CS490 : Cryptography

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

Spring 2022 Syllabus

Course Information:

Title:	CS490 : Cryptography (3 Credits)
Location:	~~PH 3417~~ EB 2170
Time:	M & W 10:00 – 11:15 a.m.
Course Website:	http://www.cs.siue.edu/~tgamage/courses/490S22
Assignment Dropbox:	https://classes.cs.siue.edu/spring-2022

Contact Information:

Office:	EB 3053
Phone:	650-2407
Email:	tgamage@siue.edu
Web Site:	http://www.cs.siue.edu/~tgamage
Office Hours:	M & W 03:00 – 04:00 p.m. *or by appointment*

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

1. To introduce fundamental cryptographic and cybersecurity *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 that aid in their professional career advancements.
The above course content and topics were derived and inspired by the IAS/Cryptography curricula guidelines on the IEEE/ACM Computing Curricula 2020 (CC2020)* and IEEE/ACM Cybersecurity Curricula 2017†. Please see the footnoted URLs for a detailed listing of topics.

1 Course Prerequisites

MATH224 : 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.

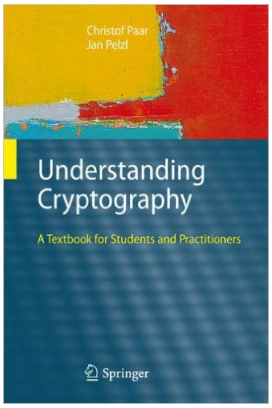
CS447 : The computer security component of this course will leverage basic understanding of the TCP/IP stack, network communication, and network programming knowledge.

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 to me within the first week of classes. I reserve the right to drop you from the course if it becomes obvious that you do not meet the prerequisites.

*https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf
†https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

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



(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/. I tend to favor a engineering/mathematical approach to my classroom explanations.
Students are **expected** to regularly check the course website and their SIUE email account for any important course related updates.

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	40%	40%
Midterm 01 20%		
Midterm 02 20%		
Participation & Problem Solving	10%	10%
Deterlab Experiments	30%	30%
Capstone Project	20%	
Graduate Standing Project	–	20%

Final Letter Grade	
[88 ++	A
[79–88)	B
[70–79)	C
[60–70)	D
– 60)	F

3.1 Exams

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

- **Midterm 01** (E1) : Wednesday February 24th 10:00 – 11:15 a.m. (75 mins)
- **Midterm 02** (E2) : Monday April 11th 10:00 – 11:15 a.m. (75 mins)

3.2 Attendance & 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. In preparation, 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 to the class as much prepared as you can.

3.3 Problem Solving

Some lectures may get supplemented with in-class problem solving sessions. In certain cases, you might be also asked to follow-up a lecture with a brief technical write-up, typically due at the beginning of next class. The frequency of these activities, will depend on the overall flow of lectures and class participation. At max, I expect there would be about ~3-5 such sessions for the whole semester.

3.4 Deterlab Experiments

You will use the DETERLab https://www.isi.deterlab.net/index.php3 infrastructure to complete 2 hands-on security experiments, each with a $2\frac{1}{2}$ weeks deadline; there will be an additional initial setup experiment with a 1 week deadline. You will be provided with login credentials to Deterlab after first day of class. Specifics of these experiments will be posted on the course website.

3.5 Technology Requirements

You are expected to have reliable Internet access on a regular basis. It is your responsibility to address any computer problems that might occur. Such problems are not an excuse for delays in meeting expectations or for missing course deadlines. At minimum, a computer with an updated operating system (Linux preferred but not required) and an updated internet browser of your choice on a stable Internet connection is expected.

3.6 Capstone Project

This course does not include a Final Exam. In its place, you are expected to complete a **themed** cybersecurity implementation project. Think of this as a (very) condensed form of your senior design and implementation project, but strictly on a cybersecurity topic. The full project scope (from proposal to final class presentation) is ~5 weeks. We might use the final exam time for project presentations as well, depending on the need. Undergraduates can team up with a maximum of 2 members per team. Important milestones for your project are:

- **Project Proposal (U1)** Due Monday April 04th, 2022 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/Execution:** 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 Capstone Project. Make sure to explicitly spell out your final product.
- **Project Demo/Presentation (U3)** During Week 16 (and possibly Finals Week) in class.
- **Project Report (U4)** Due Friday, May 06th 2022 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. A detailed walk-through on how to replicate your experiment and results.
6. Final conclusions.

Spring 2022 Theme

This semester's theme is **eBPF** https://ebpf.io/what-is-ebpf/ and how that can be used for (either a network or an operating system) for security monitoring purposes. Here's a good starting place https://www.brendangregg.com/blog/2019-01-01/learn-ebpf-tracing.html.

3.7 Graduate Standing Project

Graduate Standing Project, in essence, is an extension of the Capstone Project listed above in Sec. 3.6 that precedes with a literature survey. During the early part of the semester, the graduate students are expected to conduct a fairly comprehensive literature survey on a topic of your choosing during that would utimately lead to an implementation and/or empirical validation during the latter part of the semester. 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 Capstone Project listed in Sec. 3.6.

A typical graduate level research of this scope would include a fairly comprehensive literature survey that refers a minimum 15-20 *highly cited* research papers, culminating to a taxonomy **and** some empirical validation. In other words, your objective is to develop a hypothesis based on your reading and validate it with experimentation. You are free to choose a topic of your choice **relevant** to the theme of this course. Topics that intersects with Cybersecurity are **highly favorable**. Here's a short guide on **`How to Read a Paper`** : http://ccr.sigcomm.org/online/files/p83-keshavA.pdf.

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. Have a look at the USENIX security symposium proceedings https://www.usenix.org/conference/usenixsecurityXX/technical-sessions (*Replace XX with a 2-digit year (e.g. 19)*) for a quick "*get me up-to-speed*". Here is an excellent sample paper very much in sync with this course: https://www.ndss-symposium.org/ndss-paper/post-quantum-authentication-in-tls-1-3-a-performance-study/.

Important milestones for your project are listed below. All assignments are due at the beginning of class through Blackboard.

- (G1) Wednesday January 26th, 2022 – A one page research proposal and a justification of your proposed research.
- (G2) Monday March 28th 2022 – ~2-3 page research progress summary, including your demo plan and deliverables. In particular, how your project aligns with this semester's Capstone Project theme should be explicitly explained.
- (G3) Week 16+ – Project demo and literature survey presentation.
- (G4) Friday May 06th 2022 – Final report (in IEEE conference style).

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.

I reserve the right to decide which projects meet graduate standing and to lower the grade for any projects that don't at any point during the semester; 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.

In addition, graduate students may have additional mandatory questions in exams. Accordingly, graduate students will be graded on separate scale. Please refer Section 3 for the scale.

4 Classroom Policies

4.1 Attendance Policy

You are expected to attend all live lectures and **proactively** participate in in-class discussions and Q&A. Whenever applicable, lecture recordings and digital scribe notes will be made available to you through Discord. However, it is important for you to pay attention to the live lectures and take your own notes, rather than solely relying on my recorded lectures; recorded videos are not meant to be a substitute for missing classes, and I've had unplanned recording failures in the past.

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 Capstone Projects) with a 20% late penalty. No assignment is accepted beyond this grace period. Graduate project milestones do not have any grace periods.

5 COVID-19 Pandemic Policies Related to Classroom Instruction (Spring 2022)

5.1 Health and Safety

The measures outlined below are required and any student who does not comply may be in violation of the COVID-19 People-Focused Health and Safety Policy, as well as the University's *Student Code of Conduct*.
The full text of the *COVID-19 People-Focused Health and Safety Policy* can be found here: https://www.siue.edu/policies/Covid.shtml

5.2 Classrooms, Labs, Studios, and Other Academic Spaces

Under current University policy, whether in the classroom, lab, studio, or other academic spaces, students (regardless of vaccination status) shall wear face coverings that fully cover the nose and mouth and practice physical distancing measures to the extent practicable based on the specific classroom capacity and pedagogy. Classroom furniture should not be rearranged, and furniture that has been taped off or covered should not be used.
Students who forget to wear a face covering will be reminded of their obligation to comply with SIUE's *COVID-19 People-Focused Health and Safety Policy* and temporarily asked to leave the class until they are able to conform to the policy. Students who forget or lose their face coverings may be able to obtain replacements from a friend, a faculty member, or a nearby departmental office. Face coverings are also available for purchase in the Cougar Store (MUC). Students who refuse to wear a face covering will be asked to leave the classroom and referred to the Dean of Students for non-compliance with community health and safety protocols. Repeated non-compliance may result in disciplinary actions, including the student being administratively dropped from an on-ground/face-to-face course or courses without refund if no alternative course format is available.
If a student has a documented health condition which makes wearing a face covering medically intolerable, that student should contact ACCESS to explore options with the understanding that ACCESS will not grant accommodations which excuse the need for a face covering while on campus or in the classroom. ACCESS will work with qualifying individuals to find reasonable alternatives, whenever such solutions are available. Please call or contact the ACCESS Office via email to schedule an online appointment to discuss potential alternatives. ACCESS office (Student Success Center, Room 1203, 618-650-3726, and myaccess@siue.edu).

5.3 General Health Measures

At all times, students should engage in recommended health and safety measures, which include:

- Conducting a daily health assessment. If you have **COVID-19 Symptoms**[‡], but not yet tested positive,

[‡] https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html

have had COVID-19 close contact exposure, or are COVID-19 diagnosed as presumptive or confirmed positive, contact your health provider or SIUE Health Service at cougarcare@siue.edu or 618-650-2842. More information on reporting procedures is available at https://www.siue.edu/about/announcements/coronavirus/testing-reporting/reporting.shtml?section=students
- Frequent washing or disinfecting of hands.
- Adhere fully to the current face mask and physical distancing rules as articulated in policy: https://www.siue.edu/about/announcements/coronavirus/safety-guidelines-support/face-mask-pick-up.shtml.
- If present, adhere to directional signs and traffic flow patterns in buildings and offices. In many spaces, doors for entering and exiting buildings are designated.

5.4 Academic Integrity

Students are reminded that the expectations and academic standards outlined in the Student Academic Code (3C2) apply to all courses, field experiences and educational experiences at the University, regardless of modality or location. The full text of the policy can be found here: https://www.siue.edu/policies/3c2.shtml.

5.5 Recordings of Class Content

Faculty recordings of lectures and/or other course materials are meant to facilitate student learning and to help facilitate a student catching up who has missed class due to illness or quarantine. As such, students are reminded that the recording, as well as replicating or sharing of any course content and/or course materials without the express permission of the instructor of record, is not permitted, and may be considered a violation of the University's Student Conduct Code (3C1), linked here: https://www.siue.edu/policies/3c1.shtml.

5.6 Potential for Changes in Course Schedule or Modality

As the COVID-19 pandemic continues, there remains a possibility that planned classroom activities will need to be adjusted. Depending on circumstances and following state-issued recommendations, potential changes include alterations to distancing requirements, course modality (e.g., transition from face-to-face to online, hybrid, or hy-flex, mask wearing, in-course activities, etc). These changes would be implemented to ensure the successful completion of the course while preserving health and safety. In these cases, students may be provided with an addendum to the class syllabus that will supersede the original version. If the course schedule or modifications significantly alter expectations, a new syllabus will be issued.

6 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.

6.1 Online Repositories

If you intend 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.

6.1.1 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

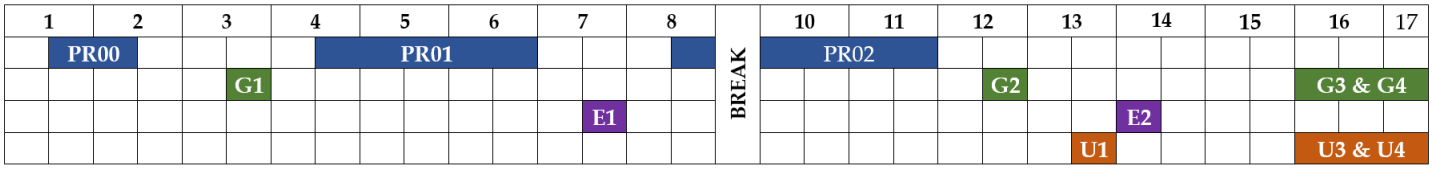
Solutions which clearly demonstrate understanding of the material, but have a minor error may receive partial credit. The final score for such problems is at the discretion of the grader and/or the instructor.

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.

7 Accessible Campus Community & Equitable Student Support

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`.

8 CS490 In a Nutshell



PR## – Deterlab Projects, G# – Graduate Standing Milestones, E# – Mid-Term Exams, U# – Capstone Project Milestones

8.1 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. 10, 12	Introduction and Course Overview **Cryptography Basics:** Terminology and Primitives	PP1e/1.1–1.4	PR00 > out
02	Jan. 17, Sep. 19	**MLK Day** MITRE ATT&CK, Historic/Classic Ciphers	PP1e/2.1–2.4	
03	Jan. 24, 26	**Introduction to Cryptanalysis**		PR00 < in G1 < in
04	Jan. 31, Feb. 02	Classical Attacks, Breaking Historic Ciphers		PR01 > out
05	Feb. 07, 09	Block Cipher Modes of Operation **Symmetric-Key Cryptosystems:** DES	PP1e/5.1, 3.1–3.5	
06	Feb. 14, 16	Finite Fields, AES	PP1e/4.2–4.5	
07	Feb. 21, 23‡	**Asymmetric-Key Ciphers:** Naive RSA, Fast Exponentiation Mid Term: Wednesday February 24th 10:00 – 11:15 a.m.	PP1e/6.1–6.3	PR01 < in
08	Feb. 28, Mar. 02	Discrete Logarithm Problem, Diffie-Hellman Key Exchange El-Gamal Encryption Scheme	PP1e/8.1–8.5	PR02 > out
09	Mar. 07†, 09†	**Spring Break**		
10	Mar. 14, 16	**Integrity:** Collision Resistance, Birthday Paradox MAC, CMAC, HMAC	PP1e/11.1, 12.1–12.4	
11	Mar. 21, 23	SHA Family	PP1e/11.3–11.4	PR02 < in
12	Mar. 28, 30	**Digital Signatures**	PP1e/10.1–10.5	G2 < in
13	Apr. 04, 06	**Key Establishment & Management**	PP1e/13.1–13.3	U1 < in
14	Apr. 11, 13	Mid Term 02: Monday April 11th 10:00 – 11:15 a.m. **Authentication Problem**		
15	Apr. 18, 20	**Security in the TCP/IP Stack:** Case Studies, PGP, TLS		
16	Apr. 25§, 27§	Capstone Project Presentations		U3/G3 < in
17	May 02§	Capstone Project Presentations		U4/G4 < in

‡Midterm Exam §Capstone Project: In class presentations