Math 116
Homework 2
Due Monday, January 25, 2016

- Please read sections 2.1–2.3, 2.7–2.9, and 2.11 of your textbook. You might also find the remaining sections of chapter 2 (especially 2.5 and 2.12) fun and interesting.

- Do Problems 19, 20, and 25 at the end of chapter 2 (section 2.13).

- Do the following additional problems:

    1. Alice and Bob agree on the key word "virgo" for Vigenère encryption between them. Alice sends Bob the encrypted message

       `ZDVOGZIMKGYZFVDDVXUBPA`

       Decrypt this message. (You can do this by hand pretty easily, but this problem is here mostly so that if you do write some computer code to do Vigenère encryption/decryption, you can test it before moving on to the next few (harder) problems.)

    2. Alice and Bob have agreed upon a 4-letter password for Vigenère encryption. You (Eve) don't know their password, but you intercept the following ciphertext sent from Bob to Alice. Use letter frequencies as outlined in class to figure out their key, and decipher the message.

       ```
       FEWCNWQBMSNSTEJYWOTMXDGVXYCVCYYODSGDQEUOFOTNBAUDQEDKLKDYWEQP
       JLKPNSROWTFOOEPNRNICXMGDQIPQHOWEBEVRNMCCJPWXLHNSWEKRJVGXNIVR
       NRVRNTKWNNQBCHGSWCNSWAVSXNVYNXRVJIPWHSGVOTQKVAPGQOTSBEUKWDUV
       NERCDNFOATJOKLCXTEVYOTJOEETIORGOMOODQAVSYRQFRDGKWDVRNNSENSVS
       XNUDQEOKWNGBRNYRRCJSYRQFRDGSC
       ```

    3. You have intercepted the following ciphertext sent from Alice to Bob. All that you know is that they are using Vigenère encryption. Figure out their key, and decipher the message.

       ```
       DOEESFDAWTSRJSXSHRZFHJGBIEAGIEOIGKWYANVWKVPHAAGYKNZLVVJBTUYP
       QROWRBREKSQUAMBUOYRELKSYENPZWPDHXOOFXRXOWACAISFGECNDOEHYFSZB
       ZOKGIFLRHVIPPHBKVRWDPSGFQNDMDBJHBKPEAALLOAZHXDCBGEWXFBIMRHCV
       JTHXJVAWEAYRWSMJOACEESBXXIKVKVPHWMZYCRXQDYQMTYSNJDTTZNYKMGDX
       JOMKCJWTLGBFWIWZSFQDWWBYUYHMRBJOMHFBLOLWHBENOWGGENLGIGDAYJWP
       WNLWQHNIMASF
       ```

For the last two problems, you will most likely want to use a computer. If you do, here are those two ciphertexts in a format that you should be able to copy and paste directly into some computer code:

```
ciphertext2 = "\
FEWCNWQBMSNSTEJYWOTMXDGVXYCVCYYODSGDQEUOFOTNBAUDQEDKLKDYWEQP\
JLKPNSROWTFOOEPNRNICXMGDQIPQHOWEBEVRNMCCJPWXLHNSWEKRJVGXNIVR\
NRVRNTKWNNQBCHGSWCNSWAVSXNVYNXRVJIPWHSGVOTQKVAPGQOTSBEUKWDUV\
NERCDNFOATJOKLCXTEVYOTJOEETIORGOMOODQAVSYRQFRDGKWDVRNNSENSVS\
XNUDQEOKWNGBRNYRRCJSYRQFRDGSC"

ciphertext3 = "\
DOEESFDAWTSRJSXSHRZFHJGBIEAGIEOIGKWYANVWKVPHAAGYKNZLVVJBTUYP\
QROWRBREKSQUAMBUOYRELKSYENPZWPDHXOOFXRXOWACAISFGECNDOEHYFSZB\
ZOKGIFLRHVIPPHBKVRWDPSGFQNDMDBJHBKPEAALLOAZHXDCBGEWXFBIMRHCV\
JTHXJVAWEAYRWSMJOACEESBXXIKVKVPHWMZYCRXQDYQMTYSNJDTTZNYKMGDX\
JOMKCJWTLGBFWIWZSFQDWWBYUYHMRBJOMHFBLOLWHBENOWGGENLGIGDAYJWP\
WNLWQHNIMASF"
```

Also for your convenience, here are the typical frequencies of letters in English, in various formats:

As a C or C++ array:

```c
float letter_frequencies[26] = {
    0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.020, 0.061, 0.070,
    0.002, 0.008, 0.040, 0.024, 0.067, 0.075, 0.019, 0.001, 0.060,
    0.063, 0.091, 0.028, 0.010, 0.023, 0.001, 0.020, 0.001
}
```

As a Python list:

```python
letter_frequencies = [
    0.082, 0.015, 0.028, 0.043, 0.127, 0.022, 0.020, 0.061, 0.070,
    0.002, 0.008, 0.040, 0.024, 0.067, 0.075, 0.019, 0.001, 0.060,
    0.063, 0.091, 0.028, 0.010, 0.023, 0.001, 0.020, 0.001,
]
```

As a Python dictionary:

```python
letter_frequencies = {
    "A": 0.082, "B": 0.015, "C": 0.028, "D": 0.043, "E": 0.127, "F": 0.022,
    "G": 0.020, "H": 0.061, "I": 0.070, "J": 0.002, "K": 0.008, "L": 0.040,
    "M": 0.024, "N": 0.067, "O": 0.075, "P": 0.019, "Q": 0.001, "R": 0.060,
    "S": 0.063, "T": 0.091, "U": 0.028, "V": 0.010, "W": 0.023, "X": 0.001,
    "Y": 0.020, "Z": 0.001,
}
```