Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS credits	Module Code	**Module Title**
		5	CMPU4007	Advanced Security 1

8.7.2. Advanced Security 1

Module author: Dr. Fredrick Mtenzi.

Module Description:

Cryptography is the science of providing security for information through the reversible transformation of data. It can also be defined as the study and practice of scrambling information in a manner that is difficult to unscramble, and making scrambled information unintelligible. It is used as the basis of much computer security, in that it can be used to keep information confidential, and also preserve the integrity of data, particularly when being stored or being transmitted. The development of digital computing revolutionized the use cryptography, and has allowed its usage in most computing activities.

Apart from government, military and organisations, users need security provided in cryptography. For example, they will need this kind of security because they may be designing new software, discussing a marketing strategy, or planning a hostile business takeover. The aim of this course is to provide a detailed understanding of the issues involved in Steganography and Cryptography algorithms and techniques used in implementation. The course will introduce and make use of the relevant mathematical concepts such as number theory and finite fields. Practical applications of Steganography and Cryptography will be demonstrated and experimented by students as part of the laboratory exercises or assignments.

Module aim

The aim of this module is.

- to introduce the students to the principles of cryptography and steganography,
- to give the students a thorough understanding of cryptography and steganography algorithms,
- to provide them with an in-depth understanding of how cryptography and steganography provides security in real-life applications.

Learning Outcomes:

On completion of this module, the student will be able to:

- Describe the underlying principles of different cryptography and steganography algorithms.
- Design and implement simple cryptography algorithms using any high level programming language.
- Evaluate the effectiveness of cryptography algorithms according to well known security requirements.
- Apply relevant/appropriate mathematical results in the design and implementation of cryptography algorithms.

Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS credits	Module Code	**Module Title**
		5	CMPU4007	Advanced Security 1

- Describe the principles and deployment of steganography techniques as applied in real-life security.
- Compare and contrast on the effectives and efficiency of cryptography and steganography algorithms.
- Recognise and justify the different scenarios of deploying cryptography and steganography algorithms.
- Select and combine different cryptography algorithms in order to achieve highly secure algorithms.
- Asses and rank cryptography and steganography algorithms according to the protection they provide in real-life applications.
- Explain the principles behind and usage rationale of various encryption techniques.

Learning and Teaching Methods:

In this module a number of teaching methods may be employed including lectures, practical sessions, tutorials and case studies. At least one industrial seminar may be arranged. Focus should be placed on empowering the students to develop their skills independently of the presence of a tutor or lecturer.

Module content:

- Introduction to cryptography
- Number theory, Discrete logarithms and Elliptic Curves
- Steganography
- Block Ciphers and Advanced Encryption Standard, Confidentiality Using Conventional Encryption.
- Public-Key Cryptography and RSA, Key management, Message Authentication and Hash Functions, Hash and Mac Algorithms, Digital Signatures and Authentication Protocols.

Module Assessment

This module should have a 60% weighting for the examination and a 40% weighting for the continuous assessment. While it is important that the student can demonstrate their technical ability with coursework, it is equally important that they demonstrate an understanding of the theoretical aspects of cryptography.

Essential Reading: (author, date, title, publisher)

William Stallings, 2005, Cryptography and Network Security: Principles and Practice, 5th ed, Prentice Hall

Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS credits	Module Code	**Module Title**
		5	CMPU4007	Advanced Security 1

Supplemental Reading: (author, date, title, publisher)

Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, 2010, Cryptography Engineering: Design Principles and Practical Applications, John Wiley & Sons. Inc.

Behrouz A. Forouzan, 2008, Cryptography and Network Security, McGraw-Hill International Edition.

Wade Trappe, Lawrance C. Washington, 2006, Introduction to Cryptography with Coding Theory, Prentice Hall.

Web references, journals and other:

IEEE security & privacy

ACM Transactions on Information and System Security (TISSEC)

http://www.sans.org/rr/

Further Details:

The module will run over one semester, with three contact hours per week. Two hours for lectures and one hour for the laboratory.

Date of Academic Council approval ……