Assignment 11 – Cryptography

due in class on Mon 5 May (40 points)

Single-substitution cipher

Your group will be provided with a piece of text encoded using a single-substitution (monoalphabetic) cipher. (Links to the texts are below, in case you lose yours or need another copy.)

Your task is to crack the code and discover the secret message.

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

- text01.crypt.pdf text06.crypt.pdf text11.crypt.pdf
- text02.crypt.pdf text07.crypt.pdf text12.crypt.pdf
- text03.crypt.pdf text08.crypt.pdf text13.crypt.pdf
- text04.crypt.pdf text09.crypt.pdf text14.crypt.pdf
- text05.crypt.pdf text10.crypt.pdf text15.crypt.pdf

Polyalphabetic substitution 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. Pass the encoded sentence **and your password** to another group.
5. Decrypt the sentence provided by the other group **using their password.**

Public/private key demonstration

6. Use my Public Key Cryptography Demo at http://cryptodemo-liucs.appspot.com/ to register your name and generate a public/private key pair.
7. Copy the private key and store it somewhere (such as in a document or text file) on your computer.
8. Send me an encrypted message (set recipient to "Chris League")

9. Send an encrypted message to other members of your group.
10. Read and decrypt messages intended for you (in the INBOX)
11. Attempt to decrypt messages NOT intended for you (click “all” instead of INBOX).