract Algebra | David S. Dummit& Richard M Foote | Wiley India Pvt. Ltd. | 2nd Edition, 2008 |
| 3 | Cryptography, Theory and Practice | Douglas A. Stinson | Chapman & Hall, CRC PressCompany, Washington | 2005 |
| 4 | Elliptic Curves: Theory and Cryptography | Lawrence C. Washington | Chapman & Hall, CRCPress Company, Washington | 2008 |

| Video Links (NPTEL, SWAYAM…) | |
|---|---|
| **Module No.** | **Link ID** |
| **1** | https://archive.nptel.ac.in/courses/106/105/106105162/ CRYPTOGRAPHY AND NETWORK SECURITY, PROF. SOURAV MUKHOPADHYAY Department of Computer Science and Engineering IIT Kharagpur |
| **2** | https://archive.nptel.ac.in/courses/106/105/106105162/ CRYPTOGRAPHY AND NETWORK SECURITY, PROF. SOURAV MUKHOPADHYAY Department of Computer Science and Engineering IIT Kharagpur |
| **3** | https://archive.nptel.ac.in/courses/106/105/106105162/ CRYPTOGRAPHY AND NETWORK SECURITY, PROF. SOURAV MUKHOPADHYAY Department of Computer Science and Engineering IIT Kharagpur |
| **4** | https://archive.nptel.ac.in/courses/106/105/106105162/ CRYPTOGRAPHY AND NETWORK SECURITY, PROF. SOURAV MUKHOPADHYAY Department of Computer Science and Engineering IIT Kharagpur |