Spring 2014 CS 5920 Applied Cryptography - 3 Credit Hours
Syllabus and Course Policies

Instructor	Chuan Yue
Email	cyue@uccs.edu
Phone	719-255-5155
Course Day & Time	M, W 06:05pm – 07:20pm 01/21/2014 – 05/16/2014
Lecture Location	Engineering Building (ENGR) Room 105
Office	Engineering Building (ENGR) Room 194
Office Hours	M, W 04:30pm - 06:00pm, or by appointment

COURSE DESCRIPTION

Basic security issues in computer communication, classical cryptographic algorithms, symmetric-key cryptography, public-key cryptography, hash functions, message authentication codes, digital signatures, key management and distribution, user authentication protocols.

COURSE OBJECTIVE

Students know the fundamental security requirements, know the limitations of classical cryptographic algorithms, know the essential symmetric-key and public-key algorithms and their differences, know the basic requirements and mechanisms of message authentication, digital signature, and user authentication.

PREREQUISITES

MATH 2150 (Discrete Mathematics), CS 3160 (Concepts of Programming Languages), CS 5220 (Computer Communication), or instructor consent.

COURSE MATERIALS

Textbook (required):
Cryptography and Network Security: Principles and Practice (5th Edition), by William Stallings
ISBN-10: 0136097049, ISBN-13: 978-0136097044

Other books (recommended):
Handbook of Applied Cryptography, by Alfred Menezes, Paul van Oorschot, and Scott Vanstone
Applied Cryptography (Second Edition), by Bruce Schneier.

Additional Class Handouts (as we go along, if possible distributed via Blackboard)
Blackboard Course Site: http://bb.uccs.edu
Course Slides: http://www.cs.uccs.edu/~cyue/teaching/2014CS5920CourseSlides/
Reading and Presentations:http://www.cs.uccs.edu/~cyue/teaching/2014CS5920ReadingList/papers.htm

EMAIL COMMUNICATION

Students are expected to check their UCCS campus e-mail account on a regular basis (at least twice in a week). Students may forward their campus e-mail to a private e-mail account, but are expected to assure the forwarding of messages is working properly so they do not miss important email communications.

COURSE SCHEDULE (TENTATIVE)

This course schedule only represents my best estimate. I reserve the right to amend it at any time.

Week	Date	Reading	Topics	Homework
1	M 01/20		Martin Luther King Holiday (No class, no office hour)	
1	W 01/22	Chap 1	Overview	
2	M 01/27	Chap 1, 2	Overview, Classical Encryption Techniques	
2	W 01/29	Chap 2	Classical Encryption Techniques	HW 1 assigned
3	M 02/03	Chap 3	Block Ciphers and the Data Encryption Standard	
3	W 02/05	Chap 3	Block Ciphers and the Data Encryption Standard	HW 1 due
4	M 02/10	Chap 4	Basic Concepts in Number Theory and Finite Fields	
4	W 02/12	Chap 4	Basic Concepts in Number Theory and Finite Fields	HW 2 assigned
5	M 02/17	Chap 5	Advanced Encryption Standard	
5	W 02/19	Chap 5, 6	Advanced Encryption Standard Block Cipher Operation	HW 2 due
6	M 02/24	Chap 6	Block Cipher Operation	HW 3 assigned
6	W 02/26	Chap 7	Pseudorandom Number Generation and Stream Ciphers	
7	M 03/03	Chap 1 to 7	Midterm Exam Review	HW 3 due
7	W 03/05	Chap 8	More Number Theory	
8	M 03/10		**Midterm Exam (06:05pm - 07:20pm)**	
8	W 03/12	Chap 8, 9	More Number Theory Public-Key Cryptography and RSA	
9	M 03/17	Chap 9	Public-Key Cryptography and RSA	
9	W 03/19	Chap 10	Other Public-Key Cryptosystems	
10	M 03/24		Spring Break (No class, no office hour) **Project Proposal Report Due (11:59pm)**	
10	W 03/26		Spring Break (No class, no office hour)	
11	M 03/31	Chap 11	Cryptographic Hash Functions	HW 4 assigned
11	W 04/02	Chapt 12	Message Authentication Codes	
12	M 04/07	Chapt 12	Message Authentication Codes	
12	W 04/09	Chapt 13, 14	Digital Signatures, Key Management and Distribution	HW 4 due
13	M 04/14	Chapt 14	Key Management and Distribution	HW 5 assigned
13	W 04/16	Chapt 15	User Authentication Protocols	
14	M 04/21	Chapt 15	User Authentication Protocols	
14	W 04/23	Chap 8 to 15	Final Exam Review	
15	M 04/28	Presentations 1 and 2	(1) “How to Share a Secret” and “DepSky: dependable and secure storage in a cloud-of-clouds” (2) “An Empirical Study of Cryptographic Misuse in Android Applications”	HW 5 due
15	W 04/30	Presentations 3 and 4	(3) “Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices” (4) “Honeywords: making password-cracking detectable”	
16	M 05/05		**Final Project Presentation**	
16	W 05/07		**Final Project Presentation**	
17	M 05/12		**Final Exam (04:45pm - 07:15pm)**	
17	W 05/14		**Final Project Report Due (11:59pm)**	

GRADING POLICY

Final grades are computed using the following weights:

Class Attendance and Participation	4%
Student Instructor Co-lecturing	4%
Homework Assignments	20%
Paper Presentation	7%
Midterm Exam (in-class, open-book, open-notes, written)	15%
Final Exam (in-class, open-book, open-notes, written)	25%
Project	25%

All grades are based on a scale from 0-100 as follows:

$93 \leq$ {A};	$90 \leq$ {A-} < 93;	
$87 \leq$ {B+} < 90;	$83 \leq$ {B} < 87;	$80 \leq$ {B-} < 83;
$77 \leq$ {C+} < 80;	$73 \leq$ {C} < 77;	$70 \leq$ {C-} < 73;
$67 \leq$ {D+} < 70;	$60 \leq$ {D} < 67;	
$60 >$ {F};		

A linear shift may be applied to **final** grade averages as a one-time scale at the professor's discretion.

CLASS ATTENDANCE AND PARTICIPATION

Your class attendance and participation will be a combination of attendance, discussion, etc. Class attendance/participation counts for 4% of your grade. Even if you have an excused absence from class (we'll work excused absences on a case-by-case basis), you are 100% responsible for all material and announcements covered in class.

STUDENT INSTRUCTOR CO-LECTURING

Each student is required to participate in one 10~15-minute co-lecturing activity with the instructor during the semester. Basically, the student will (1) choose a piece of content that will be discussed in the class in a particular day, (2) meet with the instructor in advance to confirm that piece of content and get necessary help, and (3) present that piece of content in the class. The instructor may supplement or correct the student's presentation if necessary. Each student also needs to complete two short surveys in order to claim this 4% of the overall grade.

HOMEWORK ASSIGNMENTS

Assignments are to be completed on your own unless explicitly noted by your instructor. You may discuss any component of the assignment with your classmates, but there cannot be a physical or electronic record of your conversation (no paper, files, disks, or code of any form) taken away from the conversation. While you are encouraged to discuss with each other students, **you must write your own code and/or answers, in whole.** You cannot directly use the code or answers that you have found on the Internet. **Copying any portion of the code or answers will result in an automatic zero for the assignments for all students involved. Two or more instances of this in the course will result in an automatic failure for the course.**

Assignments are due at the beginning of class on the specified due day. You should turn in the PDF electronic version (*scanned handwriting is not acceptable*) of your answers to each assignment.

To turn in your assignment:
Log into Blackboard and submit the file into the appropriate homework assignment.

Late submissions:
In case you cannot complete a homework assignment by the beginning of class on the due date, you can take **three** additional days to turn it in with the penalty of 10% for each additional day. Beyond **three** days from the specified due date, the homework shall NOT be graded without a pre-approval from the instructor.

EXAMS

Exams in this class are in-class, open-book, open-notes (must be your own), and written. The questions asked in the exam will cover the contents from the textbook and paper presentations.

There will not be any makeup exam, unless you provide convincing evidences in advance and get a pre-approval from both the instructor and our CS Program Assistant Trish Patricia Rea (prea@uccs.edu).

PAPER PRESENTATION

Two or three students will form a team to present a research paper in 25 minutes. At 25 minutes, the presentation will be stopped, regardless of whether it is finished. Your 25-minute presentation will be followed by a 10-minute Q&A session. Presentations should be made using a projector. The classroom computer has Microsoft PowerPoint and PDF reader installed. If you use other presentation software, you need to use your own laptop.

The elements of a presentation include a summary of the key points of the paper, background, motivation, and related work, a critique of the paper, and analysis of the lessons to be gained from the paper. The key to a good presentation is selecting what points to cover, not trying to cover everything. Please feel free to use the paper authors' presentation slides (if you can get them), but you should acknowledge this in your presentation and you should also add some new contents based on your understanding of the paper.

A good guideline for your presentation is to have:

- About 5 slides on preceding work, technology that existed before the publication of the paper, and other factors that led to the research described in this paper. What is the background of the paper? What issues were going on when it was written? Why was the research done?
- About 8 slides discussing the important points of the paper. This *is not a summary of the entire paper*.
- About 3 slides forming a critical analysis of the paper (both good and bad points).
- About 2 slides discussing (possible) following work, the effects of the paper, and where the idea is today. For more current papers, what are the competing ideas and what are your own ideas? What has happened to the paper since publication? Citeseer or Google Scholar can help with this, but you need to present more than just the number of citations. How has the idea been applied since then? What happened to it? Why did it (or didn't it) win?

The presenters must email an electronic copy of the presentation file (e.g., PPT or PDF file) to the instructor before the start of the presentation, so it can be made available to other students.

PROJECT

Students are required to conduct a research project in this course. At most two students can form a team to perform the same project. You are strongly encouraged to identify a good applied cryptography research topic by yourself. If you really cannot identify a good topic by yourself, you can select a topic provided by the instructor. You need to write a 2-page **project proposal report** and a 6-page **final project report**. You should use the Manuscript Templates for IEEE Conference Proceedings (two-column) to write your reports. The content organization of your reports should be similar to those of the conference papers discussed in the class. The originality and quality of your project determine the grade you can earn.

PLAGIARISM & CHEATING

Absolutely no cheating, copying, or plagiarizing on homework assignments, exams, and summaries.
Cheating will result in an AUTOMATIC ZERO (0) for the entire homework, exam, or summary. For further details on academic honesty the student is referred to the University Catalog.

LATE DROP

Dropping of a class after the deadline listed in the UCCS Course Calendar (http://www.uccs.edu/~cic/) is governed by departmental and college policy. The student must show documented evidence supporting reasons for a request to drop a class after the deadline. Each request is considered on an individual basis for determining acceptance.

GETTING HELP

I'll be available during my official office hours and by appointment. If you stop by my office outside my official office hours without an appointment, I may have time to talk with you immediately, but I may also have the right to schedule an appointment with you for a later time. You can always contact me **anytime by e-mail**; I'll reply you as soon as I can.

CAMPUS POLICIES

- UCCS Course Calendar: http://www.uccs.edu/~cic/
- UCCS Student Code of Conduct http://www.uccs.edu/dos/student-conduct.html

DISABILITIES SERVICES

Students with disabilities should turn in their disability verification letters within the first two weeks of class. For further information, contact Disability Services, Main Hall 105, 255-3354. For more information, see the Disability Services page: http://www.uccs.edu/~dservice

MILITARY STUDENTS

If you are a military student with the potential of being called to military service and/or training during the course of the semester, you are encouraged to contact your UCCS course instructor no later than the first week of class to discuss the class attendance policy. Please see the Military Students website for more information: http://www.uccs.edu/~military