**Subject Code:** 01CY0201

**Subject Name: Theory of Modern Cryptography**

**MTech Year – 1 (Semester – 2)**

**Objective:** This course is designed to understand the concept of cryptography and cryptanalysis. Mathematics behind cryptography. To understand Encryption and Decryption algorithms.

**Credits Earned:** 4 Credits

**Course Outcomes:** After completion of this course, student will be able to

* Understand basic encryption methods and algorithms, he strengths and
* Understand encryption key exchange and management
* Understand how to deploy encryption techniques to secure data stored on computer systems.
* Understand how to deploy encryption techniques to secure data in transit

**Pre-requisite of course:** Cryptography, Network Security

**Teaching and Examination Scheme**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Teaching Scheme (Hours) | Credits | Theory Marks | Tutorial/ Practical Marks | Total Marks |
| Theory | Tutorial  | Practical | ESE (E) | Mid Sem (M) | Internal (I) | Viva (V) | Term work (TW) |
| 3 | 0 | 2 | 4 | 50 | 30 | 20 | 25 | 25 | 150 |

**Contents:**

|  |  |  |
| --- | --- | --- |
| **Unit** | **Topics** | **Contact Hours** |
| 1 | Introduction to Cryptography, Classical Cryptosystem, Understanding the term like Plaintext-Ciphertext-Cryptology-Cryptanalysis- Symmetric key- Asymmetric key, Conventional Encryption, Caesar Cipher, Substitution Cipher, Vigenere Cipher, Transposition/Permutation Cipher, Frequency Analysis, Play Fair Cipher, Block Cipher | 6 |
| 2 | Data Encryption Standard (DES), Triple DES and Modes of operation, Stream Cipher, Pseudorandom Sequence, LFSR based Stream Cipher, Mathematical Background, Abstract Algebra, Number theory. | 9 |
| 3 | Modular Inverse, Extended Euclid Algorithm, Fermat’s Little Theorem, Eular Phi-Function, Eular’s theorem, Quadratic Residue, Polynomial  Arithmetic, Advanced Encryption Standard (AES), Public Key Cryptosystem, Diffie-Hellman Key Exchange, Knapsack Cryptosystem, RSA Cryptosystem. Primarily Testing, ElGamal Cryptosystem, Elliptic Curve over the Reals, Elliptic curve Modulo a Prime. | 9 |
| 4 | Generalised ElGamal Public Key Cryptosystem, Chinese Remainder Theorem, Rabin Cryptosystem, Legendre and Jacobi Symbol. Message Authentication, Digital Signature, Key Management, Key Exchange, Hash Function. Universal Hashing, Cryptographic Hash Function, Secure Hash Algorithm (SHA), Digital Signature Standard (DSS), More on Key Exchange Protocol.    | 9 |
| 5 | Cryptanalysis, Time-Memory Trade-off Attack, Differential Cryptanalysis, More on Differential Cryptanalysis, Linear Cryptanalysis. Cryptanalysis on Stream Cipher, Algebraic Attack, Implementation Attacks, side channel attack. Internetwork Security, SSL, PGP, Cloud Security, Introduction to Blockchain and Bitcoin. | 9 |
|  | **Total Hours** | **42** |

**References:**

1. William Stallings, “*Cryptography and Network Security*”, 3rd Edition, Pearson

Education, 2003.

1. Bruce Schneier, “*Applied Cryptography: Protocols, Algorithms, and Source*

*Code in C*” , John Wiley & Sons, Inc, 2nd Edition, 1996.

1. Wenbo Mao, “*Modern Cryptography Theory and Practice*”, Pearson

Education, 2004

1. AtulKahate, “*Cryptography and Network Security*”, Tata McGrew Hill, 2003.
2. Bernard Menezes, “Network Security and Cryptography”, Cengage Learning, New Delhi, 2010.
3. Douglas R. Stinson, “Cryptography: Theory and Practice”

**Suggested Theory distribution:**

The suggested theory distribution as per Bloom’s taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

|  |  |  |
| --- | --- | --- |
|  | Distribution of Theory for course delivery and evaluation |  |
| Remember | Understand | Apply | Analyze | Evaluate | Create |
| 20% | 20% | 30% | 15% | 10% | 5% |

**Suggested List of Experiments:**

1. Installing OpenSSL
2. Encryption using different classical ciphers and modes
3. Implement DES and AES ciphers.
4. Encryption Mode – ECB vs. CBC
5. Encryption Mode – Corrupted Cipher Text
6. Create a text file that is at least 64 bytes long.
7. Encrypt the file using the AES-128 cipher.
8. Unfortunately, a single bit of the 30th byte in the encrypted file got corrupted. You can achieve this corruption using a hex editor.
9. Decrypt the corrupted file (encrypted) using the correct key

**6.** Lab exercise on RSA Timing Attacks

7. Programming using the Crypto Library

**Instructional Method:**

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory.
5. Supplementary Resources:
	1. <http://nptel.ac.in/courses/108108076/>
	2. <http://nptel.ac.in/downloads/108105053/>
	3. [http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-](http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-002-circuits-and-electronics-spring-2007/video-lectures/)

002-circuits-and-electronics-spring-2007/video-lectures/

* 1. https://www.facstaff.bucknell.edu/mastascu/eLessonsHTML/EEIndex.html
	2. <http://www.electrical4u.com/nature-of-electricity/>
	3. <http://vlab.amrita.edu/index.php>