Ira A. Fulton Schools of Engineering
Arizona State University

Course Syllabus - Spring B 2022

CSE 539: Applied Cryptography

Contact Information

Instructor: Sameena Hossain

Teaching Assistants: Tariq Nasim
Sri Ajay Sathwik Ravilla

Content Questions: Weekly discussion forums

Project or Assignment Questions: Designated discussion forums

Slack Channel: Direct Link: asu-2221-cse539-35083.slack.com

Note: You must join/access this workspace using your ASURITE credentials.

Content Issues: Course "Feedback" tool

Technical Support: Coursera Learner Help Center

Note: Please make sure you are logged in so that support personnel recognize you as an ASU learner.

General Support: mcsonline@asu.edu

Note: When sending an email about this class, please include the prefix "CSE 539" in the subject line of your message.

Please use this email address for questions that are private in nature. If it is a question that would benefit your classmates, and is not private in nature, please post in the discussion forums.

Course Description

Cryptography provides the underlying security methods for the web and many other computer applications. This course covers the design usage of cryptographic protocols for online and offline computing applications. Assuring the quality, validity and privacy of information is one of the key applications of Cryptography. Applications of cryptography range from signatures and certificates to trustless multiparty computations.

Specific topics covered include:

- Large Numbers, Random Numbers, Hash Functions and Number Theory
- Encryption Methods and Common Ciphers
- Password Storage and Password Cracking
- Authentication, Key Exchange and Man in the Middle (MITM) Attacks
- Secure messaging, Kerberos and Secure Sockets Layer (SSL) or Transport Level Security (TLS)
- RSA and why it works
- Advanced Cryptographic Protocols
- Anonymity, money and secure election algorithms

Technologies covered include:

- .NET Core
- C#

Course Objectives

Learners completing this course will be able to:

- Examine Kerckhoffs's Principle.
- Analyze properties and constructions of hash and encryption functions.
- Apply number theory concepts to solve real-world problems.
- Apply algorithms for random number generation, hash functions and encryption.
- Analyze encryption and hash algorithms to find weaknesses and attacks.
- Identify methodologies for cracking passwords from hashes.
- Justify salting password hashes.
- Employ the Birthday Paradox to find a collision in a hash function.
- Recognize methods for key exchange and authentication.
- Distinguish different public key algorithms and their use cases.
- Examine methods for secure and secret communications.
- Identify the use cases for Message Authentication Codes (MAC).
- Identify techniques for certificate management.

- Implement the Diffie-Hellman Key Exchange.
- Employ existing algorithms to encrypt and decrypt data.
- Apply number theory concepts to solve real-world problems.
- Compare cut and choose strategies for enabling trust.
- Identify the uses of blind signatures for anonymous money orders.
- Analyze interactive proof systems for cryptography.
- Recognize advanced cryptographic protocols.
- Execute the proof of the RSA algorithm.
- Determine why RSA works.
- Implement the RSA algorithm.
- Test ways to work with very large prime numbers.
- Implement the Extended Euclidean algorithm.
- Apply number theory concepts to solve real-world problems.
- Evaluate the interplay between cryptography and politics.
- Analyze the usage of cryptography for political purposes.
- Examine the methods used for cryptocurrency and cash replacement algorithms.

Learning Outcomes

Learners completing this course will be able to:

- Differentiate the major algorithmic techniques used in cryptography.
- Explain the concept and correctness of cryptographic protocols.
- Perform identification of vulnerabilities in systems.
- Explain the algorithms used for constructing cryptographic computations.
- Perform steps needed for encryption, authentication, integrity, certification and data privacy.
- Explain complex protocols that involve many steps and computing agents who do not trust each other.

Estimated Workload/Time Commitment Per Week

Average of 18 - 20 hours per week

Required Prior Knowledge and Skills

This course will be very challenging, and learners are expected to learn the necessary technologies on their own time.

Proficient Mathematical Skills and Theoretical Understanding

- Discrete math
- Computer organization and architecture
- Operating systems
- Data structures
- Algorithms
- Algebra
- Data Structures
- Computer Organization
- Operating Systems

Strong Application Skills

- Linux
- Ability to effectively install and use Linux command line tools
- Ability to effectively read and write C# or confidence in your ability to learn C#
- C# on Linux: **An understanding of C or Java on Linux should be sufficient to get started with C#. If you do not know C#, but do know C or Java, there is no reason to avoid taking this course.*

Note: C# is the only language supported by the autograders.

Proficient Experience

- Clear understanding of what a file is, how it is stored on disk, and how to manipulate files
- Experience working with data at the byte level in both data structures and files
    - Manipulating bytes of data in variables and in files
- Experience working with numerical data in different radices
    - Specifically, base 2, base 10, and base 16
    - Representing constants of these bases in code
- Clear understanding of how numbers are represented
    - Endianness
    - Size restrictions (32-bit Integer, 64-bit Integer, BigInteger)
- Experience implementing Algebraic formulas
    - Especially logarithms and exponents
- Programming using C or C++ using Linux (Python or Java is useful)

Technology Requirements

Hardware

- Standard personal computer with major operating system

- Reliable, strong Internet connection
- Webcam
- Microphone

Software/Other

- Linux Operating System, Ubuntu 18.04 64-bit with administrator capability (ability to install new software).
    - You can run this OS in a virtual machine, if it is not your main machine.
- .NET Core 3.1 SDK
- Hex editor
    - You can use an online hex editor.
- Access to external websites: C# documentation, hashing calculator, encryption calculator, etc.

Note: C# is the only language supported by the autograders.

Textbook and Readings

At the graduate level, inquiry, research, and critical reading are part of the learning experience. Although not required, to support your learning process and success in completing projects and other assessments, information on a supplemental text has been provided for you; however, all assessed content is covered in the video lectures.

For interested learners, the faculty course designer *strongly* recommends the text:

> Menezes, Alfred J., van Oorschot, Paul C., & Vanstone, Scott A. *Handbook of Applied Cryptography,* digital sample chapters, CRC Press, 2007. http://cacr.uwaterloo.ca/hac/

Free, digital sample chapters of the *Handbook of Applied Cryptography* are available online. It is your responsibility to read the copyright notice on the website prior to downloading. If these should become unavailable, this will not negatively impact your learning of the necessary content to perform well on the assessments in this course (e.g., projects and exams). The lecture videos provide you the necessary information.

Access Steps

1. Go to the *Handbook of Applied Cryptography* website.
2. Read available copyright information. It is up to learners to stay current on this information and not to violate copyright laws.
3. Select the "ps" or "pdf" of the chapter listed in the course for you to read.
4. Refer to the "Contents in Brief" section for the page numbers of each section.
5. Locate the recommended section to read within the text (e.g., scroll or use a search

feature).
6. Take notes while reading the section and relate it back to the lecture video(s) and knowledge checks.

Course Content

Instruction

- Lecture Videos
- Project Overview Videos
- Suggested Readings
- Live Events (Live Sessions hosted by the Instructor/Virtual Office Hours hosted by the Course Team)

Assessments

Feedback Descriptions

- Limited: you will be able to see your Total Score, which includes the overall total percent (%) and the number (#) of points
- Partial: you will be able to see your Question Score, which includes the correct or incorrect status and the total points for each question
- Full: you will be able to see your Options and Feedback, which includes any itemized additional feedback

Assessment Types

- Knowledge checks: ungraded, full feedback, untimed, unlimited attempts
- Application Exercises: ungraded, full feedback, untimed, unlimited attempts
- Programming Projects: graded, auto-graded, partial feedback, untimed, unlimited submissions
- Practice exam(s): ungraded, auto-graded, full feedback, untimed, unlimited attempts
- Midterm Exam/Final Exam: graded, auto-graded, limited feedback, timed, proctored

Details of the main instructional and assessment elements in this course:

Each course in the MCS program is uniquely designed by expert faculty, so learners can best master the learning outcomes. As a result, course features and experiences are not the same across all MCS courses. Learners are expected to plan accordingly to accommodate for these differences.

Lecture videos: In each week, the concepts you need to know are presented through a collection of video lectures. You may stream these videos for playback within the browser by clicking on their titles or download the videos.This course's lectures were done using the Lightboard; therefore, there are no associated PDF lecture slides. Weekly overview videos, assignment videos, and project-related videos often do not have PDF lecture slides because they are not lectures and have associated documents or directions specific to them.

Readings: Readings from the *Handbook of Applied Cryptography* have been selected to accompany a variety of topics throughout the course. Although not required, they are *strongly recommended*, especially for those interested in careers in this field; however, all assessed content is covered in the video lectures.

Discussion forums: Discussion forums are present each week in the course and include designated forums for each project. Although the course team is engaged in these discussions, the forums are spaces to clarify, support, and enrich learner-to-learner communication and learning. *If you have specific questions that you would like to be considered to be addressed in the weekly Live Event hosted by the instructor, please indicate your request in your post.*

Knowledge checks (KCs): Designed to support your learning, these are short, ungraded quizzes to test your knowledge of the concepts presented in the lecture videos. You may take your time, review your notes, and learn at your own pace because knowledge checks are untimed. With unlimited attempts, you may retake these as often as you would like at any point in the course. You are encouraged to read the full feedback, review your answer choices, and compare them to the correct answers. With the feedback as your guide, you may use these as opportunities to study for other assessments and tasks in the course. *If you have specific questions that you would like to be considered to be addressed in the weekly Live Event hosted by the instructor, please indicate your request in your post. There are no late penalties.*

Application exercises: Application exercises are designed to provide you with self-guided practice opportunities. When you submit your answers, use the feedback to check your own work. You are encouraged to attempt each prompt, assess your work and reflect on your thought process based on the feedback provided, and discuss your questions in the weekly discussion forum. *There are no associated late penalties with the application exercises. Application exercises are not calculated as part of your final grade in the class.*

- Application Exercise: Introduction to Cryptography
- Application Exercise: Building Blocks

Projects: This course includes four (4) individual projects. All projects are provided in the first week of the course in the *Welcome and Start Here* section, so you can preview what is expected and design your own learning schedules to complete these on time. Each project has

a submission space at the end of the week it is due. Required projects are due at the end of the second week, third week, fifth week, and seventh week of the course. As a set of 4, the projects may be included in the Request for Faculty Review: MCS Project Portfolio submission, which is optional. *If you have specific questions that you would like to be considered to be addressed in the weekly Live Event hosted by the instructor, please indicate your request in your post. An automatic late penalty of 15% for each day late is applied to projects submitted after the scheduled due date and time. These projects count toward your final grade in the class.*

1. Steganography and Cryptanalysis Project - due at the end of Week 2 on Sunday, March 27, 2022 at 11:59PM AZ Time. Grading: auto-graded, full feedback, untimed, unlimited submissions
2. Hash Project - due at the end of Week 3 on Sunday, April 3, 2022 at 11:59PM AZ Time Grading: auto-graded, full feedback, untimed, unlimited submissions
3. Diffie-Hellman and Encryption Project - due at the end of Week 5 on Sunday, April 17, 2022 at 11:59PM AZ Time. Grading: auto-graded, full feedback, untimed, unlimited submissions
4. RSA Project - due at the end of Week 7 on Sunday May 1, 2022 at 11:59PM AZ Time Grading: auto-graded, full feedback, untimed, unlimited submissions

Request for Faculty Review: MCS Project Portfolio: This is an optional task for degree students wanting to use this course's projects as part of their portfolio degree requirement/specialization requirements. Review your onboarding course and the Welcome and Start Here section of your course for more details. The submission space is towards the end of the course. *Although there are no late penalties, these requests must be submitted by the designated deadline. The Request for Faculty Review: MCS Project Portfolio does not count toward your final grade in the class.*

- Address the four (4) projects from this course in your Request for Faculty Review: MCS Project Portfolio:

    1. Steganography and Cryptanalysis Project
    2. Hash Project
    3. Diffie-Hellman and Encryption Project
    4. RSA Project

- Request for Faculty Review: MCS Project Portfolio - due by Saturday, May 21, 2022 at 11:59 PM AZ Time.

- Faculty feedback should be received by Saturday, June 4, 2022.

Practice exam(s): To help you prepare for your proctored exams, you will have practice exams. Since they are intended to be practice opportunities and to help you learn, they are untimed, ungraded, and include feedback. You may engage with your peers in the discussion forums to address questions, share resources and strategies, and provide feedback to help one another learn. You are encouraged to read the full feedback, review your answer choices, and compare them to the correct answers. You are encouraged to submit questions in the discussion forum

for the course team to address during live sessions. Use the feedback to guide your learning and to study for the proctored exam. *If you have specific questions that you would like to be considered to be addressed in the weekly Live Event hosted by the instructor, please indicate your request in your post. There are no late penalties. Practice exams are not counted toward your final grade in the class.*

Proctored exams: You have two (2) proctored, timed exams. These consist of a Mid-term and a Final Exam. Proctored exams include limited feedback. For academic integrity purposes, once grades are made available, learners will see their overall total scores. Correct and incorrect answers and feedback to each question will ***not*** be provided. Read the Graded Quiz and Exam Policy for more information. *An automatic late penalty of 100% is applied to exams after the scheduled due date and time. No late exams will be permitted or accepted and will result in a score of zero points (0). This does not include established accommodations for learners with disabilities. Proctored exams count toward your final grade in the class.*

Mid-term Exam

Details

- **Content covered:** Weeks 1, 2, 3, and 4
- **Question type:** multiple choice questions with a single correct answer
- **Number of questions:** 25 content questions + 1 academic integrity question = 26 total questions
- **Availability:** Friday, April, 8, 2022 at 12:01 AM AZ Time - Friday, April 14, 2022 at 11:59 PM AZ time
- **Duration:** Plan for 15 minutes for proctoring set up and 2 hours (120 minutes) for the exam

Final Exam

Details

- **Content covered:** Weeks 1, 2, 3, 4, 5, 6, 7, and 8 (cumulative)
- **Question type:** multiple choice questions with a single correct answer
- **Number of questions:** 25 content questions + 1 academic integrity question **=** 26 total questions
- **Availability:** Tuesday, May 3, 2022 at 12:01 AM AZ Time - Sunday, May 8, 2022 at 11:59 PM AZ time
- **Duration:** Plan for 15 minutes for proctoring set up and 2 hours (120 minutes) for the exam

Mid-term and Final Exam Allowances

- **Hardcopy and/or digital books and/or reference materials (all)**: None
- **Calculators (all)**: None (calculations may be achieved by-hand)

- **Notes in any format of any kind (all)**: 1 page front and back, handwritten (not typed or printed), paper may be no larger than standard A-4 letter size (8.5x11)
- **Web (all)**: None
- **Software (all)**: All virtual machines need to be closed prior to starting proctoring
- **Other technologies, devices, and means of communication (all)**: None
- **Whiteboard, scratch paper, writing utensils, erasing resources**: Learners are *strongly* encouraged to use the whiteboard option instead of scratch paper.
    - If using a whiteboard, learners may have erasable whiteboard markers and what is needed to erase writing on the whiteboard; please have extra whiteboard markers and eraser resources in your testing area.
    - If using scratch paper, learners may have an unlimited amount of blank scratch paper of any size, writing utensils (e.g., pens, pencils, markers, and/or highlighters) and erasers; please have extra ones in your testing area should you run out of ink, the pencil breaks, etc.
    - Before the exam concludes and the proctoring session ends, all scratch paper must be destroyed and all whiteboard markings must be erased. The last question in the exam will be a confirmation of learners executing these ASU academic integrity actions.
- **Other**: Learners are to independently take the exam in a single session without leaving the testing space (e.g., no bathroom breaks) to ensure proctoring of the entire session. Once you open the exam, your testing session begins. You will be allowed one (1) attempt to take and complete each exam. Learners are to stay within a clear view of the proctor throughout the duration of the proctored exam session. You will be unable to open the exam until the exam proctor enters the password during the date and time you scheduled to take your exam with ProctorU.

Proctoring

ProctorU is an online proctoring service that allows learners to take exams online while ensuring the integrity of the exam for the institution.

- You are expected to scan your testing space using your webcam for the proctor. Proctoring also requires you to have sound and a microphone. Please plan accordingly.
- You are strongly encouraged to schedule your exam(s) within the first two weeks of the course to ensure you find a day and time that works best for your schedule. Time slots can fill up quickly, especially during high volume time periods.

    - You *must* set up your proctoring at least 72 hours prior to the exam.
- **The exam proctor will input the exam password**.
- Additional information and instructions are provided in the *Welcome and Start Here* section of the course.
- **When you are going to schedule exams, you *must* pick "Coursera" as your institution.**
- Learners with exam accommodations through SAILS (Student Accessibility and Inclusive Learning Services) should not schedule exams until they receive an invitation specifically for them from ProctorU.
- Your ID needs to be in English. See your MCS Onboarding Course for more information.

Course Grade Breakdown

Course Work	Quantity	Team or Individual	Percentage of Grade
Projects*	4	Individual	30%
Midterm Exam	1	Individual	30%
Final Exam	1	Individual	40%

*The project(s) count for 30% or more of the overall course grade, so this is a portfolio eligible course. See the MCS Graduate Handbook for more information about the portfolio requirement if you are a degree student.

Grade Scale

You must earn a cumulative grade of 70% to earn a "C" in this course. This course has no grade curving. All graded items will be included to calculate grades (i.e., no graded items will be dropped). Grades will not be rounded. Grades in this course will *not* include pluses or minuses.

**The instructor reserves the right to adjust individual grades based on, but not limited to: violations of academic integrity.*

A	90% - 100%
B	80% - 89%
C	70% - 79%
D	60% - 69%

E	<60%

Course Schedule and Important Dates

Course teams will not be working on ASU's days off* and those are listed by name in the Course Schedule. Please review the ASU Days Off for more details.

Week/Title	**Begins at 12:01 AM Arizona (AZ) Time**	**Ends at 11:59 PM Arizona (AZ) Time**
Week 1: Introduction to Cryptography	March 14, 2022	March 20, 2022
Week 2: Building Blocks: Random Numbers, Hash Functions, Encryption	March 21, 2022	March 27, 2022
Week 3: Passwords: Storage and Security	March 28, 2022	April 3, 2022
Week 4: Authentication, Key Exchange, Public Keys and Man-in-the-Middle (MITM) Attacks	April 4, 2022	April 10, 2022
Midterm Exam	April 8, 2022	April 14, 2022
Week 5: Cryptographic Protocols, Building Blocks, and Concepts	April 11, 2022	April 17, 2022
Week 6: RSA and Number Theory	April 18, 2022	April 24, 2022
Week 7: Advanced Cryptographic Protocols	April 25, 2022	May 1, 2022
Week 8: Money and Politics	May 2, 2022	May 7, 2022
Final Exam	May 3, 2022	May 8, 2022
Request for Faculty Review: MCS Project Portfolio submission (optional)	April 29, 2022	May 21, 2022

Faculty Feedback for the Review: MCS Project Portfolio submission (optional)	April 30, 2022	June 4, 2022

**Grades are due May 2 - 9, 2022 (Please see the ASU Academic Calendar for additional information.)*

Live Events

This course has two types of live events: **live sessions** and **virtual office hours**. Check the Live Events page in your course for your local time and access details. Although we try to be consistent for our learners' planning purposes, the Live Event schedule is subject to change throughout the course, so stay up-to-date on Live Event details by checking your Course Announcements and the Live Events page in your course.

Read about the specific policies related to Live Events in the Policy section of this syllabus: Live Events, Policy Regarding Expected Classroom Behavior, and the Student Code of Conduct for more detailed information.

Live Sessions - Weekly

Live Sessions are a valuable part of the learning experience because learners can meet with the course instructor and fellow classmates to learn more about course topics, special topics within the field, and discuss coursework. If you are able to attend these Live Sessions, you are strongly encouraged to do so. If you have specific questions or topics of interest to be discussed during the live events, please indicate your request in your discussion forum post. Although it may not be possible to address all requests live, the instructor is interested in tailoring the live events to your questions and interests. The instructor will be following a set agenda, so please be mindful of that when engaging in the live session.

CSE 539 Spring B 2022 Instructor Live Sessions will be held Tuesdays at 3:00 PM MST
Live Sessions hosted by the faculty will be recorded and uploaded to the course.

[Check the Live Events page in your course for the most up-to-date Live Session information.]

Virtual Office Hours - Weekly

Virtual Office Hours offer a chance for learners to get their questions answered from the course team. Although the course team is responsive to trends in the discussion forums and mcsonline@asu.edu emails, virtual office hours focus on addressing learners' specific questions related to content: clarifications, reteaching, assessment review, etc. These sessions are not intended to address program or course design questions or feedback. Assistants do not have the authority to weigh in or make decisions regarding those items, so please do not include

those at this time. These sessions are specific to helping learners learn materials and understand various course assessments. Feedback of that nature is best addressed in the communication channel: mcsonline@asu.edu and please include it in your course survey.

Virtual office hours are recorded, but not uploaded into the course.
CSE 539 Spring B 2022 Virtual Office Hours will be held Thursdays and Fridays at the times listed below. Live Sessions hosted by the faculty will be recorded and uploaded to the course.

[Check the Live Events page in your course for the most up-to-date Live Session information.]

- Tariq Nasim - Thursdays - March 17, 2022 - May 5, 2022 - 7:00 PM MST - 8:00 PM MST
- Sri Ajay Sathwik Ravilla - Fridays - March 11, 2022 - May 6, 2022 - 10:00 AM MST - 11:00 AM MST

Assignment Deadlines and Late Penalties

Unless otherwise noted, all graded work is due on **Sundays at 11:59 PM Arizona (AZ) time.** For the course projects, there is an automatic late penalty of 15% for each day after the scheduled day and time. For the midterm exam and final exam, there is an automatic late penalty of 100% after the scheduled due date and time.

Course Outline with Assignments

Week 1: Introduction to Cryptography (3/14 - 3/20)

Content

- ☐ Basic Concepts
- ☐ Encryption Basics

Other Tasks

- ☐ For learners needing accommodations, submit requests through Connect and review the ASU Student Accessibility and Inclusive Learning Services website.
- ☐ Schedule your proctoring with ProctorU for your proctored exam(s)
- ☐ Knowledge Checks
- ☐ Application Exercise

Graded Coursework

- ☐ None

Week 2: Building Blocks: Random Numbers, Hash Functions, Encryption (3/21-3/27)

Content

- ☐ Random Numbers
- ☐ Hash Functions
- ☐ Encryption Algorithms

- [ ] Birthday Attacks on Hash Functions

Other Tasks

- [ ] Schedule your proctoring with ProctorU for your proctored exam(s), if you have not already done so
- [ ] Knowledge Checks
- [ ] Application Exercise

Graded Coursework

- [ ] Steganography and Cryptanalysis Project [Due Sunday, 3/27 by 11:59 PM]

Week 3: Passwords: Storage and Security (3/28 - 4/3)

Content

- [ ] Password Insecurity
- [ ] Password Storage
- [ ] Rainbow Tables

Other Tasks

- [ ] Knowledge Checks

Graded Coursework

- [ ] Hash Project [Due Sunday, 4/3 by 11:59 PM]

Week 4: Authentication, Key Exchange, Public Keys and Man-in-the-Middle (MITM) Attacks (4/4 - 4/10)

Content

- [ ] Authentication
- [ ] Key Exchange
- [ ] Diffie-Hellman Key Exchange
- [ ] Public Keys and Applications

Other Tasks

- [ ] Knowledge Checks

Graded Coursework

- [ ] None

Week 5: Cryptographic Protocols, Building Blocks, and Concepts (4/11 - 4/17)

Content

- [ ] Cryptographic Protocols
- [ ] Secret Messaging
- [ ] Case Study: Kerberos

- [ ] Public Key Infrastructure (PKI)
- [ ] Case Study: Secure Sockets Layer (SSL, or TLS)

Other Tasks

- [ ] Knowledge Checks
- [ ] Application Exercise

Graded Coursework

- [ ] Diffie-Hellman and Encryption Project [Due Sunday, 4/17 by 11:59 PM]

Midterm Exam (4/8- 4/14)

Reminders

- [ ] Schedule your proctoring with ProctorU for your proctored exam(s), if you have not already done, *at least* 72 hours prior to your desired exam date and within the availability window
- [ ] Covers content from weeks 1-4
- [ ] Review the details and allowances information for this exam
- [ ] Prepare for the exam and complete the practice exam

Week 6: RSA and Number Theory (4/18 - 4/24)

Content

- [ ] Proof of RSA
- [ ] Primality Testing, Fast Exponentiation, and Computing Private Keys

Other Tasks

- [ ] Knowledge Checks
- [ ] Course Survey (strongly encouraged, appreciated, and used by the course team)

Graded Coursework

- [ ] None

Week 7: Advanced Cryptographic Protocols (4/25 - 5/1)

Content

- [ ] Cut and Choose
- [ ] Cryptographic Techniques

Other Tasks

- [ ] Request for Faculty Review: MCS Project Portfolio Submission *(optional - for degree students wanting to use this course's projects as part of their portfolio degree requirement/specialization requirements)*
- [ ] *Knowledge Checks*
- [ ] Complete the course survey before your final exam (*strongly encouraged, appreciated, and used by the course team)*

Graded Coursework

- [ ] RSA Project [Due Sunday, 5/1 by 11:59 PM]

Week 8: Money and Politics (5/2 - 5/7)

Content

- [ ] Politics and Cryptography
- [ ] Cryptocurrency and Digital Cash

Other Tasks

- [ ] Knowledge Checks
- [ ] Request for Faculty Review: MCS Project Portfolio Submission (optional - for degree students wanting to use this course's projects as part of their portfolio degree requirement/specialization requirements)

Graded Coursework

- [ ] None

Final Exam (5/1- 5/8)

Reminders

- [ ] Complete the course survey before your final exam (*strongly encouraged, appreciated, and used by the course team)*
- [ ] Schedule your proctoring with ProctorU for your proctored exam(s), if you have not already done, *at least* 72 hours prior to your desired exam date and within the availability window
- [ ] Schedule proctoring at least 72 hours prior to your exam date and within the availability window
- [ ] Covers content from weeks 1, 2, 3, 4, 5, 6, 7, and 8 (cumulative)
- [ ] Review the details and allowances information for this exam
- [ ] Prepare for the exam and complete the practice exam

Slack Channel

This course will have a unique Slack workspace where you can communicate with your classmates.

Note: You must join/access this workspace using your ASURITE credentials.

Slack is intended to provide a space to create community with your classmates. Please remember to follow the communication protocol pinned in your Slack channel to ensure that any questions or concerns you have are addressed in a timely manner. Also, please remember ASU's Academic Integrity policy, and please refrain from sharing assessment questions, answers or solutions.

Policies

All ASU and Coursera policies will be enforced during this course. For policy details, please consult the MCS Graduate Handbook and the MCS Onboarding Course.

Graded Quiz and Exam Policy

Each course in the MCS program is uniquely designed by expert faculty so that learners can best master the learning outcomes specific to each course. By design, course features and experiences are different across all MCS courses.

In the MCS program, we strive to provide learners with exercises and applied practice beyond quizzes and exams that align with the hands-on nature of the computer science industry. Ungraded practice opportunities *may* include, but are not limited to: in-video-questions (IVQs), knowledge check quizzes (KCs), weekly (i.e., unit) practice quizzes, practice exams, and other assignments or exercises. For all these learning activities, the questions and correct answers are provided to learners. When available, auto-generated typed feedback is built into the course to further help learners learn in real-time. Please thoroughly review your course to ensure that you are aware of the types of practice opportunities available to you.

For academic integrity purposes, once grades are made available, learners will see their overall total scores. Like other standardized tests, such as the GRE and SAT, learners will receive a singular grade for the graded quizzes and exams, but the questions, correct and incorrect answers, and feedback to each question will ***not*** be provided.

If learners desire 1:1 feedback for their questions on graded assessments, please submit questions to mcsonline@asu.edu. Rather than receiving the exact questions learners had correct and incorrect and the answers to those questions, learners will likely receive the concepts that were covered in the assessment questions so they will know what they need to review prior to other assessments and how to apply this information in their professional environments.

Absence Policies

There are no required or mandatory attendance events in this online course. Live Events, both Live Sessions hosted by the instructor and Virtual Office Hours hosted by the course team do not take attendance.

Learners are to complete all graded coursework (e.g., projects and exams). If exceptions for graded coursework deadlines need to be made for excused absences, please reach out to the course team by the end of the second week of the course using the mcsonline@asu.edu email address. Review the exam availability windows and schedule accordingly. The exam availability windows allow for your own flexibility and you are expected to plan ahead. Personal travel does not qualify as an excused absence and does not guarantee an exception.

Review the resources for what qualifies as an excused absence and review the late penalties in the Assignment Deadlines and Late Penalties section of the syllabus and the course:

a. Excused absences related to religious observances/practices that are in accord with ACD 304–04, “Accommodation for Religious Practices” (please see Religious Holidays and Observances)
b. Excused absences related to university sanctioned events/activities that are in accord with ACD 304–02, “Missed Classes Due to University-Sanctioned Activities”

c. Excused absences related to missed class due to military line-of-duty activities that are in accord with ACD 304–11, “Missed Class Due to Military Line-of-Duty Activities,” and SSM 201–18, “Accommodating Active Duty Military”

Live Event Expectations

The environment should remain professional at all times. Inappropriate content/visuals, language, tone, feedback, etc. will not be tolerated, reported and subject to disciplinary action. Review the Policy Regarding Expected Classroom Behavior section of the syllabus and the Student Code of Conduct for more detailed information.

Policy Regarding Expected Classroom Behavior

The aim of education is the intellectual, personal, social, and ethical development of the individual. The educational process is ideally conducted in an environment that encourages reasoned discourse, intellectual honesty, openness to constructive change, and respect for the rights of all individuals. Self-discipline and a respect for the rights of others in the university community are necessary for the fulfillment of such goals. An instructor may withdraw a student from a course with a mark of “W” or “E” or employ other interventions when the student’s behavior disrupts the educational process. For more information, review SSM 201–10.

If you identify something as unacceptable classroom behavior on the class platform (e.g., Coursera discussion forum) or communication channels (e.g., Zoom, virtual live session, virtual office hours, Slack, etc.), please notify the course team using the mcsonline@asu.edu email. In the discussion forums, you can also flag the post for our attention. For more specifics on appropriate participation, please review our Netiquette infographic.

Our classroom community rules are to:

- Be professional
- Be positive
- Be polite
- Be proactive

Academic Integrity

Students in this class must adhere to ASU’s academic integrity policy, which can be found at https://provost.asu.edu/academic-integrity/policy). Students are responsible for reviewing this policy and understanding each of the areas in which academic dishonesty can occur. In addition, all engineering students are expected to adhere to both the ASU Academic Integrity Honor Code and the Fulton Schools of Engineering Honor Code. All academic integrity violations will be reported to the Fulton Schools of Engineering Academic Integrity Office (AIO). The AIO maintains a record of all violations and has access to academic integrity violations committed in all other ASU colleges/schools.

Specific academic integrity announcements for this class include using another student’s code, past or present, even with a citation is a violation of the academic integrity policy.

There is a zero tolerance policy in this class: any violation of the academic integrity policy will result in a zero on the assignment and the violation will be reported to the Dean's office. Plagiarism is taken very seriously in this course.

Examples of academic integrity violations include (but are not limited to):

- Sharing code with a fellow student (even if it is only a few lines).
- Collaborating on code with a fellow student.
- Submitting another student's code as your own.
- Submitting a prior student's code as your own.

Posting your assignment code or anything related to exam content and projects online is expressly forbidden, and will be considered a violation of the academic integrity policy. Note that this includes working out of a public Github repo. The Github Student Developer Pack provides cool stuff in addition to the free unlimited private repositories that Github provides. If you want to impress employers with your coding abilities, create an open-source project that is done outside of class.

Copyright

The contents of this course, including lectures (Zoom recorded lectures included) and other instructional materials, are copyrighted materials. Students may not share outside the class, including uploading, selling or distributing course content or notes taken during the conduct of the course. Any recording of class sessions is authorized only for the use of students enrolled in this course during their enrollment in this course. Recordings and excerpts of recordings may not be distributed to others. (see ACD 304–06, "Commercial Note Taking Services" and ABOR Policy 5-308 F.14 for more information).

You must refrain from uploading to any course shell, discussion board, or website used by the course instructor or other course forum, material that is not the student's/learner's original work, unless the student/learner first complies with all applicable copyright laws; faculty members reserve the right to delete materials on the grounds of suspected copyright infringement.

Policy Against Threatening Behavior, per the Student Services Manual, (SSM 104-02)

Students, faculty, staff, and other individuals do not have an unqualified right of access to university grounds, property, or services (see SSM 104-02). Interfering with the peaceful conduct of university-related business or activities or remaining on campus grounds after a request to leave may be considered a crime. All incidents and allegations of violent or threatening conduct by an ASU student (whether on- or off-campus) must be reported to the ASU Police Department (ASU PD) and the Office of the Dean of Students.

Disability Accommodations

Suitable accommodations will be made for students having disabilities. Students needing accommodations must register with ASU Student Accessibility and Inclusive Learning Services.

Students should communicate the need for an accommodation at the beginning of each course so there is sufficient time for it to be properly arranged. These requests should be submitted through the online portal. See ACD 304-08 Classroom and Testing Accommodations for Students with Disabilities. ASU Student Accessibility and Inclusive Learning Services will send the instructor of record a notification of approved accommodations and students are copied on these letters. It is recommended that students reply to the faculty notification letters, introduce themselves to their instructor, and share anything they might want to disclose.

Harassment and Sexual Discrimination

Arizona State University is committed to providing an environment free of discrimination, harassment, or retaliation for the entire university community, including all students, faculty members, staff employees, and guests. ASU expressly prohibits discrimination, harassment, and retaliation by employees, students, contractors, or agents of the university based on any protected status: race, color, religion, sex, national origin, age, disability, veteran status, sexual orientation, gender identity, and genetic information.

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at https://sexualviolenceprevention.asu.edu/faqs.

Mandated sexual harassment reporter: As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, https://eoss.asu.edu/counseling, is available if you wish to discuss any concerns confidentially and privately.

Disclaimer

The information in this syllabus may be subject to change without advance notice. Stay informed by checking course announcements and the syllabus section of your course.

Course Creator(s)

Partha Dasgupta, PhD designed this course.

Dr. Partha Dasgupta is an Associate Professor in the School of Computing, Informatics, and Decision Systems Engineering at Arizona State University (ASU). His core areas of expertise are in Computer Security, Cryptography and Operating Systems. His current research focus is the use of cryptography and secure software systems to provide security and dependability of consumer computing. He has significant prior research results and publications in construction of distributed operating systems, high performance systems and secure computing infrastructures. In addition to ASU, Dr. Dasgupta has held faculty positions at Georgia Tech and New York University.