Title of Course: MATH:7030:0001 – Topics in Algebra
Course meeting time and place: 11:00-12:15 TuTh 214 MLH
Department of Mathematics: https://math.uiowa.edu

Course ICON site: To access the course site, log into Iowa Courses Online (ICON)
https://icon.uiowa.edu/index.shtml using your Hawk ID and password.

Course Home
The College of Liberal Arts and Sciences (CLAS) is the home of this course, and CLAS
governs the policies and procedures for its courses. Graduate students, however, must
adhere to the academic deadlines set by the Graduate College.

Instructor
Office location: 225J MLH
Student drop-in hours: 1:45-2:15PM TuTh in person and 7:00-8:00PM TuWe on Zoom,
or by appointment. Please send me an email if you cannot make it to my office hours.
Phone: 319-335-1514
E-mail: frauke-bleher@uiowa.edu
DEO: Prof. Ryan Kinser, 14A/25F MLH, ryan-kinser@uiowa.edu

Description of Course
We will discuss topics in cryptography, from a mathematician’s point of view.

Learning Objectives
The first goal is to give a brief introduction to cryptography, with an emphasis on public
key cryptosystems. This will include the discussion of several public key cryptosystems,
in addition to a brief discussion of information theory. The second goal is to focus on
lattice based cryptography, since this type of cryptography is believed to work in a post-
quantum world. Particular topics to be discussed are the LLL algorithm by Lenstra,
Lenstra and Lovasz, and Learning with Errors (LWE) introduced by Regev.

Textbook/Materials
No textbook is required. Selected materials from the books and articles below will be
used in this course. You can access these on ICON by clicking on “Course Materials+”

- J. Hoffstein, J. Pipher and J.H. Silverman: An introduction to mathematical
cryptography
- J. Silverman: The arithmetic of elliptic curves
- D.J. Bernstein, J. Buchmann and E. Dahmen (eds): Post-quantum cryptography
- O. Regev: On lattices, learning with errors, random linear codes, and
**Academic Honesty and Misconduct**
All students in CLAS courses are expected to abide by the [CLAS Code of Academic Honesty](#). Undergraduate academic misconduct must be reported by instructors to CLAS according to [these procedures](#). Graduate academic misconduct must be reported to the Graduate College according to Section F of the [Graduate College Manual](#).

**Student Complaints**
Students with a complaint about a grade or a related matter should first discuss the situation with the instructor and/or the course supervisor (if applicable), and finally with the Director or Chair of the school, department, or program offering the course.

Undergraduate students should contact [CLAS Undergraduate Programs](#) for support when the matter is not resolved at the previous level. Graduate students should contact the [CLAS Associate Dean for Graduate Education and Outreach and Engagement](#) when additional support is needed.

**Drop Deadline for this Course**
You may drop an individual course before the deadline; after this deadline you will need collegiate approval. You can look up the [drop deadline for this course](#) here. When you drop a course, a “W” will appear on your transcript. The mark of “W” is a neutral mark that does not affect your GPA. Directions for adding or dropping a course and other registration changes can be found on the [Registrar’s website](#). Undergraduate students can find policies on dropping and withdrawing [here](#). Graduate students should adhere to the [academic deadlines](#) and policies set by the Graduate College.

**Grading System and the Use of +/-**
The possible grades for this course are Satisfactory (S) or Unsatisfactory (U) for all students.

**Course Grades**
Every student who takes part in the following activities will receive a grade of Satisfactory:

- **Class participation:** You can choose whether you attend the lecture in person or on Zoom. Class participation can take many forms. The minimal expectation is that you speak up if you have a question. You can also send me an email after class if you have a question about the course material.

- **Suggested problems:** From time to time I will post problems on ICON under Assignments. The minimal expectation is that you read these problems and let me know if you have any questions. If you want to submit solutions to these problems, please do so on ICON by uploading a separate pdf file for each suggested problem. This is strictly voluntary. Please alert me by email if you submit a problem so I can give you feedback.
**Date and Time of the Final Exam**
There will be no final exam in this course.

Here is the general policy on final exams: The final examination date and time will be announced by the Registrar generally by the fifth week of classes and it will be announced on the course ICON site once it is known. Do not plan your end of the semester travel plans until the final exam schedule is made public. It is your responsibility to know the date, time, and place of the final exam. According to Registrar’s final exam policy, students have a maximum of two weeks after the announced final exam schedule to request a change if an exam conflict exists or if a student has more than two exams in one day (see the policy here).

**Calendar of Course Assignments and Exams**
There will be no mandatory course assignments and there will be no exams in this course. I will announce in class when I have put suggested problems into Assignments in ICON. A precise calendar of weekly lecture topics with links to assignments will be posted on ICON in a Module called Calendar.

**Attendance and Absences**
You can choose to attend lectures in person or on Zoom. The lectures will be recorded on Zoom and lecture notes will be posted on ICON. I expect you to stay home when you are sick and to send me an email when you cannot make it to class in either modality (in person or on Zoom). For the current isolation guidelines of the CDC concerning COVID-19, please see [Isolation and Precautions for People with COVID-19](#). Please also take care of yourself when you have any other illness, respiratory or otherwise.

Here is the general UI policy on absences: University regulations require that students be allowed to make up examinations that have been missed due to illness, religious holy days, military service obligations (including service-related medical appointments), or other unavoidable circumstances or University-sponsored activities. Students with UI-authorized activities must discuss their absences with the instructor as soon as possible. Religious obligations must be communicated within the first three weeks of classes.

**Communication: UI Email**
Students are responsible for all official correspondences sent to their UI email address (uiowa.edu) and must use this address for any communication with instructors or staff in the UI community. For the privacy and the protection of student records, UI faculty and staff can only correspond with UI email addresses.

**Where to Get Academic Support for This Course**
You are welcome to come to my office hours if you have questions. If you want to talk but cannot make it to my office hours, please send me an email to make another appointment.
Mental Health Resources and Student Support
Students are encouraged to be mindful of their mental health and seek help as a preventive measure or if feeling overwhelmed and/or struggling to meet course expectations. Students are encouraged to talk to their instructor for assistance with specific class-related concerns. For additional support and counseling, students are encouraged to contact University Counseling Service (UCS). Information about UCS, including resources and how to schedule an appointment, can be found at counseling.uiowa.edu. Find out more about UI mental health services at mentalhealth.uiowa.edu.

Student Care and Assistance provides assistance to University of Iowa students who are experiencing a variety of crisis and emergency situations, including but not limited to medical issues, family emergencies, unexpected challenges, and sourcing basic needs such as food and shelter. More information on the resources related to basic needs can be found at basicneeds.uiowa.edu/resources/. Students are encouraged to contact Student Care & Assistance in the Office of the Dean of Students (Room 135 IMU, dos-assistance@uiowa.edu, or 319-335-1162) for support and assistance with resources.

University Policies
The following links explain a series of important university policies.

Accommodations for Students with Disabilities
Classroom Expectations
Free Speech and Expression
Non-discrimination
Absences for Religious Holy Days
Sexual Harassment/Misconduct and Supportive Measures
Sharing of Class Recordings