A POLYTECHNIC INSTITUTION

Course Outline

School of Computing & Academic Studies
Program: Computer Systems Technology
Option: B.Tech

Comp 7402
Cryptography and Cryptanalysis

Start Date:	January 10th			**End Date:**	March 28th		
Total Hours:	45	**Total Weeks:**	12	**Term:** Fall		**Course Credits:** 3	
Hours/Week:	3.5	**Lecture:** 2	**Lab:** 1.5	**Shop:** N/A		**Seminar:** N/A	**Other:** N/A

Prerequisites: B.Tech Admission

Course No.		**Course No.**	
N/A	N/A	N/A	N/A

■ Course Description

The course teaches students the art and science of securing data (information). Course components will cover Cryptography with an introduction to Cryptanalysis, with an emphasis on the practical implementation of Cryptographic algorithms and techniques. Topics in Cryptography will include traditional substitution and transposition ciphers; monoalphabetic/polyalphabetic ciphers. Modern block ciphers such as Feistel, DES (and variants), and AES will be covered in detail. Stream ciphers such as OTP, RC4, Salsa20 and ChaCha will be covered. Applications will include bit-manipulation ciphers, secret and public-key ciphers (RSA). Topics in Cryptanalysis will include traditional techniques such as Frequency Analysis, Ciphertext-only, Known-plaintext, and Chosen-plaintext attacks. Students will also be introduced to more modern linear and differential cryptanalysis. Students will be permitted to choose programming languages of their choice in the implementation of algorithms during assignments and final projects.

■ Evaluation

Final Examination	30%	Comments: Passing mark is 60%
Midterm	20%	
Assignments/Projects	50%	
TOTAL	100%	

■ Course Learning Outcomes/Competencies

Upon successful completion, the student will:

1. Have a working knowledge of the mathematical foundations of cryptography and the importance of pseudo-random number generators.
2. Have a solid understanding of cryptographic techniques with an emphasis on practical applications.
3. Be able to implement any of the algorithms covered in the course using any programming language of choice.
4. Have a detailed understanding of cryptographic protocols; evaluate and analyze the various cryptographic techniques such as key management algorithms, symmetric and asymmetric algorithms, hashes and signatures.
5. Understand and apply various cryptanalysis techniques to retrieve plaintext messages from ciphertext.
6. Understand the basics of strong cryptographic algorithms and be able to analyze and evaluate them for potential use within an organization.
7. Acquire a solid foundation for pursuing more advanced courses in the field of Cryptology.
8. Be able to configure and deploy cryptographic tools for applications such as email, securing sensitive files, etc.

■ Verification

I verify that the content of this course outline is current.

Aman Abdulla	January 2, 2019
Authoring Instructor	Date

I verify that this course outline has been reviewed.

Program Head/Chief Instructor	Date

I verify that this course outline complies with BCIT policy.

Dean/Associate Dean	Date

Note: Should changes be required to the content of this course outline, students will be given reasonable notice.

■ Instructor

Aman Abdulla	Office Location: SW2-323	Office Phone:	(604) 432-8837
	Office Hrs.:	E-mail Address:	aabdulla@milliways.bcit.ca

■ Learning Resources

Required:

Cryptography and Network Security: Principles and Practice (latest edition)
William Stallings
Pearson

Recommended:

Applied Cryptography: Protocols, Algorithms, and Source Code in C (latest edition)
Bruce Schneier
John Wiley

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography
Simon Singh
Anchor; Reprint edition

■ Information for Students

(Information below can be adapted and supplemented as necessary.)

The following statements are in accordance with the BCIT Student Regulations Policy 5002. To review the full policy, please refer to: http://www.bcit.ca/~presoff/5002.pdf.

Attendance/Illness:
In case of illness or other unavoidable cause of absence, the student must communicate as soon as possible with his/her instructor or Program Head or Chief Instructor, indicating the reason for the absence. Prolonged illness of three or more consecutive days must have a BCIT medical certificate sent to the department. Excessive absence may result in failure or immediate withdrawal from the course or program.

Academic Misconduct:
Violations of academic integrity, including dishonesty in assignments, examinations, or other academic performances are prohibited and will be handled in accordance with the 'Violations of Standards of Conduct' section of Policy 5002.

Attempts:
Students must successfully complete a course within a maximum of three attempts at the course. Students with two attempts in a single course will be allowed to repeat the course only upon special written permission from the Associate Dean. Students who have not successfully completed a course within three attempts will not be eligible to graduate from their respective program.

Schedule

- **Topics may be omitted, replaced or added at the discretion of the instructor.**

Topic Number	Outcome/Material Covered
1	**Introduction & A Brief History of Cryptology (Cryptography and Cryptanalysis)** • Terminology • Early Cryptographic Systems • Cryptographic Developments during the World Wars • Modern Cryptography
2	**Mathematical Foundations:** • Modular Arithmetic • Modular exponentiation • Modulo2 Arithmetic and Galois Fields • Cyclic Redundancy Checks • Prime Numbers • Probability Theory
3	**Cryptographic Basics:** • Substitution and Transposition Ciphers • One-Time Pads • Stream Ciphers • Block Ciphers • Bit Manipulation Ciphers
4	**Cryptographic Protocols:** • Symmetric Cryptography • One-Way Hash Functions • Public-Key Cryptography • Digital Signatures and Encryption • Random and Pseudo-Random-Sequence Generation
5	**Basic Protocols:** • Key Exchange • Authentication • Authentication and Key Exchange • Public-Key Cryptography • Analysis of Authentication and Key Exchange Protocols • Secret Splitting • Secret Sharing
6	**Cryptographic Techniques:** • Key Length • Public Key Length • Public-Key Cryptography • Key Length Analysis and Security Requirements • Key Management and Distribution

Topic Number	Outcome/Material Covered
7	**Algorithm Types and Modes:** - Electronic Codebook Mode - Block Replay - Cipher Block Chaining Mode - Cipher Feedback Mode - Synchronous Stream Ciphers - Output Feedback Mode
8	**The Data Encryption Standard (DES) and Variants:** - DES Structure and Analysis - DES Security - Public-Key Cryptography - Multiple DES
9	**Advanced Encryption Standard (AES):** - Field Arithmetic - AES Structure and Analysis - AES Security
10	**Modern Stream Ciphers:** - Salsa20 - ChaCha
11	**Basic Cryptanalysis:** - Introduction to Cryptanalysis - Breaking Substitution Ciphers - Frequency Analysis for Ciphers - Frequency Analysis Attacks – Breaking Transposition Ciphers - Breaking Block Ciphers – Slide attack - Breaking Block Ciphers – Boom attack
*12	**Linear and Differential Cryptanalysis:** - Introduction to Linear Cryptanalysis - Software implementation of Linear Cryptanalysis - Introduction to Differential Cryptanalysis - Software Implementation of Differential Cryptanalysis

* Time Permitting

- Course resources will be posted on my Web server which you may access using the following URL:

  http://milliways.bcit.ca/c7402