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. Several symmetric ciphers, including DES
2. The RSA and ElGamal asymmetric ciphers as well as the Diffie-Helman Key Exchange Protocol and the Key Management System.
3. Algorithms to compute the Discrete Logarithm in cyclic groups, the Baby-step Giant-step Algorithm and the Index Calculus Algorithm.
4. Oblivious transfer protocols and Digital Signatures
5. Blum-Blum-Shub and Naor-Reingold number generators
6. Probabilistic algorithms to check the primality of large numbers
7. Factorization attacks: Pollard's Rho Method, Pollard's p-1 Method,

Textbook Paul Garrett: Making, Breaking Codes: An Introduction to Cryptology
Prentice Hall, ISBN#:0-13-030369-0

Evaluation and Grading

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

Grades will be based on:

Class participation	20%

Midterm	50%
Final Project	30%

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. Collaboration is not permitted.

Instructor Information

Dr. Anatoly Temkin
Computer Science Department, Metropolitan College,
Boston University, 808 Commonwealth Ave, Room 250
Boston, MA 02215
Office: 617-353-2567, FAX: 617-353-2537
Email: temkin@bu.edu

Office hours: Tuesday 5-6, Wednesday 5-6

Classes are scheduled at CGS Room 515

Schedule of Classes

9/2	The Integers (Divisibility, Unique Factorization, Euclidean Algorithm, Multiplicative Inverses, Equivalence Relations, Integers mod n)	7.1-7.8
9/9	Groups (Definition of Groups and Subgroups, Lagrange's Theorem, Index of a Subgroup, Cyclic Subgroups, Euler's Theorem)	17.1-17.8
9/16	Exponentiation Algorithm, Fields, Primitive Roots, Discrete Logs, El Gamal Cipher	**22**.2,4, 5, **27**.1, **28**.1,2
9/23	The Diffie-Hellman Key Exchange Protocol, Primitive Root Search Algorithm, Baby-Step Giant-Step Algorithm, The Index Calculus Algorithm Public-Key Ciphers	10.1-10.4
9/30	Public Key Ciphers, The RSA Cipher	12.1-12.7
10/7	Chinese Remainder Theorem, Euler Criterion, Roots Mod Composites	13.1-13.8
10/14	**Monday Schedule of Classes**	
10/21	Review	
10/28	**Midterm Exam**	
11/4	Oblivious Transfer Protocol (factorization and discrete log based) Zero knowledge proofs, The Digital Signature Algorithm	18.1-18.6

11/11	Quadratic Reciprocity and Pseudoprimes	15.1-15.5 16.1-16.3, 16.6
11/18	Pseudorandom Numbers, Fermat, Euler, and Miller-Rabin Pseudoprimes, Miller-Rabin Test	20.4-20.9, **21**.5,6
11/25	Random Number Generators (Linear Congruential Generator, Feedback Shift Generator, Noar-Reingold Number Generator, Blum-Blum-Shub Random Number Generator)	13.1-13.4
12/2	Modern Factorization Attacks (Pollard's Rho Method, Pollard's p-1 Method)	25.1-25.5
12/9	**Final Project**	

Homework Exercise Set

For Lecture 1: p.111, # 7,8,9,11,14,16; p.118, # 1,2,3,4,5,6; p.121, # 1,8,9
p.123, # 1 to 10; p.126, # 1; p.135, #1,2,3,4,9,10,14,15
Write a C++ or Java code for the Euclidean Algorithm
Write a C++ or Java code that will find a couple of integers, x and y, for given integers m and n, such that $xm + yn$ will yield the smallest positive number.

For Lecture 2: p.267, #1,3,4,5,6; p.268, #3,4,5,6,7; p.271, #2,3; p.275, #1,2,10

For Lecture 3: 12.5.01, 12.5.06; Write a C++ or Java code for the Exponentiation Algorithm

For Lecture 4: Write a C++ or Java code for a Primitive Root Search Algorithm
Write a C++ or Java code for a Baby-step Giant-step Algorithm

Have an example of the Diffie-Hellman Key Exchange Protocol, assuming it

takes place in $Z_p^{\times}$, where p = 9511

For Lecture 5: 10.2.02, 10.2.03, 10.2.06,10.2.08

For Lecture 6: 13.1.01, 13.2.02, 13.2.03, 13.3.01, 13.3.07, 13.8.01, 12.6.01, 12.6.07, 12.6.03, 12.7.01, 12.7.02, 12.7.03
Solve $x^2 \equiv -1 \bmod 13 \cdot 17 \cdot 29$

For Lecture 7: Have an example of the Oblivious Transfer Protocol (factorization based), where p = 31 and q = 103
Have an example of the Oblivious Transfer Protocol (discrete log based), where p = 103

For Lecture 8: 15.5.01, 15.5.03, 15.5.05, 15.5.06, 15.5.09, 15.5.10, 15.5.14.

Evaluate a)$\left(\frac{46}{111}\right)$, b)$\left(\frac{37}{112}\right)$, c)$\left(\frac{113}{2462}\right)$

For Lecture 9: 16.2.01, 16.6.01, 16.6.02
Write a C++ or Java code for the Miller- Rabin Test

For Lecture 10: p. 335, # 21.3.02, 21.3.03, 21.3.04; p. 336, # 21.4.01, 21.4.03
Write a C++ or Java code for the Noar-Reingold Random Number Generator

Write a C++ or Java code for the Blum-Blum-Shub Random Number Generator

For Lecture 11: 24.1.01, 24.1.02, 24.1.03; 24.2.02, 24.2.03

Write a C++ or Java code for the Pollard's p-1 method

Write a C++ or Java code for the Pollard's Rho method

Labs

MET College operates four pc laboratories as a resource for the students.
The computer labs hours are:

Fall and Spring Semester: Daily: 10:00am to 10:00pm

Labs are closed during all holidays, intersession and spring break. Please note that lab rooms get reserved for classes during certain hours.
.