

MZUZU UNIVERSITY

FACULTY OF EDUCATION

DEPARTMENT OF MATHEMATICS

SYLLABUS

1. Programme : Master of Science
2. Subject : Mathematics
3. Course Title : Cryptography II
4. Course Code : MSC 5A04/6B04
5. Semester : 10
6. Level of Study : 5/6
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 public key cryptosystems and their applications.
12. Course Objectives :
 - By the end of the course, students will be able to
 - explain encryption, decryption, security and efficiency of the ElGamal, Merkle-Hellman and McEliece cryptosystems.
 - explain how signing and verification algorithms of prominent signature schemes are constructed.
 - analyse security and efficiency of a discrete log, MD4, and SHA hash functions.
 - explain advantages and disadvantages associated with the use of various key distribution protocols.
 - carry out simple calculations on public key cryptosystems, signature schemes, hash functions and key distribution protocols.
13. Topics of the Course :

- The ElGamal Cryptosystem
 - The discrete log problem in the finite field \mathbf{Z}_p
 - The ElGamal cryptosystem in the multiplicative group \mathbf{Z}_p^*
 - Algorithms for solving the discrete log problem
 - The discrete log problem in a general finite group G
 - The “generalized” ElGamal cryptosystem in a subgroup H
 - Galois fields
 - Elliptic curves

- The Merkle -Hellman Knapsack Cryptosystem
 - The subset sum problem
 - A super increasing instance of the subset sum problem
 - Modular transformation

- McEliece Cryptosystem
 - Nearest neighbour decoding
 - Syndrome decoding
 - McEliece cryptosystem based on Goppa codes

- Signature Schemes
 - RSA signature scheme
 - The ElGamal signature scheme
 - The Digital signature standard
 - Undeniable signatures
 - One-time signatures

- Hash Functions
 - Collision-free hash functions
 - A hash function based on a discrete log problem
 - Extending hash functions
 - The MD4 hash function
 - The Secure hash standard
 - Time stamping

- Key Distribution and Key Agreement
 - Blom key predistribution scheme
 - Kerberos
 - Diffie-Hellman key exchange
 - MTI key agreement protocols

14. Prescribed Texts:

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) G. J. Simmons, *Contemporary cryptology – the science of information integrity*, IEEE press, 1992.
- d) O. Goldreich, *Foundations of cryptography*, Cambridge University press, 2001.