Course information

Math 447, Fall 2015
Line Number: 71648
Time and Place: Mon, Wed.: 10:30--11:45 am, WXLR 108
Instructor: Andrew Bremner
E-mail: bremner@asu.edu
Office Hours: WXLR 731, Mon 3:00-4:00 pm, Tues 9:00--10.00 am, Weds 3:00--4:00 pm; and by appointment

Text: Introduction to Cryptography with Coding Theory, by Wade Trappe and Lawrence C. Washington

A tentative weekly schedule for the material to be covered is as follows (material will roughly follow the presentation in Trappe and Washington):

Aug 24-26: Classical ciphers: Caesar, substitution, Playfair, Railfence, Trifid, Vigenere

Good descriptions of these ciphers (and others) are available on the webpage maintained by Dr. Childress.
Aug 31-Sep 2: Secs 3.1, 3.2, 3.3
Sept 7-9: Secs 3.4, 3.5
Sept 14-16: Secs 3.6, 3.7
Sept 21-23: Secs 3.8, 3.9
Sep 28-30: Secs 3.10, 3.11
Oct 5-7: Block ciphers, affine, Hill ciphers
Oct 10-13: Fall Break, classes excused
Oct 14: Secs 6.1, 6.2

Oct 17: CryptoRally
Oct 19-21: Secs 6.3, 6.4
Oct 26-28: Sec 6.5, 6.6, 6.7
Nov 2: Test 1
Nov 4: Sec 7.1, 7.2
Nov 9: Sec 7.4, 7.5, 8.1
Nov 11: Veterans Day, classes excused
Nov 16-18: Sec 8.2, 8.3
Nov 23-25: Sec 8.4, 8.5
Nov 26: Thanksgiving Day, classes excused
Nov 30-Dec 2: review
Dec 4: (Last day of class)
Dec 7 (Monday): Final Exam, WXLR 108, 9:50--11:40 am

This tentative schedule is subject to amendment by in-class announcement. There will be a midterm Test, on Nov 2. A comprehensive Final Examination will be given on Monday Dec 7.

The grade for this class will be determined by a weight of 40% for the midterm Test and Final, and a weight of 20% for homework assignments.

There is a computational component to this class. You will be expected to use Mathematica or Maple or a program of your choice to undertake simple exercises both in decoding cipher texts and in performing computations with the underlying mathematics. You can download relevant Mathematica programs from Washington's website (see the book), and you can access relevant Maple programs here. If you use this Maple code, please consult the file readme.
CryptoRally is a fun sponsored event involving competitive solving of ciphers (and prizes) for teams of two participants. Details to follow.

H1 (text of codes is here), H2:
Due: (both H1,H2) Wed 9 Sept

H3:
Due: Wed 16 Sept

H4:
Due: Wed 23 Sept
H5:
Due: Wed 30 Sept

H6:
Due: Wed 7 Oct

H7:
Due: Wed 21 Oct

H8:
Due: Mon 9 Nov

H8:
Due: Wed 18 Nov

H9:
Due: Wed 25 Nov

H10:
Due: Wed 2 Dec
Student Obligations

Academic Integrity Policies

Disability Accommodations:
Qualified students with disabilities who will require disability accommodations in this class are encouraged to make their requests to me at the beginning of the semester either during office hours or by appointment. Note: Prior to receiving disability accommodations, verification of eligibility from the Disability Resource Center (DRC) is required. Disability information is confidential.

Establishing Eligibility for Disability Accommodations: Students who feel they will need disability accommodations in this class but have not registered with the Disability Resource Center (DRC) should contact DRC immediately. Their office is located on the first floor of the Matthews Center Building. DRC staff can also be reached at: 480-965-1234 (V), 480-965-9000 (TTY). For additional information, visit: www.asu.edu/studentaffairs/ed/drc. Their hours are 8:00 AM to 5:00 PM, Monday through Friday.