

MZUZU UNIVERSITY

FACULTY OF EDUCATION

DEPARTMENT OF MATHEMATICS

SYLLABUS

1. Programme : Master of Science
2. Subject : Mathematics
3. Course Title : Cryptography I
4. Course Code : MSC 5903/5A03
5. Semester : 9
6. Level of Study : 5
7. Duration: : 14 weeks
8. Lecture hours per week : 2
9. Tutorial hours per week : 1
10. Assessment and Weighting : A student grade shall solely come from a 3-hour exam which shall be marked out of 100.
11. Course Aims : To introduce students to the basics of cryptography.
12. Course Objectives : By the end of the course, students will be able to
 - do encryption, decryption and cryptanalysis of classical cryptosystems, Data Encryption Standard (DES) and RSA cryptosystem.
 - explain the application of information theory in cryptography.
13. **Topics of the Course :**
 - Classical ciphers
 - shift
 - substitution
 - affine

- Vigenere
 - Hill
 - permutation
 - stream ciphers
- Cryptanalysis of classical ciphers
 - affine
 - Vigenere
 - Hill
 - LFSR-based stream cipher
- Shannon's approach to cryptography
 - perfect secrecy
 - use of information theory in cryptography
 - spurious keys and unicity distance
 - product cryptosystems
- The Data Encryption Standard (DES)
 - description of DES
 - the DES controversy
 - DES modes of operation
 - a time-memory trade-off (an attack on DES)
 - attacks on DES (differential cryptanalysis)
- Public key cryptography
 - the RSA cryptosystem
 - implementing RSA
 - setting up RSA
 - probabilistic primality testing
 - attacks on RSA

14. Prescribed Text :

D. R. Stinson (1995), *Cryptography, theory and practice*, CRC Press.

15. Recommended Texts:

- a) G. J. Simmons(1992), *Contemporary cryptology - The science of information integrity*, IEEE Press.
- b) W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*.
- c) O. Goldreich, *Foundations of cryptography*, Cambridge University press, 2001.