

## CMSC 198B: Computer Science— A Hands off Approach

(NOTE- this document is two pages so don't miss the second page.)

**Overview:** We study cryptography, combinatorics, probability, graph theory, and some algorithms. These are all topics useful for computer science that do not involve programming.

**Class Time and Place:** July 13-July 31

**Note:** This is part of Univ of MD's Young Scholars Program.

Website for CMSC 198: [www.cs.umd.edu/~gasarch/198/Su15/Su15.html](http://www.cs.umd.edu/~gasarch/198/Su15/Su15.html)

**Text:** Notes will be made available.

**Prerequisites:** High School Algebra. More math is a plus. No programming needed. If you DO know how to program then there will be some optional programming assignments for fun.

### Content

1. **Classical Crypto:** Alice and Bob get to meet. Later they can secretly communicate even if Eve intercepts the message! (Shift Cipher, Linear Cipher, Vigenere Cipher, Matrix Cipher, 1-time pad, others). We will show several codes are UNCRACKABLE and then CRACK them.
2. **Modern Crypto:** Alice and Bob do not have to meet! Diffie-Helman Key Exchange. We will show that this code is UNCRACKABLE and then CRACK it.
3. **Secret Sharing with polynomials:** Any three or more of Alice, Bob, Carol, Donna, Eve can read the message but no two can. UNCRACKABLE!
4. **Secret Sharing with cards:** Alice and Bob can establish a shared secret key right in front of Eve! UNCRACKABLE!
5. **The Millionaires Problem:** Alice and Bob are both wealthy. They want to compare salaries. But they don't want to actually reveal their salaries. Is there a protocol so that in the end they know who makes more money, but neither one knows the other ones salary? Yes!
6. **Error-correcting Codes:** You transmit a long sequence of digits. But there may be an error in transmission! Can you detect it? Can you correct it?
7. **Nim Games:** Simple games with nice patterns!
8. **Misc Topics Based on Time and Tastes!**

### POLICY

The policies below may change slightly over the course of the course.

**GRADING:** There will be (roughly) daily HW, one midterm, and one final. Class participation is worth 10%, HW is worth 20%, the midterm is worth 30%, and Final is worth 40%.

*MIDTERM*: July 22 *FINAL*: July 30). 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:** Any missed work requires a documented excuse.

**Office Hours and Contact Information** Prof Gasarch, AVW 3245, 405-2698, [gasarch@cs.umd.edu](mailto:gasarch@cs.umd.edu).  
Off. Hrs: TBD

**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 weeks of the semester.