# Faculty of Computer Science & Applications
## Master of Computer Application with Cyber Security
## (W. E. F.: 2023-24)

Document ID: SUTEFCAM-01

| | | |
|---|---|---|
| **Name of Faculty** | : | Faculty of Computer Science & Applications |
| **Name of Program** | : | Master of Computer Application with Cyber Security |
| **Course Code** | : | 2MCY03 |
| **Course Title** | : | Computer Cryptography & Network Security |
| **Type of Course** | : | Professional core |
| **Year of Introduction** | : | 2023-24 |

| | | |
|---|---|---|
| **Prerequisite** | : | Programming Languages, statistics and mathematics, Graph and most importantly zeal to learn |
| **Course Objective** | 1 | To understand basics of Cryptography and Network Security. |
| | 2 | To be able to secure a message over insecure channel by various means. |
| | 3 | To learn about how to maintain the Confidentiality. |
| | 4 | To understand various protocols for network security to protect against the threats in the networks |
| **Course Outcomes** | : | After learning the course the students will be able to: |
| | CO1 | Provide security of the data over the network. |
| | CO2 | Do research in the emerging areas of cryptography and network security. |
| | CO3 | Implement various networking protocols. |
| | CO4 | Protect any network from the threats in the world. |

**Teaching and Examination Scheme**

| **Teaching Scheme (Contact Hours)** | | | **Credits** | **Examination Marks** | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | **Theory Marks** | | **Practical Marks** | | **Total Marks** |
| **L** | **T** | **P** | **C** | **SEE** | **CIA** | **SEE** | **CIA** | |
| 2 | 0 | 2 | 3 | 70 | 30 | 30 | 20 | 150 |

*Legends: **L**-Lecture; **T**–Tutorial/Teacher Guided Theory Practice; **P**– Practical ,**C** – Credit, **SEE** – Semester End Examination, **CIA** - Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations /MCQ Tests, etc.))*

**Course Content**

| Unit No. | Topics | Teaching Hours | Weightage | Mapping with CO |
|---|---|---|---|---|
| 1 | **Introduction to Cryptography and Block Ciphers:** Introduction to security attacks - services and mechanism - introduction to cryptography - Conventional Encryption: Conventional encryption model - classical encryption techniques - substitution ciphers and transposition ciphers – cryptanalysis – steganography - stream and block ciphers - Modern Block Ciphers: Block ciphers principals - Shannon's theory of confusion and diffusion - fiestal structure - data encryption standard(DES) - strength of DES – differential and linearcrypt analysis of DES - block cipher modes of operations - triple DES – AES. | 07 | 20% | CO1 |

| | | | | |
|---|---|---|---|---|
| 2 | **Confidentiality and Modular Arithmetic:** Confidentiality using conventional encryption - traffic confidentiality - key distribution – random number generation - Introduction to graph - ring and field - prime and relative prime numbers - modular arithmetic - Fermat's and Euler's theorem - primality testing - Euclid's Algorithm - Chinese Remainder theorem - discrete algorithms. | 07 | 20% | CO2 |
| 3 | **Public key cryptography and Authentication requirements:** Principles of public key crypto systems - RSA algorithm - security of RSA - key management – Diffle-Hellman key exchange algorithm introductory idea of Elliptic curve cryptography - Elgamel encryption - Message Authentication and Hash Function: Authentication requirements - authentication functions - message authentication code - hash functions - birthday attacks – security of hash functions and MACS. | 07 | 20% | CO2 |
| 4 | **Integrity checks and Authentication algorithms:** MD5 message digest algorithm - Secure hash algorithm (SHA) Digital Signatures: Digital Signatures - authentication protocols - digital signature standards (DSS) - proof of digital signature algorithm - Authentication Applications: Kerberos and X.509 - directory authentication service - electronic mail security-pretty good privacy (PGP) - S/MIME. | 08 | 20% | CO3 |
| 5 | **IP Security and Key Management:** IP Security: Architecture - Authentication header - Encapsulating security payloads – combining security associations - key management.<br>**Web and System Security:** Web Security: Secure socket layer and transport layer security - secure electronic transaction (SET) - System Security: Intruders - Viruses and related threads - firewall design principals – trusted systems. | 07 | 20% | CO4 |

| **Suggested Distribution of Theory Marks Using Bloom's Taxonomy** | | | | | | |
|---|---|---|---|---|---|---|
| **Level** | Remembrance | Understanding | Application | Analyse | Evaluate | Create |
| **Weightage** | **20** | **30** | **30** | **20** | **0** | **0** |

*NOTE: This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.*

### Suggested List of Experiments/Tutorials

| Sr. No. | Name of Experiment/Tutorial | Teaching Hours |
|---|---|---|
| 1 | Write a C program that contains a string (char pointer) with a value \Hello World'.The programs should XOR each character in this string with 0 and display the result. | 01 |
| 2 | Write a C program that contains a string (char pointer) with a value \Hello World'. The program should AND or and XOR each character in this string with 127 and display the result. | 01 |
| 3 | Write a Java program to perform encryption and decryption using the following algorithms:<br>a. Ceaser Cipher<br>b. Substitution Cipher<br>c. Hill Cipher | 02 |
| 4 | Write a Java program to implement the DES algorithm logic. | 01 |
| 5 | Write a C/JAVA program to implement the Blowfish algorithm logic. | 01 |
| 6 | Write a C/JAVA program to implement the Rijndael algorithm logic. | 01 |
| 7 | Write the RC4 logic in Java Using Java Cryptography, encrypt the text "Hello world" using Blowfish. Create your own key using Java key tool. | 02 |
| 8 | Write a Java program to implement RSA Algorithm. | 01 |
| 9 | Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript. | 01 |
| 10 | Calculate the message digest of a text using the SHA-1 algorithm in JAVA. | 01 |

### Major Equipment/ Instruments and Software Required

| Sr. No. | Name of Major Equipment/ Instruments and Software |
|---|---|
| 1 | C/JAVA, Ubuntu. |
| 2 | I3/ I5 processor; 8GB RAM; 250GB HDD |

### Suggested Learning Websites

| Sr. No. | Name of Website |
|---|---|
| 1 | http://nptel.ac.in/courses/106105031/lecture by Dr. Debdeep Mukhopadhyay IIT Kharagpur |
| 2 | https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-033-computer-system-engineering-spring-2009/video-lectures/ lecture by Prof. Robert Morrisand Prof. Samuel Madden MIT. |

### Reference Books

| Sr. No. | Name of Reference Books |
|---|---|
| 1 | W. Mao, "Modern Cryptography – Theory and Practice", Pearson Education. |
| 2 | Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing – Prentice Hall of India. |