Homework 2
CSE108

Due: April 28, 11:59 pm PST

Programming Assignment

Decrypt the supplemented ciphertext (encoded in Hex[1]) using the Vigenére cipher. You can use English character frequencies or ASCII character frequencies (that you can find online) to do this. Your solution should include the recovered secret key and plaintext as well as the code you used. Show also the asymptotic complexity of your attack. You can use the language of your choice. Python and C code to encrypt and decrypt are also provided.

[Finding the key length: For all keys $1 \leq l \leq L$ (Assume an L and increase it if you don't find a good l), on the first stream (characters $0, l, 2l$, etc.). compute $\sum_{i=0}^{255} q_i^2$, where q_i is the frequency of the i-th ASCII character. You can also look at other streams that start from a different position than 0. Assume the l that gives the highest value as the key length and try the next one if you don't get good results.
Finding the key: On each stream (which corresponds to one character of the key), try to maximize $\sum_{i=0}^{255} q_i p_i$ by testing different key characters. Here, p_i is the expected frequency of character i (e.g., from the English letter frequencies).]

Deliverables

You should submit a zip file that contains the following:

- Submit a brief description of your approach and the recovered secret key and plaintext (PDF file).
- The source code you created.

Your answers **must** be typed and **not** handwritten.
File name format (CruzID is the alphanumeric part before the @ in your UCSC email address):

- `cse108_hw<homework-number>_<CruzID>.pdf`
- `cse108_hw<homework-number>_<CruzID>.py # Or any other language extension.`

For example, for CruzID `jdoe@ucsc.edu` and homework 2, the submission should look like this:

```
cse108_hw2_jdoe.zip

   +-- cse108_hw2_jdoe.py
   +-- cse108_hw2_jdoe.pdf
```

[1] Here are a couple of references that show you how to convert text to hex in Python, and Java. See also the provided sample codes.