MTH352 Cryptography

Level: 3

Credit Units: 5 Credit Units

Language: ENGLISH

Presentation Pattern: EVERY JULY

Synopsis:

MTH352 Cryptography introduces students to the mathematics behind encryption and decryption. The course examines many deployed protocols and analyses the feasibility and the issues of implementing the algorithms covered. Students will learn how to implement the algorithms learnt from theory in Sage. The course will cover practical computational aspects of cryptography such as discrete logarithms and hash functions.

Topics:

- Classical Ciphers
- Cryptanalysis
- Linear Complexity
- Data Encryption
- RSA Cryptosystem
- Primality Testing
- Factorisation of Integers
- Discrete Logarithms
- Digital Signatures
- Hash Functions
- Threshold Schemes
- Stream Ciphers

Textbooks:

Fundamentals of Cryptography: Introducing Mathematical and Algorithmic Foundations Duncan Buell
Springer
ISBN-13: 9783030734923

MTH352 Study Guide
ISBN-13: SG-1626

MTH352-Handbook
ISBN-13: OT-4458

Learning Outcome:

- Compare and contrast a range of different cryptosystems
- Analyze the applicability and limits of existing authentication and key agreement protocols
- Explain the role of hash functions in information security
- Implement suitable algorithms to decrypt or encrypt messages of various ciphers
- Apply suitable factoring algorithms to factorize large integers
- Calculate the number of operations required in various cryptography algorithms

Assessment Strategies - Regular Semester (Evening Class):

Components	**Description**	**Weightage Allocation (%)**
Overall Continuous Assessment	COMPUTER MARKED ASSIGNMENT 1	10
	TUTOR-MARKED ASSIGNMENT 1	20
Overall Examinable Components	Written Exam	70
Total		**100**

*The information listed is subject to review and change.