CMSC 198B: Computer Science– A Hands off Approach

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

Overview: (1) Alice and Bob want to communicate in secret, so that even if Eve intercepts their message, she cannot tell what they said. We present several ways for Alice and Bob to do this, some of which do not require Alice and Bob to ever meet! (Public Key Cryptography) (2) Zelda has a secret. She wants that if four of her eight friends get together they can discover it, but if three of them get together they cannot. We present several ways for Zelda to give shares of the secret to her friends so that this happens. These may sound like fun puzzles, and they are. But they also have vast implications and applications for modern day cryptography and security.

Class Time and Place: July 11-July 29

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

Website for CMSC 198: `www.cs.umd.edu/~gasarch/198/Su16/Su16.html`

Text: Notes will be made available.

Prerequisites: High School Algebra. More math is a plus. You should be comfortable with logarithms, so if you don't know what they are please learn them before the course begins. 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 I:** 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. **Modern Crypto II:** Alice and Bob do not have to meet! RSA protocol. We will show that this code is UNCRACKABLE and then CRACK it.

4. **Secret Sharing:** Zelda wants to share a secret with some subsets of her friends (e.g., all subsets with at least four people in them) but not others. How can she do this? YES!

5. **CIA problem:** Similar to Secret Sharing. What if some of Zelda's friends are not really Zelda's friend but only pretending? Can Zelda share her secret in a way such that if someone is out out to sabotage the operation, they will be discovered? YES!

6. **Secret Sharing with Short Shares:** Variant on Secret sharing where Zelda wants to give short messages to her friends. you

7. **Secret Sharing with cards:** Alice, Bob, and Eve are all dealt cards. Can Alice and Bob establish a shared secret key right in front of Eve! YES!

8. **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!

9. **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? YES and YES

10. **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 approx 15%, the midterm is worth approx 30%, and Final is worth approx 40%.
MIDTERM AND FINAL: Midterm day will be decided later but it will be in he second week. The final is the second to last day.
HONESTY IS THE BEST POLICY: 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.

Contact Information: Prof Gasarch, AVW 3245, 405-2698, `gasarch@cs.umd.edu`. Grader: Justin Shen.

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 one week of the semester.