Cryptography (CS-352)

Administrativia

Course Information

- Course: CPSC-352 (3 credits)

Section	Day	Time	Place
01	Monday	7:00 pm – 9:45 pm	CS 104 - Teaching Lab

- Course Website: Canvas

Course Information

- Instructor: Mikhail I. Gofman, Ph.D., CISSP
  - Email: mgofman@fullerton.edu
  - Phone: (657) 278-7304 (office)
  - Office: CS-429
  - Office Hours:
    - Monday: 4:15 pm -- 6:45 pm
    - Tuesday: 4:15 pm – 6:45 pm
    - Thursday: 4:15 pm – 6:45 pm
    - And by appointment

Prerequisites

- Prior to taking this course, you must satisfy all of the following prerequisites (strictly enforced):
  - CPSC-253: Cybersecurity Foundations and Principles
  - CPSC-131: Data Structures, AND
  - MATH-170B: Mathematical Structures II, AND
  - Computer Science or Computer Engineering major or minor

OR

  - Have Computer Science or Computer Engineering Graduate Standing, OR
  - Have the permission from the Computer Science Department

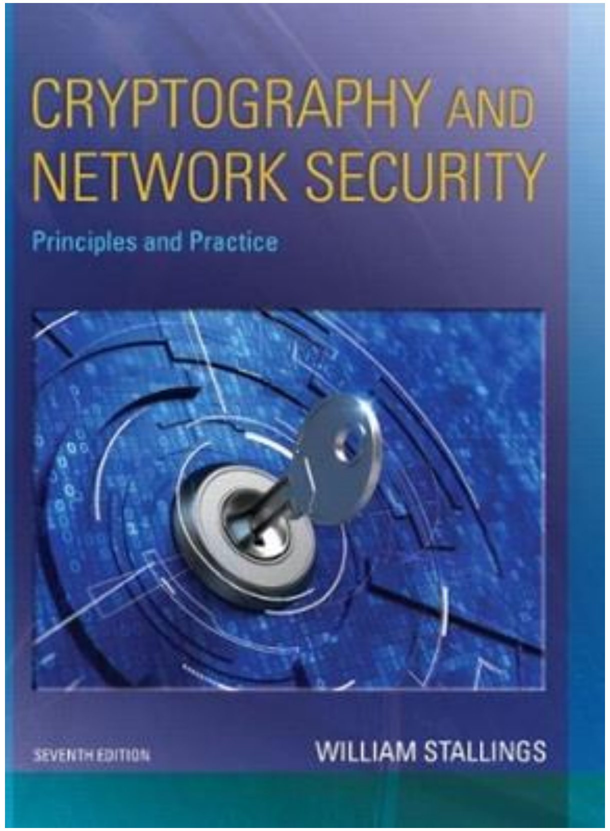
- Failure to meet the prerequisites may result in you being dropped administratively.

Course Objectives

- To journey through principals and practices of cryptography, network security:
  - Fundamentals of network and network security.
  - Cryptography:
    - Encryption and decryption techniques
    - Cryptonalytic Techniques
    - Classical Ciphers
    - Symmetric Encryption
    - Public Key Cryptography
    - Key management
    - Digital signatures
    - Authentication and Key Exchange protocols

Texts

- William Stallings Cryptography and *Network Security Principles and Practice*, Sixth/Seventh Edition. ISBN-13: 9780134444284 ISBN: 0134444280



- All additional materials shall be posted on Canvas.

Evaluation (1)

- Course grade breakdown:
  - Assignments: 25% (around 4 Assignments)
  - Quizzes/Lab Exercises: 15% (may drop 1 lowest)
  - Attendance and participation: 3% (may miss 1 class)
  - Midterm: 20%
  - Final Exam: 22%
  - Final Project: 15%
- The course grade shall be curved over the entire class, and (strictly) assigned according to the following range:

A+: 98-100	A: 93-97	A-: 90-92
B+: 87-89	B: 83-86	B-: 80-82
C+: 77-79	C: 73-76	C-: 70-72
D+: 67-69	D: 63-66	D-: 60-62
F: 0-59		

Evaluation (2)

- All assignments shall be averaged together.
- All Quizzes/Labs shall be averaged together.
- The raw score is a weighted mean of:
  - Assignment average
  - Quizzes/Lab averages
  - Midterm exam
  - Final Exam
  - Final Project
  - Attendance and participation
- Curve:
  - The raw score shall be curved over an entire class.
  - The amount of curving depends on how everyone scores.
  - Curving shall not cause your grade to decrease.

Evaluation (3)

- Computing your raw score.
- Suppose John Doe receives the following scores:
  - Assignments:
    - Assignment 1: 100/100
    - Assignment 2: 80/100
    - Assignment 3: 70/100

    Average = (100 + 80 + 70) / 3
    = 83.33
  - Quizzes/Labs:
    - 50/100
    - 90/100
    - 80/100
    - 100/100

    Average =
    (90 + 80 + 100) / 3 = 90 (the lowest grade is dropped).
  - Midterm Exam: 70/100
  - Final Exam: 50/100
  - Attendance: 100/100
  - Final Project: 100/100

Evaluation (4)

Item	Category Average	Category Weight	Result (avg * weight)
Assignments	83.33/100	25	(83.33/100) * 25 = 20.83
Quizzes/Labs	90/100	15	(83.33/100) * 15 = 13.5
Midterm	70/100	20	(70/100) * 20 = 14
Final Exam	50/100	20	(50/100) * 20 = 10
Attendance	100/100	5	(100/100) * 5 = 5
Final Project	100/100	15	(100/100) * 15 = 15

Sum: (20.83 + 13.5 + 14 + 10 + 5 + 15) = 78.33

Assignments

- Programming assignments: may contain both, theoretical and programming questions.
  - To be done individually unless stated otherwise.
  - Must be completed on Tuffix virtual machine, unless stated otherwise:
    - VM download link: https://bit.ly/3gqtl1T
  - Students may use C, C++, Java, Python or C# (unless specified otherwise).
  - Familiarity with basic C and Unix is assumed.
- All completed assignments must be submitted via Canvas.
- Late assignments shall be penalized 10%.
- No assignment shall be accepted after 24 hours from the deadline.

Quizzes

- In-Class quizzes:
  - Closed book.
  - Test your understanding of the material presented in class.
  - Missed quizzes shall earn a grade of 0 (unless you can provide written evidence of a legitimate excuse e.g. doctor's note).
- Lab Exercises:
  - Require critical thinking (and creativity!).
  - Late submissions shall be penalized 10%.
  - No quiz shall be accepted after 24 hours from the deadline.

Exams

- All exams are comprehensive and closed book.
- Exam 1 (Tentative Dates):

Section	Day	Time	Place
01	3/18/2024	7:00 pm - 9:45 pm	CS 104 – Teaching Lab

- Final Exam:

Section	Day	Time	Place
01	5/13/2024	7:00 pm - 8:50 pm	CS 104 – Teaching Lab

- Missed exams shall be dealt with according to University policies on incompletes and withdrawals.

Attendance and Participation

- The attendance is mandatory and shall be taken at beginning of every class.
- ***Please don't forget to sign the attendance sheet!***
- You may miss 1 class without incurring attendance penalties.
- Participate in class discussions (don't be afraid!).
- Ask questions!

Handouts

- The handouts are provided *for your benefit*
  - Help follow lectures, prepare for class examinations, and contain interview and certification exam questions
- *Will not be collected or graded*
- Highly *encouraged to complete them*
- If you attempt a handout question and get stuck*, the instructor will be happy to help*

Final Project

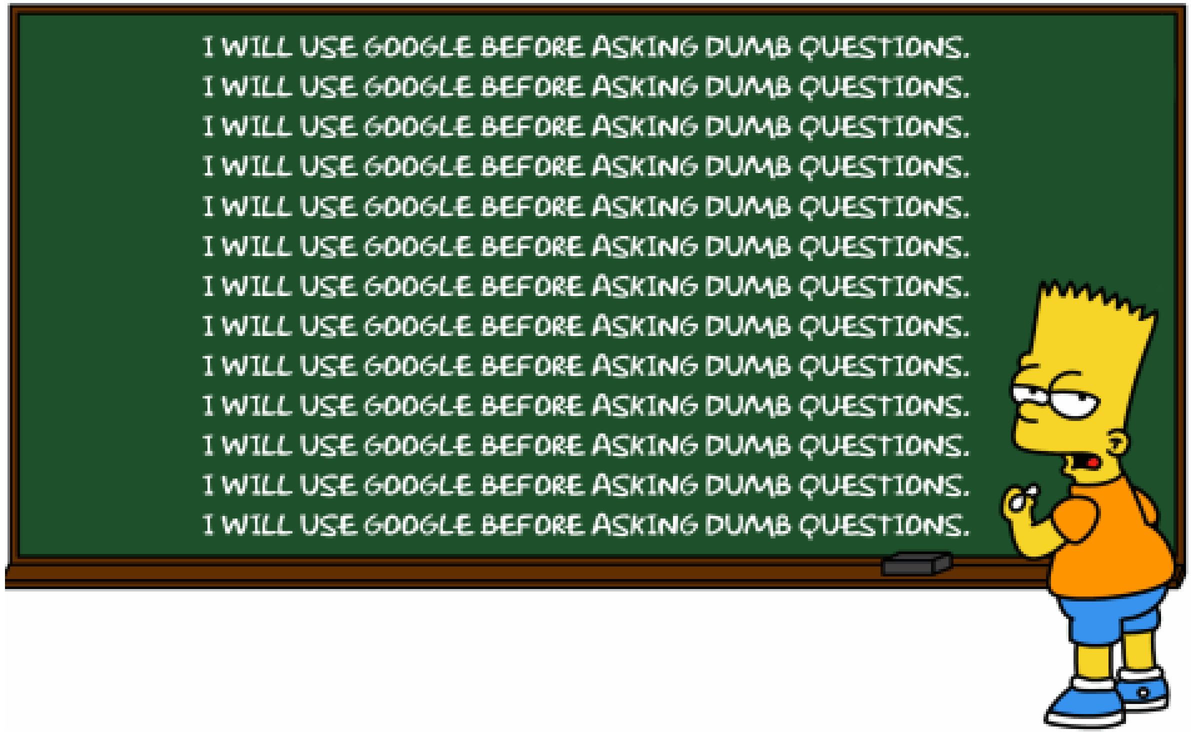
- The culminating experience of the class
  - Critical and creative application of the skills learned in class
  - Includes real-world security applications
  - Good resume booster
- May choose to do either a programming or a practical skills project
- Shall include a written component and a video or in-person presentation
- A list of choices was already posted on CANVAS
- **Please start working on the project as soon as possible. You can find the project details on the course website. The project will require you to apply the concepts learned in class, as well as conduct some extra research and use your creativity. The project is due by the end of the semester.**

Extra Credit

- Some assignments, exams, and quizzes may include bonus sections.
- No other forms of extra credit shall be granted.

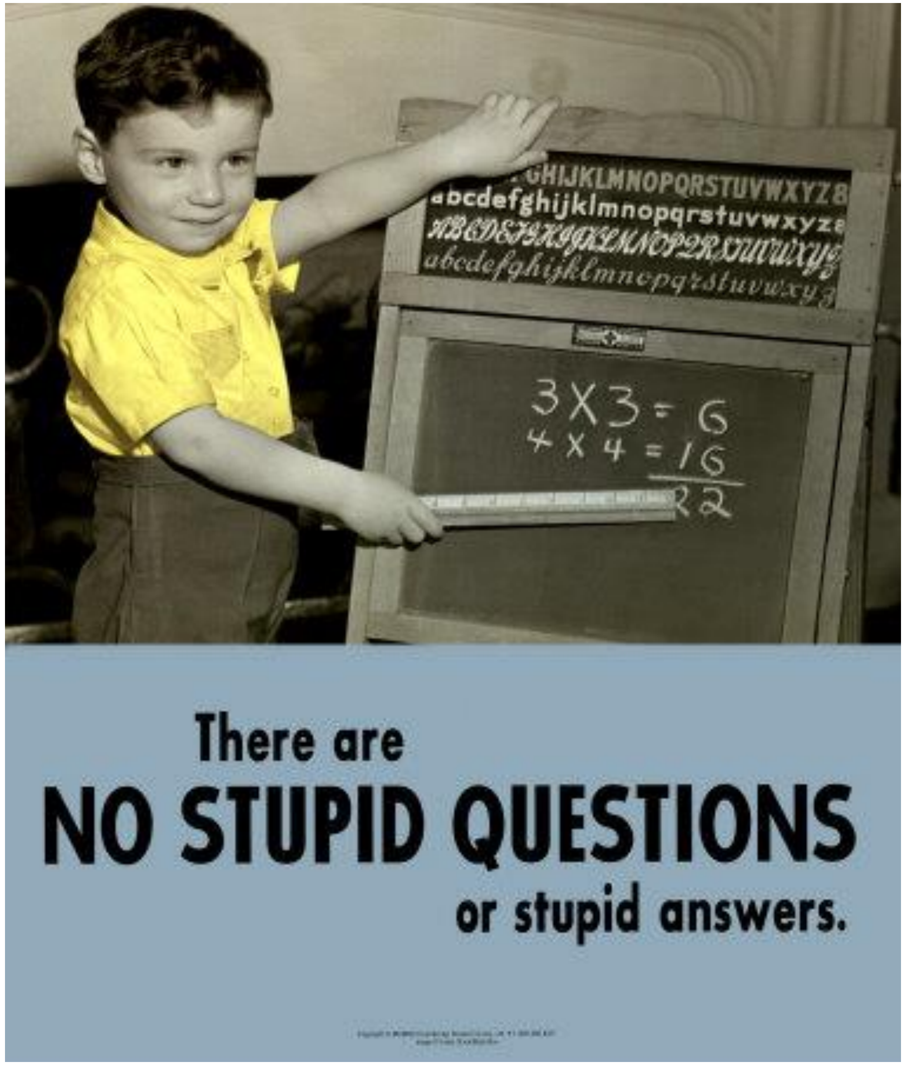
Asking Questions

- Never be afraid to ask:
  - In class or after class.
  - During office hours.
  - Make Google your friend (can't beat the availability and response time!...and avoid awkward moments...)


I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.
I WILL USE GOOGLE BEFORE ASKING DUMB QUESTIONS.

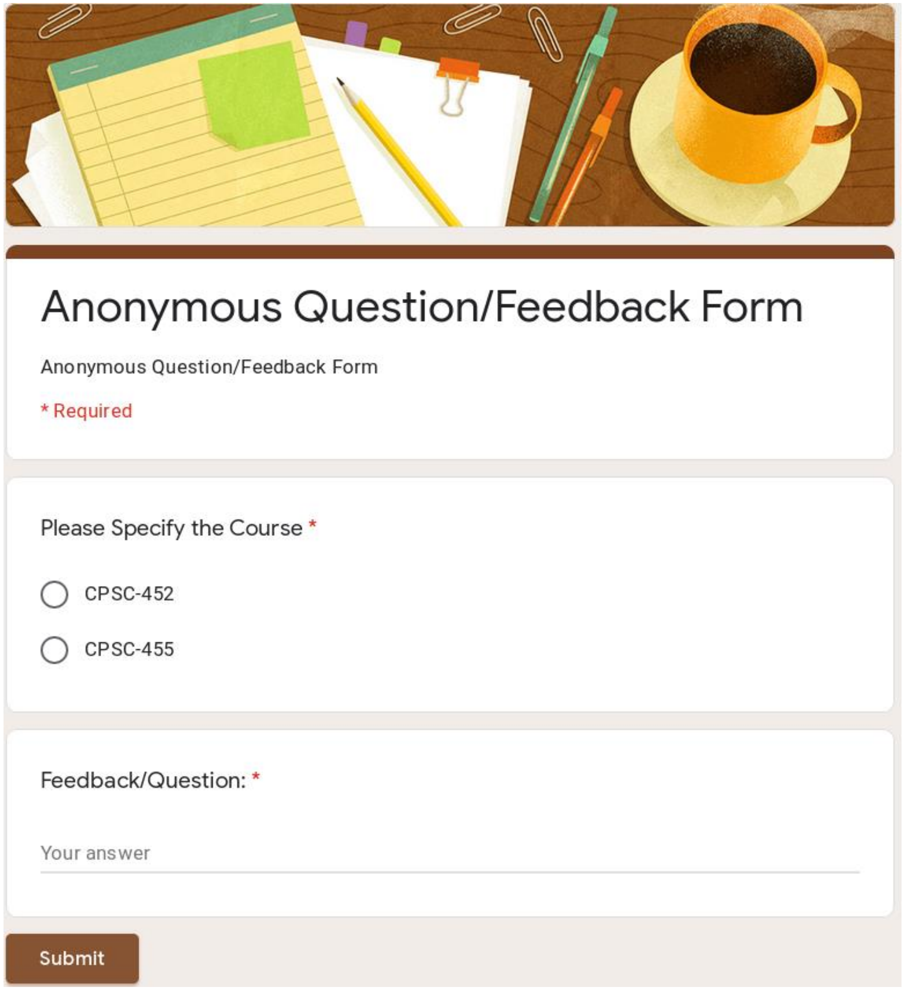
Asking Questions

- Remember, there is no such thing as a stupid question!



Anonymous Feedback

- Please feel free to anonymously submit your comments and suggestions about the course through:
  - https://bit.ly/2uyM2Oz



Anonymous Question/Feedback Form

Anonymous Question/Feedback Form

* Required

Please Specify the Course *

○ CPSC-452

○ CPSC-455

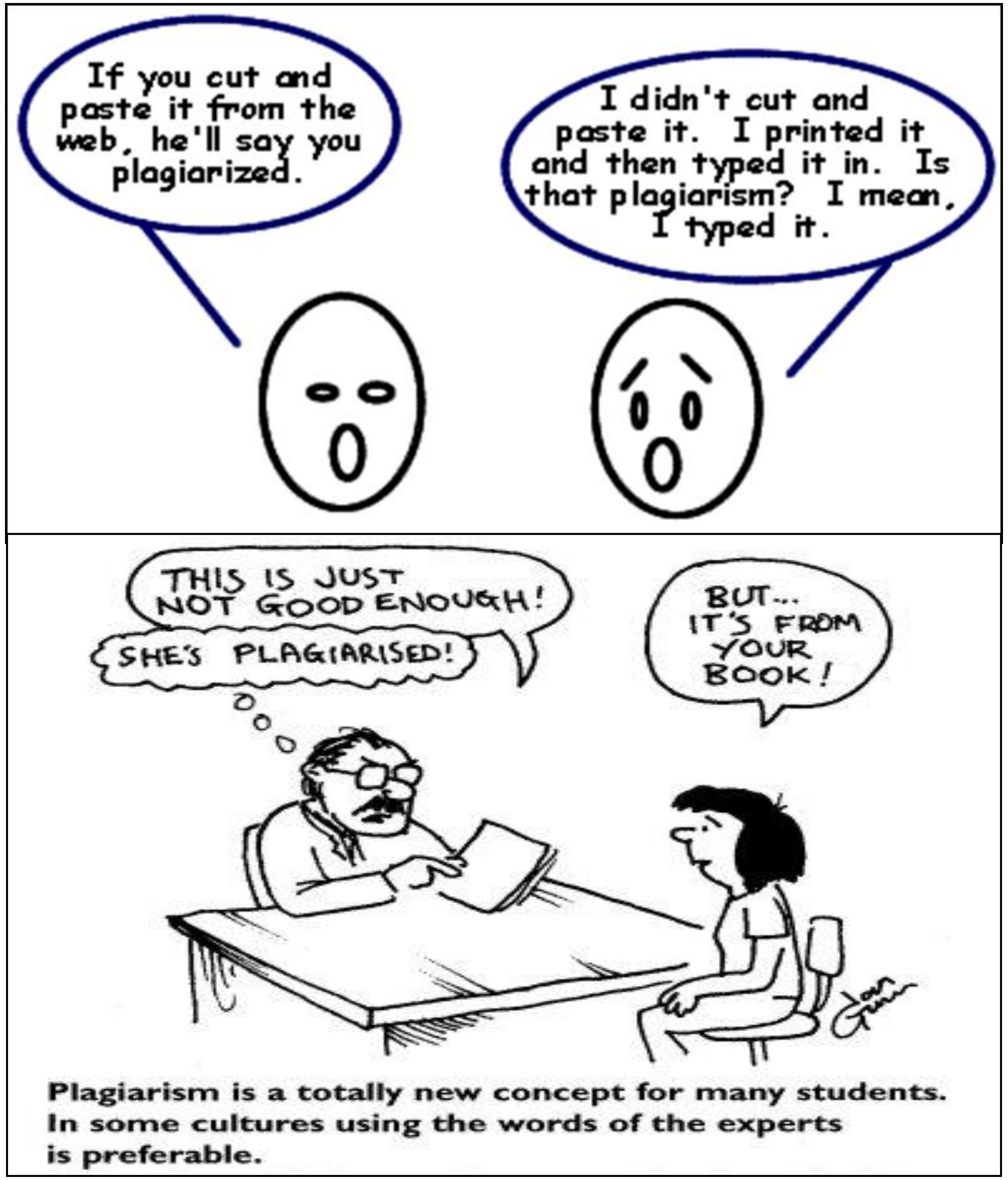
Feedback/Question: *

Your answer

Class Cancellation Policy

- All class cancellations shall be announced by email.
- Instructor does not arrive within the first 15 minutes of class = class is canceled.

Academic Honesty


If you cut and paste it from the web, he'll say you plagiarized.
I didn't cut and paste it. I printed it and then typed it in. Is that plagiarism? I mean, I typed it.
THIS IS JUST NOT GOOD ENOUGH!
SHE'S PLAGIARISED!
BUT... IT'S FROM YOUR BOOK!
Plagiarism is a totally new concept for many students. In some cultures using the words of the experts is preferable.

Academic Honesty

- Incidents of cheating shall be treated with utmost seriousness.
- Will be reported to the office of Student Conduct.
- You may discuss the problems with other students, however, you must write your own solutions.
- Discussing solutions to the problem is NOT acceptable.
- Copying an assignment from another student or allowing another student to copy your work may lead to an automatic F for this course.
- If you have any questions about whether an act of collaboration may be treated as academic dishonesty, please consult the instructor before you collaborate.
- Moss shall be used to detect plagiarism in programming assignments.
- All students are required to read and understand the UPS 300.021 ACADEMIC DISHONESTY university policy document.

Academic Honesty

CHEATING

- ***No argument*** will excuse academic misconduct, including:
  - “I was left with no other choice”
  - “Please have mercy, because I have _________ going on”
  - “Everybody else cheated too!”
  - “Try to put yourself in my shoes!”
  - 😭😭😭

- **NOTE**: historically *students have been reported* to student affairs and *some have been expelled without the possibility of readmission (this includes graduate and international students).*

Academic Honesty

- In addition…if cybersecurity career is your goal, cheating can ***destroy it*** before it starts
  - Some security certificates have a code of ethics the holders must follow – cheating can cause the certifying authority ***to revoke your certificate***
  - ***No*** security instructor will recommend you
  - ***No*** employer will trust you to protect them

- **Bottom line:** Cheating is simply not worth it!!

Emergency Policy

- Please familiarize yourself with the actions to take in case of an emergency.
- The information can be found at https://adminfin.fullerton.edu/emergency/

Disabled Student Services

- Information for students with disabilities can be found at: http://www.fullerton.edu/DSS/

Course Syllabus

- You are required to read the syllabus!
- A copy of the syllabus is available on CANVAS.
- If something is not clear, ask the instructor.