University of Salahaddin-Hawler
College of Science
Department of Computer Science& Information Technology

Course Book

Information Theory

Undergraduate Degree in Computer Science
4rd Year Class -
Academic year 2015-2016

Assistant Instructor
Sheelan K.Sharaza
M.Sc.degree in Applied Mathematics
Email: shelan2001@yahoo.com

Class hours: Tuesday 10:30 am – 12:30 pm
Thursday 9:30 am – 10:30 am
Office hours: Monday12:30 pm – 2:30 pm

Format

3 hrs/week of lecture,

Unit Value: 6 units

Course Description

This is intended to be a straightforward and accessible course on information theory. Information theory is the mathematical theory that deals with the fundamental aspects of communication systems. As such, its primary goal is not to deliver practical solutions to communications problems, but rather to answer the question whether encoding and decoding schemes exist or not for a given combination of a source model and a channel model. The two main outcomes of single-user information theory are that any source requires a minimum description rate to represent its output faithfully (source coding theorem) and that any channel is characterized by a maximum transmission rate above which the probability of error cannot be made arbitrarily small (channel coding theorem). The purpose of this course is to develop the fundamental ideas of information theory and to indicate where and how the theory can be applied.

Course Goals

This course will provide students with an in-depth understanding of the many applications of Information Theory including data compression, channel coding, encryption.

Student Evaluation

Midterm exam1: 20 % marks.

Midterm exam2: 20 % marks.

Final exam: 60 % marks.

The examination schedule will be announced by the department.

Recommended references

- Bruce Schneier, **Applied cryptography**(second edition), 1996.
- Johannes Buchmann, **Introduction to Cryptography** (Second Edition), Springer 2000.
- Nigal Smart, **Cryptography, An Introduction** (Second Edition), 2007(available free at http://www.cs.bris.as.uk/~nigel/Crypto Book/).
- Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman **An Introduction to Mathematical Cryptography** , 2008
- Matt Bishop **Introduction to Computer Security** ,2005
- R. W. Hamming, **Coding and Information Theory**, 2nd Ed., Prentice-Hall Inc.,1986

Weekly Topics

- **Cryptography:**

Weeks 1,2 : Introduction of Computer Security and basic terminology of Computer security.

Weeks 3,4 :Classical cipher systems will be chosen monoalphabtics cipher, Message Reversal ,permutation cipher, Caesar cipher , additive cipher, Keyword Cipher, Polybius Square.

Week 5 : Polyalphabetic ciphers: Vigenere cipher, Beaufort Cipher,
Weeks 6,7 : Polygraphic Ciphers : Playfair Cipher, Bifid Cipher, Trifid Cipher, Four-square Cipher. Other Ciphers and Codes
Week 8,9 : Number theory topics will be chosen from: prime numbers, greatest common divisor, Least Common Multiple (LCM) , Modular ,prime factorization of long integers, Euler's function, Inverse Algorithm (inv) , fast exponentiation algorithm , Matrices, Inverse of Matrix,

Weeks 10,11,12 : Public key crypto-systems ,Summary and examples Block and stream ciphers,

-Information Theory -

Weeks13,14:**Principles of Information Theory:**

Some rules of probability theory.

-Basic concepts of Information Theory:

Self Information , Average amount of information -
(Entropy), Joint and Conditional Entropies(Mutual -
Information), Properties of the Information Measures.

Weeks 15,16 :**-Communication systems and Information channels:**

Definitions, Channel Capacity, Redundancy, and -
Transmission Efficienc

-

Weeks 17,18.19: **-Some Special Channels and there capacity:**

Ideal channel,completley Noisy ,completely Lossy -
channel,Noiseless channel,Lossless channel , Uniform
channel , Binary symmetric channel BSC,Binary
Erasure channel BEC, General Binary Channel GBC,Cascaded -
channels or channels in series , Channels in Parallel.

-Extension of a Source. Extension of a Channel. -

- Coding

Week 20:- Introduction, source coding and there types.

Weeks 21,22,23:- Efficiency of an encoding procedure.

-Relative redundancy of the code
- Shannon –Fano encoding procedure.
- Huffman encoding procedure
- Error –Detecting and Error-Correcting Codes
- Hamming cod

Final exam will be determined by the exam board of the college.

Notice that this syllabus may be subject to changes; we may take either longer or shorter time to finish them.