CS 65500 Computer Security

Samuel Wagstaff

August 18, 2017

CS 65500, Fall, 2017, 1:30–2:45 PM, LWSN B134.

Instructor: Samuel Wagstaff
Office: 1167 LWSN
Phone: 494-6022
Email: ssw@cs.purdue.edu
Office Hours: Tuesday 3–4 PM, Wednesday 10:30–11:30 AM.

Course Description

This course considers advanced topics in cryptography. CS 65500 covers these topics, among others:

- Differential cryptanalysis.
- elliptic curves: factoring, prime proving, cryptosystems
- AES: square attack
- SHA: attacks by Chabaud+Joux and Biham+Joux
- Discrete logarithms
- Lattices
- Attacks on RSA

Prerequisites

The student should have some basic knowledge of cryptography, as taught in CS 55500.

Course Goals

The course goals are to learn advanced topics in cryptography.

Learning Objectives

In CS 65500, the student should learn topics like:

- Differential cryptanalysis
- elliptic curves: factoring, prime proving, cryptosystems
- AES: square attack
- SHA: attacks by Chabaud+Joux and Biham+Joux
- Discrete logarithms
- Lattices
- Attacks on RSA

Course Requirements

Students should attend most of the classes and read the text. Some material on the exams will appear only in the text or only in class. There will be one midterm exam and one final exam. There will be three to six homeworks, some of them written and some of them (very simple) computer projects. The grading weights will be 25% homework, 25% midterm exam and 50% final exam. Each item will be scored with a number between 0 and 100.

Please format your written homework using a word processor. If we can't read it, then we can't give you credit for it.

Textbook

The text will be *Algorithmic Cryptanalysis* by A. Joux, Chapman & Hall/CRC. A copy of this book may be on reserve in the Mathematics Library.

Course Policy

Students may ask the instructor questions by email. These email questions will be answered as soon as possible. The instructor receives several hundred emails per day and often takes a few days to answer all those that need answers.

Students may leave and enter the class room during class, but should try to do so quietly.

Cell phones should be turned off during class. Students who need to use a phone, either to talk or text, during class should leave the room.

Students may use (laptop) computers during class.

Grading

The last time the instructor taught this class, the average numerical scores were converted to letter grades as follows: 100 A 77 B 66 C 55 D 33 F 0. The conversion cutoffs for this semester will probably be different.

It often happens that students receive higher numerical scores on homework than on exams. All scores for homework and the midterm exam will be put on the class web page.

All regrading of homework and midterm exam must be done within two weeks of the day the work was returned to the class.

Academic Dishonesty

Purdue prohibits "dishonesty in connection with any University activity. Cheating, plagiarism, or knowingly furnishing false information to the University are examples of dishonesty." Furthermore, the University Senate has stipulated that "the commitment of acts of cheating, lying, and deceit in any of their diverse forms (such as the use of substitutes for taking examinations, the use of illegal cribs, plagiarism, and copying during exams) is dishonest and must not be tolerated. Moreover, knowingly to aid and abet, directly or indirectly, other parties in committing dishonest acts is in itself dishonest."

While it is all right to discuss homework in this class with other students in general terms, do not copy another student's homework or let anyone copy your homework. When two identical homeworks are found, both are sent to the Dean of Students to determine who copied from whom.

Students may use calculators during exams. They may not use cell phones, computers, notes, cheat sheets, photographic equipment, radios, televisions, books, Morse code, signals or sign language during exams. Do not look at exams of other students or let others see your exam while the exam is in progress. Communicate only with the instructor during an exam.

Penalties for academic dishonesty range from a 0 grade on one assignment to a failing grade in the class and even expulsion from the University. A hearing at the Dean of Students' Office can ruin your whole day.

In CS 65500, students may learn some techniques used in computer crime. These techniques may be used only in the controlled conditions of the lab and homework, if at all. If you use them in any way other than that specified in a class assignment, you may be subject to criminal prosecution in addition to any academic penalties.

Attendance

University policy states that students are expected to attend every meeting of every class in which they are enrolled. Only the instructor can excuse a student from a course requirement or responsibility. When conflicts or absences can be anticipated, such as for job interviews and religious observances, the student

should inform the instructor in advance of the situation and plan to make up the missed work. For unanticipated or emergency absences when advance notification to an instructor is not possible, the student should contact the instructor by email. When direct contact with the instructor is not possible because of circumstances beyond the student's control, or in cases of bereavement, the student or the student's representative should contact the Office of the Dean of Students.

Federal law requires instructors to take attendance at least once near the beginning of the semester and again near the end of the semester. (The purpose of this law is to insure that students who receive financial aid actually take and attend classes.) Other than these two occasions, I will not take attendance in class. You should attend class because (1) either you paid for it or someone else paid for you to attend and (2) I might discuss a topic in class that is not in the text, but will appear on an exam. Make friends with other students in class so that you can copy their notes when you miss a class.

Grief Absence Policy

Purdue University recognizes that a time of bereavement is very difficult for a student. The University therefore provides the following rights to students facing the loss of a family member through the Grief Absence Policy for Students (GAPS). GAPS policy: Student will be excused for funeral leave and given the opportunity to earn equivalent credit and to demonstrate evidence of meeting the learning outcomes for missed assignments or assessments in the event of the death of a member of the student's family.

Missed or Late Class Work

If a student misses a homework because he or she didn't get around to doing it, then the grade will be 0 for that homework. If a student has a planned absence for a class when homework is due, the student should turn in the homework before it is due or email it to both the instructor and the teaching assistant by the time it is due. There is a penalty for late homework in this case. Homework will be accepted late without penalty in case of serious illness or bereavement.

If a student misses an exam, then the grade will be 0 for that exam, except in case of serious illness or bereavement, in which case the student will be given an opportunity to make up the exam. If a student has a planned absence for a class when an exam will be given, the student should make arrangement before the planned absence to take the exam early or to take a makeup exam after returning to campus.

Violent Behavior Policy

Purdue University is committed to providing a safe and secure campus environment for members of the university community. Purdue strives to create an educational environment for students and a work environment for employees that promote educational and career goals. Violent behavior impedes such goals. Therefore, violent behavior is prohibited in or on any University facility or while participating in any university activity.

Students with Disabilities

Purdue University is required to respond to the needs of the students with disabilities as outlined in both the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990 through the provision of auxiliary aids and services that allow a student with a disability to fully access and participate in the programs, services, and activities at Purdue University.

The ODOS Testing Center is an excellent place for students with disabilities to take exams for this class. Please tell the instructor at least one week in advance if you wish to take the exams there. If you have a disability that requires other special accommodation, please tell the instructor early in the semester. It is the student's responsibility to notify the Disability Resource Center of an impairment/condition that may require accommodations and/or classroom modifications.

Emergencies

In the event of a major campus emergency (such as a tornado, earthquake, flu epidemic or terrorist attack), course requirements, deadlines and grading percentages are subject to changes that may be necessitated by a revised semester calendar or other circumstances beyond the instructor's control. Relevant changes to this course will be posted onto the course website or can be obtained by contacting the instructor or TA via email or phone. You should read your Purdue email frequently.

Nondiscrimination

Purdue University is committed to maintaining a community which recognizes and values the inherent worth and dignity of every person; fosters tolerance, sensitivity, understanding, and mutual respect among its members; and encourages each individual to strive to reach his or her own potential. In pursuit of its goal of academic excellence, the University seeks to develop and nurture diversity. The University believes that diversity among its many members strengthens the institution, stimulates creativity, promotes the exchange of ideas, and enriches campus life.

Purdue University prohibits discrimination against any member of the University community on the basis of race, religion, color, sex, age, national origin or ancestry, marital status, parental status, sexual orientation, disability or status as a veteran. The University will conduct its programs, services and activities consistent with applicable federal, state and local laws, regulations and orders and in conformance with the procedures and limitations as set forth in Executive Memorandum No. D-1, which provides specific contractual rights and remedies.

The instructor agrees completely with all Purdue policies mentioned in this document.

Privacy

The Federal Educational Records Privacy Act (FERPA) protects information about students, such as grades. If you apply for a job and wish to use the instructor as a reference, you should tell the instructor beforehand. Otherwise, the instructor cannot say anything about you to a prospective employer who might call. The instructor is happy to provide references and to write letters of recommendation for his students as needed.

Class Schedule

See the online day-by-day list of topics covered and the online list of readings for this class.

This syllabus is subject to change.