

MAS 6217: NUMBER THEORY AND CRYPTOGRAPHY

Department of Mathematical Sciences
Fall 2023
Credit Hours: 3

CRN: 14850
Prerequisites: Enrolled in M.S.T. program or permission of instructor.

CONTACT INFORMATION

Instructor: Dr. Zvi Rosen
Office Location: Room 224, Building SE-43, Boca Raton Campus
Office Hours: Tuesday 3 – 4 PM or by appointment
Email: rosenz@fau.edu
Video Conferencing Tool: Zoom
Zoom: <https://fau-edu.zoom.us/my/rosenz?pwd=eStHMVg2d0RHbmpuZGx5cUpaU2FwZz09>

COURSE DESCRIPTION

This course provides mathematical background in number theory and cryptography for high school teachers. Topics include congruences and modular arithmetic, finite fields, public-key cryptography (RSA), primality testing and factoring. This course is not intended for Ph.D. students in mathematics.

COURSE OBJECTIVES

Upon successful completion of this course, students will be able to:

1. Explain mathematical concepts related to number theory and cryptography, using a spreadsheet. (CO: 1)
2. Apply number theory and cryptography concepts to teaching in the K-12 setting. (CO: 2)
3. Solve mathematical equations related to number theory and cryptography. (CO: 3)

COURSE DELIVERY MODE

This is a fully online course accessible only through FAU's learning management system, Canvas. You must log into Canvas with your FAU ID and Password to access the materials and assignments in this course. If you do not know your FAU ID or Password, [contact OIT for help](#).

The course is organized into seven modules with due dates. Unless otherwise specified, each module begins on Monday at 12:00am, EST, and ends on Sunday at 11:59pm, EST. The course begins with the Start Here module, which will familiarize you with the organization and navigation of the course. You will open a new learning module to access the relevant materials for each subsequent module.

TIME COMMITMENT PER CREDIT HOUR

This course has 3 credit hours. For traditionally delivered courses, not less than one (1) hour of classroom or direct faculty instruction each week for fifteen (15) weeks per Fall or Spring semester, and a minimum of two (2) hours of out-of-class student work for each credit hour.

Equivalent time and effort are required for Summer Semesters, which usually have a shortened timeframe. Fully Online courses, hybrid, shortened, intensive format courses, and other non-traditional modes of delivery will demonstrate equivalent time and effort.

REQUIRED TEXT

No texts or materials are required. All materials will be provided in the course.

COURSE ASSESSMENTS, ASSIGNMENTS & GRADING POLICY

GRADING CRITERIA

INTRODUCTIONS AND SYLLABUS QUIZ (0%)

You will introduce yourself in the discussion board, respond to other students' introductions, and take a syllabus quiz. You may take the syllabus quiz as many times as necessary to achieve 100%.

HOMEWORK (30%)

For each module of the course, you will be asked to complete and show your work for posted homework assignment in Canvas. (You will be asked to scan and upload your solutions into Canvas as a PDF-file. Please be sure you have an app or access to a scanner for your homework; you will only be allowed to submit your solutions as PDF-files.) Homework will be graded on a complete/incomplete basis. You can ask the instructor for hints as well as discuss challenges with other students through the Discussions tab in Canvas.

PROJECTS (30%)

For each module of the course, you will be asked to implement, in a computer spreadsheet, a concept from that module, as a project. (You will be asked to upload the spreadsheet into Canvas as an XLS-file.) You can ask the instructor for hints as well as discuss challenges with other students through the Discussions tab in Canvas.

DISCUSSION BOARDS (30%)

In this course, you will write a reflective post based on the lectures, homework assignment, and assigned project from each module of the course, in a discussion board associated to that module. Your post will include a short description of the main concepts and how you might use these concepts in the classroom. You will also be responsible to post at least two substantive replies to the posts made by your peers.

FINAL REFLECTION (10%)

For the final reflection, you will be asked to comment on how you can apply the information learned in this course to your teaching or to your discipline. This reflection should be sufficiently detailed to explain what you learned in the course and provide a practical application to your teaching (or discipline). You may be asked to share your experience throughout the course on how this course has affected your teaching and learning overall.

| Assessment | Percentage (%) |
|-------------------------------------|----------------|
| Introductions and Syllabus Quiz (1) | 0% |
| Homework (7) | 30% |
| Projects (7) | 30% |
| Discussion Boards (7) | 30% |
| Final Reflection (1) | 10% |
| TOTAL: | 100% |

GRADE SCALE

| | | | | | |
|-----------------------|------------|------------|------------|------------|------------|
| Grade | A | A- | B+ | B | B- |
| Percentage (%) | 90 – 100% | 87 – 89.9% | 84 – 86.9% | 80 – 83.9% | 77 – 79.9% |
| Grade | C+ | C | D | F | |
| Percentage (%) | 70 – 76.9% | 60 – 69.9% | 50 – 59.9% | 0 – 49.9% | |

LATE ASSIGNMENTS POLICY

If you expect to be late on an assignment for an excusable reason, please notify the instructor well in advance, and he may afford an opportunity for partial credit. Please note that students will not be penalized for absences due to illness or participation in University-approved activities, including athletic or scholastic teams, musical and theatrical performances, and debate activities. The instructor will allow these students to make up missed work without any reduction in the student's final course grade. Reasonable accommodation will also be made for students participating in a religious observance.

INCOMPLETE GRADE POLICY

The University policy states that a student who is passing a course but has not completed all work due to exceptional circumstances, may, with consent of the instructor, temporarily receive a grade of incomplete ("I"). The assignment of the "I" grade is at the discretion of the instructor but is allowed only if the student is passing the course.

MINIMUM TECHNOLOGY & COMPUTER REQUIREMENTS

HARDWARE & SOFTWARE REQUIREMENTS

Hardware

- Dependable computer
- Computer speakers
- Headset with microphone
- Webcam

Software

- [Microsoft 365 Suite](#)
- Reliable web browser (recommended [Chrome](#) or [Firefox](#))
- Canvas mobile app: Download instructions for [iOS device](#) or [Android device](#)
- [Adobe Reader](#)
- [Adobe Flash Player](#)
- Scanning device (app or software)

Internet Connection

- Recommended: Broadband Internet connection with a speed of 4 Mbps or higher.
- To function properly, Canvas requires a high-speed Internet connection (cable modem, DSL, satellite broadband, T1, etc.). The minimum Internet connection speed to access Canvas is a consistent 1.5 Mbps (megabits per second) or higher.
- [Check your Internet speed here.](#)

Computer Requirements

Basic Computer Specifications for Canvas

- Operating system: Windows 10 or macOS Sierra (or higher).

- [Specifications](#)

Peripherals

- A backup option should be available to minimize the loss of work. This can be an external hard drive, a USB drive, cloud storage, or your folder on the FAU servers.

Software

- Once logged in to Canvas make sure your Internet browser is compatible.
- Other software may be required for specific learning modules. If so, the necessary links to download and install will be provided within the applicable module.
- Presentation Software (i.e. PowerPoint)
- Recording tool to present content
- App or software that will scan or convert images or physical documents to PDF

Minimum Technical Skills Requirements

The general and course-specific technical skills you must have to succeed in the course include but are not limited to:

- Accessing Internet.
- Scanning a physical paper to PDF
- Convert image to PDF
- Using Canvas (including taking tests, attaching documents, etc.).
- Using email with attachments.
- Creating and submitting files in commonly used word processing program formats such as Microsoft Office Tools.
- Copying and pasting functions.
- Downloading and installing software.
- Using presentation, graphics, and other programs.
- Posting and commenting in an online discussion.
- Searching the FAU library and websites.

Technical Support

In the online environment, technical issues are always possible (e.g., lost connection, hardware or software failure). Many of these can be resolved relatively quickly, but if you wait until the last minute before due dates, the chances of these glitches affecting your success are greatly increased. Please plan appropriately. If a problem occurs, it is essential you take immediate action to document the issue so your instructor can verify and take appropriate action to resolve the problem. Most issues in Canvas can be resolved by clicking on the “Help” tab located on the menu bar.

When a problem occurs, click “Help” to:

- Report a Problem
- Live Chat with Canvas Support
- Search Canvas Guides

Additional Technical Support

1. Contact the eLearning Success Advisor for assistance: (561) 297-3590
2. If you can, make a Print Screen of the monitor when the problem occurs. Save the Print Screen as a .jpg file. If you are unfamiliar with creating a Print Screen file, see [Print Screen instructions.](#)
3. Complete a [Help Desk ticket](#). Make sure you complete the form entirely and give a full description of your problem so the Help Desk staff will have the pertinent information to assist you properly. This includes:
 - a. Select “Canvas (Student)” for the Ticket Type.
 - b. Input the Course ID.
 - c. In the Summary/Additional Details section, include your operating system, Internet browser, and Internet service provider (ISP).
 - d. Attach the Print Screen file, if available.
4. Send a message within Canvas to your instructor to notify him of the problem. Include all pertinent information of the incident (2b-d above).
5. If you do not have access to Canvas, send an email to your instructor with all pertinent information of the incident (2b-d above).
6. If you do not have access to a computer, call your instructor with all pertinent information of the incident. If he is not available, make sure you leave a detailed message.
7. If you do not hear back from the Help Desk or your instructor within a timely manner (48 hours), it is your responsibility to follow up with the appropriate person until you obtain a resolution.

CHAT-GPT AND ARTIFICIAL INTELLIGENCE

With the advent of AI tools like ChatGPT and Bard, students may be wondering what they can and can't do. In this class, students should not feel like they are tying their hands behind their backs to not use online tools. Instead, our two guiding principles will be:

1. **human-mediated work**, and
2. **transparency**.

Make sure that you fully digest and fact-check any AI-produced text, and that you report all prompts you used to produce your text. The following example would be accepted in homework:

Q. Decrypt the text “KGT CZDPY” which was encrypted with a shift cipher of shift 11.

A. I input the question verbatim into ChatGPT (GPT 3.5) and I received the following response:

To decrypt the text "kgt czdpy" encrypted with a shift of 11, we need to shift each letter 11 positions backward in the alphabet. Let's decrypt the message:
Original: k g t c z d p y
Shifted: t p i r o w e n
So, the decrypted text is "tpi rowen".

This message didn't look right, so I double-checked the math, and the shifts in positions 1, 2, and 6 were off; instead, they should be Z, V and S. So the encrypted text is "ZVI ROSEN".

COURSE POLICIES

CODE OF ACADEMIC INTEGRITY POLICY STATEMENT

Students at Florida Atlantic University should endeavor to maintain the highest ethical standards. Academic dishonesty is a serious breach of these ethical standards because it interferes with the University mission to provide a high-quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive to the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see [University Regulation 4.001](#).

PLAGIARISM

[Plagiarism](#) is unacceptable in the University community. Academic work must be an original work of your own thought, research, or self-expression. When students borrow ideas, wording, or organization from another source, they must acknowledge that fact in an appropriate manner. Plagiarism is the deliberate use and appropriation of another's work without identifying the source and trying to pass off such work as one's own. Any student who fails to give full credit for ideas or materials taken from another has plagiarized. This includes all discussion board posts, journal entries, wikis, and other written and oral presentation assignments. If in doubt, cite your source.

ONLINE ATTENDANCE POLICY

Since the course is **online live-lecture**, you are expected to attend the Zoom lectures on Monday and Wednesday. Furthermore, you should access the course website at least **three times a week** to ensure you do not miss pertinent postings, messages, or announcements. It is imperative that you meet course deadlines and stay active in discussion boards, group projects,

etc. If you are experiencing major illness, absences due to University duties, or other large-scale issues, contact the instructor immediately to formulate a resolution.

CLASSROOM ETIQUETTE/DISRUPTIVE BEHAVIOR POLICY STATEMENT

Disruptive behavior is defined in the FAU Student Code of Conduct as "... activities which interfere with the educational mission within classroom." Students who disrupt the educational experiences of other students and/or the instructor's course objectives in a face-to-face or online course are subject to disciplinary action. Such behavior impedes students' ability to learn or an instructor's ability to teach. Disruptive behavior may include but is not limited to non-approved use of electronic devices (including cellular telephones); cursing or shouting at others in such a way as to be disruptive; or, other violations of an instructor's expectations for classroom conduct.

For more information, please see the [FAU Office of Student Conduct](#).

COMMUNICATION POLICY

EXPECTATIONS FOR STUDENTS

Announcements

You are responsible for reading all announcements posted by the instructor. Check the course announcements each time you log in.

Email/Video Conferencing

You are responsible for reading all your course email and responding in a timely manner.

Course-Related Questions

Post course-related questions to the FAQ discussion board. This allows other participants with the same question to benefit from the responses. Also, make sure you review this forum prior to posting a question. Someone may have already asked and answered the question in previous posts.

INSTRUCTOR'S PLAN FOR CLASSROOM RESPONSE TIME & FEEDBACK

Email/Video Conferencing Policy

Except for weekends and holidays, the instructor will typically respond to email (Canvas inbox

or FAU email) within 48 hours. You should ask course-related questions in the FAQ discussion board. If you have questions of a personal nature, you should email the instructor.

Assignment Feedback Policy

The instructor will provide feedback on submitted assignments within one week of the submission date. Some assignments may require a longer review period, which the instructor will communicate to you.

Course-Related Questions Policy

Except weekends and holidays, the instructor will generally answer questions within 48 hours.

Electronic Communication Policy

In addition to the University's policy, please consider the following:

- Privacy, confidentiality, and security in all electronic communications.
- All electronic communication resources must be used for the course and in alignment with the University mission.
- Prohibited use of false identity, false identity pseudonyms, or anonymous (sender's name or electronic identification is hidden).
- Access without consent.
- Disruption of services including introducing computer contaminants (viruses).
- Harassment of any kind.

Please see the Office of Information Technology's policies on [Cyber Security Awareness](#).

SUPPORT SERVICES & ONLINE RESOURCES

- [Center for eLearning and Student Success](#)
- [Counseling and Psychological Service \(CAPS\)](#)
- [FAU Libraries](#)
- [Freshmen Academic Advising Services](#)
- [Math Learning Center](#)
- [Office of Information Technology Helpdesk](#)
- [Office of International Programs and Study Abroad](#)
- [Office of Undergraduate Research and Inquiry](#)
- [Student Accessibility Services](#)
- [University Center for Excellence in Writing](#)

CAPS STATEMENT

Life as a university student can be challenging mentally, emotionally, and physically. Students who find stress negatively affecting their ability to achieve academic or personal goals may wish to consider utilizing FAU's Counseling and Psychological Services (CAPS) Center. CAPS provides FAU students a range of services to help improve and maintain well-being. For CAPS services, students need to be currently enrolled, have paid the health fee, be physically located in Florida when services are provided, have phone or videoconferencing capabilities, and have access to a safe/private location for sessions. For those outside of Florida, CAPS will assist students in getting connected to services/providers in your area for ongoing support. For more information, go to <http://www.fau.edu/counseling/> or call 561-297-3540.

FACULTY RIGHTS & RESPONSIBILITIES

Florida Atlantic University respects the rights of instructors to teach and students to learn. Maintenance of these rights requires classroom conditions that do not impede their exercise.

To ensure these rights, faculty members have the prerogative to:

- Establish and implement academic standards.
- Establish and enforce reasonable behavior standards in each class.
- Recommend disciplinary action for students whose behavior may be judged as disruptive under the *Student Code of Conduct*.

SELECTED UNIVERSITY & COLLEGE POLICIES

ACCESSIBILITY POLICY STATEMENT

In compliance with the Americans with Disabilities Act (ADA), students who require special accommodations to properly execute coursework due to a disability, must register with Student Accessibility Services (SAS) located in the Boca Raton, Davie, and Jupiter campuses and follow all SAS procedures. For additional information, please consult [Student Accessibility Services](#).

Contact

- **Boca Raton:** (561) 297-3880
Fax: (561) 297-2184, TTY: 711
- **Davie:** (954) 236-1222
Fax: (954) 236-1123, TTY: 711
- **Jupiter:** (561) 799-8721
Fax: (561) 799-8721, TTY: 711

GRADE APPEAL PROCESS

You may request a review of the final course grade when you believe that one of the following conditions apply:

- There was a computational or recording error in the grading.
- The grading process used non-academic criteria.
- There was a gross violation of the instructor's own grading system.

[Chapter 4 of the University Regulations](#) contains information on the grade appeals process.

RELIGIOUS ACCOMMODATION POLICY STATEMENT

In accordance with rules of the Florida Board of Education and Florida law, students have the right to reasonable accommodations from the University in order to observe religious practices and beliefs regarding admissions, registration, class attendance, and the scheduling of examinations and work assignments. For further information, please see [Academic Policies and Regulations](#).

UNIVERSITY APPROVED ABSENCE POLICY STATEMENT

In accordance with rules of the Florida Atlantic University, students have the right to reasonable accommodations to participate in University approved activities, including athletic or scholastics teams, musical and theatrical performances and debate activities. It is your responsibility to notify the instructor at least one week prior to missing any course assignment.

DROPS/WITHDRAWALS

You are responsible for completing the process of dropping or withdrawing from a course. Please click on the following link for more information on dropping and/or withdrawing from a course. Please consult the [FAU Registrar Office](#) for more information.

* * *

The instructor reserves the right to adjust this syllabus as necessary.