Math 473/673: Cryptology
Course Information Sheet and Syllabus[1]
Spring 2016

Instructor:

Dr. Susan Cooper

Office: Minard Hall, Room 408E38 *Email:* susan.marie.cooper@ndsu.edu *Phone:* 701-231-8174
Office Hours: Mondays & Wednesdays & Fridays 10:00 a.m. – 10:50 a.m.; or by appointment
Correspondence: The most reliable way to contact me is via email.

Class Times and Location: MWF 9:00 a.m. – 9:50 a.m., Minard Hall – Room 210

Prerequisites: Math 420 or Math 472

Credit Hours: 3

Course Web-Page: We will use *Blackboard* which can be found at https://bb.ndsu.nodak.edu/.

Textbook: *An Introduction to Mathematical Cryptography* by J. Hoffstein, J. Pipher, and J. H. Silverman (2nd Edition); errata: http://www.math.brown.edu/~jhs/MathCryptoHome.html.

Bulletin Description: Cryptography and cryptanalysis of ciphers. Discrete logarithms, Diffie–Hellman key exchange, the RSA cryptosystem, elliptic curve cryptography, and selected topics.

Course Introduction and Objectives: The science of cryptography deals with sending and receiving coded messages. Governments, financial institutions, and businesses need to frequently transfer sensitive information from one user or from one computer to another in such a way that even if a message is intercepted by the wrong party, it cannot be read. The general public also needs secure methods of transmitting information, so that, for example, a credit card purchase made over the Internet does not allow one's name and credit card number to fall into the hands of an unscrupulous thief. The United States government has a very strong interest in cryptography, both for devising break-proof codes and for cracking the codes of others. In fact, the National Security Agency is the largest employer of Ph.D. mathematicians in the world.

Math 473/673 is a one-semester course that investigates the mathematics underlying public key cryptography. Areas of mathematics that will be used will include number theory, abstract algebra, probability, and information theory. Depending on student backgrounds, we will aim to study the following topics:

- *Basic Introduction:* Simple substitution ciphers, cryptography before the computer age, symmetric and asymmetric ciphers.
- *Preliminary Topics:* Modular arithmetic, greatest common divisors, prime numbers, and primitive roots in finite fields.
- *Discrete Logarithms & Diffie–Hellman Key Exchange:* The discrete logarithm problem, Diffie–Hellman key exchange, Elgamal public key cryptosystem, algorithms for the logarithm problem.
- *Integer Factorization & RSA:* Euler's Formula, RSA public key cryptosystem, primality testing, factoring algorithms. Optional topics include: index calculus, quadratic residues, probabilistic encryption.
- *Digital Signatures:* RSA digital signatures, Elgamal digital signatures and DSA.
- *Elliptic Curves & Cryptography:* Elliptic curves and finite fields, the elliptic curve discrete logarithm problem, elliptic curve cryptosystems.
- *Information Theory:* Combinatorics, probability, collision algorithms, Shannon's information theory, complexity theory.

[1] *The details stated in this course syllabus are subject to change at the discretion of the instructor. Announcements concerning all (if any) changes will be made in a timely fashion.*

Problem Sets: Mathematics is not a spectator sport. The best way to learn mathematics is by doing mathematics. Homework will be assigned on a weekly basis. For most Problem Sets, exercises will be assigned on Wednesdays and solutions will be due by the *beginning* of class the following Wednesday. A subset of the solutions will be graded based on correctness, clarity, and style/creativity. The Problem Sets are intended to gauge your understanding of the material and all feedback is meant to improve your mathematical abilities and communication. Please see the handout "Guidelines for Problem Sets" for expectations.

Course Project: All students will complete a course project; for undergraduate students the project will be completed in groups. The project will consist of both a written paper and class presentation. All participants in a group will receive the same grade, so it is important that each person in the group participate fully and equally in the project tasks. Important dates to keep in mind for the project are:

Task	Due Date
Project Proposals (Members and Topics)	February 26
Project Approvals (Members, Topics, and Presentation Schedule)	February 29
Papers	April 18
Graduate Presentations	April 29
Undergraduate Presentations	May 2, May 4, and May 6

Full details for the project assignment requirements and topics will be given later in the semester.

Exams: There will be two midterm examinations and one cumulative final examination. Examinations may involve a take-home portion – details will be announced at least one week before the in-class portion. In-class examination dates and times are:

Exam	Date	Time and Location
Exam 1	Wednesday, February 17	9:00 a.m. – 9:50 a.m., Minard Hall – Room 210
Exam 2	Wednesday, April 6	9:00 a.m. – 9:50 a.m., Minard Hall – Room 210
Final Exam	Wednesday, May 11	1:00 p.m. – 3:00 p.m., Minard Hall – Room 210

A crucial step in being successful in mathematics is developing the ability to remember definitions and statements of key theorems. As such, books and notes will not be allowed during the in-class portions of examinations.

Graduate Credit: Students who will take the course for graduate credit will be required to complete additional homework and exam problems. In addition, graduate students will work alone on the course project. In all work submitted, a higher level of rigor and clarity is expected from graduate students.

Missed/Late Work Policies: Late submissions of Problem Sets, take-home exams, and make-up exams will only be granted for unavoidable, documented circumstances as described below:

Circumstance	Required Documentation
illness or other medical situation	official note from clinic, hospital, doctor, nurse, or other health care provider
military service	official military activation orders
funeral or other family emergency	official documentation from newspaper, funeral, or medical official
sports or other official NDSU activity	official documentation from NDSU athletics or activity's faculty adviser

Please note that recreational activities do not qualify for make-ups or late submissions. If you have a pre-existing conflict with an exam, homework deadline or class meeting, you are expected to make alternative arrangements *beforehand*. No extensions will be granted for the course project papers and presentations will only be rescheduled for unavoidable, documented circumstances.

Course Grades: Final course grades will be determined as follows:

Task	Percentage of Grade
Problem Sets	20%
Course Project	15%
Midterm Examinations	20% each
Final Examination	25%

Percentage Grade	Grade Earned
90% – 100%	A
80% – 89%	B
70% – 79%	C
60% – 69%	D
0% – 59%	F

Attendance and Participation: Your understanding of the course material will be greatly supported by regular attendance and engagement in class meetings. Indeed, a given topic will depend heavily on previously explored topics and so missing one class can make a huge difference in your understanding the material. According to NDSU Policy 333: Class Attendance Policy and Procedure (see `www.ndsu.edu/fileadmin/policy/333.pdf`), attendance in classes is expected. Although you are expected to attend every class meeting, attendance will only be taken on the first two meetings of the class. You are responsible for any missed material when absent. Veterans and student service members with special circumstances or who are activated are encouraged to notify the instructor as soon as possible and are encouraged to provide Activation Orders.

Tentative Course Schedule and Calendar of Events:

Dates(s)	Topic/Event	Project Deadline/Exam
January 13–January 20	Introduction	
January 18	Martin Luther King Day (no class)	
January 22–February 3	Preliminary Topics	
February 5–February 22	Discrete Logarithms and Diffie–Hellman	
February 15	Presidents' Day (no class)	
February 17		Exam 1 (in-class portion)
February 24–March 11	Integer Factorization and RSA	
February 26		Project Proposals Due
February 29		Project Approvals
March 14–March 18	Spring Break Week (no classes)	
March 21–April 1	Digital Signatures	
March 25–28	Spring Recess (no classes)	
April 4–April 25	Elliptic Curves and Cryptography	
April 6		Exam 2 (in-class portion)
April 18		Course Papers Due
April 29		Graduate Presentations
May 2–6		Undergraduate Presentations
May 11, 1:00–3:00 p.m.		Final Examination

Other Resources: Please note the following:

- *Computer Program:* Much of the work you will do in this course will be simplified with the use of a computer algebra system. For example, you will need to find large prime numbers as well as prime factorizations for large composite numbers. In practice, such tasks can be completed with the use of a regular calculator but doing so can be very tedious. It is recommended that you use the system Maxima which can be downloaded at `http://maxima.sourceforge.net/`. Prior knowledge of such a system is not required; I will provide necessary instructions for Maxima as needed throughout the semester.
- *Notes:* It is your responsibility to prepare clear and thorough notes – these will provide you with clarifying examples and reasoning behind the theory seen in class.
- *Email Announcements:* Periodically, course announcements will be sent to you via Blackboard. It is your responsibility to check your NDSU email account regularly.

Special Concerns: Any students with disabilities or other special needs, who need special accommodations in this course, are invited to share these concerns or requests with the instructor and contact the Disability Services Office (231-8463; `http://www.ndsu.edu/disabilityservices/`) as soon as possible.

Academic Honesty: The academic community is operated on the basis of honesty, integrity, and fair play. NDSU Policy 335: Code of Academic Responsibility and Conduct applies to cases in which cheating, plagiarism, or other academic misconduct have occurred in an instructional context. Students found guilty of academic misconduct are subject to penalties, up to and possibly including suspension and/or expulsion. Student academic misconduct records are maintained by the Office of Registration and Records (`https://www.ndsu.edu/registrar/`). Informational resources about academic honesty for students and instructional staff members can be found at `www.ndsu.edu/academichonesty`.

Any student found guilty of academic dishonesty will receive a grade of 0 for the task in question. In addition, every such student will be reported to the Chair of Mathematics, the Dean of their major college, the Dean of the College of Science and Mathematics, the Provost, and the Registrar. The Registrar will add any such student to NDSU's Student Academic Misconduct Database. (Multiple entries in this database may result in additional sanctions from NDSU.) Students found guilty of a second offense of academic dishonesty in this course will receive a course grade of F.

Classroom Atmosphere and Courtesy: A part of learning is making mistakes. We want to establish a classroom atmosphere where the inevitable false starts and mistakes become an opportunity to improve – not an opportunity for embarrassment. Please be constructive and polite in questioning your colleagues in class. In addition, cellular telephones, pagers, and other similar devices are not to be used and are to be turned off or set to vibrate-mode during class-time.

Expectations and Tips for Success: I ask that you have a well-defined sense of professionalism, that you always put forth your best effort, and that you develop a sense of responsibility to your educational community. I ask that you exhibit a persistent desire to learn. In return I will provide you with significant support. Also:

- Be positive, open, and responsive to feedback.
- Be an active participant - mathematics is learned by doing; this includes participating fully in classroom activities, completing the Problem Sets, critically thinking about the mathematics during and outside of class. *In order for this class to be successful, it is imperative that you commit to coming to class regularly, that you commit to coming to class prepared, and that you commit to participating in class!*
- Be/become a "risk taker".
- Be committed, take pride in your work, and take your work seriously.
- Be patient with yourself - it takes time to master newly learned things. Ask for assistance when it is needed. Constantly try to improve yourself as a mathematician.
- Starting with the first class, study in-depth and regularly.
- It is tempting to just copy available solutions. However, struggling through the exercises on your own is an important phase of the learning process.
- Get help as soon as you need it: ask questions in class and office hours; form a study group with your classmates; consider getting a tutor, etc.
- Everyone wants you to succeed. Please speak with me regarding any concerns you may have.
- Relax and have fun with the course!