CSE XXX: APPLIED CRYPTOGRAPHY

Programme: PhD CSE Year**: First** **Semester:** Third
Course: Elective **Credits:** 3 **Hours:** 40 hours (Theory)

Course Context and Overview (100 words):

The course provides an up-to-date treatise of the principles, techniques, and algorithms of interest in cryptographic practice using Elliptic Curve and Pairing Based Cryptography. This emphasis on those aspects which are most practical and applied. The attractiveness of Elliptic Curve Cryptography (ECC) is that it is more secure and provides equivalent security with smaller key sizes which results in faster computation, lower power, and memory and bandwidth usage storage efficiency. ECC has the highest strength-per-bit compared to other public key cryptosystems. Cryptography using pairings (PBC) is an emerging field related to Elliptic Curve Cryptography which has been attracting the interest of the international cryptography community, since it enables the design of lightweight and efficient cryptographic schemes.

Prerequisites Courses: Courses on Cryptography and Cryptanalysis as

1. Discrete Mathematical Structure
2. Cryptographic Algorithms
3. Cryptography and Security

Course outcomes (COs):

The Outcomes of this Course are
CO1 Understand the concept of well-known Cryptographic algorithms /Primitives based on Elliptic Curve and Pairing based Cryptography.
CO2 Understand the principle of Provable Security in Random Oracle model
CO3: Discuss Side Channel Attacks, Differential Power analysis attack and its countermeasures
CO4: Discuss the Cryptanalysis of Discrete logarithm and Integer factorization Problem

Course Topics

Contents		Lecture Hours	
UNIT – 1 (Mathematical Preliminaries and Assumptions)			4
1.1	Algebra: Group, Subgroup, Cosets, Morphism of Group	1	
1.2	Finite fields, Galois field, Extension of finite fields, the arithmetic's of F_{q^k}	1	
1.3	Mathematical Hard problems-Integer Factorization, Discrete Logarithm Problem, Diffie-Hellman, Decisional Diffie-Hellman, Gap Diffie-Hellman Problem.	2	
UNIT-2 (Cryptographic Hash Functions)			
2.1	Security of Hash function: The Methodology of "Provable Security", Random Oracle model, Algorithms in the Random oracle model.	1	5
2.2	Comparison of Security Criteria Adversary and Security model- History of Adversarial Models, Security notion	2	
2.4	Message Authentication Code: Nested MACs and HMAC	1	
2.5	CBC-MAC	1	
UNIT-3 Public Key Cryptosystem based on Discrete Logarithm Problem			10
3.1	Elliptic Curve Arithmetic: Simplified Weierstrass curves, Group law, Group order	1	
3.2	Point representation and the group law, projective coordinate.	1	
3.3	The Elliptic Curve Discrete Logarithm Problem- Pohlig-Hellman attack	2	
3.4	Pollard's rho attack, Index calculus attack	2	
3.5	ElGamml Cryptosystem, The Elliptic Curve Digital Signature Algorithm(ECDSA)	2	
3.6	Security of ElGamal Systems-Bit Security of DL	2	
UNIT-4 Pairing Based Cryptography			7
4.1	Bilinear Pairing, definition of Tate pairing	1	
4.2	Properties of Tate Pairing, Tate pairing over Finite Field	1	
4.3	The Weil Pairing	1	
4.4	Key Distribution Scheme	2	

4.5	Identity-Based Encryption	2	
UNIT-5 Implementation Techniques			14
5.1	Software implementation-Integer arithmetic, floating point arithmetic, scalar multiplication for P-224, SIMD (single instruction multiple data) and field arithmetic.	3	
5.2	Hardware implementation- Field arithmetic processors, Addition, Multiplication, Squaring, Inversion.	3	
5.3	Side-Channel Analysis, Secure implementation, Power analysis attack and countermeasure	3	
5.4	Simple Side-Channel Attack (SCA) on Point Multiplications	2	
5.5	Differential Power Analysis Attack and countermeasure	3	

Textbook references (IEEE format):
Text Book:

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

2. **Nadia El Mrabet & Marc Joye- Guide to Pairing-based Cryptography**
3. **Darrel Hankerson, Alferd Menezes & Scott Vanstone, Guide to Applied Cryptography, Springer**

Reference books:

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

Evaluation Methods:

Item	Weightage
Mid Term	25
Research paper-I	15
Research paper-II	15
End Term	45

Prepared By: Jayaprakash Kar
25-01-2021