<table>
<tr><td>Course Title</td><td colspan="5">Introduction to Cryptography</td></tr>
<tr><td>Course Code</td><td colspan="5">MAT212</td></tr>
<tr><td>Course Type</td><td colspan="5">Elective</td></tr>
<tr><td>Level</td><td colspan="5">Bachelor (1st Cycle)</td></tr>
<tr><td>Year / Semester</td><td colspan="5">4th Year / 7th Semester</td></tr>
<tr><td>Teacher’s Name</td><td colspan="5">TBA</td></tr>
<tr><td>ECTS</td><td>6</td><td>Lectures / week</td><td>3 hours / 14 weeks</td><td>Laboratories / week</td><td>N/A</td></tr>
<tr><td>Course Purpose and Objectives</td><td colspan="5">This objective of this course is to provide a comprehensive presentation of basic encryption and decryption cryptosystems. Through the development of mathematical structures and tools, students will be equipped with the necessary skills and knowledge that are required in performing reliable encryption and decryption of messages.</td></tr>
<tr><td>Learning Outcomes</td><td colspan="5">Upon successful completion of this course students should be able to:
• Describe the basic principles of cryptography.
• Use mathematical structures relevant to cryptography such as groups, rings and fields
• Use many mathematical tools from abstract algebra and number theory
• Explain the different kinds of encryption methods (symmetric, asymmetric) and the differences between them.
• Classify and describe a number of different encryption algorithms and the way that they work.
• Practice to encrypt and decrypt messages using symmetric and public-key cryptosystems</td></tr>
<tr><td>Prerequisites</td><td colspan="2">MAT170, MAT150, MAT206</td><td colspan="2">Co-requisites</td><td>None</td></tr>
<tr><td>Course Content</td><td colspan="5">Introduction:
Motivation – why is cryptography important, historic examples, the fundamental goals of cryptography: confidentiality, data integrity, authentication and non-repudiation.
Basic mathematical tools required:
Background on functions including one-to-one, onto, bijections, inverse functions, one-way and trapdoor one-way functions, permutations and involutions.</td></tr>
</table>

	Basic terminology and concepts: Encryption domains and codomains, encryption and decryption transformations, achieving confidentiality, communication participants, channels, security. Symmetric-key encryption: Overview of block ciphers and stream ciphers, substitution ciphers - homophonic and polyalphabetic ciphers, the Vigenere cipher, transposition ciphers, composition of ciphers, product ciphers, stream ciphers – the Vernam cipher, one-time pad. Mathematical background: The integers - divisibility, representation of integers, the O-notation, cost of addition, multiplication and division with remainder, greatest common divisor, Euclidean algorithm, extended Euclidean algorithm, factoring into primes, prime number theorem, fundamental theorem of arithmetic, modular arithmetic, the group of integers (residue class) modulo n, semigroups, groups, rings, division in the residue class ring, the multiplicative group of the integers (residues) modulo n, Euler phi function, the order of an element and generators in the multiplicative group of integers (residues) modulo n, the structure of the multiplicative group of residues modulo a prime number, quadratic residues modulo n, square roots modulo n, Euler’s theorem, Fermat’s little theorem, fast exponentiation, Chinese remainder theorem Public-key encryption: RSA Cryptosystem, key generation, encryption/decryption, security of the secret key, efficiency Rabin encryption, key generation, encryption/decryption, efficiency, security, Diffie-Hellman key exchange, discrete logarithms, key exchange, security, ElGamal encryption, key generation, encryption/decryption, efficiency. Recent developments and contemporary issues pertaining to the subject-matter of the course.
Teaching Methodology	Face- to- face
Bibliography	Schneier, B., APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, Wiley Menezes, A., van Oorschot,P. & Vanstone, S., HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC Press Forouzan B., CRYPTOGRAPHY AND NETWORK SECURITY, McGraw-Hill Paar C., Pelzl J., UNDERSTANDING CRYPTOGRAPHY: A Textbook for Students and Practitioners, Springer

	Buchmann, J. A., INTRODUCTION TO CRYPTOGRAPHY, Springer
Assessment	Examinations 50% Assignments 40% Class Participation 10% 100%
Language	English