CSE 4402
INTRODUCTION TO CRYPTOGRAPHY
FALL 2025

Instructor's Name: Professor Brian Garnett

Instructor's Email: bcgarnett@wustl.edu

Instructor's Office: Urbauer 227

Contact: If you need to reach me, it's preferred that you contact me on our course's Piazza page (you can find a link on Canvas). You can control the visibility of your post, for instance if you want to talk directly to me.

If you do email, please begin the subject with "CSE 4402," so that I may easily find it in my inbox.

Office Hours: MW 4-5pm in my office. There may also be TA office hours, information about which will be posted. Additional meetings available on request.

Class times and locations MW 2:30-3:50pm in Eads 103.

Prerequisites: CSE 240 and CSE 247. It is highly recommended that if you are taking this course, you are very comfortable with mathematical reasoning and probability. Your assessments will primarily consist of writing mathematical proofs, many of which involve probabilistic reasoning.

Course Description: This course is an introduction to modern cryptography, with an emphasis on its theoretical foundations. Topics will include one-way functions, pseudorandom generators, public key encryption, digital signatures, and zero-knowledge proofs.

Textbook: You do not need to purchase a textbook. We will treat a set of freely available lecture notes as our "textbook." This along with other resources will be posted on Canvas.

Academic Integrity: All students in the course are expected to be familiar with and abide by the academic integrity policy (https://washu.edu/policies/academic-integrity-policy-for-undergraduate-students/). Violations of the policy are taken very seriously.

You may not consult ChatGPT, Chegg, Course Hero, or any similar website for assistance with any assessment in this course. Not sure how to do a homework problem or want to check your answer? Ask me for help! Still struggling? Ask for

help again!

Homework:. There will be approximately 6 homework assignments throughout the semester.. You will submit your work to the respective assignment on Gradescope. Your attachments can be scanned images or pictures of handwritten work (possibly from a tablet), or you may type your solutions if you wish (LaTex is preffered for typing math). Always check to make sure your documents are readable.

Exams: There will be a midterm and a final. The midterm will replace our class session on Monday, October 20 OR Wednesday, October 22 (I'll see what you prefer). The final will take place on December 15, 3:30-5:30pm.

Gradescope: As mentioned above, you will be submitting homework on Gradescope. You should be added to our course's site through Canvas, but in case you aren't the entry code is 6KWEEW. On Gradescope you will receive feedback for homework and the midterm exam. If you believe there was a grading mistake, you may use the "regrade request" option up to a week after the grades are posted, unless otherwise specified. However, please do not use this option to dispute the rubric itself. I will not post the grades to canvas until all regrade requests have been addressed.

Lateness: Please allow enough time to submit your assignment, in case you have technical issues. *It is your responsibility to be aware of the due date and time and make sure you have submitted your work before this time.* For each homework assignment there will be a regular deadline and a late deadline. If you want to receive full credit for your work, please ensure that you submit by the regular deadline. However, if the regular deadline has passed, you have a second chance to submit before the late deadline with a penalty. The penalty will not exceed 20% per 24-hour period. You cannot submit after the late deadline.

Course Grade: Here is the breakdown of how your final grade will be computed:

Problem sets	50 %
Midterm	25 %
Final	25 %
Total	100 %