# CS 490/590 : Cryptography and Computer Security

Instructor: Thoshitha Gamage, Ph.D.
Southern Illinois University at Edwardsville

Spring 2020 Syllabus

Course Information:

| | |
|---|---|
| Title: | CS 490/590 : Cryptography and Computer Security (3 Credits) |
| Location: | ~~DH 1015~~ EB 3140 |
| Time: | T & R 11:00 – 12:15 p.m. |
| Course Website: | `http://www.cs.siue.edu/~tgamage/courses/490S20` |
| Assignment Dropbox: | `https://classes.cs.siue.edu/spring-2020` |

Contact Information:

| | |
|---|---|
| Office: | EB 3053 |
| Phone: | 650-2407 |
| Email: | `tgamage@siue.edu` |
| Web Site: | `http://www.cs.siue.edu/~tgamage` |
| Office Hours: | M & W 01:30 – 03:00 p.m.<br>T 10:00 – 11:00 a.m. *or by appointment* |

This course is a cross listed advanced undergraduate and graduate level introduction to cryptography and computer security. This is a **research and experimentation emphasis** course with the following objectives.

1. To introduce fundamental modern cryptographic and computer security *constructs* and *concepts*;
2. To facilitate a learning environment that strengthens participants' *theoretical* and *empirical* knowledge, and understanding through hand-on experiments;
3. To improve participants' critical thinking, reading, and writing skills;
4. To introduce *recent advances*, *broader challenges*, and *current trends* in computer security; and
5. To spur self-curiosity in and a research appetite for advanced and/or specialized topics – network, application, web, cloud, OS, etc. – in (more generally) **cybersecurity**.

By the end of the semester, students are expected to be proficient in cryptographic and computer security basics, security exploits, and defensive mechanisms to aid them in their professional career advancements.
The content of this course is influenced by and was developed in accordance to the IEEE/ACM Computer Science Curriculum Guidelines (2013) `https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf`.

## 1 Course Prerequisites

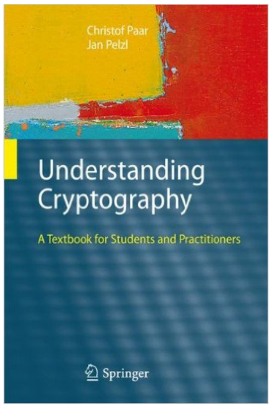
**MATH 224 :** The cryptographic component of the course is substantially formal and mathematical in context and in substance, and will either introduce or revise concepts in number theory, finite fields, modular arithmetic, probability theory, statistics, linear algebra etc.

**CS 447 :** The computer security component of this course will leverage basic understanding of the TCP/IP stack, network communication, and network programming knowledge.

Also *fluency and significant experience* in programming (C++, Java, Python, etc.,) and **Unix/Linux** will be essential. If you do not meet these prerequisites, you **MUST** come and talk with me the first week of class. I reserve the right to drop you from the course if it becomes obvious that you do not meet the prerequisites.

## 2 Textbook & Resources

[**Required**] [**PP1e**] Understanding Cryptography: A Textbook for Students and Practitioners 1st ed., Paar, Pelzl, and Preneel, Springer, ISBN 978-3-642-44649-8 Online: http://www.crypto-textbook.com/


Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

(a) [**PP1e**]

My lecture notes are based on numerous textbooks from my personal library and recent literature. A complementary set of publisher provided lecture slides can be found on the course website. Additional resources along with video lectures for **PP1e** can be found at http://www.crypto-textbook.com/. Material I present in class typically have a **strong mathematical flavor** to them.

## 3 Assigned Work and Tentative Grading Policy

The following grade allocation breakdown is ***tentative***, and may change during the semester. Unless the circumstances change, I am **NOT** planning on curving or rounding the final grade.

| **Grading Allocation** | | **BS** | **MS** |
|---|---|---|---|
| Exams | | 30% | 30% |
| Midterm 01 | 15% | | |
| Midterm 02 | 15% | | |
| Attendance & Scribing | | 5% | 5% |
| Problem Solving | | 15% | 10% |
| Deterlab Experiments | | 35% | 35% |
| Final Project | | 15% | |
| Graduate Standing Project | | – | 20% |

| **Final Letter Grade** | |
|---|---|
| 90–100 | A |
| 80–89 | B |
| 70–79 | C |
| 60–69 | D |
| below 60 | F |

### 3.1 Exams

All exams and quizzes will be held in the lecture room.

- **Midterm 01** : Tuesday February 18th 11:00 – 12:15 p.m.
- **Midterm 02** : Tuesday March 24th 11:00 – 12:15 p.m.

### 3.2 Class Participation

You are expected to **proactively** participate in in-class discussions. This aids your learning and that of your classmates, and provides valuable feedback on the lecture. Constructive and proactive participation in in-class

discussions and scribing accounts for 5% of your final grade. I, therefore, expect you to attend each and every class.
In preparation for each lecture, you are expected to read the relevant sections from **PP1e** (*see Tentative Schedule below*). I will try my best to direct you to other relevant resources where applicable, but I fully expect you to **take the responsibility of your own learning** and come fully prepared to the class.
Each student is required to submit their scribe notes a **minimum of twice** for the semester, preferably once before the mid-term and once after. Scribe notes are due through *Moodle* within **48 hours** after the lecture. Only the top two scribe submissions (based on Moodle timestamp) will be counted as valid submissions. Scribe notes serve as a baseline set of complementary notes to you and to your colleagues, hence please pay your due diligence to make them legible.
Students are also **required** to check the course website and the @siue.edu email regularly for important updates.

## 3.3 Problem Solving

There will be roughly ~3-4 problem solving sessions (take-home and/or in-class) during the course of the semester. In preparation for in-class sessions, I will ask you to research and read about specific topics, that you may or may not find on the textbooks. I will try my best to direct you to relevant resources where applicable, but I am fully expecting you to **take the responsibility of your own learning** and come fully prepared to the class.

## 3.4 Deterlab Experiments

The first component is roughly ~3 hands-on security experiments based on DETERLab `https://www.isi.deterlab.net/index.php3` with a 2 weeks deadline (except the initial setup lab, which has a 1 week deadline). You will be provided with login credentials to Deterlab soon after the first day of class. Specifics of these experiments will be posted on the course website.

## 3.5 Final Project

The final project is a **security themed** research project (preferably) of your own interest. Both analytical and theoretical studies are acceptable, but they **must be** your own genuine contributions. For full points, you are strongly encouraged to include an empirical component in your study either in simulation form or in performance comparison form. You will be required to present your findings to the class during Week 16. Depending on the size of the class, we might also use the final exam time slot for this purpose as well. In addition, a IEEE conference style 8 page paper of your findings will be due on the day of your presentation as the final report.
Undergraduate students can team-up for the final project with my prior approval. Each team can have a maximum two members.
Important milestones for your project are:

- **Project Proposal** Due Thursday March 26th, 2020 at the beginning of class through Moodle. Your project proposal should include the following:
  1. **Executive Summary:** A high level, to-the-point summary of the project. Don't be too wordy! I should be able to read the executive summary and know exactly what you are planning to do without too much detail. The rest of the proposal will contain these details.
  2. **Plan of Attack:** Explain how you plan to execute your proposed work. This will naturally include a listing of software, software techniques, third-party software modules, or any other logistics you plan to use to achieve your target product. Be as explicit as much as possible. This will help you spell out any roadblocks you might run into.
  3. **Planned Deliverables:** This is what you are proposing to produce as your final project. Make sure to explicitly spell out your final product.
- **Project Demo** During Week 16 (and possibly Finals Week) in class.
- **Project Report** Due Tuesday, April 28th 2020 through Moodle. Your final report will include the followings:
  1. Motivation and objective of the experiment.

2. A detailed methodology of your experiment. You must be able explain the commands, tools, procedures you've used. Don't simply list the commands. I want you to explain what you've done and why you did it. Screenshots highly recommended.
3. A detailed testing plan and test results.
4. Justification of your observations. You must be able to justify and/or argue why (or why not) your method worked.
5. Final conclusions.

I will give you the option to choose a language of your choice for programming (though C++, Java, or Python is recommended) but the development platform is fixed to Unix/Linux.

### 3.6 Graduate Standing Project

Graduate students are required to extend the final project (see Sec. 3.5 above ) in to a mini-research project that is worth 20% of their final grade. The distinction between the two is a fairly comprehensive literature survey of a topic of your choosing during the early part of the project followed up with empirical validation and/or experimental results towards the end of the semestser. In other words, the graduate standing project has two phases: (i) A literature survey phase with the deadlines listed below; and (ii.) Implementation phase aligned with the final project listed in Sec. 3.5.
Your topic should be relevant to the theme of this course. All assignments are due at the beginning of class through Moodle.

- Thursday January 30th, 2020 – **M1:** One page research proposal and a justification of your proposed research.
- Thursday March 19th 2020 – **M2:** ~3-4 page intermediate report of your research progress.
- Tuesday April 16th 2020 – **M3:** Project presentation slides.
- Tuesday April 23rd 2020 – **M4:** Final report.

Places to look for a research topic includes (but not limited to) IEEE FOCS, ACM STOC, ISAAC, SODA, IEEE S&P, ACM CCS, SOCG, IEEE CCC, ACM PODC, IEEE IPDPS, CSF, DSN, IEEE ICDCS, USENIX, etc. Topics in Cybersecurity are **highly favorable**.
A typical graduate level research of this scope would include a bare-minimum 15-20 *highly cited* research papers. I reserve the right to decide which projects meet graduate standing and lower the grade for those who don't; hence, make sure to clearly exchange your research ideas with me, find out about my expectations, and set yourself up for success **early** in the semester.
You are to present your research to the class at the conclusion of your research during weeks 15 and 16. In addition, you are required to produce an IEEE conference style minimum 8-page paper of your research. A template can be found at `http://www.ieee.org/conferences_events/conferences/publishing/templates.html`. You are **highly encouraged** to produce your report using Latex.
In addition, graduate students may have additional mandatory questions in exams. Accordingly, graduate students will be graded on separate scale. Please refer Section 3.

# 4 Course Requirements and Policies

## 4.1 Attendance Policy

Based on University Class Attendance Policy 1I9: It is the responsibility of students to ascertain the policies of instructors with regard to absence from class, and to make arrangements satisfactory to instructors with regard to missed course work. Failure to attend the first session of a course may result in the student's place in class being assigned to another student. You may be dropped from the course at any time for the following reasons:

- Failure to attend the first scheduled class
- Missing an exam or quiz without an acceptable reason
- Missing more than one week of class or two class sessions

**There will be no opportunities to make up missed exams or quizzes!**

## 4.2 Late Policy

Unless otherwise noted or announced in-class, all deadlines are hard deadlines and assignments are due at the beginning of class on the due date. Assignments may be turned within 48 hours *grace period* after the deadline (except any final projects) with a 20% late penalty. No assignment is accepted beyond this grace period. Graduate project milestones do not have any grace periods.

## 4.3 Responsible Learning Policy

There is a no tolerance policy with regards to cheating. **Anyone caught cheating will fail the course**. Do your own work. Your exams, homeworks, and programming projects are subject to the academic honor code. Following activities will be considered academic dishonesty:

- Submitting work (such as assigned work, projects, and code) done by somebody else (this includes any human/electronic sources (such as web sites));
- Watching and copying your neighbors' solutions during problem solving and/or exams;
- Collaboratively develop solutions to individual assignments;
- Using materials not allowed during problem solving and exams;
- Using materials not allowed for the programming projects.

You are expected to know and observe the SIUE Student Conduct Code (3C1) and Student Academic Code (3C2) found at `http://www.siue.edu/policies`. If you are unsure about what constitutes as plagiarism, check this website: `https://www.siue.edu/education/psychology/plagiarism.shtml`

### 4.3.1 Online Repositories

If you indent to keep any project source code in online repositories, ensure those repositories are **private** and **only accessible to you**. By making source code publicly available to others, you might be involuntarily participating in plagiarism.

### 4.3.2 Advice

This course will require a substantial amount of time reading and solving problems outside of class time. It is imperative that you keep up with the assigned reading and other tasks as much as possible. If you do not, it will be very difficult to be successful in this course.

Know the information, how to approach the problem/solution, and present it in a clear and organized manner. On exams and in programming projects, you are attempting to demonstrate understanding of concepts and the ability to solve problems. If I have to try to determine **how** you came up with your answer, then you will **not** receive full credit.

The following conditions are subject to loss of some or all credit for a given problem:

- Illegible work/answers
- work/answers that cannot be easily located
- no work
- missing/incorrect units
- compile-time and/or run-time errors

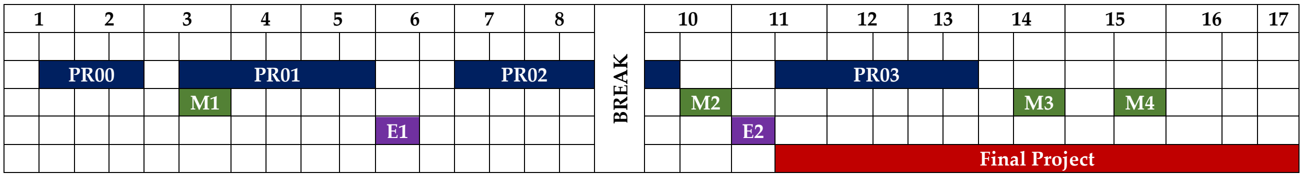
Solutions which clearly demonstrate understanding of the material, but have a minor error may receive partial credit. The final score for such problems is at the discretion of the grader and/or the instructor.

a. Don't wait until the last minute to do homework or projects. Labs get busy, computers break down, and people get sick. These are not sufficient excuses for an extension.
b. Save early; save often!
c. Contact me if you are confused. Don't wait for office hours; send an email.
d. I strongly discourage you from getting into discussions with me about grades and how you can get a better one. This includes emailing me about possible ways to "bump" your grade. Such requests only mean one thing; that you have already fallen behind on your own expectations.

### 4.4 Accessible Campus Community & Equitable Student Support: http://www.siue.edu/access

Students needing accommodations because of medical diagnosis or major life impairment will need to register with Accessible Campus Community & Equitable Student Support (ACCESS) and complete an intake process before accommodations will be given. Students who believe they have a diagnosis but do not have documentation should contact ACCESS for assistance and/or appropriate referral. The ACCESS office is located in the Student Success Center, Room 1270. You can also reach the office by e-mail at myaccess@siue.edu or by calling 618.650.3726. For more information on policies, procedures, or necessary forms, please visit the ACCESS website at `www.siue.edu/access`.

# 5 CS 490 In a Nutshell



WS## – Wireshark Labs, M# – Graduate Standing Project Milestones, PR## – Programming Projects, E# – Mid-Term Exams

## 5.1 Tentative Schedule*

*Subject to adjustment and change. I reserve the right to change topics or add an item of related interest. All changes will be announced in class.

| Week | Dates | Topics | References | Assignments/Exams |
|---|---|---|---|---|
| 01 | Jan. 14, 16 | Introduction and Course Overview<br>Security Objectives, Policies, and Mechanisms | | PR00 > out |
| 02 | Jan. 21, 23 | **Cryptography Basics:** Stream Ciphers | **PP1e**/02 | PR00 < in |
| 03 | Jan. 28, 30 | Basic Cryptanalysis | **PP1e**/02 | PR01 > out, M1 < in |
| 04 | Feb. 04, 06 | **Symmetric-Key Ciphers:** DES<br>Finite Fields | **PP1e**/03 | |
| 05 | Feb. 11, 13 | AES<br>**Asymmetric-Key Ciphers:** RSA | **PP1e**/04<br>**PP1e**/06 | PR01 < in |
| 06 | Feb. 18‡, 20 | Midterm Exam 01 | | |
| 07 | Feb. 25, 27 | RSA Fast Exponentiation<br>DHKE | **PP1e**/07<br>**PP1e**/08 | PR02 > out |
| 08 | Mar. 03, 05 | **Integrity:** MDC, MAC, WHIRLPOOL<br>Random Oracle Model | **PP1e**/11,12 | |
| 09 | Mar. 10†, 12† | **Spring Break** | | |
| 10 | Mar. 17, 19 | SHA Family | **PP1e**/11,12 | PR02 < in<br>M2 < in |
| 11 | Mar. 24‡, 26 | Midterm Exam 02 | | PR03 > out, Proposal < in |
| 12 | Mar. 31, Apr. 02 | Digital Signatures<br>**Key Management:** Kerberos | **PP1e**/10<br>**PP1e**/13 | |
| 13 | Apr. 07, 09 | **Authentication:** Zero Knowledge Proofs | | PR03 < in |
| 14 | Apr. 14, 16 | **Network Security:** SSL and TLS | | |
| 15 | Apr. 21, 23§ | *Topic TBA* | | M3 < in |
| 16 | Apr. 28§, 30§ | *Final Project Presentations* | | M4 < in |
| 17 | May. 06§ | *Final Project Presentations* 10:00 a.m. onwards | Report < in | |

†Spring Break ‡Midterm Exam §Final Project: In class presentations