TCET/FRM/IP-02/09

Revision: A

**Semester Plan**
**(Theory)**

**Semester**:   VII

**Course**: EXTC

**Subject**: Data Compression and Encryption (Elective: ETE 701)

**Class**: BE EXTC A & B

| S.No. | Bridge courses/Technology | Duration (Week/hrs) | Modes of Learning | Recommended Sources |
|---|---|---|---|---|
| **1.** | **Prerequisite course:** Random Signal Analysis, Analog Communication and Digital Communication (NPTEL Course) | 08 Hours | Technology Based learning | RSA : lecture 3 to 5 http://nptel.ac.in/courses/117105085/ Acom: lectures 39 to 42 http://nptel.ac.in/courses/117102059/ |

Class Room Teaching:

| Sr. No | Module No. | Lesson No. | Topics Planned (Technology to be used) | Teaching Aids Required | Planned /Completion Date | Resource Book Reference | Remarks |
|---|---|---|---|---|---|---|---|
| 1 | | L1.1 | SOP: DCE Theory | M1: Black Board & chalks M2: Projector & Laptop | 12/07/17 | All Modules | |
| 2 | | L1.2 | SOP: DCE lab | M1: Black Board & Chalks M2: Projector & Laptop | 12/07/17 | All Modules | |
| 3 | | L1.3 | SOP: DCE OBE | M1: Black Board & Chalks M2: Projector & Laptop | 12/07/17 | All Modules | |
| 4 | 1 | L1.4 | Loss less compression, Lossy compression, measure of performance, modeling and coding, different types of models, and coding techniques | M1: Black Board & Chalks M2: Projector & Laptop | 13/07/17 | Module 1 | |
| 5 | 1 | L1.5 | Huffman and Minimum variance Huffman coding, | M1: Black Board & Chalks M2: Projector & Laptop | 14/07/17 | Module 1 | |

| | | | | M1: Black Board & Chalks M2: Projector & Laptop | | | |
|---|---|---|---|---|---|---|---|
| 6 | 1 | L3.1 | Extended Huffman coding, | M1: Black Board & Chalks M2: Projector & Laptop | 14/07/17 | Module 1 | |
| 7 | 1 | L3.2 | Adaptive Huffman coding. | M1: Black Board & Chalks M2: Projector & Laptop | 17/07/17 | Module 1 | |
| 8 | 1 | L3.3 | Arithmetic coding. | M1: Black Board & Chalks M2: Projector & Laptop | 19/07/17 | Module 1 | |
| 9 | 1 | L3.4 | Dictionary coding techniques ,LZ 77 and LZ 78 | M1: Black Board & Chalks M2: Projector & Laptop | 20/07/17 | Module 1 | |
| 10 | 1 | L4.1 | Dictionary coding techniques LZW | M1: Black Board & Chalks M2: Projector & Laptop | 26/07/17 | Module 1 | |
| 11 | 2 | L4.2 | High quality digital audio, frequency and temporal masking. | M1: Black Board & Chalks M2: Projector & Laptop | 26/07/17 | Module 2 | Topics are small can be covered in 1 lecture |
| 12 | 2 | L4.3 | Lossy sound compression, $\mu$-law and A-law companding | M1: Black Board & Chalks M2: Projector & Laptop | 27/07/17 | Module 2 | Topics are small can be covered in 1 lecture |
| 13 | 2 | L4.4 | MP3 audio standard | M1: Black Board & Chalks M2: Projector & Laptop | 28/07/17 | Module 2 | Topics are small can be covered in 1 lecture |
| 14 | 3 | L5.1 | Image compression using PCM and DPCM | M1: Black Board & Chalks M2: Projector & Laptop | 3/08/17 | Module 3 | |
| 15 | 3 | L5.2 | Image transform | M1: Black Board & Chalks M2: Projector & Laptop | 3/08/17 | Module 3 | |
| 16 | 3 | L5.3 | JPEG standard | M1: Black Board & Chalks M2: Projector & Laptop | 4/08/17 | Module 3 | |
| 17 | 3 | L6.1 | JPEG –LS and JPEG 2000 standard | M1: Black Board & Chalks M2: Projector & Laptop | 5/08/17 | Module 3 | |

| 18 | 3 | L7.1 | JPEG –LS and JPEG 2000 standard | M1: Black Board & Chalks  M2: Projector & Laptop | 9/08/17 | Module 3 | |
|---|---|---|---|---|---|---|---|
| 19 | 3 | L7.2 | Concepts of video compression: Intra frame coding | M1: Black Board & Chalks  M2: Projector & Laptop | 9/08/17 | Module 3 | |
| 20 | 3 | L7.3 | Concepts of video compression: Motion estimation and compensation | M1: Black Board & Chalks  M2: Projector & Laptop | 10/08/17 | Module 3 | |
| 21 | 3 | L7.4 | Introduction to MPEG - 2  standard | M1: Black Board & Chalks  M2: Projector & Laptop | 11/08/17 | Module 3 | |
| 22 | 3 | L8.1 | H-264 encoder and decoder | M1: Black Board & Chalks  M2: Projector & Laptop | 16/08/17 | Module 3 | |
| 23 | 4 | L8.2 | Security goals, Cryptography, stenography | M1: Black Board & Chalks  M2: Projector & Laptop | 16/08/17 | Module 4 | Topics are small can be covered in 1 lecture |
| 24 | 4 | L8.3 | Cryptographic attacks, services and mechanics. | M1: Black Board & Chalks  M2: Projector & Laptop | 18/08/17 | Module 4 | |
| 25 | 4 | L8.4 | Integer arithmetic and modular arithmetic | M1: Black Board & Chalks  M2: Projector & Laptop | 24/08/17 | Module 4 | |
| 26 | 4 | L9.1 | Linear congruence | M1: Black Board & Chalks  M2: Projector & Laptop | 30/08/17 | Module 4 | Topics are small can be covered in 1 lecture |
| 27 | 4 | L9.2 | Substitution cipher, transposition cipher and stream cipher | M1: Black Board & Chalks  M2: Projector & Laptop | 30/08/17 | Module 4 | |
| 28 | 4 | L9.3 | Block cipher, and arithmetic modes for block ciphers , Data encryption standard | M1: Black Board & Chalks  M2: Projector & Laptop | 31/08/17 | Module 4 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 29 | 4 | L9.4 | Block cipher, and arithmetic modes for block ciphers , Data encryption standard | M1: Black Board & Chalks M2: Projector & Laptop | 01/09/17 | Module 4 | |
| 30 | 4 | L10.1 | Double DES, triple DES, attacks on DES | M1: Black Board & Chalks M2: Projector & Laptop | 06/09/17 | Module 4 | |
| 31 | 4 | L10.2 | AES and key distribution center. | M1: Black Board & Chalks M2: Projector & Laptop | 06/09/17 | Module 4 | |
| 32 | 5 | L10.3 | Primes, factorization, Fermat's little theorem, | M1: Black Board & Chalks M2: Projector & Laptop | 07/09/17 | Module 5 | |
| 33 | 5 | L10.4 | Euler's theorem | M1: Black Board & Chalks M2: Projector & Laptop | 08/09/17 | Module 5 | Topics are small can be covered in 1 lecture |
| 34 | 5 | L11.1 | Extended Euclidean algorithm | M1: Black Board & Chalks M2: Projector & Laptop | 13/09/17 | Module 5 | |
| 35 | 5 | L11.2 | RSA, attacks on RSA | M1: Black Board & Chalks M2: Projector & Laptop | 13/09/17 | Module 5 | |
| 36 | 5 | L11.3 | Diffie Hellman key exchange and key management, | M1: Black Board & Chalks M2: Projector & Laptop | 14/09/17 | Module 5 | |
| 37 | 5 | L11.4 | Basics of elliptical curve cryptography | M1: Black Board & Chalks M2: Projector & Laptop | 15/09/17 | Module 5 | |
| 38 | 5 | L12.1 | Message integrity, message authentication. | M1: Black Board & Chalks M2: Projector & Laptop | 20/09/17 | Module 5 | |
| 39 | 5 | L12.2 | MAC, hash function, H MAC | M1: Black Board & Chalks M2: Projector & Laptop | 20/09/17 | Module 5 | |

| 40 | 5 | L12.3 | Digital signature algorithm | M1: Black Board & Chalks M2: Projector & Laptop | 21/09/17 | Module 5 | |
|---|---|---|---|---|---|---|---|
| 41 | 6 | L12.4 | Malware, Intruders and Intrusion detection system | M1: Black Board & Chalks M2: Projector & Laptop | 22/09/17 | Module 6 | |
| 42 | 6 | L13.1 | firewall design, antivirus and techniques | M1: Black Board & Chalks M2: Projector & Laptop | 04/10/17 | Module 6 | |
| 43 | 6 | L13.2 | Digital Immune systems and biometric authentication. | M1: Black Board & Chalks M2: Projector & Laptop | 04/10/17 | Module 6 | |
| 44 | 6 | L14.1 | Ethical hacking. | M1: Black Board & Chalks M2: Projector & Laptop | 05/10/17 | Module 6 | Topics are small can be covered in 1 lecture |
| 45 | All Modules | L14.2 | University paper and doubt solving session | M1: Black Board & Chalks M2: Projector & Laptop | 06/10/17 | Module 6 | |
| Remark:: Course: | | Syllabus Coverage: | | | Practice Session: | | Beyond Syllabus: |
| No. of (lectures planned)/(lecture taken): 45 | | | | | | | |

**Bridge Course:**

| **Bridge courses Objective:** Bridging of gaps with respect to prerequisites and industry skills or to carryout research in data compression, encryption field**. ( 20 Hrs / Semester / student)** | | | | |
|---|---|---|---|---|
| **S.No.** | **Bridge courses/Technology** | **Duration (Week/hrs)** | **Modes of Learning** | **Recommended Sources** |
| **1** | **Advanced course:** Cryptography and network security | 20 Hours | Technology Based learning | http://nptel.ac.in/courses/106105031/ |

**Text Books:**

1. Khalid Sayood, ― *Introduction to Data Compression*‖ ,Morgan Kaufmann, 2000
2. David Saloman, ―*Data Compression: The complete reference*‖ , Springer publication
3. Behrous Forouzen, ―*Cryptography and Network Security*‖, Tata Mc Graw –Hill Education 2011

**Reference Books:**

4. Berard Menezes, ―*Network Security and Cryptography*‖, learning publication Cengage
**5.** William Stallings, ―*Cryptography and Network Security*‖, Pearson Education Asia Publication, 5th
 edition

**Digital Reference:**

1. http://nptel.ac.in/courses/106102064/19
2. ube.ege.edu.tr/~dalkilic/courses/ube528/emailsecurityStallings5.ppt
3. https://www.elsevier.com/.../introduction-to-data-compression/sayood/978-0-12-6208..

|  |  |  |
|---|---|---|
| **SD** | **SD** | **SD** |
| **Ms. Kalawati Patil** | **Dr. Vinitkumar Dongre** | **Dr. R. R. Sedamkar** |
| Name & Signature of Faculty | Signature of HOD | Signature of Dean Academic |
| Date:14/07/2017 | Date: 14/07/2017 | Date: 14/07/2017 |

**M1: Lecture interspersed with discussions**
**M2: Lecture with visual annotations**
**Note:**
1. Plan date and completion date should be in compliance
2. Courses are required to be taught with emphasis on resource book, course file, text books, reference books, digital references etc.
3. Planning is to be done for 15 weeks where 1st week will be AOP, 2nd -13th for effective teaching and 14th -15th week for effective university examination oriented teaching, mock practice session and semester consolidation.
4. According to university syllabus where lecture of 4 hrs/per week is mentioned minimum 55 hrs and in case of 3 lectures per week minimum 45 lectures are to be engaged are required to be engaged during the semester and therefore accordingly semester planning for delivery of theory lectures shall be planned.
5. In order to improve score in NBA, faculty members are also required to focus course teaching beyond university prescribed syllabus and measuring the outcomes w.r.t learning course and programme objectives.
6. Text books and reference books are available in syllabus. Here only additional references w.r.t. non –digital/ digital sources can be written (if applicable)
7. Technology to be used in class room during lecture shall be written below the topic planned within the bracket.