COURSE CONTENT

APPLIED CRYPTOGRAPHY								
I Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
2515809	**Foundation**	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		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 fundamentals of cryptography and secure communication techniques.
2. To study symmetric and public-key cryptographic algorithms and their applications.
3. To develop skills in implementing digital signatures, authentication, and encryption protocols.
4. To analyze advanced cryptographic protocols for secure data sharing and communication.
5. To understand real-world cryptographic standards and security mechanisms used in modern information systems.

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

1. Apply substitution, transposition, XOR, and one-time pad techniques to secure data communication in confidential messaging systems.
2. Analyze symmetric and public-key algorithms, key lengths, and cipher modes to design secure encryption systems for financial transactions.
3. Implement public-key algorithms and digital signature schemes such as RSA, DSA, and ECC to ensure authentication and integrity in e-commerce platforms.
4. Design advanced cryptographic protocols, including zero-knowledge proofs, secret sharing, and oblivious transfer, for secure multiparty computations.
5. Evaluate real-world cryptographic standards and protocols such as Kerberos, PGP, and PKCS for securing enterprise communication and payment systems.

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)

MATERIALS ONLINE:

11. Course template
12. Tutorial question bank
13. Tech talk and Concept Video topics
14. Open-ended experiments
15. Definitions and terminology
16. Assignments
17. Model question paper – I
18. Model question paper – II
19. Lecture notes
20. E-Learning Readiness Videos (ELRV)