MAD 6477 Cryptography
Syllabus - 09/2013

Instructor: Koray Karabina, Office SE 266, Tel: 297-0809.

Class time and place: T-Th 12:30 - 1:50 pm BU 112.

Office hours: T-Th 3:00 - 4:30 pm, or by appointment.

TEXT:

- Douglas R. Stinson, *Cryptography – Theory and Practice*, (Third Edition) Chapman & Hall/CRC Press, isbn 1-58488-508-4/5,
- A. J. Menezes, P. c. van Oorschot, s. A. Vanstone *Handbook of Applied Cryptography*, CRC Press, Boca Raton, New York, London, Tokyo, 1997. (Available at http://www.cacr.math.uwaterloo.ca/hac)

COURSE OBJECTIVES: The course assumes the student had a previous course in cryptology/information security, a course in graduate algebra or number theory and is familiar with notions of probability and statistics. Adequate mathematical maturity and facility with computation is also assumed. We will discuss classical ciphers, Shannon theory, symmetric cryptography, public key cryptography, hash functions, and signature schemes. We will also discuss some recent developments in the design and analysis of cryptographic schemes.

DISABILITY POLICY:

In compliance with the Americans with Disabilities Act (ADA), students who require reasonable accommodations due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) (SR 110 (561-799-8010)) and follow all OSD procedures.

ACADEMIC INTEGRITY:

Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see University Regulation 4.001.

GRADING POLICY:

There will be 2 quizzes, $\{Q_1, Q_2\}$, 1 midterm (hourly) exam, $\{M_1\}$, 3 homework projects, $\{H_1, H_2, H_3\}$. In addition, each student will give a 25 min presentation and hand in a brief report, $\{P\}$, on an advanced topic in cryptography. These topics should be selected with the help of the instructor and decided by mid October. The weights for these marks are as follows:

ITEM	DATE	POINTS	ITEM	DATE	POINTS
H_1	September 12	50	M_1	November 7	100
Q_1	September 26	50	H_3	November 14	50
H_2	October 10	50	P	TBA	100
Q_2	October 24	50			

For homework assignments, the dates mentioned above are the dates by which assignments will be web-posted / handed out. Each assignment will be collected on the due date mentioned on the assignment. **No late assignments** will be accepted. For quizzes and the midterm exam, the dates show when quizzes/exams will be given. Quizzes and the exam will be given in class.

Your grade in the course will be determined by your cumulative performance in the quizzes, midterm exam, homework assignments, and your project. Your average score will be computed as $\Sigma = (M_1 + \sum_{i=1}^{3} H_i + \sum_{i=1}^{2} Q_i + P)/450$, and your letter grade will be determined based on the following catalog:

95% - 100%	A
90% - 94%	A^-
85% - 89%	B^+
80% - 84%	B
75% - 79%	B^-
70% - 74%	C^+
65% - 69%	C
60% - 64%	C^-
55% - 59%	D^+
50% - 54%	D
45% - 49%	D^-
below 45%	F