

M425/505

Cryptological Mathematics

Fall 2019

Instructor: Dr. Joel Iiams

Office: Witmer 324

Office Hours: 9-11 MWF & by appt.

Office Phone: 7-4608

Text: Cryptological Mathematics, Robert Edward Lewand.

e-mail: joel.iiams@und.edu

Grading Scheme: The letter grade for the course will be based on i) homework, ii) two one-hour exams, iii) a cryptanalysis score and iv) a cumulative final exam. Each component will comprise 20% of the grade. The scale used to determine the letter grade is the standard 90 – 80 – 70 – 60.

Homework Policy: Homework will be collected on a per class basis with few exceptions. Homework is due at the beginning of the subsequent class unless otherwise specified. Reading guide pages accrue as homework. Late homework will not be accepted without prior excuse having been made. Homework percentages for M425 students will be calculated based on 90% of the total points possible.

Graduate Credit: Students earning graduate credit for M505 will complete all extra credit homework exercises as well as all bonus exam questions. Their homework percentage will be calculated based on total points possible (including extra credit points) and performance on exam bonus questions will bear on exam scores.

Material Covered: The plan is to cover the first three chapters of the text in linear order. There will then be some material from external sources. Handouts will be forthcoming. The course will conclude with material from chapter 4, and possibly more material from external sources.

Exam 1: (9/20) Sections 1.1-1.6

Exam 2: (10/23) Sections 2.5-3.3 plus

The above exam dates are tentative.

There will be around a half a dozen out of class cryptanalysis assignments not counted as regular homework spread out over the semester. Students will generally have at least a week to complete the work. Whereas the lion's share of the points accrued will be based on successful decryption, full marks will only be given for complete cryptanalysis. Thus all pertinent supporting data and computations must be included in the materials handed in.

Last day to withdraw is **Friday, November 15**.

The cumulative final examination is at **10:15 a.m., Wednesday, December 18**.

General Information:

If you have emergency medical information to share with me, if you need special arrangements in case the building must be evacuated, or if you need accommodations in this course because of a disability, please make an appointment with me during the office hours listed in the opposite side, or by arrangement. If you plan to request disability accommodations, you are expected to register with the Disability Support Services office at 190 McCannel Hall - 777-3425.

Occurrences of academic dishonesty will minimally result in zero points being assigned for the assessment.