COURSE HANDOUT

CRYPTOGRAPHY AND COMPUTER SECURITY

(MCSE21B)

MTECH CSE 2ND Semester

ACADEMIC YEAR: 2024-25

Ms. Vani Malagar

Assistant Professor

Department of Computer Science and Engineering

Department of Computer Science and Engineering

Model Institute of Engineering & Technology (Autonomous)

Kot Bhalwal, Jammu - 181122

www.mietjammu.in

SYLLABUS

Course Code	Course Name	Cd	L	T	P	Marks		
						Internal	Final Exam	Total
MCSE21B	Cryptography and Computer Security	3	3	0	0	25	75	100
Faculty Details	Vani.cse@muetjammu.in							

UNIT- 1

Introduction: Security mind-set, Computer Security Concepts (CIA), Threats, Attacks and Assets. **(05 hrs)**

UNIT- 2

Cryptographic Protocols: Introduction to Protocols, Communications using Symmetric Cryptography, Substitution Ciphers and Transposition Cipher, Block Cipher, Steam Cipher, Modes of Operation, Symmetric and Asymmetric cryptography. **(6 Hrs)**

UNIT- 3

Cryptographic Techniques: Key Length & Management: Symmetric Key Length, Public-Key Key Length, Comparing Symmetric and Public-Key Key Length, Generating Keys, Algorithms: DIFFIE-HELLMAN, RSA, DES. **(08 hrs)**

UNIT- 4

Practical Cryptography: Encryption, Authentication, Hashing, Symmetric and Asymmetric cryptography, Digital Signatures and Certificates. **(08 hrs)**

UNIT- 5

Network Security and Protocol Standards: Network security issues, sniffing, IP Spoofing, Common threats, Email security, Secure Socket Layer (SSL), Transport Layer Security (TLS), SSH, IPSEC, Pretty Good Privacy (PGP), Intruders, Virus, Worms, Firewalls: need and features of firewall, Types of firewall, Intruder Detection Systems. **(08 hrs)**

Text Books

S. No.	Name of the Books	Author	Publisher	Edition (Pub. Yr.)
1	Introduction to Modern Cryptography	Jonathan Katz and Yehuda Lindell	CRC Press	2nd (2014)
2	Cryptography and Network Security	William Stallings	Pearson	6th (2013)

Reference Books

S. No.	Name of the Books	Author	Publisher	Edition (Pub. Yr.)
3	Applied Cryptography: Protocols, Algorithms and Source Code in C	Bruce Schneier	John Wiley & Sons	2nd(1996)
4	Cryptography Theory and Practice	CRC Press	Pearson	4th (2013)

COURSE PLAN

Unit-I		
Unit No.	**Topic**	**Recommended Books**
Unit-I	**Introduction**	
1	Security mindset	**Book 2, Ch.1**
2	Computer Security Concepts (CIA)	**Book 2, Ch.1**
3	Threats, Attacks, and Assets	**Book 2, Ch.1**
Unit-II	**Cryptographic Protocols**	
4	Introduction to Protocols	**Book 1, Ch.1**
5	Communications using Symmetric Cryptography	**Book 2, Ch.2**
6	Substitution Ciphers and Transposition Cipher	**Book 2, Ch.2**
7	Block Cipher, Stream Cipher	**Book 2, Ch.3**
8	Modes of Operation	**Book 2, Ch.3**
9	Symmetric and Asymmetric Cryptography	**Book 2, Ch.2**
Unit-III	**Cryptographic Techniques**	
10	Key Length & Management	**Book 1, Ch.5**
11	Symmetric Key Length	**Book 1, Ch.5**
12	Public-Key Key Length	**Book 1, Ch.5**
13	Comparing Symmetric and Public-Key Key Length	**Book 1, Ch.5**
14	Generating Keys	**Book 1, Ch.5**
15	DIFFIE-HELLMAN Algorithm	**Book 1, Ch.10**
16	RSA Algorithm	**Book 1, Ch.10**
17	DES Algorithm	**Book 2, Ch.3**
Unit-IV	**Practical Cryptography**	
18	Encryption	**Book 1, Ch.7**
19	Authentication	**Book 1, Ch.7**
20	Hashing	**Book 1, Ch.9**
21	Symmetric and Asymmetric Cryptography	**Book 2, Ch.2**
22	Digital Signatures and Certificates	**Book 1, Ch.12**
Unit-V	**Network Security and Protocol Standards**	
23	Network security issues	**Book 2, Ch.18**
24	Sniffing	**Book 2, Ch.19**
25	IP Spoofing	**Book 2, Ch.19**
26	Common threats	**Book 2, Ch.19**
27	Email security	**Book 2, Ch.19**
28	Secure Socket Layer (SSL)	**Book 2, Ch.19**
29	Transport Layer Security (TLS)	**Book 2, Ch.19**
30	SSH	**Book 2, Ch.19**
31	IPSEC	**Book 2, Ch.19**
32	Pretty Good Privacy (PGP)	**Book 2, Ch.19**
33	Intruders	**Book 2, Ch.20**
34	Virus	**Book 2, Ch.20**
35	Worms	**Book 2, Ch.20**

36	Firewalls: Need and Features	**Book 2, Ch.21**
37	Types of Firewalls	**Book 2, Ch.21**
38	Intruder Detection Systems	**Book 2, Ch.21**

ADDITIONAL WEB RESOURCES

S. No.	Resource Name	Description	Link
1	**MOOC: Cryptography I (Coursera)**	A comprehensive course on cryptographic primitives, encryption, and secure protocols.	https://www.coursera.org/learn/crypto?action=enroll&authType=google&completeMode=existingCourseraAccount
2	**NPTEL: Cryptography and Network Security**	Video lectures by Prof. D. Mukhopadhyay, IIT Kharagpur, covering cryptographic algorithms and network security.	https://onlinecourses.nptel.ac.in/noc22_cs90/preview
3	**Online Tool**	Online Cryptography tool	https://www.onlinecryptographytools.com/index.html
4	**Security Week Blog**	News and insights on cybersecurity.	https://www.securityweek.com/

- **GRADING AND ASSESSMENT**
  - **Sessional Test -I & II**: 15 marks
  - **Assignment**: 05 marks
  - **Attendance**: 05 marks
  - **Final Examination**: 75 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**
    Vani.cse@mietjammu.in