COSC 483/583: Applied Cryptography

Exercise Set 1

**Ground Rules.** You may choose to work with one other student if you wish. Only one submission is required per group, please ensure that both group members names are on the submitted copy. Work must be submitted in typeset hard copy by the start of class. Questions marked as COSC 583 are required for those enrolled in the 583 section. If you are in the 483 section you are more than welcome to attempt any of them, extra credit will be awarded for correct answers.

1. **Breaking Shift and Vigenere.** [20 pts]

   The goal of this question is for you to break both a Shift Cipher and a Vigenere Cipher as a cipher text only adversary. This will require a small amount of programming, for reference my implementation in python is about 110 lines of code, so nothing too crazy. Two text files can be found on the class calendar where you found this exercise set. One is `shift-enc` and the other is `vig-enc`, these are cipher texts encrypted using a shift and Vigenere cipher respectively. To make your life a bit easier I have also included two supplemental files `shift-freq` and `vig-freq` that are the letter frequencies of each plain text file. Note that the sum of squares of letter distribution is slightly different than standard English, 0.066 in both cases.

   (a - 5pts) Break the shift cipher. To demonstrate success provide for me the first 50 or so characters along with what key (shift was used).

   (b - 5pts) Break the Vigenere cipher. Again, to demonstrate success provide both the first 50 or so characters and the recovered key. Hint, you should be able to call into the overwhelming majority of your shift cipher code, saving you some time.

   (c - 10pts) Provide the source code of your attack. If your source code is exceptionally bulky we need to talk about proper code structure...

2. **Chosen Plaintext Attackers and Classical Ciphers.** [15 pts]

   Show that the shift, substitution, and Vigenere ciphers are all trivial to break for an adversary executing a chosen plaintext attack. How much chosen plaintext is needed to recover the key for each of the ciphers?

3. **Repeated Uses of OTPs.** [10 pts]

   We know that One Time Pads are Perfectly Secret, assuming that the key size is the same as the message size and that we do not re-use keys. Demonstrate that if a OTP is re-used multiple times the cipher is no longer perfectly secret. To do this build a Cipher Text Only attack which recovers the OTP pad given "enough" cipher texts. For a fun historical note, you are replicating an attack launched by American cryptographers during the cold war against Soviet diplomatic messages.

   *COSC 583*

4. **Equivalence of Perfectly Secret and Adversarial Indistinguishable.** [20 pts]

   Prove that an encryption scheme is perfectly secret if and only if it is adversarially indistinguishable (lemma 2.6 from Katz).