# SILVER OAK UNIVERSITY

**School of Technology, Design and Computer Application**
**Silver Oak College of Computer Application**
**Department of Computer Application**
**Master of Science Cyber Security & Digital Forensics**
**Course Name: Cryptography and Basics of MSF**
**Course Code: 1040147103**
**Semester: 1st**

**Prerequisite:** Fundamentals of Cipher,Public key and Private key,Basics working of Bitcoins,Hashing types and techniques.

**Course Objective:** The objective of studying Cryptography is to understand cryptographic principles, algorithms, and techniques for securing information and communications. Similarly, the objective of learning the Basics of MSF is to gain proficiency in Microsoft's operating systems, software development frameworks, and application development tools.

**Teaching Scheme:**

| Teaching Scheme | | | | |
|---|---|---|---|---|
| L | T | P | Contact Hours | Credit |
| 3 | 1 | 0 | 4 | 4 |

**Content:**

| Unit No. | Course Contents | Teaching Hours | % Weightage |
|---|---|---|---|
| 1 | **Classical Ciphers:** Caesar Cipher, Vigenère Cipher, Rail-fence Cipher, Row Transposition Cipher, Requirement and Basic Properties, Main Challenges (Confidentiality, Integrity, Availability, Non-Repudiation), Secret Key Cryptography, Data Encryption Standard (Symmetric Ciphers: Stream Cipher & Block Cipher), Advanced Encryption Standard (AES), Triple DES, Blowfish, RC4, RC5/RC6 family. | 10 | 24 |
| 2 | **Public Key Cryptography:** Principles of public key cryptosystems, The RSA algorithm, Key management, Diffie-Hellman Key exchange, Elgamal Algorithm, Polynomial Arithmetic, Elliptic curve arithmetic, Elliptic curve cryptography, Cryptanalysis. | 8 | 18 |
| 3 | **Bitcoins & Blockchain:** Bitcoin introduction, Working of Bitcoin, Blockchain crucial to Bitcoin, Blockchain operation with bitcoins, Bitcoin glossary, Bitcoin wallets, Setup for Bitcoin payments, Bitcoin mining. | 10 | 24 |

| | | | |
|---|---|---|---|
| 4 | **Message authentication code and Hash Functions:** Message authentication code authentication functions, Hash Functions including MD5 and Secure Hash Algorithm, Digital Signatures encompassing Authentication Protocols and Digital Signature Standard, Digital Certificates, and Public Key Infrastructure. | 10 | 24 |
| 5 | **Industrial Cryptographic:** Secure Communication Protocols, Data Encryption for Industrial Data, Integrity Verification Mechanisms, Secure Key Management Practices, Secure Remote Access and Authentication, Cryptographic Agility and Compliance, Secure Firmware and Software Updates. | 4 | 10 |

**Course Outcomes:**

| Sr. No. | CO-Statement | Unit No |
|---|---|---|
| CO-1 | Utilize classical ciphers for encryption, applying cryptographic principles practically. | 1 |
| CO-2 | Understand public key cryptography principles demonstrating clear comprehension. | 2 |
| CO-3 | Evaluate the role and functionality of blockchain technology in Bitcoin transactions, assessing its effectiveness and implications. | 3 |
| CO-4 | Demonstrate mastery in implementing message authentication codes and hash functions | 4 |
| CO-5 | Able to design, implement, and maintain secure cryptographic solutions tailored to the specific security needs of industrial systems. | 5 |

**Teaching & Learning Methodology: -**

1. The course includes a laboratory, where students have an opportunity to build an appreciation for the concepts being taught in lectures.
2. Projector and Computer
3. Experiments shall be performed in the laboratory related to course contents

**List of Tutorials:** **Total Hours: 14**

| Sr. No. | Tutorial Name |
|---|---|
| 1. | Prepare Case Study On Below Topics:<br>1. Advanced Encryption Standard (AES)<br>2. Triple DES-Blowfish,<br>3. RSA algorithm<br>4. Elliptic curve arithmetic<br>5. Bitcoins<br>6. Blockchain |

| | |
|---|---|
| | 7. Secure Hash Algorithm<br>8. Secure Communication Protocols in Industrial Systems<br>9. Key Management and Encryption Practices for Data |

**Major Equipment:**

1. Computer System
2. LAN cable

**Books Recommended:**


1. William Stallings “Cryptography and Network Security: Principles and Practice” Pearson
2. Alfred J Menezes and Scott A Vanstone “Handbook of Applied Cryptography” CRC Press
3. Neal Koblitz “A Course in Number Theory and Cryptography” Springer


**CO-PO-PSO MATRIX:**

| Co.No | PO1 | PO2 | PO3 | PO4 | PO5 | PO6 | PO7 | PSO1 | PSO2 |
|---|---|---|---|---|---|---|---|---|---|
| CO-1 | 2 | 2 | 1 | 2 | | 2 | | 3 | 2 |
| CO-2 | 2 | 3 | 1 | 2 | | 2 | | 2 | 3 |
| CO-3 | 1 | 3 | 3 | 1 | | | | 3 | 3 |
| CO-4 | 1 | 3 | 2 | 3 | | 2 | | 3 | 1 |
| CO-5 | 1 | 2 | 2 | | | | | 2 | 1 |