COURSE CONTENT

APPLIED CRYPTOGRAPHY								
I Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
2415816	**Foundation**	**3**	**0**	**0**	**3**	**40**	**60**	**100**
Contact Classes: 45	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: cryptographic techniques to secure digital data.								

Course Overview:

This focuses on the practical use of cryptographic techniques to secure digital data, communications, and information systems. The course introduces students to how cryptographic algorithms and protocols protect confidentiality, integrity, and authenticity in real-world computing environments.

Course Objectives:

1. To understand the fundamental concepts, principles, and importance of cryptography in information security.
2. To study classical and modern cryptographic techniques including symmetric and public key cryptography.
3. To learn various cryptographic protocols, digital signatures, hashing techniques, and secure communication methods.
4. To analyze different encryption algorithms, key management techniques, and cryptographic modes of operation.
5. To explore real-world applications of cryptography in secure systems, electronic payments, authentication, and data protection.

Course Outcomes: After Completion of the Course, Students should be able to

1. Implement substitution and transposition ciphers, XOR operations, and hashing methods for data protection.
2. Evaluate the security implications of different key lengths and cipher modes to determine their suitability for specific applications.
3. Implement public-key algorithms such as RSA, ElGamal, and elliptic curve cryptosystems.
4. Evaluate the effectiveness of advanced cryptographic protocols, including probabilistic and quantum cryptography, for secure communication and computation.
5. Implement real-world security mechanisms such as Kerberos, PGP, PEM, and PKCS for authentication and secure message exchange.

UNIT-I:

Foundations:

Terminology, Steganography, Substitution Ciphers and Transposition Ciphers, Simple XOR, One- Time Pads, Computer Algorithms, Large Numbers,

Cryptographic Protocols: Protocol Building Blocks

Introduction to Protocols, Communications Using Symmetric Cryptography, One-Way Functions, One- Way Hash Functions, Communications Using Public-Key Cryptography, Digital Signatures, Digital Signatures with Encryption, Random and Pseudo-Random-Sequence Generation.

UNIT – II:

Cryptographic Techniques Key length: Symmetric Key length, public key length, comparing symmetric and public key length. **Algorithm types and modes:** Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Cipher, Self-Synchronizing Stream Ciphers, Cipher-Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mod, Counter Mode, Other Block-Cipher Modes.

UNIT-III:

Public-Key Algorithms: Background, Knapsack Algorithms, RSA, Pohlig-Hellman, Rabin, ElGamal, McEliece, Elliptic Curve Cryptosystems, LUC, Finite Automaton Public-Key Cryptosystems

Public-Key Digital Signature Algorithms: Digital Signature Algorithm (DSA), DSA Variants, Gost Digital Signature Algorithm, Discrete Logarithm Signature Schemes, Ong-Schnorr-Shamir, ESIGN.

UNIT - IV:

Special Algorithms for Protocols: Multiple-Key Public-Key Cryptography, Secret-Sharing Algorithms, Subliminal Channel, Undeniable Digital Signatures, Designated Confirmer Signatures, Computing with Encrypted Data, Fair Coin Flips, One-Way Accumulators, All-or-Nothing Disclosure of Secrets, Fair and Failsafe Cryptosystems, Zero- Knowledge Proofs of Knowledge, Blind Signatures, Oblivious Transfer, Secure Multiparty Computation, Probabilistic Encryption, Quantum Cryptography.

UNIT - V:

Real World Approaches: IBM Secret key management protocol, ISDN, Kerberos, Krypto Knight, Privacy enhanced mail (PEM), Message security protocol (MSP), PGP, Public-Key Cryptography Standards (PKCS), Universal Electronic Payment System (UEPS).

TEXT BOOKS:

1. Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C.

REFERENCE BOOKS:

1. Cryptography and Network Security: Principles and Practice — William Stallings, Pearson Publications.
2. Handbook of Applied Cryptography — Alfred J. Menezes, Paul C. van Oorschot & Scott A. Vanstone, CRC Press Publications.

ELECTRONIC RESOURCES:

1. https://www.coursera.org/specializations/introduction-applied-cryptography
2. https://www.shiksha.com/online-courses/applied-cryptography-course-udacl27
3. https://www.coursera.org/learn/introduction-to-applied-cryptography
4. https://cursa.app/en/free-course/advanced-topics-in-cryptography-ecie

MATERIALS ONLINE:

1. Course template
2. Tutorial question bank
3. Tech talk and Concept Video topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. E-Learning Readiness Videos (ELRV)