CSEXXX: Cryptographic Algorithms

Programme: B.Tech (CSE) **Year:** Third **Semester:** Fifth
Course: Program Elective **Credits:** 3 **Hours:** 40 hours (Theory)

Course Context and Overview (100 words):

Cryptographic algorithms and protocols are necessary to keep a system secure, particularly when communicating through an untrusted network such as the Internet. This course discusses mathematical foundations of cryptographic protocols/primitives. It defines on multiple notions of security under random and standard models with a focus on provable guarantees of security. Also, this course describes how to apply cryptographic primitives and algorithms having weak security properties to construct schemes satisfying very strong notions of security. The emphasis will be on cryptographic algorithms using conventional symmetric and public key cryptography. This includes various encryption schemes with respective algorithms, digital signature, message authentication, key distribution and deniable authentication protocols. Also discuss about how to design and develop novel cryptographic protocols using Elliptic Curve and Pairing based cryptography with a number of examples and applications. The focus will be analysis of 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.

Prerequisites Courses:
Discrete Mathematical Structure

Textbook references (IEEE format):
Text Book:

Handbook of Applied Cryptography,
A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press.

Reference books:

1. **Cryptography-Theory & Practices**
   Douglas R.Stinson
2. **An Introduction to Mathematical Cryptography**
   Hoffstein, Jeffrey, Pipher, **Jil**l, **Silverman**, **J.H.**

Course outcomes (COs):

The Outcomes of this Course are
CO1: Define the problems, security notions, design principles and proof techniques for selected cryptographic protocols and primitives
CO2: Discuss various encryption Algorithms and cryptanalysis
CO3: Define the algorithms of authentication protocols; commitment protocols; zero-knowledge techniques; consensus/multiparty computations; privacy-preserving protocols, and formal specification and reasoning
CO4: Understand the principle of Provable Security and security and adversary model
CO5: Discuss well known public key encryption scheme and algorithms with security and key establishment protocols

Course Topics

Contents		**Lecture Hours**	
UNIT – 1 (Mathematics of Cryptography)			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, Different 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-2 (Knowledge & Provable Security)			
2.1	When Does a Message Convey Knowledge? A Knowledge-Based Notion of Secure Encryption	1	5
2.2	Zero-Knowledge Interactions, Interactive Protocols, Interactive Proofs	1	
2.4	Applications of Zero-knowledge	1	

	Zero-knowledge proofs		
2.5	Shannon's Treatment of Provable Secrecy, Shannon Secrecy	1	
2.6	Perfect Secrecy, The One-Time Pad	1	
UNIT-3 Public Key Encryption Schemes (Algorithms)			
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	12
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-4 Authentication Protocols			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-5 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	
5.3	Fiat-Shamir signature schemes	1	
5.4	The ElGammal Signature Scheme Variants of the ElGammal Signature Scheme	1	
5.4	The Schooner Signature Scheme	2	

	The Digital Signature Algorithm		
5.5	The Elliptic Curve DSA	1	
UNIT-6 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	
6.3	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	

Evaluation Methods:

Item	**Weightage**
Mid Term	40
End Term	60

Prepared By: Jayaprakash Kar
Last Update: 02-12-2017