

Assignment 8 – Cryptography

due at midnight on Fri May 8 (50 points)

There are three parts to this assignment. To get full credit, you must submit three files on Blackboard, and send one (encrypted) email to me.

(1) Monoalphabetic cipher

You will be **provided with a piece of text** encoded using a single-substitution (monoalphabetic) cipher. Your task is to crack the code and discover the secret poem.

You should start by doing a **frequency analysis** of the letters in your text.

When finished, type in (or take a picture of) your decrypted text, and submit that on Blackboard.

(2) Vigenère cipher

1. Choose a password that is 5–8 letters, and write it down.
2. Write down a sentence that is about 4–6 times the length of your password.
3. Use the **polyalphabetic substitution table** to encode the sentence using your password.
4. Type the encrypted sentence **and the password** into a text file, and submit that on Blackboard.
5. You'll get full credit for this portion only if I can make sense of your sentence by decrypting using your password. So you may want to give that a test run with a friend: give them your encrypted sentence and password, and see if they get it right.

(3) Public key cryptography (GPG)

1. Use some variant of GNU Privacy Guard (GPG) or Pretty Good Privacy (PGP). Here are some options:
 - Windows:
 - Software: <http://www.gpg4win.org/> (free)
 - Video: <https://vimeo.com/113980848>
 - Mac:
 - Software: <https://gpgtools.org/> (free)

- Video <https://vimeo.com/114185832>
 - iPhone/iPad:
 - Software: <https://ipgmail.com/> (\$2)
 - Android phone/tablet:
 - Software: <https://play.google.com/store/apps/details?id=org.thialfihar.android.apg&hl=en> (free)
 - Video <https://vimeo.com/114048258>
2. Once you have one of the GPG apps installed, generate a new key pair using your email address and password. If using a lab computer, you should back up your key to a USB drive (ideally) or store it somewhere in the cloud. (In real life, you should not let your private key leave your control, but we can be more relaxed for this exercise.)
 3. Import [my public key](#), which you can get at that link, or by searching a key server for the ID 4F31B08B.
 4. Export your public key to a .txt file, and upload that file to Blackboard.
 5. Compose a short message to me, then sign it with your key and encrypt it with my key. Send the encrypted version of the message via email to christopher.league@liu.edu