Prerequisite: CMSC 250. Informal Prerequisite: that you LIKED CMSC 250.

Overview: We will go through a sequence of Crypto Systems, first proving they are UN-CRACKABLE and then CRACKING them. We will then study Secret Sharing (but don’t tell anyone!).

Class Time and Place: M-Tu-W-Th-Fr 1:00-2:00, CSI 3117. Jan 3-Jan 23; however we get Martin Luther King Day (Monday Jan 16) off.

GRADING: There will be (roughly) daily HW, one midterm, and one final. HW is worth 25%, the midterm is worth 30%, and final is worth 45%. MIDTERM: Wedendsay Jan 11. 4:30-6:00 (NOTE THE TIME, AT NIGHT) FINAL: Monday Jan 23 4:30-6:00 (NOTE THE TIME- AT NIGHT) ALSO NOTE- I NEED TO GET THE ROOMS SO THIS MIGHT CHANGE A BIT TO 5:00 For HW, Midterm, Final you must hand in your own work– academic dishonesty will be dealt with harshly, resulting in a hearing in front of the acad honor council. HW must be neatly written. You will lose points for sloppiness.

HW, Mid, Final Excuse Policy: The HW will typically given on day n and due on day n + 1 at the beginning of class since I may go over it IN class. There will be roughly 10 HW’s. No late HW will be accepted except with a documentation (e.g., a doctors note). If you miss an exam and can provide a documented excuse within a day then you will get a makeup. If you know you will not be able to take an exam or do a HW on time ahead of time for Religious or other reasonable reasons, let me know ASAP.

Office Hours and Contact Information Prof Gasarch, AVW 3245, 405-2698, gasarch@cs.umd.edu. Off. Hrs: 11-12:45 every day, though I am usually around 2-5 also. You can always email me. Graders: Justin Shen and Phong Dinh.

Accommodations: Students requesting academic accommodations due to a disability should make such a request to the instructor in office hours, with a letter of accommodation from the Office of Disability Support Services (DSS) within the first two days of the semester.

Course Evaluations There may be official course evals for this course. In any case I will be asking to fill out a course eval that I make up to help me teach this course better in the future.

Text: There is no text but notes may be posted online at times.

Laptop Policy: Laptops not allowed in class unless you are taking notes with it.