COMPUTER SCIENCE DEPARTMENT
MET CS 789 CRYPTOGRAPHY

Course Overview

The course covers the main concepts and principles of cryptography with the main emphasis put on public key cryptography. It begins with the review of integers and a thorough coverage of the fundamentals of finite group theory followed by the RSA and ElGamal ciphers. Primitive roots in cyclic groups and the discrete log problem are discussed. Baby-step Giant-step and the Index Calculus probabilistic algorithms to compute discrete logs in cyclic groups are presented. Naor–Reingold and Blum–Blum–Shub Random Number Generators as well as Fermat, Euler and Miller-Rabin primality tests are thoroughly covered. Pollard's Rho, Pollard's p-1 factorization algorithms are presented. The course ends with the coverage of some oblivious transfer protocols and zero-knowledge proofs. There are numerous programming assignments in the course.

Prerequisites

MET CS 248 Discrete Mathematics and MET CS 566 Analysis of Algorithms

Learning Objectives

By the end of this course, the student will have learned

1. Concepts of symmetric and public key cryptography;
2. The RSA and ElGamal asymmetric ciphers as well as the Diffie-Hellman Key;
3. Exchange Protocol and the Key Management Systems;
4. Algorithms to compute the Discrete Logarithm in cyclic groups, the Baby-step Giant-step Algorithm and the Index Calculus Algorithm;
5. Oblivious Transfer Protocols, Zero Knowledge Proof protocols, and Digital Signatures;
6. Blum-Blum-Shub and Naor-Reingold pseudorandom number generators;
7. Probabilistic algorithms to check the primality of large numbers;
8. Factorization attacks including Pollard's Rho Method, and Pollard's p-1 Method.

Required Textbook

There is no required textbook for this course. The course notes should be sufficient for all the subjects covered. In the past, *Making, Breaking Codes: An Introduction to Cryptology* by Paul Garrett has been used, but unfortunately this textbook is now difficult to get and so won't be used, or required. There just aren't any other textbooks that cover all the materials for the course. However, there are some textbooks that you might find useful. They're optional

Recommended Reference Textbooks—In Order of Preference

Garrett, Paul—*Making, Breaking Codes: An Introduction to Cryptology, 2nd Edition*
Prentice Hall, ISBN-10: 0-13-186146-8
Amazon: https://www.amazon.com/dp/B01FEKZJOC/ref=cm_sw_em_r_mt_dp_slgtFb2XW8ZHK

It's ridiculously expensive new, if you can find it, but if you can get Garrett's book, it is quite good at explaining the basic mathematics covered in this course, but it isn't necessary. There are a lot of mistakes in the text, though, so be sure to check out the Errata[1].

[1] http://www-users.math.umn.edu/~garrett/crypto/Errata2.html

Smart, Nigel—*Cryptography: An Introduction*
McGraw-Hill College, ISBN-13: 978-0077099879
Amazon: https://www.amazon.com/dp/0077099877/ref=cm_sw_em_r_mt_dp_EigtFbSE7YVY1

I quite like this book and it does a better job of explaining cryptology and topics that Garrett doesn't cover, but it doesn't provide the more strong mathematical treatment that you'll get from Garrett.

Other Resources

Forouzan, Behrouz—*Cryptography and Network Security*,
McGraw Hill, ISBN-13 978-0-0-7332753-2
Amazon: https://www.amazon.com/dp/0073327530/ref=cm_sw_em_r_mt_dp_gIgtFb6NP8JGY

This book is quite good and is the main text for MET CS 799, Advanced Cryptography. I find it superior in almost everyway to the following Stallings text.

Stallings, William—*Cryptography and Network Security. Principles and Practice, 7th Edition*
Prentice Hall, ISBN-10: 0-13-444428-0
Amazon: https://www.amazon.com/dp/0134444280/ref=cm_sw_em_r_mt_dp_8VgtFbSX7ZVGZ

The Stallings book is one of the most popular cryptology textbooks, but it frankly isn't very good helping the student understand the mathematical underpinnings of cryptology. It is, however, useful as a reference work because it covers a large number of topics.

Evaluation and Grading

There will be a midterm exam and a final project. If any grading event will be missed, it is the responsibility of the student to arrange a mutually agreeable schedule for completion.

Class Participation	20%
Midterm	50%
Final Project	30%

What does "Class Participation" mean? It is attending the lectures, asking questions, answering questions, and commenting on topics in the lecture, where appropriate. The lecture notes and the homework problems will be made available prior to class. **Please print the lecture notes and bring them with you to class, or otherwise have them available, so you can focus on the lecture and not taking free form notes.** The Midterm is open book and open notes; you can even use the algorithms you developed in the course, but you must not browse the web or use any materials you haven't carried in with you.

The Final Project will be described in more detail later, but it entails creating a set of programs that allows you to encrypt, decrypt, and as an attacker, break encryption. All the programs you need to complete the Final Project are in the homework assignments. You may use any program language you like, but I strongly recommend a programming language with infinite magnitude integers that are unbounded in size, since the size of the integers you'll be working with will exceed the size of a single computer word, in most cases—Python is a good choice.

Note that homework is not graded and is there to challenge the student and help them grasp whether they have mastered the materials. It is extremely important to note that the programming assignments associated with the homework makes up the bulk of the final project. If you don't do the homework assignments you won't be prepared for either the midterm or the final project, so do the homework assignments when assigned. You don't want to wait until the end of the semester and have to rush and get your programming done all at once.

Many students find this class challenging. I very **strongly** encourage students to keep current with the homework, programming assignments, and form small study groups (unfortunately remote for this fall) in order help each other to master the material.

Academic Honesty

The course is governed by the Academic Conduct Committee policies regarding plagiarism (any attempt to represent the work of another person as one's own). This includes copying (even with modifications) of a program or segment of code. You can discuss general ideas with other people, but the work you submit must be your own. Cheating and plagiarism will not be tolerated in any Metropolitan College course. They will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code[2]:

This should not be understood as a discouragement for discussing the material or your particular approach to a problem with other students in the class. On the contrary, you should share your thoughts, questions and solutions. Naturally, if you choose to work in a group, which is encouraged, you will be expected to come up with more than one and highly original solutions rather than the same mistakes. Your code should be your own.

Class Location

~~Although we have a majority of Learn from Anywhere (LfA) students, some students still desire the in-person format. So, I'll be teaching this course at Boston University,~~ **~~College of General Studies Building, 871 Commonwealth Avenue, Room 121~~**~~, in person. While delivered in-person, the classes will be available on Zoom in Blackboard also, consistent with the LfA approach. I've never given the course like this before, so please bear with me as we try to work the bugs out of this.~~

The class will be taught completely remotely on Zoom in Blackboard. I've never given the course like this before, so please bear with me as we try to work the bugs out of this.

COVID-19 Precautions

Since we'll be doing the class completely remotely the following should not be necessary, but when going to campus please kindly observe the following precautions.

For those attending in-person, classrooms on campus have new capacities that follow guidelines issued by state and local health and government authorities related to COVID-19 and physical distancing. Please review the links below.

All students returning to campus will be required, through a digital agreement, to commit to a set of Health Commitments and Expectations[3] including face coverings, symptom attestation, testing, contact tracing, quarantine, and isolation. The agreement makes clear that compliance is a condition of being a member of our on-campus community.

You have a critical role to play in minimizing transmission of COVID-19 within the University community, so the University is requiring that you make your own health and safety commitments. Additionally, if you will be attending this class in person, you will be asked to show your Healthway[4] badge on your mobile device to the instructor in the classroom prior to starting class, and wear your face

[2] http://www.bu.edu/academics/policies/academic-conduct-code/
[3] http://www.bu.edu/dos/policies/lifebook/covid-19-policies-for-students/
[4] https://www.bu.edu/healthway/

mask over your mouth and nose at all times. If you do not comply with these rules you will be asked to leave the classroom. If you refuse to leave the class, the instructor will inform the class that they will not proceed with instruction until you leave the room. If you still refuse to leave the room, the instructor will dismiss the class and will contact the academic Dean's office for follow up.

Boston University is committed to offering the best learning environment for you, but to succeed, we need your help. We all must be responsible and respectful. If you do not want to follow these guidelines, you must participate in class remotely, so that you do not put your classmates or others at undue risk. We are counting on all members of our community to be courteous and collegial, whether they are with classmates and colleagues on campus, in the classroom, or engaging with us remotely, as we work together this fall semester.

Schedule of Classes

09/14 Integers—Divisibility, Unique Factorization, Euclidean Algorithm, Multiplicative Inverses, Equivalence Relations, and Modular Arithmetic

09/21 Groups—Definition of Groups and Subgroups, Lagrange's Theorem, Index of a Subgroup, Cyclic Subgroups, and Euler's Theorem

09/28 Exponentiation Algorithm, Fields, Primitive Roots, Discrete Logs, ElGamal Cipher, and Diffie-Hellman Key Exchange

10/05 Primitive Root Search Algorithm, Baby-Step Giant-Step Algorithm, The Index Calculus Algorithm, and Public-Key Ciphers

10/12 **NO CLASS**—Columbus Day—Class on Tuesday

10/13 RSA Public Key Encryption

10/19 The Chinese Remainder Theorem, Euler Criterion, and Roots Mod Composites

10/26 **Midterm Exam**

11/02 The Oblivious Transfer Protocol (factorization and discrete log), Zero Knowledge Proofs, and the Digital Signature Algorithm

11/09 Quadratic Reciprocity and Pseudoprimes

11/16 Pseudorandom Numbers, Fermat, Euler, and Miller-Rabin, Pseudo and Probabilistic Primes, and the Miller-Rabin Test

11/23 Random Number Generators—Linear Congruent Generator, Feedback Shift Generator, Naor-Reingold Number Generator, Blum-Blum-Shub Random Number Generator

11/30 Factorization Attacks—Pollard's Rho Method, Pollard's p-1 Method

12/07 No Class or Possible Makeup—Additional time to work on final project

12/14 **Final Project**

Instructor Information

Geoffrey Pascoe
Computer Science Department, Metropolitan College,
1010 Commonwealth Avenue, 3rd Floor
Boston, MA 02215
Cell: 603-866-1067
Email: gpascoe@bu.edu
Office hours by appointment via Zoom or Google Meeting