Programs & Courses

COMP 7402 - Topics in Computer Programming - Cryptology

School:	School of Computing and Academic Studies
Program:	Bachelor of Technology - Computer Systems
Course Credits:	3
Minimum Passing Grade:	60%
Start Date:	January 10, 2019
End Date:	March 28, 2019
Total Hours:	36
Total Weeks:	12
Hours/Weeks:	3
Delivery Type:	Lecture/Lab
CRN:	86173

Instructor Details

Name: Aman Abdulla
Email: Instructor to provide
Location: SW02-323
Office Hours: Instructor to provide

Course description

This 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 substitution and transposition ciphers, including stream and block ciphers. Applications will include bit-manipulation ciphers, secret and public-key ciphers. Topics in Cryptanalysis will include traditional techniques such as 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.

Course goals

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.

Course learning outcomes / competencies

Upon successful completion of this course, the student will be able to:

- Explain the mathematical foundations of cryptography and the importance of pseudo-random number generators.
- Demonstrate use of cryptographic protocols.
- Evaluate and analyze the various cryptographic techniques such as key management algorithms, symmetric and asymmetric algorithms, hashes and signatures.
- Apply various cryptanalysis techniques to retrieve plaintext messages from ciphertext.
- Explain the basics of strong cryptographic algorithms and their applications.
- Analyze and evaluate cryptographic algorithms for potential use within an organization.
- Configure and deploy cryptographic tools for applications such as email, securing sensitive files, etc.
- Implement any of the algorithms covered in the course using any programming language of choice.

Evaluation criteria

Criteria	%	Comments
Final Examination	30%	
Midterm	20%	
Assignments/Projects	50%	

TOTAL	100%	

The passing grade for this course is 60%.

Attendance requirements

Attendance in class is mandatory.

In case of illness or other unavoidable cause of absence, the student must communicate as soon as possible with his/her instructor indicating the reason for the absence.

Prolonged illness which causes the student to miss 10% or more of the labs will require a BCIT-approved medical certificate submitted to the department, substantiating the reason for the absence.

Unapproved absence of 10% or more of the labs may result in failure or forced withdrawal from this course.

Learning resources

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[1]

John Wiley

The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography

Simon Singh

Anchor; Reprint edition

Course schedule and assignments

- **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 and Key Exchange • Public-Key Cryptography • Analysis of Authentication and Key Exchange Protocols • Secret Splitting • Secret Sharing

Topic Number	Outcome/Material Covered
6	**Cryptographic Techniques:** • Key Length • Public Key Length • Public-Key Cryptography • Key Length Analysis and Security Requirements • Key Management and Distribution
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

BCIT policy