Math 316-01, Applied Math and Modeling II, Spring 2017

MWF 9:35-10:40 pm, BEC LL03

Instructor: Amy DeCelles

Email: adecelles@stthomas.edu
Webpage: http://personal.stthomas.edu/dece4515/
Office: OSS 203
Office phone: 2-5695
Tentative office hours: MWF 11-12, Tu 2-3, Th 4-5, and by appointment

Course Prerequisites: A grade of C- or above in MATH 210 and MATH 240, or permission of instructor.

Credits and Workload Expectations: 4 credits: 8-10 hours per week outside the classroom.

Textbook: *Making, Breaking Codes: An Introduction to Cryptology*, by Paul Garrett. See Garrett's website for errata: http://www.math.umn.edu/∼garrett/crypto/.

Course Objectives:

- Gaining factual knowledge
- Learning fundamental principles, generalizations, and theories
- Learning to apply course material
- Developing skill in expressing myself orally or in writing

Homework: Homework will typically be assigned in a "rolling trio": reading assignments, discussion problems, and written problems. For example, for Fri Feb 3, you are to write up the solution to a problem from Section 1.3 (which we will have discussed already, in class Wed Feb 1), work on discussion problems for Section 1.5 and 1.6 (which we will discuss in class on Fri Feb 3), and read and answer questions on Section 1.7 (which we will discuss in class Mon Feb 6).

Late Work: Late work is typically not accepted. The lowest three scores in each assignment category will be dropped at the end of the semester. Extensions may be granted if requested before the due date, and work may certainly be submitted before the due date, if arrangements have been made with the professor in advance. If there is a serious, unforeseeable reason for missing more than three days of class, it is the student's responsibility to contact the professor as soon as possible and to make appointments with the professor and with Academic Counseling upon returning to classes to make a plan for making up missed work.

Missed Exams: Make-up midterm exams or quizzes may be given to students with legitimate excuses such as serious illness, university sponsored events, etc., as long as the make-up exam can be taken within a reasonable time frame. If it is not possible to schedule a make-up exam within a reasonable time frame, the grade for the midterm may be prorated from the final exam. Written documentation may be required. Rescheduling the final is not possible except under very extreme circumstances.

Final Course Grade: The overall score for this course will be computed as outlined below. Final letter grades will be assigned based on the overall score, with the two mastery components, written work and exams also being considered separately. In particular, the final letter grade will not be higher than one letter grade above the level of the work on written work or the work on exams. Exceptional performance on the final may also be taken into account.

- Homework, quizzes, and participation (45%): reading questions (5%), discussion problems (5%), quizzes (5%), written problems and oral presentations (30%)
- Midterm Exams (30%): tentatively scheduled for Feb 20, Mar 15, Apr 21
- Final Exam (20%): cumulative; 8:00 am - 10:00 am Wed May 17
- Best Exam (5%): at the end of the semester, your best exam score will count an extra 5%

Disability Accommodations: Academic accommodations will be provided for qualified students with documented disabilities including but not limited to mental health diagnoses, learning disabilities, Attention Deficit Disorder, chronic medical conditions, visual, mobility, and hearing disabilities. Students are invited to contact the Disability Resources office about accommodations early in the semester. Appointments can be made by calling 651-962-6315 or in person in Murray Herrick, room 110. For further information, you can locate the Disability Resources office on the web at http://www.stthomas.edu/enhancementprog/.

Math 316-01, Guidelines for Written Work

A significant objective of this class is learning to explain mathematical results clearly and carefully in writing. There are (at least) two reasons why mathematical writing is an important part of your education as a mathematician: (1) because it deepens your understanding of the mathematics: the process of writing your ideas in a coherent way forces you to think deeply and carefully, and (2) because effectively communicating your mathematical ideas is an essential aspect of being a scholar.

The written work you submit in this course will be graded for clarity and coherence of exposition, as well as mathematical writing style and correctness. I am not requiring volumes of written work, so I expect that the work you do submit is written thoughtfully and presented neatly. Show me your best work.

A good rule of thumb for writing a solution to a computational problem is that your work should stand on its own as an explanation of the relevant concepts as well as the solution to a specific problem.

Please make sure your homework is neatly assembled in a stapled packet and clearly labeled with name, date, problem number, etc. I reserve the right to take off points if your homework is not neat.

Guidelines for written problems:

- Make sure your work is readable. If necessary, use a word processor.
- Restate the question. If you are asked to prove something, restate the question in the form of a claim followed by a proof.
- Explain the relevant concepts.
- In a computation, show all your steps, and make your reasoning clear.
- Cite relevant theorems, definitions, or previous exercises to back up your claims.
- You will not usually need to write full paragraphs, but you should use helpful transitional words and phrases like, "first we will . . . ," "next we need to verify . . . ," "therefore," "thus," "one one hand . . . on the other hand," . . . "we can conclude that . . . ," etc.

Rubric for written problems:

- Very Nice (4): clear, correct, and complete solution of the problem and good presentation
- Right Idea (3): essentially correct, but some small gaps, lack of clarity, or poor presentation
- Good Start (2): shows partial understanding, e.g. correct start, but significant flaws or gaps
- Good Effort (1): inappropriate approach, faulty reasoning, or wrong problem
- No Attempt (0): recopy problem but do not attempt to solve it

The numbers are "messages" not points! For example, getting an all 3s and 4s (with a few more 4s) would be very good, A-level work, whereas consistently scoring 2s would mean that your work does not demonstrate sufficient understanding to move on (D-level work).

Math 316, Spring 2017. Tentative Semester Schedule

Mon	Wed	Fri
Jan 30, 2017	Feb 1, 2017	Feb 3, 2017
Introduction; 1.1 Shift Ciphers	1.2 Reduction/Division Algorithm 1.3 The One-Time Pad	1.4 Divisibility 1.5 Multiplicative Inverses 1.6 Integers mod m
Feb 6, 2017	Feb 8, 2017	Feb 10, 2017
1.7 The Affine Cipher	6.2 The Euclidean Algorithm, 6.3 Computing Inverses	2.1 Counting; 2.2A Basic Ideas
Feb 13, 2017	Feb 15, 2017	Feb 17, 2017
2.2B Basic Ideas	2.3, 2.4 Statistics of English, Attack on the Affine Cipher	4.1 The Vigenere Cipher
Feb 20, 2017	Feb 22, 2017	Feb 24, 2017
Exam 1	4.4 Expected Values	4.5A Friedman Attack
Feb 27, 2017	Mar 1, 2017	Mar 3, 2017
4.5B Friedman Attack	7.1 Trapdoors, 7.2 RSA Cipher	9.5 Exponentiation Algorithm
Mar 6, 2017	Mar 8, 2017	Mar 10, 2017
7.3 Primitive Roots, Discrete Logs, 7.4 DH Key Exchange	7.5 ElGamal Cipher	13.1, 13.2 F. Pseudprimes, Non-prime Pseudoprimes
Mar 13, 2017	Mar 15, 2017	Mar 17, 2017
10.8, 12.1-12.3 Euler's Criterion, Quadratic Symbols	**Exam 2**	3.1, 3.2 Cryptograms, Anagrams
Mar 20, 2017	Mar 22, 2017	Mar 24, 2017
Spring Break	Spring Break	Spring Break
Mar 27, 2017	Mar 29, 2017	Mar 31, 2017
12.4, 12.5 Quadratic Reciprocity, Fast Comp'n	13.3, 13.4 Euler Ps-primes, Solovay-Strassen Test	13.5, 13.6 Strong Ps-primes, The Miller-Rabin Test
Apr 3, 2017	Apr 5, 2017	Apr 7, 2017
10.1, 10.2 Sun Ze's Thm; 14.1, 14.2 Basic Public-Key Protocol, Secret-Sharing	14.3, 14.4 Oblivious Transfer, Zero Knowledge Proofs	16.1, 16.2, 16.3 pRNGs, LCGs
Apr 10, 2017	Apr 12, 2017	Apr 14, 2017
16.4 LFSGs	16.6 BBS Generator	Good Friday
Apr 17, 2017	Apr 19, 2017	Apr 21, 2017
Easter Monday	9.1-9.4 Factoring Special Expressions	**Exam 3**
Apr 24, 2017	Apr 26, 2017	Apr 28, 2017
18.1 Pollard's Rho Method	18.2 Pollard's p-1 Method	18.3 Lucas-Pocklington-Lehmer Criterion
May 1, 2017	May 3, 2017	May 5, 2017
18.4 Strong Primes	18.5 Primality Certificates	19.2 Random Squares Factoring
May 8, 2017	May 10, 2017	May 12, 2017
19.1, 19.3 Gaussian Elimination, Dixon's Alg.	19.4 Non-Sieving Quadratic Sieve	19.5-19.7 Continued Fraction Sieve, Quadratic Sieve

Final Exam: 8:00-10:00 am Wed May 17

Math 316, S2017, Unit 1 Plan

Mon	**Wed**	**Fri**
Jan 30, 2017	Feb 1, 2017	Feb 3, 2017
Intro to course; 1.1 Shift Ciphers *Due today:* RQ 1.1-1.3 *For next class:* RQ 1.4, 1.5, 1.6 D 1.2: 3, 7, 14, 15; 1.3: 1, 2, 7 W 1.1: 12	1.2, 1.3 Reduction/ Division Algorithm, The One-Time Pad *For next class:* RQ 1.7 D 1.5: 3, 4, 1.6: 3, 4, 5, 7, 9 W 1.3: 3	1.4, 1.5, 1.6 Divisibility, Multiplicative Inverses, Integers mod m *For next class:* RQ 6.2, 6.3 D 1.7: 1, 6, 7, 10, 12, 13 W 1.6: 10
Feb 6, 2017	Feb 8, 2017	Feb 10, 2017
1.7 The Affine Cipher **Quiz 1** (1.1-1.6) *For next class:* RQ 2.1, 2.2A D 6.2: 1, 2, 6.3: 1*, 2* W 1.7: 11	6.2, 6.3 The Euclidean Algorithm, Computing Inverses mod m *For next class:* RQ 2.2B D 2.1: 7-10, 12; 2.2: 3, 4, 5 W 6.2: 3	2.1, 2.2A Counting, Basic Ideas in Probability *For next class:* RQ 2.3, 2.4 D 2.2: 7, 8, 10 W 2.1: 11
Feb 13, 2017	Feb 15, 2017	Feb 17, 2017
2.2B Basic Ideas in Probability (con't) *For next class:* RQ 4.1 D 2.3: 1, 2, 3; 2.4: 1 W 2.2: 12 (w/o using prop'n.)	2.3, 2.4 Statistics of English, Attack on the Affine Cipher *For next class:* RQ 4.4 D 4.1: 5, 6, 7, 8, 9 W 2.4: 2	4.1 The Vigenere Cipher *For next class:* Study for exam. W 4.1: 1
Feb 20, 2017	Feb 22, 2017	Feb 24, 2017
Exam 1 *For next class:* RQ 4.5A D 4.4: 1, 2, 5, 9, 10	4.4 Expected Values *For next class:* RQ 4.5B D 4.5A W 4.4	4.5A Friedman Attack *For next class:* RQ 7.1, 7.2 D 4.5B W 4.5