BOSTON UNIVERSITY
METROPOLITAN COLLEGE
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.

Recommended Textbooks—In Order of Preference

Garrett, Paul — *Making, Breaking Codes: An Introduction to Cryptology, 2nd Edition*
Prentice Hall, ISBN-10: 0-13-186146-8

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 at http://www-users.math.umn.edu/~garrett/crypto/Errata2.html

---

Forouzan, Behrouz, A. — *Cryptography and Network Security*,
McGraw Hill, ISBN-13 978-0-0-7332753-2

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

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 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 encourage students to form small study groups to 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.

Class Location: PSY, 64-86 Cummington Mall, Room B45

Schedule of Classes

9/9 Integers—Divisibility, Unique Factorization, Euclidean Algorithm, Multiplicative Inverses, Equivalence Relations, and Modular Arithmetic

9/16 Groups—Definition of Groups and Subgroups, Lagrange's Theorem, Index of a Subgroup, Cyclic Subgroups, and Euler's Theorem

9/23 Exponentiation Algorithm, Fields, Primitive Roots, Discrete Logs, ElGamal Cipher, and Diffie-Hellman Key Exchange

9/30 Primitive Root Search Algorithm, Baby-Step Giant-Step Algorithm, The Index Calculus Algorithm, and Public-Key Ciphers

10/7 RSA Public Key Encryption

10/14 **NO CLASS**—Columbus Day—Class on Tuesday

10/15 The Chinese Remainder Theorem, Euler Criterion, and Roots Mod Composites

10/21 **Midterm Exam**

10/28 The Oblivious Transfer Protocol (factorization and discrete log), Zero Knowledge Proofs, and the Digital Signature Algorithm

11/4 Quadratic Reciprocity and Pseudoprimes

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

11/18 Random Number Generators—Linear Congruent Generator, Feedback Shift Generator, Naor-Reingold Number Generator, Blum-Blum-Shub Random Number Generator

11/25 Factorization Attacks—Pollard's Rho Method, Pollard's p-1 Method

12/2 No Class or Possible Makeup—Additional time to work on final project

12/9 **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