| Course Code | Course Title | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 116h55C301 | Applied Cryptography | | | | | | | |
| | TH | | P | | | TUT | | Total |
| Teaching Scheme(Hrs.) | 03 | | -- | | | -- | | 03 |
| Credits Assigned | 03 | | -- | | | -- | | 03 |
| Examination Scheme | Marks | | | | | | | |
| | CA | | ESE | TW | O | P | P&O | Total |
| | ISE | IA | | | | | | |
| | 30 | 20 | 50 | -- | -- | -- | -- | 100 |

**Course prerequisites (if any):**
Some mathematical maturity, in terms of understanding and working with mathematical definitions, concepts, and proofs, and elementary notions of logic, set theory, number theory, probability and statistics;

**Course Objectives**
In the era of Digital Computers and internet ensuring confidentiality, authentication, integrity of data during communication is very critical. This course impart students the knowledge of cryptographic algorithms and techniques to achieve same. It also introduces students to the advances in the area of cryptography

**Course Outcomes**
**At the end of successful completion of the course the student will be able to**

| | |
|---|---|
| **CO1** | Explain fundamentals of Information Security and cryptography |
| **CO2** | Demonstrate various Cryptographic Algorithms for securing systems |
| **CO3** | Comprehend cryptographic hash functions, Message Authentication Codes and Digital Signatures for Authentication |
| **CO4** | Realize advances in the field of cryptography |

| Module No. | Unit No. | Details | Hrs. | CO |
|---|---|---|---|---|
| 1 | **Introduction to Information Security & Cryptography** | | 05 | CO 1 |
| | 1.1 | Information Security and its goals, Vulnerability Threats and Attacks | | |
| | 1.2 | Encryption and Decryption, Symmetric and Asymmetric Key Cryptography, Cryptanalysis | | |
| | 1.3 | Substitution Techniques, Transposition Techniques | | |
| 2 | **Symmetric Key Cryptography** | | 09 | CO2 |
| | 2.1 | DES Structure, DES Analysis: Properties, Design Criteria, DES Weaknesses, DES Security, Multiple DES, 3DES | | |
| | 2.2 | AES Structure, Key Expansion, Analysis of AES: Security, Implementation, Simplicity and Cost | | |
| | | IDEA, RC4 | | |
| | | **#Self Learning - RC5, Block Cipher Modes** | | |
| 3 | **Asymmetric Key Cryptography** | | 10 | CO3 |
| | 3.1 | Public key cryptography: Principles of public key cryptosystems, The RSA algorithm, attacks on RSA | | |
| | 3.2 | Key management: Diffie Hellman Key exchange, Man-in Middle attack | | |
| | 3.3 | Elliptic Curve Cryptography: Elliptic curves, The Addition Law, Elliptic curve Mod p, Factoring with Elliptic Curves, Elliptic Curve Cryptosystems | | |
| | | **#Self Learning : Rabin Cryptosystem** | | |
| 4 | **Message Authentication and Digital Signatures** | | 11 | CO3 |
| | 4.1 | Message Authentication Approaches. Hash Function, Cryptographic Hash Function Requirements, Cryptographic Hash Function Security, Cryptographic Hash Function Structure, SHA, HMAC, MD5. | | |
| | 4.2 | Using Symmetric Encryption for Message Authentication, Message Authentication Code (MAC), Digital Authentication Algorithm (DAA) | | |
| | 4.3 | Using Public Key for Authentication, Digital Signatures, Properties of Digital Signatures beyond Message Authentication, DSS, Authentication Applications: Kerberos, X.509 Authentication Service | | |
| | | **#Self Learning : RSA and Schnorr Digital Signature** | | |
| 5 | **Introduction to Advances in Cryptography** | | 10 | CO4 |
| | 5.1 | Quantum Cryptography, Quantum key distribution-QKD | | |
| | 5.2 | Homomorphic Encryption | | |
| | 5.3 | Secure Multi-Party Computation (MPC) In particular, Zero-Knowledge Proofs | | |
| | 5.4 | Cryptographic Obfuscation | | |
| | | **Total** | 45 | |

**# Students should prepare all Self Learning topics on their own. Self-learning topics will enable students to gain extended knowledge of the topic. Assessment of these topics may be included in IA and Laboratory Experiments.**

## Recommended Books:

| Sr. No. | Name/s of Author/s | Title of Book | Name of Publisher with country | Edition and Year of Publication |
|---|---|---|---|---|
| 1. | Behrouz A. Forouzan | Cryptography and Network Security | Mc Graw Hill | 3rd Edition, 2017 |
| 2. | William Stallings | Computer Security Principles and Practice | Pearson Education | 2016. 5th Edition |
| 3. | Mark stamp | Information Security Principal and Practice | Wiley | 2008, 3rd Edition |
| 4. | Bruce Schneier | Applied Cryptography | Wiley | 2015, Second Edition |
| 5. | Jaydip Sen | Theory and practice of cryptography and network security protocols and technologies | Intech Publishers, Croatia, Europe | 2013. First Edition |
| 6. | Oded Goldreich | Foundations of Cryptography – A Primer | Foundations and Trends® in Theoretical Computer Science: Vol. 1: No. 1, pp 1-116 | 2005 |

<table>
<tr><th>Course Code</th><th colspan="8">Course Title</th></tr>
<tr><td>116h55L301</td><td colspan="8">Applied Cryptography</td></tr>
<tr><td></td><td colspan="3">TH</td><td colspan="2">P</td><td colspan="2">TUT</td><td>Total</td></tr>
<tr><td>Teaching Scheme(Hrs.)</td><td colspan="3">-</td><td colspan="2">02</td><td colspan="2">--</td><td>02</td></tr>
<tr><td>Credits Assigned</td><td colspan="3">-</td><td colspan="2">01</td><td colspan="2">--</td><td>01</td></tr>
<tr><td rowspan="3">Examination Scheme</td><td colspan="8">Marks</td></tr>
<tr><td colspan="2">CA</td><td rowspan="2">ESE</td><td rowspan="2">TW</td><td rowspan="2">O</td><td rowspan="2">P</td><td rowspan="2">P&O</td><td rowspan="2">Total</td></tr>
<tr><td>ISE</td><td>IA</td></tr>
<tr><td>-</td><td>-</td><td>-</td><td>25</td><td>25</td><td>--</td><td>--</td><td>50</td></tr>
</table>

**Term-Work:**

Term work will consist of experiments/ tutorials covering entire syllabus of the course ‘Applied Cryptography’. Students will be graded based on continuous assessment of their term work.