Cryptography and Data Security (CT805-C02) Credits: 4

Level : M. Sc.
Program : MSNCS

Year : I
Part : I

This course provides an in-depth knowledge about the evolution of cryptography, various cryptographic algorithms, their implementation, vulnerabilities, and security measures. This also discusses about the public key infrastructure and explores fundamental concepts around data security and privacy.

Course Objective:

- Understand the fundamental principles of cryptography and its role in network and cyber security.
- Design cryptographic algorithms and protocols for ensuring confidentiality, integrity, authentication, and non-repudiation.
- Analyze and mitigate cryptographic attacks and vulnerabilities in real-world scenario.
- Understand cryptographic hash functions, applications, and PKI.
- Identify common cyber threats and vulnerabilities.
- Explore legal and regulatory requirements for data protection
- Understand the basic concepts of cyber security and data privacy.
- Explore emerging trends in cryptography and security

Learning Outcomes	Chapter Contents	Credit Hours	Teaching Methods
• Understand the history and evolution of cryptography.	**1 Introduction to Cryptography** 1.1 History and evolution of	6	• Lectures and discussions on cryptographic history and principles.

• Identify fundamental cryptographic terminologies and concepts. • Explain Kerckhoff’s law and zero-knowledge proof. • Comprehend the goals of cryptography: confidentiality, integrity, authentication, and non-repudiation. • Analyze classical cryptographic methods and cryptanalysis techniques.	cryptography 1.2 Basic cryptographic terminologies and concepts 1.3 Kerchoff’s law 1.4 Zero knowledge proof 1.5 Goals of cryptography: Confidentiality, integrity, authentication, and non-repudiation 1.6 Classical cryptography: substitution ciphers, transposition ciphers 1.7 Cryptoanalysis techniques		• Demonstrations of substitution and transposition ciphers. • Hands-on exercises in basic cryptanalysis techniques.
• Explain symmetric key encryption and its properties. • Understand block ciphers (DES, 3DES, AES) and their modes of operation. • Explore stream ciphers and analyze their security aspects. • Discuss the principles and security of public-key cryptography. • Examine cryptographic algorithms like RSA, Diffie-Hellman, and	**2 Symmetric and Asymmetric Key Cryptography** 2.1 One time pad and perfect secrecy 2.2 Block Ciphers (BC) 2.3 DES, 3DES and AES 2.4 BC Modes of Operation 2.5 Stream Ciphers, RC4 2.6 Attacks on symmetric key cryptosystem and counter measures 2.7 Principles of public-key cryptography 2.8 Deffie-Hellmen key exchange algorithm, security properties and vulnerabilities 2.9 RSA algorithm, key generation	12	• Interactive lectures and algorithm breakdown sessions. • Hands-on exercises implementing DES, AES, and RSA. • Group discussions on cryptographic attacks and their mitigation. • Problem-solving sessions on key exchange and encryption models.

elliptic curve cryptography. • Identify attacks and countermeasures for both symmetric and asymmetric encryption.	process, key length considerations, applications 2.10 Elliptic curve cryptography, key generation, parameter selection 2.11 Attacks on asymmetric key cryptosystems and counter measures		
• Understand the role and properties of cryptographic hash functions. • Compare different cryptographic hash functions and their applications. • Analyze cryptographic hash function vulnerabilities, including collision and length extension attacks. • Explore hash function applications in password hashing, digital signatures, and blockchain.	**3 Cryptographic Hash Functions** 3.1 Definition and properties of cryptographic hash functions 3.2 Common cryptographic hash functions and comparison 3.3 Cryptoanalysis of hash functions: collision attacks, length extension attacks, time memory trade off attacks 3.4 Applications: password hashing, digital signature, Blockchain and cryptocurrency.	8	• Demonstrations of hash function implementations. • Group exercises on cryptographic attacks and their impact. • Hands-on activities using cryptographic tools to analyze hash outputs.
• Understand the purpose and significance of Public Key Infrastructure (PKI). • Identify key components of PKI, including Certificate Authorities and digital certificates.	4 **Key Management** 4.1 Definition, historical context, and importance of PKI 4.2 Key components: Certificate authority, registration authority, certification revocation list,	8	• Lectures on PKI components and trust models. • Hands-on exercises on certificate creation and management. • Discussions on real-world PKI implementations and challenges.

• Explore certificate generation, revocation, renewal, and trust models.	certificate repository 4.3 Digital certificates: structure, contents, formats, certificate chains and hierarchies 4.4 PKI Operations: generation, revocation, renewal 4.5 PKI trust models, standards, and protocols.		
• Understand data security concepts, threats, and challenges. • Learn techniques for securing data at rest and in transit. • Explore methods like obfuscation, tokenization, and data loss prevention. • Analyze security considerations for mobile and cloud data.	**5 Data Security** 5.1 Data security concepts, terminology, and principles. 5.2 Data security risks, challenges, and threats 5.3 Securing data at rest and transit 5.4 Data classification and data labelling 5.5 Basic operations: obfuscation and tokenization 5.6 Data loss prevention 5.7 Mobile data security, cloud data security	10	• Case studies on data breaches and security failures. • Hands-on activities on encryption techniques for securing data. • Group discussions on cloud and mobile data security issues.
• Understand fundamental cybersecurity principles and common threats. • Analyze security mechanisms like firewalls and Intrusion Detection Systems (IDS). • Explore data privacy laws, regulations, and compliance frameworks. • Examine privacy concerns	**6 Cyber Security and Data Privacy** 6.1 Overview of cybersecurity and data privacy 6.2 Common cyber security and data threats 6.3 Firewalls and intrusion detection systems (IDS) 6.4 General trends in data privacy, information collection, processing, storage, deletion	12	• Lectures on cybersecurity concepts and real-world case studies. • • Hands-on IDS implementation and log data analysis. • • Group discussions on privacy regulations and legal frameworks. • • Problem-solving exercises on

in big data and social media. • Understand concepts of user behavior analytics and personal data protection.	6.5 Privacy issues in the age of social media and big data 6.6 Overview of data privacy laws, regulations, and compliance 6.7 Consent and right to erasure 6.8 Data governance and privacy impact assessments 6.9 Introduction to Cyber Physical Systems 6.10 User Behavior Analytics 6.11 Personally Identifiable Information and Personal Health Information		cybersecurity threat mitigation.
• Explore advances in cryptographic research, including quantum and post-quantum cryptography. • Understand concepts of homomorphic encryption and federated learning security. • Analyze the role of AI and ML in cryptography and security. • Examine supply chain security and threat intelligence methodologies.	**7 Emerging trends in Cryptography and Security** 7.1 Threat intelligence and predictive analytics 7.2 Overview of quantum, post-quantum, and quantum-safe cryptography 7.3 Homomorphic encryption 7.4 Overview of supply chain security 7.5 Security aspects in federated learning 7.6 Artificial intelligence and machine learning in cryptography and data security 7.7 Other emerging trends in security	6	• Lectures and discussions on emerging trends and future challenges. • Case studies on AI and ML applications in cybersecurity. • Interactive activities exploring quantum cryptography.

Laboratory Works:

Laboratoyy works shall include

- implementation of classical cryptosystem, one-time pad, block ciphers, stream ciphers, DES and RSA.
- attack on the cryptographic systems
- IDS implementation
- Log data analysis

References Books:

1. “Cryptography and Network Security: Principles and Practice” by *William Stallings*
2. "Introduction to Modern Cryptography" by *Jonathan Katz and Yehuda Lindell*
3. “Computer security, art and science” by *Matt Bishop*

Evaluation Scheme:

The questions will cover all the chapters of the syllabus. A tentative distribution of the marks is given below however this is subject to change without prior notice.

Chapter	1	2	3	4	5	6	7
Topics	All	All	All	All	All	All	All
Marks	6	12	8	8	8	12	6