

Course Brief and Outline

Ling Cheng

School of Electrical and Information Engineering
University of the Witwatersrand



Outline

- 1 Course Brief and Outline
- 2 Overview of Course Contents
- 3 Information to Support the Course



Course Coordinator

Ling Cheng

Office: CM4 380

Tel no: 011 - 7177228

Webpage: <http://dept.ee.wits.ac.za/~cheng/ELEN3015/>



Consultation Times

- Modified open door policy - have to show attempt at problem
- Call me to see if available (any time)
- Otherwise email and confirm an appointment



Course Content

The following areas are covered in the course:

- Security
- Information Integrity
- Compression



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, cryptographic hardware/software requirements and tradeoffs



Course Content - Information Integrity

Integrity checking - parity checks, checksums, CRC, Error correction FEC, Hamming distances and codes, Reed-Solomon coding, line codes



Course Content - 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 (telecomms and multimedia), sensitivity of compressed information to errors - methods of dealing with this problem, effect of compressed information on network traffic patterns.



Assessment

- Laboratories: 20 %
- Class Test: 20 %
- Exam: 60 %



Arrangements

- Lectures: Thursdays - Periods 1, 2; Fridays - Period 1
- Tutorials: Fridays - Period 2 (Flexible according to the course progress)
- Laboratories: Mondays and Tuesdays - More info to be provided later
- Class test and exam dates: Refer to School schedules



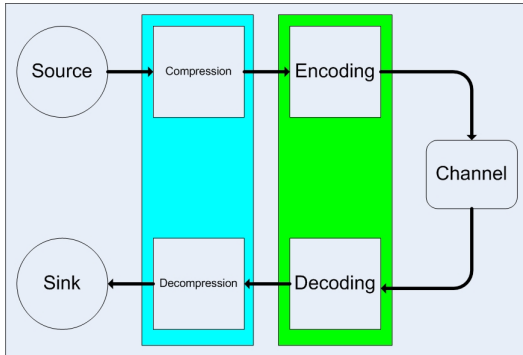
Compression and Information Integrity

Simplistic model for digitized voice transmission ?

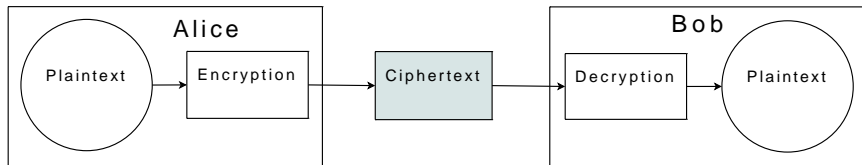
(Example - Telephone, Cellphone → point-to-point communication)



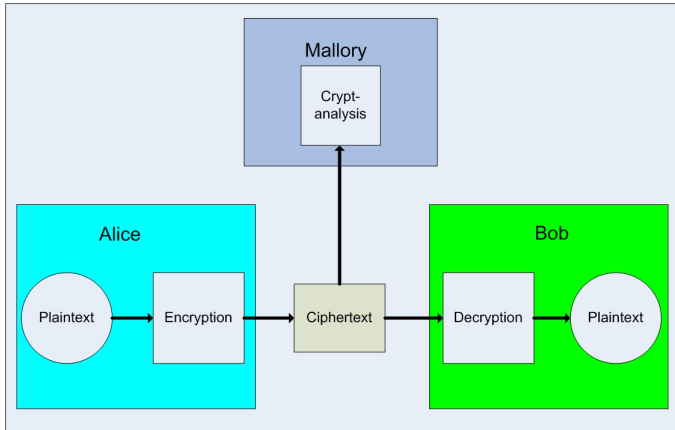
Compression and Information Integrity



Cryptography



Cryptanalysis



Prescribed Textbook:

No prescribed textbook for course.

Prescribed reading material comprises handouts, www links and library references

Recommended book:

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.



All students are expected to regularly consult the course home page.

