Course Brief and Outline – <~~2019~~>

Academic Staff:

Prof. L. Cheng
Room: CM4 380
Tel number: 011 7177228
e-mail: ling.cheng@wits.ac.za

1 Course Background

Information Engineering has a substantial body of fundamental and specialist knowledge, such as cryptography, data compression and error control coding. This course provides a foundation for much of them.

2 Course Objectives

The objective of this course is to provide the future Information Engineering Option graduate with the tools needed to deal effectively with information in its many forms. The course focuses on the information itself information laws, information conversion and representation, special properties of information which can be exploited for the purposes of storage and transmission, and methods of protecting information from natural and human hazards.

3 Course Outcomes

On successful completion of this course, the student is able to:

1. Recognise, compare, correctly apply and comment on the merits of a variety of cryptographic, compression and error detection and correction algorithms.
2. Identify types and properties of information in an information processing environment, and hence be able to devise architectures and choose algorithms for dealing appropriately with the information at hand.
3. Demonstrate an understanding of fundamental information laws and theorems, and will be able to engineer information systems in accordance with these laws and theorems.

4 Course Content

- Security: Cryptography, cryptology and cryptanalysis, encryption, measures of effectiveness of encryption algorithms, symmetric and asymmetric (public key) algorithms, standards, block ciphers and stream ciphers, public key algorithms, authentication, integrity and non-repudiation, key handling, multiple public key cryptography, secret sharing, SET (secure electronic transactions), e-commerce, cryptographic hardware/software requirements and tradeoffs, Network security, IDS (Intrusion Detection Systems), viruses, worms, trojans.
- Information integrity: Integrity checking - parity checks, checksums, LRC, CRC, Error correction FEC, Hamming distances and codes, Reed-Solomon coding,

matching the coding scheme to the channel error characteristics, line codes, LDPC principles.

- Compression: Entropy of information, source modelling, origins of redundancy, compressibility and compression to remove redundant information, lossless and lossy compression, statistical methods and dictionary-based methods, examples of lossless compression algorithms - lossless video and audio compression, lossy compression algorithms for different source types (telecommunications and multimedia), sensitivity of compressed information to errors - methods of dealing with this problem, effect of compressed information on network traffic patterns.

5 Prior Knowledge Assumed

The following prior knowledge is assumed on the part of students starting this course:

Pre-requisites: Signals and Systems I, Data Structures and Algorithms
Co-requisites: Computational Mathematics, Signals and Systems II

The prerequisites and co-requisites to register for this course are defined in the current *Rules & Syllabuses: Faculty of Engineering and the Built Environment*.

6 Assessment

6.1 Formative Assessments Elements

All submissions must be in strict accordance with the guidelines contained in the School's Blue Book and the rules contained in the School's Red Book. No exceptions will be considered.

6.2 Summative Assessment

Table 1: Summative assessment contributions

Summative Assessment Contributor	Duration h	Component Yes/No	Method & Weight %	Calculator Type 0/1/2/3	Permitted Supporting Material
Test	1h30	Yes	20	2	A4 handwritten information sheet (no examples or fully worked solutions allowed)
Lab	68h45	Yes	20	N/A	N/A
Exam	3h00	Yes	60	2	A4 handwritten information sheet (no examples or fully worked solutions allowed)

6.3 Assessment Methods

As per the rule G-13 as posted on the student notice board as well.

The course knowledge area will be assessed by means of one (1) test, six (6) laboratories and one (1) exam.

7 Satisfactory Performance (SP) Requirements

For the purpose of Rule G.13 *satisfactory performance in the work of the class* means attendance and completion of prescribed laboratory activities, attendance at tutorials designated as compulsory in this CB&O, submission of assignments, writing of scheduled tests unless excused in terms of due procedure.

8 Teaching and Learning Process

8.1 Teaching and Learning Approach

The students would be required to mathematically model and solve a number of problems related to the aspects mentioned in Section 4 (Course Content), and eventually analyse and interpret the obtained solution.

Application of knowledge of basic mathematics and basic communication engineering learned to model and solve problems related to the aspects mentioned in Section 4 (Course Content) and/or analysis for a given set of specifications.

Lab work a involving use of tools to analyse the aspects mentioned in Section 4 (Course Content).

The use of a programming language to develop a basic application, using the programming skills, in the course labs.

Technical report about the labs would be submitted by the students and assessed.

Labs will be conducted by a team of 2 students.

The Labs will require management of the complete lab lifecycle, involving the precise specification of the lab, features to be implemented, division of tasks, creation of timeline and allocation of resources and then eventual execution of the lab and its submission by the deadline.

8.2 Information to Support the Course

No prescribed textbook for course. Prescribed reading material comprises handouts, www links and library references.

Recommended monograph and book:

L. Cheng, “A short course on error control coding”. Class handout.

Bruen et al., “Cryptography, information theory, and error-correction: a handbook for the 21st century”, John Wiley and Sons Inc., 2005, ISBN 0-471-65317-9.

8.3 Learning Activities and Arrangements

Lectures:

There are twenty (20) double 45-minute lectures scheduled as shown on the third year first semester timetable and provided by the course coordinator. Lectures will be used to cover some material not included in course notes. The final examination will assume that students are familiar with all material covered in the notes, in the laboratories, in the project and during lecture periods.

Tutorials:

There are six (6) 45-minute tutorial sessions as shown on the timetable provided by the course coordinator. The venue information will be found on the same timetable.

Laboratory:

There are six (6) laboratory submissions as shown on the course website updated by the course coordinator. The venue is the D-Lab on Mondays/~~Tuesdays~~ during the first semester teaching blocks.

Consultation:

All questions arising from the laboratories must be directed to the demonstrator responsible. Questions relating to the use of the laboratory and its equipment must be directed to the lecturer. Questions relating to lectures and course material must be directed to the lecturer either during lectures or during formal consultation periods. Formal consultation periods will be scheduled at students' request. Students must, however, try to resolve any problems amongst themselves first.

9 Course Home Page

Further information and announcements regarding the course are posted on the course home page:

http://dept.ee.wits.ac.za/%7Echeng/ELEN3015/

All students are expected to consult the course home page at regular intervals.