# GUJARAT TECHNOLOGICAL UNIVERSITY

**Program Name: Engineering**

**Level: Postgraduate**

**Branch: Computer Engineering (Cybersecurity**

**Course / Subject Code : ME01059071**

**Course / Subject Name : Cryptography in Cyber security: Principles and Practices**

| | |
|---|---|
| w. e. f. Academic Year: | 2024-25 |
| Semester: | I |
| Category of the Course: | Program Elective Course-02 |

| | |
|---|---|
| **Prerequisite:** | • Basic concepts of cryptography and cyber security. |
| **Rationale:** | • The subject covers various aspects related to Cyber Security based on Cryptographic techniques.<br>• The subject also covers the various applications of cryptography for cyber security and prevention of attacks. |

**Course Outcome:**

After Completion of the Course, Student will able to:

| No | Course Outcomes | RBT Level |
|---|---|---|
| 01 | Understand the concept of Cryptography for Cybersecurity along with various types of attacks on the network. | UN |
| 02 | Differentiate various types of symmetric and asymmetric key cryptography techniques for encryption and decryption. | AP |
| 03 | Apply hash based techniques for secure authentication and data protection. | AP |
| 04 | Analyses Digital Signature and other authentication techniques for user authentication. | AN |
| 05 | Evaluate the network security and web security based on various cryptographic algorithms. | EL |

**Revised Bloom's Taxonomy (RBT)*

**Teaching and Examination Scheme:**

| Teaching Scheme (in Hours) | | | Total Credits L+T+ (PR/2) | Assessment Pattern and Marks | | | | Total Marks |
|---|---|---|---|---|---|---|---|---|
| | | | | Theory | | Tutorial / Practical | | |
| L | T | PR | C | ESE (E) | PA / CA (M) | PA/CA (I) | ESE (V) | |
| 3 | 0 | 2 | 4 | 70 | 30 | 20 | 30 | 150 |

# GUJARAT TECHNOLOGICAL UNIVERSITY

**Program Name: Engineering**

**Level: Postgraduate**

**Branch: Computer Engineering (Cybersecurity**

**Course / Subject Code : ME01059071**

**Course / Subject Name : Cryptography in Cyber security: Principles and Practices**

**Course Content:**

| Unit No. | Content | No. of Hours | % of Weightage |
|---|---|---|---|
| 1. | **Unit-I: Introduction to cryptography:** Symmetric Cipher Model, Cryptography, Cryptanalysis; Substitution and Transposition techniques. Stream ciphers and block ciphers, Block Cipher structure, Data Encryption Standard (DES) with an example, the strength of DES, Design principles of block cipher, AES with structure, its transformation Functions, key expansion, example and implementation. | 8 | 20 |
| 2. | **Unit-II: Cryptosystems:** MD5, Secure Hash Algorithm (SHA), HMAC, Message Authentication Codes, its requirements and security, MACs based on Hash Functions, Macs based on Block Ciphers, Cryptographic Protocols like SSL and PGP, Digital Signature and Digital Certificate, X.509 certificates, public key infrastructure. | 8 | 20 |
| 3. | **Unit-III: Introduction to Web Security:** Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET), Intruders, Viruses and related threats. Firewall Design principles, Trusted Systems, MIME | 6 | 20 |
| 4. | **Unit-IV: Cryptographic Attacks and Cryptanalysis:** Brute Force Attack, Dictionary Attack, Rainbow Table Attack, Man-in-Middle attack, Collision Attack, and Pre-image Attack, The concept of Cryptanalysis with case study | 8 | 20 |
| 5. | **Unit-V: Advanced Tools from Modern Cryptography:** Secure Multi-Party Computation, Functional Encryption, (Full) Homomorphic, Private Information Retrieval, Oblivious RAM, Symmetric Searchable Encryption, Oblivious RAM. | 6 | 10 |
| 6. | **Unit-VI: Future Trends:** Latest development in the field of Modern Cryptography for cyber security, threat prevention and privacy preservation. | 4 | 10 |
| | **Total** | | 100 |

**Suggested Specification Table with Marks (Theory):**

| Distribution of Theory Marks (in %) | | | | | |
|---|---|---|---|---|---|
| **R Level** | **U Level** | **A Level** | **N Level** | **E Level** | **C Level** |
| - | 20 | 40 | 20 | 20 | - |

*Where R: Remember; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create (as per Revised Bloom's Taxonomy)*

**References/Suggested Learning Resources:**

**(a) Books:**

1. Cryptography And Network Security, Principles And Practice Sixth Edition, William Stallings, Pearson
2. Ronald Cramer, Ivan Bjerre, Jesper Buus "Secure Multiparty Computation and Secret Sharing", Cambridge University Press, 2015
3. Information Security Principles and Practice By Mark Stamp, Willy India Edition
4. Cryptography & Network Security, Forouzan, Mukhopadhyay, McGraw-Hill
5. Cryptography and Network Security Atul Kahate, TMH
6. Cryptography and Security, C K Shyamala, N Harini, T R Padmanabhan, Wiley-India
7. Information Systems Security, Godbole, Wiley-India

**(b) Open source software and website:**

- Bitlocker, DiskCryptor, LUKS, Calculator, FTK, SIFT, Eraser, AVG Shredder, CCleaner, Steg, Our Secret, OpenPuff

**Suggested Course Practical List:**

- The practical work will be carried out based on the content covered during the academic sessions.

**List of Laboratory/Learning Resources Required:**

**Suggested Project List:**

**Suggested Activities for Students: If any**

**Any Other:**

* * * * * * *