CSE XXX: INTRODUCTION TO CRYPTANALYSIS

Programme: PhD (CSE) **Year:** PhD **Semester:** Level Seven
Course: Program Elective **Credits:** 3 **Hours:** 40 hours

Course Context and Overview (100 words):

The course focus on the study of mathematical techniques to break various cryptosystems and cryptographic hash functions. This synthesizes the various cryptanalysis techniques such as linear cryptanalysis, differential cryptanalysis, Side Channel Attack, solving integer factorization problem, Discrete logarithm problem and algebraic attack etc. The course also focusses significant attention to how the cryptographic algorithms/primitives are being attacked by solving mathematical hard problems.

Prerequisites Courses:

Discrete Mathematics, Cryptography

Course outcomes (COs):

The Outcomes of this Course are
CO1: Discuss mathematical aspect of various cryptosystem.
CO2: Understand cryptanalysis techniques use to break the cryptosystem and revel the secret.
CO3: Understand the principle of Differential and Simple power analysis attack and
CO4: Discuss the attacks on mathematical hard problem such as Integer factorization(IF) and Discrete Logarithm Problem(DLP)
CO5: Study of attacks on Cryptographic hash functions.

Course Topics

Contents		Lecture Hours	
UNIT – 1 (RSA Cryptosystem and Factoring Integers)			10
1.1	RSA Algorithms (Key generation, Encryption and Decryption), Euler Totient functions $\phi(n)$, Computation and properties of $\phi(n)$.	3	
1.2	Factoring Algorithms- The Pollard $p-1$ algorithm, The Pollard Rho Algorithm	2	
1.3	Dixon's Random Squares Algorithm	2	
1.4	Factoring algorithm in practice, The Decryption Exponent,.	2	
1.5	Wiener's Low Decryption Exponent Attack	2	
UNIT-2 (Discrete Logarithm Problem)			10
2.1	Introduction to set Z_q^*, Additive and Multiplicative group, Definition of DLP, Generalized DLP.	2	
	Introduction to Elliptic Curve (Addition of points, doubling of points and formation of group), ECDLP.	2	
2.1	Shank's Algorithm	2	
2.2	The Pollard Rho Discrete Logarithm Algorithm	2	
2.4	The Pohlig-Hellman Algorithms	2	
2.5	The Index Calculus Method	1	
UNIT-3 Linear and Differential Cryptanalysis			6
3.1	Advanced Encryption Standard (Complete Algorithms)	3	
3.2	Substitution-Permutation Networks	1	
3.3	The Piling-up Lemma	2	
UNIT-4 Side Channel Attack			7
4.1	Power attack on Elliptic Curve Cryptosystem(ECC), Simple power analysis on ECC,	2	
4.2	Attacking Scalar multiplication method, Breaking Discrete Logarithm Problem	1	
4.3	SPA countermeasure-Coron's Dummy Method	2	
4.4	Differential Power analysis on ECC, DPA on binary method	2	

UNIT-5 Cryptanalysis on Hash functions (MD4, MD5 and SHA-I			7
5.1	The Modular Differential Attack	2	
5.2	Iterating Process for Hash Functions, Merkle-Damgard Meta method	2	
5.3	Iterating Process for Hash Functions, Bit tracing method	2	
5.4	Collision Attack on SHA-1	1	

Textbook references (IEEE format):
Text Book:

Douglas R.Stinson, Cryptography-Theory & Practices , Fourth edition, CRC Press, 2019.

Reference books:

1. **A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.**

2. **Hoffstein, Jeffrey, Pipher, Jill, Silverman, J.H., An Introduction to Mathematical Cryptography, Springer, 2008.**

Evaluation Methods:

Evaluation component	Weightage %
Mid-tem	25
Research Paper on Cryptanalysis-I	15
Research Paper on Cryptanalysis-I	15
End-term	45

Prepared By: Jayaprakash Kar
2023-12-11