COURSE HANDOUT

FUNDAMENTALS OF CRYPTOGRAPHY (COM-403)

BE-IVTH SEMESTER

ACADEMIC YEAR (2024-25)

Dr. Mir Aadil
Assistant Professor

Department of Computer Science Engineering

Department of Computer Science Engineering

Model Institute of Engineering & Technology (Autonomous)

Kot Bhalwal, Jammu - 181122

www.mietjmu.in

SYLLABUS

Course Code	Course Name	Course Type	Cd	L	T	P	Marks		
							Sessional	Final Exam	Total
COM-403	Foundations of Cryptography	Core	4	3	1	0	50	100	150
Faculty Details	aadil.cse@mietjammu.in								

Section-A

Unit 1: Mathematical Foundations: Integer Arithmetic, Set of Integers, Binary Operations, Integer Division, Divisibility, Linear Diophantine Equations, **modular arithmetic:** Modulo Operator, Set of Residues: Zn, Congruence, Operations in Zn, Inverses, Addition and Multiplication Tables, Different Sets for Addition and Multiplication**.** **(8 Hrs)**

Unit 2: Introduction to Simple Encryption techniques: Secret-key encryption, public-key, block and stream ciphers, hybrid encryption, Message authentication codes, Nonrepudiation, certificates. **(8 Hrs)**

Unit 3: Classical Encryption Techniques: The Shift Cipher, Substitution Cipher, Affine Cipher, Hill Cipher, Permutation Cipher, Stream Cipher, Cryptanalysis: Affine Cipher, Substitution Cipher, Vigenere Cipher, Hill Cipher Stream Cipher, One-Time Pad. **(8 Hrs)**

Section-B

Unit 4: Modern Encryption Techniques: Piling-up Lemma, Linear Approximations of S-boxes, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Hash Functions and data integrity, SHA-512, Message and Message Digest encryption. **(9 Hrs)**

Unit 5: Public Key Encryption Techniques: ElGamal Cryptosystem, Shanks' Algorithm, Diffie-Hellman Problems, RSA algorithm, Signing and Encrypting, Multivariate encryption technique. **(7 Hrs)**

Text Books

S.No.	Name of the Books	Author	Publisher Name	Edition (Pub. yr.)
1	Cryptography and Network Security Principles and Practice	William Stallings	Prentice Hall	7th (2017)
2	Cryptography and Network Security.	Behrouz A. Forouzan	McGraw Hill Education	2nd (2020)

Reference Books

S.No.	Name of the Books	Author	Publisher Name	Edition (Pub. Yr.)
1	Cryptography Theory and Practice	Douglas R. Stinson Maura B. Paterson	CRC Press	6th (2019)

COURSE PLAN

S.No	Topics	Recommended Books
Unit-I		
1	Integer Arithmetic	Book 1, Ch.1
2	Set of Integers, Binary Operations	Book 1, Ch.1
3	Integer Division, Divisibility	Book 1, Ch.1
4	Linear Diophantine Equations	Book 2, Ch.1
5	Modular Arithmetic: Modulo Operator,	Book 2, Ch.1
6	Set of Residues: Zn, Congruence	Book 2, Ch.1
7	Operations in Zn, Inverses, Addition and Multiplication Tables	Book 2, Ch.1
8	Different Sets for Addition and Multiplication	Book 2, Ch.1
Unit-II		
9	Introduction to Simple Encryption Techniques	Book 1, Ch.2
10	Secret-key encryption,	Book 1, Ch.2
11	Public-key encryption	Book 1, Ch.2
12	Block and stream ciphers, Hybrid encryption	Book 2, Ch.2
13	Message authentication codes	Book 2, Ch.2
14	Nonrepudiation	Book 2, Ch.2
15	Certificates	Book 2, Ch.2
16	Certificates	Book 2, Ch.2
Unit-III		
17	Classical Encryption Techniques	Book 2, Ch.3
18	The Shift Cipher, Substitution Cipher	Book 2, Ch.3
19	Affine Cipher, Hill Cipher,	Book 2, Ch.3
20	Permutation Cipher, Stream Cipher	Book 2, Ch.3
21	Cryptanalysis Techniques:	Book 2, Ch.3
22	Affine Cipher, Substitution Cipher,	Book 2, Ch.3
23	Vigenère Cipher, Hill Cipher	Book 2, Ch.2
24	Stream Cipher, One-Time Pad	Book 2, Ch.2
Unit-IV		
28	Piling-up Lemma	Book 2, Ch.3
29	Linear Approximations of S-boxes	Book 1, Ch.4
30	Data Encryption Standard (DES)	Book 1, Ch.4
31	Data Encryption Standard (DES)	Book 1, Ch.4
32	Advanced Encryption Standard (AES)	Book 1, Ch.4
33	Advanced Encryption Standard (AES)	Book 1, Ch.4
34	Hash Functions and Data Integrity	Book 1, Ch.3

35	SHA-512	Book 1, Ch.3
36	Message and Message Digest Encryption	Book 1, Ch.3
Unit-V		
37	Public Key Encryption Techniques	Book 2, Ch.5
38	ElGamal Cryptosystem	Book 1, Ch.5
39	ElGamal Cryptosystem	Book 1, Ch.5
40	Shanks' Algorithm	Book 2, Ch.5
41	Diffie-Hellman Problems	Book 2, Ch.5
42	RSA Algorithm	Book 1, Ch.5
43	Signing and Encrypting	Book 2, Ch.5
44	Signing and Encrypting	Book 2, Ch.5
45	Multivariate Encryption Technique	Book2, Ch. 5

ADDITIONAL WEB RESOURCES

1.	**NPTEL:** Foundations of Cryptography By Prof. Ashish Choudhury | IIIT Bangalore Foundations of Cryptography - Course

GRADING AND ASSESSMENT

- **Sessional Test**: 20 marks
- **Assignment**: 20 marks
- **Attendance**: 10 marks
- **Final Examination**: 100 marks

COURSE POLICIES

- **Attendance**: Minimum 75% attendance is mandatory to appear in the final examination of the course.
- **Academic Integrity**: MIET's academic integrity policies apply. Plagiarism will not be tolerated.
- **Late Submissions**: Assignments and projects must be submitted by the specified timelines.

FACULTY INFORMATION

- **Office Hours**

  Monday (12:05 PM - 12:55 PM)
  Friday (12:05 PM - 12:55 PM)

- **Contact Information**
  aadil.cse@mietjammu.in