CS490/590 : Cryptography

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

Spring 2021 Syllabus

Course Information:

Title:	CS490/590 : Cryptography (3 Credits)
Location:	*thru* Microsoft Teams
Time:	M & W 08:00 – 09:15 a.m.
Course Website:	http://www.cs.siue.edu/~tgamage/courses/490S21
Assignment Dropbox:	https://classes.cs.siue.edu/spring-2021

Contact Information:

Office:	EB 3053 (*unmanned*)
Phone:	650-2407 (*unmanned*)
Email:	tgamage@siue.edu
Web Site:	http://www.cs.siue.edu/~tgamage
Office Hours:	pre-arranged thru Zoom https://siue.zoom.us/j/6186502407

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 content of this course is influenced by the IAS/Cryptography curricula guidelines on the IEEE/ACM Computer Science Curriculum Guidelines (2013)[*] and IEEE/ACM Cybersecurity Curricula 2017[†].

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.

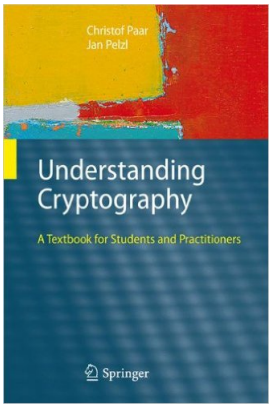
CS447 : The computer security component of this course will leverage basic understanding of the TCP/IP stack, network communication, and network programming knowledge.

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 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.

[*] https://www.acm.org/binaries/content/assets/education/cs2013_web_final.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/. 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	35%	35%
Midterm 01 15%		
Midterm 02 20%		
Attendance	5%	5%
Problem Solving	10%	10%
Deterlab Experiments	35%	30%
Final Project	15%	
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) : Monday March 01st 08:00 – 09:15 a.m. (75 mins)
- **Midterm 02** (E2) : Wednesday March 31th 08:00 – 09:15 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 3 hands-on security experiments, each with a 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 soon after the first day of class. Specifics of these experiments will be posted on the course website.

3.5 Final Project

This course does not include a Final Exam. In its place, you are expected to complete a **cybersecurity themed** implementation project (preferably) of your own choosing/interest. Think of this a (very) condensed mini senior design and implementation project but strictly on a cybersecurity topic. The full project scope is 5 weeks, which includes a class presentation during the last week of class and a report of your findings. Undergraduates can team up with a maximum of 2 members per team. Important milestones for your project are:

- **Project Proposal (M2)** Due Wednesday March 24th, 2021 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 (M3)** During Week 16 (and possibly Finals Week) in class.
- **Project Report (M4)** Due Thursday, May 06th 2021 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 Standing Project, in essence, is an extension of the Final Project listed above in Sec. 3.5 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 leads up to implementation and/or empirical validation during the latter part. 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. 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's a sample for your review: https://dl.acm.org/citation.cfm?id=3047307.

- (M1) Wednesday February 03rd, 2021 – A one page research proposal and a justification of your proposed research.
- (M2) Wednesday March 24th 2021 – ~2-3 page research progress summary, including your demo plan and deliverables.
- (M3) Week 15 and 16 – Project demo and literature survey presentation.
- (M4) Thursday May 06th 2021 – Final report (in IEEE conference style).

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.

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. Recordings of all lectures will be available through Microsoft Teams. I will also share all my live scribe notes. It is important for you to pay attention to the live lecture, take your own notes, and not solely depending on recorded lectures; recorded videos are not meant to be a substitute for missing classes when you can avoid it.

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 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 changes in course modality (e.g., transition from face-to-face to online) or in course scheduled meetings. These changes would be implemented to ensure the successful completion of the course. In these cases, students will be provided with an addendum to the class syllabus that will supersede the original version.

5 COVID-19 Pandemic Policies (Fall 2021)

5.1 Health and Safety

Consistent with the Illinois Board of Higher Education guidance contained in "Safely Launching Academic Year 2021" released on June 23, 2021 and guidelines established by Governor J. B. Pritzker and Restore Illinois, Southern Illinois University Edwardsville has implemented a new policy to help ensure the safety of all students, faculty and employees during the pandemic. 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

While in the classroom, lab, studio, or other academic spaces, students shall practice social distancing measures by maintaining a distance of at least six feet from others in the classroom and wearing a face covering. Extra care should be taken upon entering and leaving the classroom spaces. 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 mask or face shield 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).

5.2.1 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, have had COVID-19 close contact exposure, or are COVID-19 diagnosed as presumptive or confirmed positive, stay home and contact your health provider or SIUE Health Service at cougarcare@siue.edu or 618-650-2842. More information is available on the SIUE COVID-19 website.
- Frequent washing or disinfecting of hands.
- Social distancing by maintaining a distance of at least six feet from others.
- Face masks or face coverings that cover the nose and mouth are required in indoor public spaces regardless of the ability to maintain social distance. Indoor public spaces include common spaces or community settings that anyone can access, such as reception areas with walk-in access, restrooms, hallways, classrooms, teaching and research laboratories, as well as common spaces in residence halls, conference rooms, lobbies, and break rooms.
- Adhere to directional signs and traffic flow patterns in buildings and offices. Doors for entering and exiting buildings will be designated. Where multiple doors exist, in and out doors will be marked with "Entrance" and "Exit" signs. Plans that consider traffic flow in and out of buildings, and within buildings (i.e. stairs, hallways, etc. where possible) will be marked.

6 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.

6.1 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.

6.2 Recordings of Class Content

Faculty recordings of lectures and/or other course materials are meant to facilitate student learning and to help facilitate student(s) catch up after a missed class due to illness. As such, students are reminded that the recordings, as well as replicating or sharing of any course content and/or course materials without the instructor's express permission 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.

6.3 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.

6.3.1 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

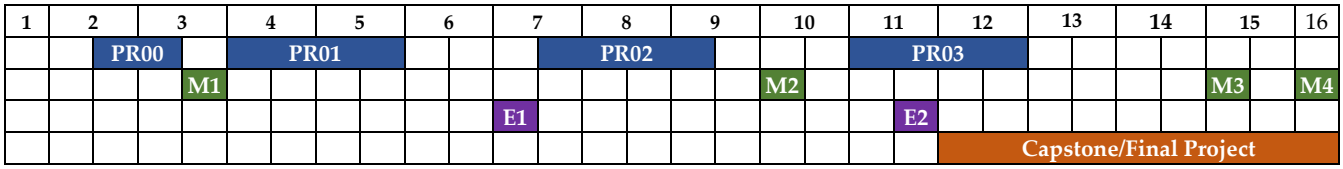
Solutions which clearly demonstrate understanding of the material, but have a minor error may receive partial credit. The final score for such problems is at the discretion of the grader and/or the instructor.

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



M# – Graduate Standing Project/Capstone Project Milestones, PR## – Programming Projects, E# – Mid-Term Exams

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. 20	Introduction and Course Overview		
02	Jan. 25, 27	**Cryptography Basics:** Terminology and Primitives Attackers and Their Capabilities	PP1e/02	PR00 > out
03	Feb. 01, 03	**Introduction to Cryptanalysis:** Historic Ciphers	PP1e/02	PR00 < in PR01 > out, M1 < in
04	Feb. 08, 10	Classical Attacks, Breaking Historic Ciphers	PP1e/03	
05	Feb. 15, 17	**Symmetric-Key Cryptosystems:** Block Ciphers, Modes of Operation DES, Finite Fields	PP1e/04 PP1e/06	PR01 < in
06	Feb. 22, 24	AES Attacks: Linear, Differential, and Meet-in-the-Middle		
07	Mar. 01‡, 03	Mid Term 01: Monday March 01st 08:00 – 09:15 a.m. **Asymmetric-Key Ciphers:** Naive RSA, Fast Exponentiation	PP1e/07 PP1e/08	PR02 > out
08	Mar. 08, 10	El-Gamal Encryption, Diffie-Hellman Key Exchange Rho method, Pohlig-Hellman, RSA Weaknesses	PP1e/11,12	
09	Mar. 15, 17	**Integrity:** MAC, CMAC, HMAC Collision Resistance, Birthday Paradox	PP1e/11,12	PR02 < in
10	Mar. 22, 24	SHA Family	PP1e/11,12	M2 < in PR03 > out
11	Mar. 29, 31‡	Digital Signatures Mid Term 02: Wednesday March 31th 08:00 – 09:15 a.m.		
12	Apr. 05, 07	**Key Management:** Kerberos Public-Key Infrastructure (PKI)	PP1e/10 PP1e/13	PR03 < in
13	Apr. 12, 14	**Entity Authentication:** Challenge-Response Protocols Zero Knowledge Proofs		
14	Apr. 19, 21§	**Network Security:** SSL and TLS		M3 < in
15	Apr. 26§, 28§	Final Project Presentations		M4 < in
16	May. 06§	Final Project Presentations		

‡Midterm Exam §Final Project: In class presentations