MATH 536.01W: CRYPTOGRAPHY
SUMMER II 2015

CONTACT INFORMATION:

NAME	: Dr. Hasan Coşkun
OFFICE	: Binnion Hall BIN 314
PHONE	: 903.886.5951
WEB	: http://faculty.tamu-commerce.edu/hcoskun/
E-MAIL	: hasan.coskun@tamuc.edu
OFFICE HOURS	: MTWR 11:00a-12:30p (Skype), otherwise by appointment

DESCRIPTION AND POLICIES:

1. CLASS SCHEDULE: Online (Section 01W)

2. TEXTBOOK: An Introduction to Cryptography with Coding Theory, 2nd edition, by Trappe and Washington

3. WEBSITE & INTERNET: An eCollege website has been created for the course which may be accessed from student myLEO accounts following the eCollege and then the My Courses tabs. All files and documents that the instructor shares with the class will be posted in the Doc Sharing folder in the course website. All material posted at the course website is copyrighted ©. You are allowed to retain one copy of each file for your personal use, but the files should not be duplicated and distributed in any form. The office hours will meet online via Skype at times indicated above. Please make sure to make a Skype account if you don't have one already, and add instructor's Skype ID to your contacts. This program allows working problems live by sharing screens; a webcam is not required, but a quality microphone is needed.

4. COURSE DESCRIPTION: The course begins with some classical cryptanalysis (Vigenere ciphers, etc). The remainder of the course deals primarily with number-theoretic and/or algebraic public and private key cryptosystems and authentication, including RSA, DES, AES and other block ciphers. Some cryptographic protocols are described as well. Prerequisites: Graduate standing in mathematics or Consent of the Instructor.

5. SOFTWARE: *Mathematica* software is required for the course. It will be used for carrying out computations in discussion sessions, homework exercises, exams and projects. Mathematica 10 is installed and available in Mathematics computer lab in BIN 328, and in computer labs at the Metroplex center. Personal student licenses may be purchased online at the Wolfram Mathematica website http://www.wolfram.com/mathematica/how-to-buy/education/.

6. Tests & Projects: There will be a midterm test/project (200 points) and a comprehensive final/project (200 points). No make-up test will be given without an official, written, university accepted excuse. The student must contact the instructor the next working day and present the documented excuse to make up a test.

7. Homework: Homework will be assigned in every class meeting on a regular basis. Selected assignments and problems will be graded only, but all homework problems should be worked out. The assignments will be turned in electronically (in form of a Mathematica notebook) by due dates to the Dropbox for that week at the eCollege website. Student name and homework number should be printed at the top of each notebook. You may work in groups unless otherwise instructed, however the paper you turn in must be your own work. Late homework is not accepted. Homework is worth 50 points of the total semester grade.

8. Learning Outcomes: Students who complete this course successfully will
   a) learn the *terminology* of cryptography;
   b) learn the *methods* used in most common cryptosystems;
   c) learn the *applications* of theoretical results to practical problems.

9. Tentative Course Outline:

   0. Intrduction to Mathematica (Week 1)
   1. Number Theory Review (Week 1 & Week 2)
   2. Classical Cryptosystems (Week 2 & Week 3)
   3. The DES (Data Encryption Standard) (Week 4)
   4. The RSA Algorithm (Week 5)

10. Grading Scale: All scores will be added and a letter grade will be assigned according to the following table.

    A 406 - 450 pts
    B 361 - 405 pts
    C 316 - 360 pts
    D 271 - 315 pts
    F 0 - 270 pts

11. Tentative Exam Schedule:

Midterm	200 pts	Wednesday July 29, 2015
Final	200 pts	Thursday August 13, 2015

12. Other Important Dates:

August 3, 2015	Last day to drop a class
August 9, 2015	Last day to withdraw from Summer II
August 13, 2015	Last class day

13. Miscellaneous: Your enrollment in this course indicates that you agree to observe all the conditions and regulations of this syllabus and the Student Handbook. Your test and homework scores may be filed to be used anonymously for educational research.

    It is your responsibility to secure the software licenses and other resources (such as a personal computer with proper operating system to run the software, broadband internet access to view the video recordings and participate in online discussion sessions, etc.) to be able to complete and communicate all assignments, tests and projects to the instructor as required. The access information to Library resources, and Help Desk for technical support are available through the eCollege website.

    Policies pertaining to scholastic dishonesty are identical to TAMU-Commerce regulations given in the Student Handbook, available online at the website `http://web.tamuc.edu/studentLife/documents/studentGuidebook.pdf`. All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment (See Student's Guide Handbook, Policies and Procedures, Conduct). Disruptive behavior and scholastic dishonesty in any form will not be tolerated.

    Students requesting accommodations for a disability should contact the Office of Student Disability Resources and Services, Texas A&M University-Commerce, Gee Library, Room 132, Phone: (903) 886-5150 or (903) 886-5835, Fax: (903) 468-8148, or Email: `StudentDisabilityServices@tamuc.edu`.

    Any possible changes to be made in this syllabus by the instructor during the semester will be announced by email.