Boston University Metropolitan College

ADVANCED CRYPTOGRAPHY

MET CS 789

Scott Dyer
sldyer@bu.edu
Office hours: by appointment

Course Description

This course builds on the material covered in CS 789 Cryptography. It begins with the coverage of commutative rings, finite fields, rings of polynomials, and finding of the greatest common divisor in the ring of polynomials. Irreducible polynomials are discussed. Field extensions and fields $F_p[x]/P$ are thoroughly covered. The main emphasis is put on elliptic curves over F_p and F_{2^n} and the ElGamal cipher on elliptic curves is presented. Block ciphers DES and double and triple DES are introduced. AES and WHIRLPOOL block ciphers and modes of operation are covered. The course continues with the introduction of message integrity and message authentication. In the last part of the course cryptographic hash functions SHA-512 and WHIRLPOOL as well as various digital signatures are introduced. Finally, entity authentication and key management issues are discussed.

Prerequisites

MET CS 789 Cryptography

Book (recommended, not required)

William Stalling: Cryptography and Network Security. Pearson ISBN 978-0134444284

Class Policies

1) **Attendance & Absences** – Class attendance is part of the participation grade. Please inform your instructor prior to class if you are unable to attend.
2) **Assignment Completion & Late Work** – assignments will be handed in each week at the start of class.
3) **Academic Conduct Code** – 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:

http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html.

Grading Criteria

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 40%
Final Project 40%

Class Schedule

Date	Topic	reading
1/25	Commutative Rings, Finite fields, Rings of Polynomials, Division and the gcd in the Ring of Polynomials, Irreducible polynomials	Handouts
2/8	Field Extension. Fields [ ]/ p F x P. Multiplication table, inverses	Handouts
2/16	Elliptic curves over R, Elliptic curves over F_p **note: Monday is a holiday, class will meet on Tuesday**	Handouts
2/22	Elliptic curves over F_{2^n} . ElGamal cipher on Elliptic curves	Handouts
3/1	Feistel cipher, DES, Double and triple DES Modes of operation	Handouts
3/8	AES, implementation and security of it and WHIRLPOOL cipher	Handouts
	Sprint Recess, Classes suspended	
3/15	Midterm Exam	
3/22	Message integrity, message authentication, Random Oracle model	Handouts
3/29	Cryptographic hash functions, SHA, WHIRLPOOL	Handouts
4/5	Digital signatures, including Elliptic curve digital signature scheme	Handouts
4/12	Entity authentication	Handouts
4/21	Key management (Symmetric key agreement, public key distribution, etc) **Note: Meet Wednesday due to Holiday**	Handouts
4/26	Review	
5/3	Final Project	