Assignment # 1

Homework

Homework problems are a preparation for the quizzes. They are *not* graded. Please use the `piazza` forum to post questions you have on these problems.

- 1.3, 1.4, 1.5, 1.6, 1.8, 1.9, 1.10

Project

1. The following ciphertext which has been encoded with a shift cipher:

   `AOLLULTFRUVDZAOLZFZALT`.

   (a) Perform an attack against the cipher using one of the attacks discussed in class. What is the key? What is the plaintext?

2. The ciphertext printed below was encrypted using a substitution cipher. The objective is to decrypt the ciphertext without knowledge of the key.

   Ciphertext:

```
NVIFABE NVIFABE BINNBE MNWL
PGV I VGFCEL VPWN YGQ WLE
QH WOGUE NPE VGLBC MG PITP
BIAE W CIWDGFC IF NPE MAY

VPEF NPE OBWZIFT MQF IM TGFE
VPEF PE FGNPIFT MPIFEM QHGF
NPEF YGQ MPGV YGQL BINNBE BITPN
NVIFABE NVIFABE WBB NPE FITPN

NPEF NPE NLWUEBEL IF NPE CWLA
NPWFAM YGQ SGL YGQL NIFY MHWLA
PE RGQBC FGN MEE VPIRP VWY NG TG
IS YGQ CIC FGN NVIFABE MG
```

   (a) Provide the relative frequency of all letters A...Z in the ciphertext.

   (b) Decrypt the ciphertext with help of the relative letter frequency of the English language (e.g., search Wikipedia for letter frequency analysis). Note that the text is relatively short and might not completely fulfill the given frequencies from the table.

   (c) Who wrote the text? What are the missing words?

3. Vigenère proposed a stronger cipher than the *Vigenère cipher*. This cipher is an *autokey cipher*, where the plaintext itself is used as key. It works by starting with a keyword, and using plaintext characters after that.

Plaintext	`l e h r u n d k u n s t`
Key	`w p i l e h r u n d k u`
Ciphertext	`H T P C Y U U E H Q C N`

   (a) Check the above example.

   (b) Provide a formal definition of the `Gen`, `Enc`, and `Dec` algorithms for this cipher. Make sure to include the equation that defines the encryption and decryption operations.

   (c) Provide an implementation of this cipher. You may either use Python or sage, or another common programming language, such as C.

   (d) Decrypt the following ciphertext using the key `plato`:
   `CZGHCQRKSRJRIWXTDYFCFWYQ`

4. Another autokey cipher by Vigenère uses the letters of the ciphertext instead of the plaintext to form new key letters:

Plaintext	`l e h r u n d k u n s t`
Key	`w p i h t p y n c b x w`
Ciphertext	`H T P Y N C B X W O P P`

   (a) Show that this is a much weaker cipher than the other: Explain a brute force attack that can recover most of the plaintext quickly.

   (b) Decrypt the following ciphertext that has been encrypted with the above method. It is ok to miss the first few letters.
   `NEASJFINVCMMZJPQKSQXIKXJBZXLXO`

Good Luck and Have Fun!