Programme: **B. Tech. (CSE)**	**Course Title: Cryptographic Algorithms**			**Course Code:** **CSE-3112**
Type of Course: **Program Core**	**Prerequisites:** Discrete Mathematical Structure			**Total Contact Hours:** **40**
Year/Semester: **Even**	**Lecture Hrs/Week:** **3**	**Tutorial Hrs/Week:** **0**	**Practical Hrs/Week:** **0**	**Credits:** **3**

Learning Objective:

This course discusses cryptographic protocols/primitives with multiple notions of security under random oracle and standard models. This includes various encryption schemes with respective algorithms, digital signature, message authentication, key distribution and authentication protocols. The course emphasizes provable properties, using theoretical tools like one-way functions, collision-resistant hashing, pseudo randomness, and number-theoretic results. Other advanced topics that could be covered are commitment schemes, zero-knowledge proofs, random oracles, secret sharing, advanced notions of security, and multi-party cryptographic protocols

Course outcomes (COs):

On completion of this course, the students will have the ability to:		**Bloom's Level**
CO-1	Understand the problems, security notions, design principles and proof techniques for selected cryptographic protocols and primitives	**2,3**
CO-2	Understand and apply various encryption Algorithms, Digital Signature Scheme and cryptanalysis	**3**
CO-3	Define the algorithms of authentication protocols; commitment protocols; zero-knowledge techniques; consensus/multiparty computations; privacy-preserving protocols, and formal specification and reasoning	**2**
CO-4	Understand the principle of Provable Security and security and adversary model	**3, 4**
CO-5	Understand the principle of well-known public key encryption scheme and algorithms with security and key establishment protocols	**2**

Course Topics	Lecture Hours	
UNIT – I (Mathematics of Cryptography)	**4**	**4**
1.1 (Set of Integers, Binary Operations, Integer Division, Divisibility, Linear Diophantine Equations), Modular Operator, Set of Résiduels, Congruence, Operations in Z_n, Addition and Multiplication Tables, Diffèrent Sets	**1**	
1.2 Algebraic Structure (Groups, Rings, Fields)	**1**	
1.3 Primes and Related Congruence Equations(Definition, Cardinality of Primes, Checking for Primness , Euler's Phi-Function, Fermat's Little Theorem, Euler's Theorem, Generating Primes.	**2**	
UNIT – II (Knowledge & Provable Security)	**5**	**5**
2.1 When Does a Message Convey Knowledge? A Knowledge-Based Notion of Secure Encryption	**1**	
2.2 Zero-Knowledge Interactions, Interactive Protocols, Interactive Proofs	**1**	
2.3 Applications of Zero-knowledge , Zero-knowledge proofs	**1**	
2.4 Shannon's Treatment of Provable Secrecy, Shannon Secrecy	**1**	
2.5 Perfect Secrecy, The One-Time Pad	**1**	
UNIT – III Public Key Encryption Schemes (Algorithms)	**12**	**12**
3.1 Algorithm for Discrete Logarithm Problem, Shanks Algorithm	**2**	
3.2 Elliptic Curves, Elliptic Curve over prime and binary filed.	**1**	
3.3 Elliptic Curve over prime, Computing point Multiples on Elliptic Curves	**1**	
3.4 RSA public-key encryption , Security of RSA public key encryption scheme	**2**	
3.5 Rabin public-key encryption , Security of Robin encryption scheme	**2**	
3.6 ElGamal public-key encryption, Security of ElGamal public-key encryption	**2**	
3.7 Bit-Security of ElGammal Systems, The Diffie-Hellman Problem	**2**	
UNIT-IV Authentication Protocols	**5**	**5**
4.1 Zero-knowledge Authentication	**1**	

4.2 Passwords (weak authentication)	1	
4.3 Challenge-response identification (strong authentication)	1	
4.4 Attacks on identification protocols	2	
UNIT-V Digital Signature (Algorithms)	**8**	
5.1 A framework for digital signature mechanisms , Security Requirement for Signature Scheme	2	
5.2 RSA and related signature schemes	1	**8**
5.3 Fiat-Shamir signature schemes	1	
5.1 The ElGammal Signature Scheme, Variants of the ElGammal Signature Scheme	1	
5.2 The Schooner Signature Scheme, The Digital Signature Algorithm	2	
5.3 The Elliptic Curve DSA	1	
UNIT-V Key Establishment Protocols and Analysis	**6**	
6.1 Classification and framework, Key transport based on symmetric encryption	1	
6.2 Analysis of key establishment protocols	1	6
6.3 Key agreement based on symmetric techniques	1	
6.4 Key transport based on public-key encryption	1	
6.5 Key agreement based on asymmetric techniques and Secret sharing	2	

Text Book:

Cryptography-Theory & Practices, Douglas R.Stinson, Third edition, CRC Press, 2005.

Reference books:

1. *Handbook of Applied Cryptography A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996.*
2. *An Introduction to Mathematical Cryptography Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H., Springer, 2008.*

Evaluation Method	
Item	**Weightage (%)**
Quiz-I	10
Quiz-II	10
Mid Term	25
Quiz-III	10

Assignment	10
End Term	35

*Please note, as per the existing institute's attendance policy the student should have a minimum of 75% attendance. Students who fail to attend a minimum of 75% lectures will be debarred from the End Term/Final/Comprehensive examination.

CO and PO Correlation Matrix

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1			2		1								2		
CO2	1	2			1	1					1		1	1	2
CO3	1	3	1	2	1						1				2
CO4	2		1		1	2							2		1
CO5		2	3								1		2	1	2

Prepared By: Jayaprakash Kar
24-10-2021