MATH 4282 – Winter 2019
Cryptography

Instructor

- Name: Dr. David Pike
- Office: Henrietta Harvey Building – Room 2024
- Phone: 864-8096
- Email: *dapike@mun.ca*

- Office Hours: 11:00–12:00 on Tuesday and Thursday, or by appointment

Course Info

- Location: Henrietta Harvey Building – Room 3015
- Class Times: 14:00–15:15 on Tuesday and Thursday
- Prerequisite: MATH 3370 (Introductory Number Theory) and a computing course
- Textbooks:
  - "Introduction to Cryptography" by Alexander Stanoyevitch. CRC Press.
  - "Cryptography: Theory and Practice" by Douglas Stinson. CRC Press.
- Webpage: somewhere at `www.math.mun.ca/~dapike`

Course Outline

Topics will include private-key cryptosystems (such as classical ciphers, the Hill cipher, etc.), computational complexity and relevant number theoretic problems (such as primality testing, factoring, and the discrete logarithm problem), public-key cryptosystems (such as RSA, Rabin, and ElGamal), digital signatures, and authentication protocols.

The following outline offers further details on the topics that are likely to be included in the course. Note that emphasis will be placed upon the mathematics that is involved in the encryption and decryption protocols of ciphers, as well as in their security (or lack thereof). In that sense, the focus is on *why* things work, not just *how* they work.

1. Introduction to Data Security

   Included in this topic will be the question of how secure a cryptosystem is. For instance, what types of attack might it be susceptible to, such types including known plaintext attacks, chosen plaintext attacks, and known ciphertext attack. Also there's the distinction between absolute security and computational security.

2. Classical Ciphers

   (a) shift cipher
   (b) substitution cipher
   (c) Vigenère cipher
   (d) Hill cipher

   In addition to studying the encryption/decryption protocols of each cipher, we will analyse the security of each cipher and show how each is insecure.

3. Some comments on Private-Key Cryptosystems

   Up to this point all ciphers mentioned have been private-key systems. The nature of private-key cryptosystems is such that there are issues of key management and distribution. There are also the issues of how to achieve authentication (which introduces the concept of a digital signature), as well as how to agree upon a key in the first place (this would be a good spot to discuss the Diffie-Hellman key exchange protocol, but doing so first requires a discussion of the discrete logarithm problem).

4. Public-Key Cryptography

   The first cipher to be discussed is RSA. To fully appreciate and understand the mechanics and theoretical reliability of the RSA cryptosystem requires that we also study the topics of primality testing and factoring, which is where we get into some advanced number theory (particularly when discussing primality testing, where we look at quadratic residues, Legendre symbols, and Jacobi symbols). With respect to factoring, several methods are discussed:

   (a) the naïve method
   (b) Pollard rho
   (c) Pollard $p - 1$
   (d) Random squares
   (e) Quadratic Sieve
   (f) Number Field Sieve

   RSA can be used to implement digital signatures and authentication protocols, which we then discuss.

   The Rabin cryptosystem is introduced as a cipher whose security is provably equal to the difficulty of factoring.

   The ElGamal cryptosystem is an example of a cipher based upon the discrete logarithm problem. Methods for solving the discrete logarithm problem are therefore discussed.

Method of Evaluation and Related Policies

- Assignments will be due at the time and date announced when distributed. Assignments should be submitted to the designated assignment box in the corridor near the Math & Stats General Office, located in the Henrietta Harvey Building. Late assignments will not be accepted and will receive a grade of zero.

- Plagiarism, cheating, and academic dishonesty will not be tolerated. The minimum penalty for any form of cheating on an assignment, test, etc. will be a grade of zero for the corresponding assignment, test, etc.

- It shouldn't need to be said, but inevitably somebody puts me through this test: on homework, quizzes, tests, etc., I expect you to show your work. Simply stating the ultimate answer (even if it is correct) will rarely get you full credit; the work behind your answer is usually given more credit than the answer itself. In short, your job is to *show* that you know *how* to do the exercises.

  Moreover, your work should reflect clear content as well as coherent reasoning and organised structure. Part of what this means is that your work should be clear to follow and should

show a logical progression of thought. Arguments that wander around the point, or which include extraneous and/or irrelevant side details, are inferior to arguments that do not go astray at times. Likewise, if you have to guide me through your work in order to point out your thought process (again, even if you got the correct answer in the end), then you should not expect to get full credit.

- Be aware that not all learning takes place in the classroom. Expect to devote personal time to ensure that you fully comprehend and understand the material. This will likely entail reading from the textbook, consulting with additional resources, engaging in interactive discussions, as well as doing exercises beyond those which are assigned.

- Quizzes and/or tests will be regularly administered. Crib sheets will not be allowed.

  Expect to have photo-id checked during each test and exam.

  Accommodation for missed quizzes or tests will be given only for legitimate absences, and only if the request for accommodation is brought to my attention promptly, in writing, and in accord with university regulations; otherwise, a score of zero will be assigned for any missed quizzes and/or tests.

  March 21 is a likely date for one of the tests.

  In the event that a test is cancelled due to inclement weather, the test will be automatically rescheduled for the next lecture time.

- The final exam will be comprehensive.

- Final course grades will be based upon the following scheme

Homework:	30
Quizzes and/or Tests:	30
Final Exam:	40
	100

  Notwithstanding the above formula, a combined score of at least 30 out of the 70 possible points must be achieved on the quizzes/tests and the final exam in order to pass the course.

- Requests for "extra-credit" projects will be denied. Put simply, your grade will be based upon the required course-work as indicated in this syllabus.

If You're Thinking of Majoring in Math...

... but aren't sure what career options would be available with a Math degree, then here are some resources that you can look at:

- "101 Careers in Mathematics" by Andrew Sterrett. Call Number: QA 10.5.A15 1996
- "She Does Math!" by Marla Parker. Call Number: QA 27.5.S53 1995
- `www.ams.org/careers/`
- `www.cms.math.ca/Education/MathAtWork`

If you want to talk to somebody for academic advice concerning undergraduate programmes of study in Mathematics, you can see Tara Stuckless in the Henrietta Harvey Building, Room 3004. Also, the Department of Mathematics and Statistics has information about its courses and programmes of study, located at: `www.mun.ca/math/undergraduate/ugrad-msprograms`