



# Final exam and getting out of it

CSE 468 Fall 2024  
jedimaestro@asu.edu



# Final is the same format as the midterm

- Both the final and midterm are 100 points
- Both are the same length and number of problems
- Final is in the place and time scheduled by the university (7:15am on December 12<sup>th</sup>, here in the same room we have class in)
- You have 1 hour and 15 minutes for the final (not the fully scheduled time we have the room for)

# New for the final

- Come on time and use the restroom *before* coming to the final.
  - If you need accommodations related to this, let me know ASAP because that will go through SAILS.
  - Once the first person turns in their final and leaves we will not hand out any more blank final exams, you will need to do a grade appeal or similar process to make up the final.
- Bring your ASU student ID and be prepared to show it when you turn in your exam. Write your ID number on the exam.

# Extra Credit

- If, at least one week before the final, you receive an email confirmation from me saying you're definitely done with the extra credit and don't have to take the final, then you have two options:
  - Don't take the final, we'll put "100" for your grade on the final.
  - Take the final, and whichever score is lower between your midterm and final score we'll replace with "100".

# Extra Credit Option 1

- Carry out a chosen plaintext attack on 3-round AES, specifically a differential cryptanalysis attack.
- You have to give me:
  - The recovered plaintext
  - Your source code, which should be 100% your own individual effort

# Extra Credit Option 2

- Demonstrate Einstein's theory of relativity using GPS signals and SDR
- You'll need two RTL-SDRs (about \$40 on Amazon) and a friend in a different geographic location
  - Record raw GPS signals at the same time from two different parts of the globe, *e.g.*, Arizona vs. east coast
- You must give me:
  - Raw SDR recordings of the signals
  - Source code and instructions to run it to extract info and show partial orderings
  - Slides (preferably in OpenOffice format) introducing GPS and showing what you did and what you found

# Extra Credit Option 3

- Ratchetness
- You'll be updating it for a new semester
- You'll probably want to add a new transport layer, for your own sanity
- You'll also need to add a double ratchet
  - Need to think about when Alice, Bob, and Eve come online and go offline, etc.