CS-555: Cryptography (Fall 2018)

Instructor: Professor Jeremiah Blocki (jblocki@purdue.edu)
Office: LWSN 1165
Lecture: 3-4:15 PM at Lawson B134 on Tuesday and Thursday
Required Textbook: Introduction to Modern Cryptography (2nd Edition)
Instructor Office Hours: Mon/Fri @ 1:30PM
Course Website: https://www.cs.purdue.edu/homes/jblocki/courses/555_Fall18/index.html
TA: Duc V. Le (le52@purdue.edu)
TA Office Hours: Mon/Wed @ 10AM (HAAS G050)

Course Outline: Private-key Cryptography, Pseudorandomness, MACs, Hashing, Public-key Cryptography, Digital Signatures, Multi-party Computation.

Prerequisites: Basic knowledge of Algorithms (CS 580).

Requirements and Grading: Students should attend most of the classes and read the text. Some material on the exams may appear only in the text or only in class. There will be one midterm exam and one final exam. There will be four to five homeworks. Homeworks must be formatted using a word processor (preferably, Latex). The percentage of the total course grade are:

- Course Participation: 5% (attendance, participation in lecture, good answers on piazza)
- Homework: 40%
- Midterm: 25%
- Final Exam: 30%

Anticipated grade ranges are: A – 90-100%; B—78%-89%; C – 65%-77%; D—55%-64%; F-- < 55%. These may be adjusted downward by up to 10%; there may also be minor upward adjustments.

Course Materials: We will use the textbook Introduction to Modern Cryptography (2nd Edition) by Jonathan Katz and Yehuda Lindell. Each lecture will additionally be accompanied by lecture slides, pointers to additional materials and videos. Additional links will be provided to supplementary reading materials and other courses which are similar in spirit to this course.

Course Policies

Announcements: Course announcements will be made through the course Piazza page https://piazza.com/purdue/fall2018/cs555/home. You are expected to enroll on Piazza and check regularly for information related to the class. Important announcements on Piazza will also be e-mailed to all students enrolled in the piazza page.

Conduct and Courtesy: Students are expected to maintain a professional and respectful classroom environment. This includes: silencing cellular phones, arriving on time for class, speaking respectfully to

others and participating in class discussion. You may use non-disruptive personal electronics for the purpose class participation (e.g., taking notes).

Correspondence with the instructor: The easiest way to communicate with the instructor is through Piazza. The Piazza platform allows you to ask private questions which are visible only to course staff (instructor(s)/TA(s)). We request that general clarification questions be posted publicly on Piazza. If you would like to address a question to the instructor only then you should use e-mail. Please prefix all course-related emails with the string "CS-555:" to help filter email. The instructor will make every effort to answer promptly (within 48 hours). However, replies could be delayed due to circumstances outside the instructor's control.

Missing or Late Work: Homework is due at the beginning of class on the given due date. If you have a planned absence for a class on a date when homework is due, then you should email your completed assignment to the TA *before* the deadline. The following penalties apply for late homeworks:

- Late reports turned in within 24 hours of the deadline will receive a 10% penalty.
- Reports turned in 24 hours late, but within 48 hours of the deadline will receive a 25% penalty.
- Reports turned in more than two days after the deadline will be counted as a zero.

The score for a missed exam is 0. Exceptions will be made to the above policies in case of serious illness or bereavement. 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 take a makeup exam after returning to campus.

Grading: All re-grading of homework and midterm exams must be done within two weeks of the day the work is returned to the class.

Academic integrity: Behavior consistent with cheating, copying, and academic dishonesty is not tolerated. Depending on the severity, this may result in a zero score on the assignment or exam, and could result in a failing grade for the class or even expulsion. Purdue prohibits "dishonesty in connection with any University activity. Cheating, plagiarism, or knowingly furnishing false information to the University are examples of dishonesty." (Part 5, Section III-B-2-a, University Regulations) 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 examinations) 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." (University Senate Document 7218, December 15, 1972). You are expected to read both Purdue's guide to academic integrity (http://www.purdue.edu/purdue/about/integrity_statement.html) and Prof. Gene's Spafford's guide (http://spaf.cerias.purdue.edu/integrity.html) as well. You are responsible for understanding their contents and how it applies to this class.

- **Homeworks:** Students may discuss problem sets with others in this class and ask for clarification on the Piazza discussion forum for this course. However, the solutions they turn in must be their own and **they must *completely understand* the solutions they submit.** Do not copy another

student's homework and do not allow another student copy your homework. Discussions with other students should be appropriately acknowledged. Turning in a solution that you could not explain to the instructor is considered cheating.

- **Exams:** You may use calculators during exams. However, you may not use cell phones, smart watches, computers, cameras, radios, televisions, books, Morse code, signals or sign language during exams. Do not look at other student's exams or let others see your exam while the exam is in progress. Communicate only with the instructor (or TA) during an exam.

Posting Class Material: Posting material associated with this class (e.g., solutions to homework sets or exams) without the written permission of the instructor is forbidden and may be a violation of copyright.

Purdue's Honor Pledge: As a boilermaker pursuing academic excellence, I pledge to be honest and true in all that I do. Accountable together - we are Purdue.
https://www.purdue.edu/provost/teachinglearning/honor-pledge.html

In CS 55500, students may learn some techniques used in computer crime. These techniques may only be used 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: Students are expected to be present for every meeting of the classes 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 many University sponsored activities and religious observations, the student should inform the instructor of the situation as far in advance as possible and plan to make up for missed work.

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). According to GAPS Policy, students 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.

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.

CAPS Information: Purdue University is committed to advancing the mental health and well-being of its students. If you or someone you know is feeling overwhelmed, depressed, and/or in need of support, services are available. For help, such individuals should contact Counseling and Psychological Services (CAPS) at (765)494-6995 and http://www.purdue.edu/caps/ during and after hours, on weekends and

holidays, or through its counselors physically located in the Purdue University Student Health Center (PUSH) during business hours.

Students with Disabilities: Purdue University strives to make learning experiences as accessible as possible. If you anticipate or experience physical or academic barriers based on disability, you are welcome to let me know so that we can discuss options. The instructor requests that you make an appointment within the first three weeks of the semester to discuss any adjustments. *We cannot arrange special accommodations without confirmation from the Disability Resource Center*. It is the student's responsibility to notify the Disability Resource Center (website: http://www.purdue.edu/drc, e-mail: drc@purdue.edu, phone: 765-4941247) of an impairment/condition that may require accommodations and/or classroom modifications.

Emergencies: In the event of a major campus emergency, 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 and/or announced via email. You are expected to read your purdue.edu email on a frequent basis. Emergency Preparedness: Emergency notification procedures are based on a simple concept: If you hear an alarm inside, proceed outside. If you hear a siren outside, proceed inside. Indoor Fire Alarms are mean to stop class or research and immediately evacuate the building. Proceed to your Emergency Assembly Area away from building doors. Remain outside until police, fire, or other emergency response personnel provide additional guidance or tell you it is safe to leave. All Hazards Outdoor Emergency Warning sirens mean to immediately seek shelter (Shelter in Place) in a safe location within the closest building. "Shelter in place" means seeking immediate shelter inside a building or University residence. This course of action may need to be taken during a tornado, a civil disturbance including a shooting or release of hazardous materials in the outside air. Once safely inside, find out more details about the emergency. Remain in place until police, fire, or other emergency response personnel provide additional guidance or tell you it is safe to leave. In both cases, you should seek additional clarifying information by all means possible: Purdue Home page, email alert, TV, radio, etc. Review the Purdue Emergency Warning Notification System multi-communication layers at http://www.purdue.edu/ehps/emergency_preparedness/warning-system.html. Please review the Emergency Response Procedures at https://www.purdue.edu/emergency_preparedness/flipchart/index.html. Please review the evacuation routes, exit points, emergency assembly area and shelter in place procedures and locations for our building. Video resources include a 20-minute active shooter awareness video that illustrates what to look for and how to prepare and react to this type of incident. See http://www.purdue.edu/securepurdue/police/video/

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.

Instructor absence: The instructor will be away for a few classes. There will be a guest instructor for these classes. If we need to reschedule additional classes, we will do so on an as-needed basis. Our plan is to use video lectures to supplement for any missing class periods.

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.

Changes to the syllabus: This syllabus is subject to change. Updates will be posted and dated on the course website.