University of Michigan, Computer Science and Engineering | Handout 1
EECS 475: Introduction to Cryptography | January 8, 2014
Instructor: Prof. Kevin Fu

Course Information

Instructor:	**Prof. Kevin Fu** Lecture: Mondays/Wednesdays 10:30-12:00 (1610 IOE) Office Hours: Wednesdays 12:00–1:00, or by appointment via jcpatt@umich.edu Room 4628 BBB, kevinfu@umich.edu
Teaching Assistants:	**Emily Graetz** Discussion: Fridays 10:30 (1005 EECS) and 11:30 (185 EWRE) Office Hours: Mondays/Wednesdays 1:30-3:00, or by appointment Room 1637 BBB, graetzer@umich.edu
	Alexander James Discussion: Fridays 1:30 (3150 DOW) and 2:30 (1010 DOW) Office Hours: Tuesdays 3:00-4:30, Thursdays 4:00-5:30, or by appointment Room 1637 BBB, ajarctic@umich.edu
Administrative Assistant:	**Jessica Patterson** Room 4816 BBB, 936–8875, jcpatt@umich.edu
Web page:	http://www.eecs.umich.edu/courses/eecs475/
Piazza:	https://piazza.com/class/hp0pf3sgflt2ap
Email:	eecs475staff@umich.edu

1 Overview

This course aims to teach students both the foundations of cryptography and the humility of building practical cryptographic systems. The assignments will involve a blend of both theory and programming. Topics will include fundamentals of cryptography, applications, attacks, and theory. The class will draw on material from public key cryptography, number theory, usable security, hash functions, symmetric cryptography, secure storage, cryptographic protocols, homomorphic encryption, theoretical notions of security, and cryptographic attacks.

Intended audience. This 4-unit course is intended for upper-level undergraduates with demonstrated interest in the mathematics and application of cryptography. This is not an IT course on how to secure a network or your computer. This course will not satisfy graduate-level requirements in CSE. Workload may vary depending on your background. For instance, students who have not yet mastered algorithms or low-level computer architecture will likely require more time. Some weeks will have more deadlines than others, so plan ahead.

Prereqs. See Wolverine Access for the official prerequisites. This course shall assume mastery of the material from EECS 280 (programming and data structures) and EECS 203 (discrete math). Courses on security, number theory, or operating systems may be helpful, but are not necessary.

Lecture and Discussion Sections. You must be registered for the lecture section and the discussion section for this course.

Lectures will be held in IOE 1610 on Mondays and Wednesdays from 10:30AM to 12:00PM modulo Michigan Time. Show up on-time with proper tools for note taking. Use of laptop computers in class may be restricted if distracting. A schedule of topics will be posted on the Web. Students are expected to have read the assigned reading material before the start of lecture.

There are four discussion sections where the TAs will facilitate interactive lessons ranging from reinforcement of lecture material to discussion of cutting edge applications of the methods.

Textbook and reading. The textbook for the course is *Cryptography: Theory and Practice, 3rd edition* by Douglas Stinson. Notify the course staff via Piazza if you have trouble locating the book. Note that the 3rd edition is nearly a complete rewrite of the book; do not use older versions of the book. We will assign reading and homework from both the book and research papers. We have put one copy of the textbook on reserve in the library.

Getting help via Piazza. We will be using Piazza to host a course forum. You are required to read this regularly; it is the venue we will use for important course announcements and project clarifications. In addition, it will be a significant source of help and hints on the homework. Use a professional tone on the forums.

We do not answer general questions via email. In order to save everyone time, we want all students to have the benefit of seeing each question and its answer. If you do send us email, don't be surprised if we ask you to either post the question to the forum or visit the next available office hour.

2 Grades and methods of evaluation

Final grades will be based on the scores earned on on homework, two exams, and a team project.

Homework	25%
Team project	25%
Exam 1	25%
Exam 2	25%
Total	100%

Homework. There will be regular homework assignments—approximately once per week. Assignments will vary by topic, but may include mathematics, programming, and essay writing.

Homework will generally be assigned on Mondays, and be due the following Monday before the start of lecture (10:39AM). **Late homeworks will not be accepted**. If you have trouble coming to lecture on-time and wish to avoid a zero, make sure to find a friend to submit your homework for you. We do not accept emailed, faxed, tweeted, modulated, etc. homework. Please use analog paper or printouts so we can provide you with our analog feedback on your discrete math.

Late homeworks will receive a zero without exception, unless there is a documented medical emergency that could not have been foreseen. We are extremely strict about deadlines. One second late is late.

However, we realize that life will sometimes interrupt schedules. Therefore, we will ignore your lowest homework grade when computing your final course grade. In other words, the lowest grade received by each student (including zeros for missed assignments) will be discarded. By throwing out the lowest score, I allow you to miss a homework assignment for reasons of illness, a death in the family, a special event, a computing problem, crowded computing sites, accidental erasure or loss of files, a flat tire, outside conflicting commitments, or any other reason. If you plan to be away during a deadline and wish to conserve this virtual "freebie" homework, you should submit your homework early. You should not squander this resource; if you miss an assignment early in the term because you do not feel like turning in the assignment, you may regret it later.

Homework: Format. Please write your answers clearly and neatly, or type them, to avoid problems when the grader is correcting your homework. Also answer the questions in the order they are assigned; that will help to prevent problems such as questions left ungraded. Show all your work, and state any special assumptions you make.

Homework: Collaboration policy. You may consult with other students in the class when doing homework. However, *the version you turn in must be in your own words, written (or typed) in your own hand.*

To ease handling of homework, staple all your homework sheets. On the front page, top right corner provide the following items:

- Print your name
- Print your uniqname
- Print the homework-problem number.

The result should then look like this for the first problem of homework #4:

```
Name: John P. Doe
Uniqname: johnpdoe
Problem: 4-1
```

Homework: Regrade requests. If there is a mistake in the grading of your homework, you have one week to request a regrade after the homework is returned to you. When requesting a regrade, attach a cover page to your homework explaining clearly which questions need to be regraded and why. Note that I think I deserve more points for this question is not a valid reason for a regrade. Homework regrades should be submitted to the TA of your discussion section.

Homework: Submitting programs. Some of the homework will involve programming. For these assignments, you must submit your work via CTools by the deadline listed in each assignment. We do not accept homework submissions by any other means (e.g., email does not count). Check with the TA regarding file formats that are accepted. If you have special circumstances and wish to request deviation from this submission procedure, consult with the TA well ahead of the deadline. Last minute requests will not be looked upon favorably.

2.1 Team project

A significant part of this course is a team project. This year all term projects will involve applications of cryptography on a low-power microcontroller with a RISC-like instruction set. We will assign you to a team of 2–3 people. One goal of this course is to expose you to the realistic joys and challenges of working in teams. As such, you will be responsible for organizing team meetings around your many schedule constraints. Effective teamwork is essential. Details about the project milestones will be distributed later in class.

We do not accept requests for particular team members. However, we will take student input to minimize (but not eliminate) schedule incompatibilities. There will also be a "please don't pair me with..." option. You are not allowed to work with people outside your team. A late team project will receive a 15% grade reduction for each day late. One second late is late. The "lowest grade dropped" policy does not apply to the team project. *If you are having difficulties with the project, you may consult the professor or GSI, but no one else.*

The Engineering Honor Code applies to the project and homework. Suspected cases of cheating or other Honor Code violations will be reported to the Engineering Honor Council and will be dealt with severely. If you are unclear about these rules, contact the professor for clarification. Keep this in mind: If you are having trouble finishing an assignment, it is far better to do your own work and receive a low score than to go through an academic judiciary case and suffer the penalties, which may be severe.

What is cheating on a project or homework?

- on a project—having someone not on your team write your program, algorithm, or do your analysis, in whole or in part.
- copying someone else's work, in whole or in part.
- collaborating with someone on homework to the extent that the homework assignments are identifiably similar, in whole or in part.
- collaborating with someone from another team to the extent that the project assignments are identifiably similar, in whole or in part.

What is not cheating?

- talking to someone in general about topics and concepts involved.
- getting help with the specifics of syntax. (Don't share your program or written solutions, though!)
- utilizing information given to you by the instructor; for example, copying a paragraph describing the problem from the assignment write-up, or copying parts of code from handouts used this course.

2.2 Exams

The Engineering Honor Code applies to the exam. There will be two exams. Both exams will be closed book. Calculators and other computing devices are **not allowed** during exams. For each exam you will be allowed to bring one sheet of 8.5 x 11 paper with anything you like written on it (both sides). Do not bring a blue book. If you cannot take an exam at the scheduled time, notify the instructor at least two weeks in advance so that alternative arrangements can be made. A missed exam is a zero except in the case of a documented medical emergency that could not have been foreseen.

There are two evening exams. There is no final exam. The first exam is **Wednesday, March 19 from 7:00-8:30PM** and the second exam is **Monday, April 21 from 7:00-8:30PM**.

If there is a mistake in the grading of your midterm, you have one week to request a regrade after the exams are made available to pick up (not necessarily a week after you pick up your exam).

You are expected to take both exams at the scheduled times. If you miss an exam, and a documented medical or personal emergency is not involved, you will receive a zero for that exam. **If you anticipate an exam in another course or a religious holiday which conflicts with our exam time, you must notify the instructor at least two weeks before the exam date.** Similarly, any exam accommodation requests must be submitted to the instructor at least two weeks before the exam date, but ideally the first week of class. The exam dates are given at the beginning of the term so that you can avoid scheduling job interviews or other commitments on exam days; hence job interviews, etc. are not considered valid reasons for missing an exam.