# CS 490/590 : Cryptography and Computer Security

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

Spring 2019 Syllabus

Course Information:

| | |
|---|---|
| Title: | CS 490/590 : Cryptography and Computer Security (3 Credits) |
| Location: | SE 2216 |
| Time: | T & R 11:00 – 12:15 p.m. |
| Course Web site: | http://www.cs.siue.edu/~tgamage/S19/CS490 |

Contact Information:

| | |
|---|---|
| Office: | EB 3053 |
| Phone ☎: | 650-2407 |
| Email ✉: | tgamage@siue.edu |
| Web Site 🏠: | http://www.cs.siue.edu/~tgamage |
| Office Hours: | M & W 01:20 – 02:20 p.m.<br>T 09:30 – 10:30 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 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) http://www.acm.org/education/CS2013-final-report.pdf

## 1 Course Prerequisites

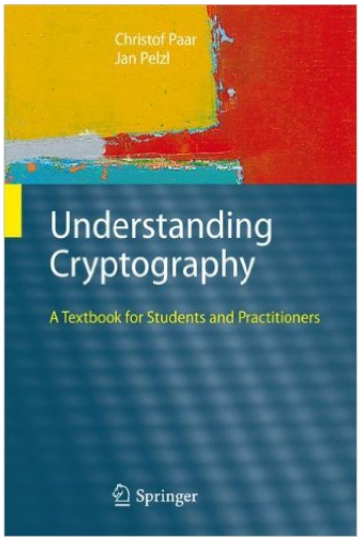
**MATH 224 :** The cryptographic component of the course is substantially formal and mathematical in context and in substance, and will either introduce or revise concepts in number theory, finite fields, modular arithmetic, probability theory, statistics, linear algebra etc.

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

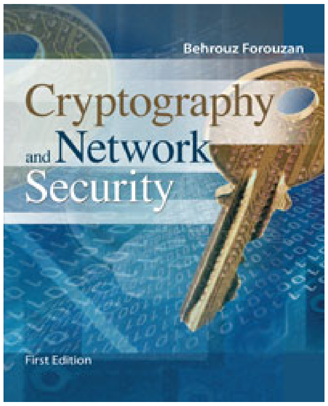
Also *fluency and significant experience* in programming (C++, Java, Python, etc.,) and **Unix/Linux** will be essential. If you do not meet these prerequisites, you **MUST** come and talk with me the first week of class. I reserve the right to drop you from the course if it becomes obvious that you 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/`
**[Required]** [**BF1e**] Cryptography and Network Security 1st ed., Behrooz Forouzan, McGrew-Hill, ISBN 978-0073327532


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

(a) [**PP1e**]



(b) [**BF1e**]

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% | 10% |
| Graduate Standing Project | | – | 10% |

| **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 19th 11:00 – 12:15 p.m.
- **Midterm 02** : Tuesday March 26th 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. Graduate students may team up with one undergraduate student.
Important milestones for your project are:

- **Project Proposal** Due Thursday March 28$^{nd}$, 2019 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 May 06th 2019 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 conduct a mini-research project that is worth 10% of their final grade. Ideally, this would be a fairly comprehensive literature survey of a topic of your choosing with some empirical validation and/or experimental results. Your topic should be relevant to the theme of this course. Important milestones for your project are listed below. All assignments are due at the beginning of class through Moodle.

- Thursday January 31st, 2019 – **M1:** One page research proposal and a justification of your proposed research.
- Thursday March 21st 2019 – **M2:** ~3-4 page intermediate report of your research progress.
- Thursday April 23rd 2019 – **M3:** Project presentation slides.
- Thursday May 02nd 2019 – **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 20-25 *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

I allow you to miss at most 2 classes for the semester without any penalties. Medical emergencies are outside this "absentee allowance", but should be accompanied by proper documented proof of medical services. For planned absences, assignments should be turned in before the absence rather than after. I reserve the right to lower the grade of any student who is markedly deficient in attendance and/or in in-class participation. If you miss a class, it is *your* responsibility to find out what happened and to collect any material that was handed out in the class.

### 4.2 Late Policy

Unless otherwise noted or announced in-class, any leftover questions from in-class problem solving sessions are due within a week at the beginning of the next immediate class. Programming assignments typically have a 2 week deadline. Assignments may be turned within 48 hours *grace period* after the deadline with a 20% late penalty. No assignment is accepted beyond that.

### 4.3 Responsible Learning Policy

I expect *you* to *own* your degree of success in this class *and*, I expect you to contribute to the success of others. Examples:

- Read outside the class on your own in preparation for each lecture, jot down any questions your encounter on your reading (strongly encouraged), and bring those to the class as discussion points;
- Be respectful of the learning environment. Refrain from activities that may disturb the flow of the lecture or the environment;
    - Refrain from engaging in disruptive *"little talk"* while I am conducting the lecture; if you have a concern, raise your hand and grab my attention. be respective of your colleagues time and desire to learn.
    - Put your cell phones to vibrate mode and refrain from using your computers for casual web browsing. Take full advantage of the opportunity to learn.
- Cooperate with other students and to share your knowledge during in-class discussions. Respect the differences in learning and understanding of each other. Seek ways of taking advantage of those differences;
- If another student is confused, help him or her out without disturbing the class;
- I enjoy engaging in technical conversations with students with the goal of helping them create an accurate understanding of course material. Participating in such conversations is very favorable for your class participation grade;
- If I am systematically doing something that inhibits your learning, tell me;
- Engage in *proactive learning*: speak up when you don't understand, question assumptions, relate course material to your experience outside class, seek out additional experience and reading related to the class. You must *construct* your understanding of the material;
- If a lecture point is unclear, ask questions and ask me to repeat what I said, preferably in class, during office hours, or by e-mail. You are probably not alone in your confusion;
- Promptly review feedback you receive from me or other students to actively clarify the feedback if the material is still unclear and to incorporate the feedback in your future work;
- Spend adequate time on the course. Adequate time includes getting enough rest so that time you spend on course tasks is well-spent time. Adequate time includes proofreading and reviewing your assignments before you hand them in;
- Have high expectations of yourself: set goals for yourself and try to do your very best. Consciously think about the balance between what you do to earn a grade and what you do to learn (If I'm doing something that puts these in opposition to each other, please let me know.); and,
- Check your SIUE assigned student email and the course website regularly for important class announcements.

**IMPORTANT**: 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.

Do your own work. Your exams, homeworks, and programming projects are subject to the academic honor code. **DO NOT CHEAT IN ANY WAY: DO YOUR OWN WORK!**. 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 quizzes and/or exams;
- Using materials not allowed during quizzes and exams;
- Using materials not allowed for the programming projects.

It is quite acceptable to ask others things like "Have you come across this particular issue/error/exception before?," and even having them briefly look briefly at your stack trace and/or its code. To have them spend hours helping develop or seriously rearrange your program's logic, on the other hand, is not acceptable. And, of course, it is unacceptable for two or more people to collaboratively develop the solutions to assignments. If you are tempted to collaborate on such assignments, **DON'T!!**.

I expect you to know and observe the SIUE Student Conduct Code (3C1) and Student Academic Code (3C2). Copying of other students' work, working together on individual assignments, plagiarism of published sources and other forms of academic dishonesty will result in zero credit on the assignment for all students involved and a lower grade in the class. A second offense (across the University) will result in an automatic **F** in the course and exposes the violator to University sanctions up to and including expulsion. All offenses will be reported to Student Affairs.

### 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.

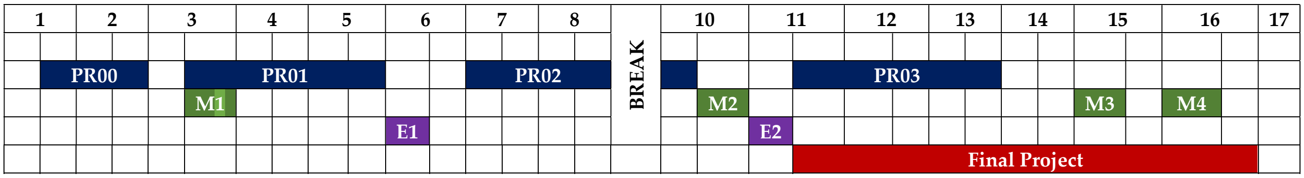
### 4.3.2 Advice

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.

## 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. 15, 17 | Introduction and Course Overview<br>Security Objectives, Policies, and Mechanisms | <br>**BF1e**/01 | <br>PR00 > out |
| 02 | Jan. 22, 24 | <br>**Cryptography Basics:** | **PP1e**/02<br>**BF1e**/01 | <br>PR00 < in |
| 03 | Jan. 29, 31 | BLP Model, Basic Security Theorem<br>Cipher Techniques, Cryptanalysis | **PP1e**/02,03<br>**PP1e**/02,03 | <br>PR01 > out, M1 < in |
| 04 | Feb. 05, 07 | **Symmetric-Key Ciphers:** DES, 3DES, One-time Pads<br>Finite Fields | **BF1e**/06,07,10<br>**BF1e**/10 | |
| 05 | Feb. 12, 14 | AES<br>**Asymmetric-Key Ciphers:** RSA | **PP1e**/06,07<br>**BF1e**/09,10 | <br>PR01 < in |
| 06 | Feb. 19‡, 21 | Midterm Exam 01<br>RSA Fast Exponentiation | | |
| 07 | Feb. 26, 28 | Diffie-Hellman Key Exchange<br>**Integrity:** MDC, MAC, HMAC | **PP1e**/10,11<br>**BF1e**/11,12 | PR02 > out |
| 08 | Mar. 05, 07 | Attacks on Prefix/Postfix MACs<br>**Hashing:** SHA, WHIRLPOOL | **BF1e**/13 | |
| 09 | Mar. 12†, 14† | **Spring Break** | | |
| 10 | Mar. 19, 21 | **Key Management:** Kerberos<br>**Authentication:** Zero Knowledge Proofs | **PP1e**/13<br>**BF1e**/15 | PR02 < in<br>M2 < in |
| 11 | Mar. 26‡, 28 | Midterm Exam 02<br>Malicious Logic, Intrusion Detection | <br>**BF1e**/01 | <br>PR03 > out, Proposal < in |
| 12 | Apr. 02, 04 | Chinese Wall Model, Confinement Problem<br>**Network Security:** SSL and TLS | <br>**BF1e**/16,17 | |
| 13 | Apr. 09, 11 | IPSec, PGP<br>DNS Security, Secure Routing | <br>**BF1e**/18 | <br>PR03 < in |
| 14 | Apr. 16, 18 | *Topic TBA* | | |
| 15 | Apr. 23, 25§ | *Topic TBA* | | M3 < in |
| 16 | Apr. 30§, May 02§ | *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