School of Computer Engineering

Kalinga Institute of Industrial Technology (KIIT)
Deemed to be University
Bhubaneswar-751024

Cryptography – CC3021 (L-T-P:2-1-0)

Semester: 5th
Session: Autumn 2022

Instructor:

Name : Dr. Partha Pratim Sarangi
Chamber : Block-C, Campus-14
Contact Number : 7008034997
Email : pp.sarangifcs@kiit.ac.in

Lecture Hours:

CS-2 (C-LH-202)
Mon (3 – 4PM)
Wed (4 - 5PM)
Thu (4 - 5PM)

Course Objective

This is an elective course, open to 3rd year B.Tech. (CS, CSCE, and IT) students. The course (CC3021) objective is to introduce the student to the areas of cryptography and cryptanalysis. Our aim is to understand the mathematics used in the cryptography in the first few classes. Following to this, discuss a number of cryptographic primitives for encipherments. Then, the basic security concepts along with the nitty – gritty of public and private key cryptography. Finally, students will be discussed security on integrity, access control, authentication, and key management techniques.

Course Plan

Topics to be covered	No. of lectures (Lecture Nos)
Mathematical Foundations for Cryptography • GCD and Modular Arithmetic (Factorization, Euclid's algorithm, extended Euclid's theorem) (1) • Quadratic Residues and Discrete Logarithmic Problems (1) • Group, Ring and Field (2) • Primes, Primality Test, Factorization & Chinese Remainder Theorem (2)	7 (1-7)
Tutorials / Activity (1)	

Introduction to Computer Security ● Security Goals and Principles, Security Services, Security Mechanisms, Cryptographic Attacks (2) ● Different Types of Ciphers (Substitution, Transposition, Stream and Block) (4)	7 (8 -14)
Tutorials / Activity (1)	
Symmetric key Cryptography	8
● Modern Block and Stream Cipher (1) ● Data Encryption Standard (DES), 2DES, 3DES (2) ● Blowfish Scheme (1) ● Advanced Encryption Standard (AES) (2) ● Diffie Hellman Key Exchange Protocol (1)	(15 - 22)
Tutorials / Activity (1)	
Asymmetric Key Cryptography ● Difference between Symmetric and Asymmetric Key Cryptography (1) ● Rabin Cryptosystem (1) ● Elgamal Cryptosystem (1) ● Elliptic Curve Cryptosystems (2)	6 (23 - 28)
Tutorials / Activity (1)	
Integrity Authentication and Key Management ● Message Authentication Code (MAC) (1) ● Message Digest (MD5) (1) ● Secure Hash Functions (SHA) (2) ● Digital Signature (ElGamal, RSA and Elliptic Curve Digital signature schemes) (3) ● Digital Signature Standard (DSS) (1) ● Entity Authentication (1) ● Key Management: Key Distribution Center (KDC), Kerberos (1)	12 (29 - 40)
Tutorials / Activity (1)	

Day-Wise Lesson Plan

Week - 1	**Lecture No.**	**Topic to covered**
Unit - 1	**Introduction to Computer Security**	
	1	Security Goals and Principles, Security Services, Security Mechanisms
	2	Cryptographic Attacks (Passive and Active)
	3	Activity 1
Unit - 2	**Mathematical Foundations for Cryptography (I)**	

Week - 2	4	• Euclidean algorithm to compute GCD • Modulo Operator • Set of Residues • Congruence
	5	• Residue Classes • Additive Inverse • Multiplicative Inverse • Extended Euclidean Algorithm to compute GCD and multiplicative inverse
	6	• Group, Ring and Field
Unit - 3	**Different Types of Ciphers**	
Week – 3	7	• Activity - 2
	8	• Substitution Ciphers (Mono-Alphabetic and Poly-Alphabetic) • Mono-Alphabetic: Additive, Multiplicative, and Affine Ciphers
	9	• Poly-Alphabetic: Autokey Cipher, Playfair Cipher
Week - 4	10	• Vigenere Cipher, Hill Cipher, Vernam Cipher
	11	• Transposition Cipher: Keyed, Keyless, Keyed + Keyless, Double Transposition Ciphers
	12	• Activity 3
Unit - 4	**Symmetric key Cryptography**	
Week - 5	13	• Modern Block and Stream Ciphers
	14	• Data Encryption Standard (DES)
	15	• Double (2DES) and Triple (3DES)
Week - 6	16	• Advanced Encryption Standard (AES)
	17	• Blowfish Scheme
	18	• Modes of operation (ECB, CBC, CFB, OFB, CTR)
Unit - 5	**Mathematical Foundations for Cryptography (II)**	
Week - 7	19	• Quadratic Residues and Discrete Logarithmic Problems
	20	• Primes, Euler’s Phi-Function and Fermat’s Little Theorem
	21	• Primality Test Algorithms
Week - 8	22	• Chinese Remainder Theorem
Unit - 6	23	• Activity 4
		Asymmetric Key Cryptography
	24	• Difference between Symmetric and Asymmetric Key Cryptography
Week - 9	25	• Diffie Hellman Key Exchange Protocol
	26	• RSA Cryptosystem

	27	• Elgamal Cryptosystem
Week - 10	28	• Elliptic Curve Cryptosystems
	29	• Elliptic Curve Cryptosystems
	30	• Activity 5
Unit - 7	• Integrity and Authentication	
Week - 11	31	• Message Authentication Code (MAC)
	32	• Cryptographic Hash Functions
	33	• Message Digest (MD5)
Week - 12	34	• Secure Hash Functions (SHA)
	35	• Digital Signature
	36	• Digital Signature Standard (DSS)
Unit - 8	• Key Management	
Week - 13	37	• Entity Authentication
	38	• Key Management and Key Distribution Center (KDC)
	39	• Kerberos
	40	• Activity 6

Course Outcome: At the course end, the students will be able to

CO1:	Gain knowledge about the Mathematics of Symmetric and Asymmetric Key Cryptography.
CO2:	Understand the basic concepts and goals of the security.
CO3:	Understand the fundamentals of symmetric key cryptosystems and their applications.
CO4:	Understand the fundamentals of public key cryptosystems and their applications.
CO5:	Understand the requirement of Key management.
CO6:	Evaluate a range of access control and authentication mechanisms.

Text books:

1. Cryptography and Network Security: Behrouz A Forouzan and Debdeep Mukhopadhyay, McGraw Hill Education, 3rd edition 2018.

Reference books:

1. Cryptography and Network security: Principles and Practice, William Stallings, Pearson Education, 7th edition, 2018
2. Cryptography and Network Security: Atul Kahate, Tata McGraw Hill Education, 3rd edition, 2018

Grading Policy:

- Activities (6 No.s) : **30 Marks**
- Mid-semester exam : **20 Marks**
- End-semester exam : **50 Marks**