CSCI 568 – CRYPTOGRAPHY
(SPRING 2015)

(Last updated: December 16, 2014)

INSTRUCTOR

Instructor: Jinoh Kim, Ph.D.
Office: JOUR 217
Office hours: M/W/R 10:00AM-12:00PM, W 1:00PM-3:00PM, or by appointment
Phone: 903-468-6084, Fax: 903-886-5404
Email: Jinoh.Kim@tamuc.edu (Please indicate the course number in the email subject line)

CLASS MEETING

Location: JOUR 104
Time: W 4:30–7:10PM (3 credits)

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.

EXPECTED STUDENT LEARNING OUTCOMES

-

PREREQUISITES

- Prerequisites: CSci 532, Math 331, or consent of instructor
- Co-requisites: CSci 563, or consent of instructor

COURSE MATERIAL

- **Cryptography and Network Security**, William Stallings, 6th edition, Prentice Hall, ISBN 0133354695, 2013 (required).

GRADING (TENTATIVE)

Homework	30%	A: 90 or above
Midterm Exam	20%	B: 80 – 89.x
Final Exam	30%	C: 70 – 79.x
Class Participation	20%	D: 60 – 69.x
		F: Below 60

LATE POLICY

The deadline for any assignment can be extended with a 15% penalty per day. No deadline can be extended by more than two days. Assignments will NOT be accepted 48 hours after the due date.

MAKEUP POLICY

There will be no makeup exams in general. Makeup exams may be given to students under extreme circumstances, such as hospitalization, serious injury, death in the family, etc, with prior notification *and* valid documents.

COLLABORATION POLICY

Students are encouraged to talk to each other, to the instructor, or to anyone else about any of the assignments. Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. *Each student must write out his or her own solutions to the homework*. Consulting another student's or group's solution is prohibited, and submitted solutions may not be copied from any source. These and any other form of collaboration on assignments constitute cheating. If you have any question about whether some activity would constitute cheating, please feel free to ask.

ACADEMIC INTEGRITY

Your commitment as a student to learning is evidenced by your enrollment at Texas A &M University-Commerce. "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 Procedure, Conduct). All phones, pagers, and other communication devices are to be turned off or place on silent mode during class. Instances of academic dishonesty will not be tolerated. Cheating on exams or plagiarism (presenting the work of another as your own, or the use of another person's ideas without giving proper credit) will result in a failing grade and sanctions by the University. For this class, all assignments are to be completed by the individual student unless otherwise specified.

Anyone cheating will receive a zero on the work they are doing, and subsequent cheating will result in a failing grade.

STUDENTS WITH DISABILITIES

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

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
StudentDisabilityServices@tamu-commerce.edu

BASIC TENETS OF COMMON DECENCY

"All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (Student's Guide Handbook, Policies and Procedures, Conduct.) This means that rude and/or disruptive behavior will not be tolerated.

SMOKE, VAPOR & TOBACCO FREE ENVIRONMENT

University Procedure 34.05.99.R1 now prohibits the use of vapor/electronic cigarettes, smokeless tobacco, snuff and chewing tobacco inside and adjacent to any building owned, leased, or operated by A&M – Commerce.

DISCLAIMER

This syllabus is meant to provide general guidance of what to expect from this course. The instructor reserves the right to make changes as appropriate based on the progress of the class. All changes made to this syllabus during the semester will be announced. This document has been posted electronically. If you print a copy of it, please be sure to consult the last modified date of the online version to verify that your printed copy is current.

SCHEDULE (TENTATIVE)

WEEK	CONTENT	READING
1 (1/19)	Course introduction and overview	--
2 (1/26)	Cryptography overview	Chapter 1
3 (2/2)	Classical encryption techniques	Chapter 2
4 (2/9)	Block ciphers and DES	Chapter 3
5 (2/16)	Basic concepts in number theory and finite fields	Chapter 4
6 (2/23)	AES	Chapter 5
7 (3/2)	Block cipher operation	Chapter 6
8 (3/9)	Midterm Exam	--
9 (3/16)	No class (Spring Break)	--
10 (3/23)	Pseudorandom number generation and stream ciphers	Chapter 7
11 (3/30)	Number theory	Chapter 8
12 (4/6)	Public-key cryptography and RSA	Chapter 9
13 (4/13)	Cryptographic hash functions	Chapter 11
14 (4/20)	Message authentication codes	Chapter 12
15 (4/27)	Digital signatures	Chapter 13
16 (5/4)	Advanced topics in cryptography	--
17 (5/11)	Final Exam	--