MATH 195: CRYPTOGRAPHY
HOMEWORK #2

Problem 2.7. *A disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword* CIPHER*, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:*

```
plain:   a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher:  C I P H E R A B D F G J K L M N O Q S T U V W X Y Z
```

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generated the sequence by reading down the columns:

```
C I P H E R
A B D F G J
K L M N O Q
S T U B W X
Y Z
```

This yields the sequence:

```
C A K S Y I B L T Z P D M U H F N V E G O W R J Q X
```

Such a system is used in the example in Section 2.3*:*

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
itwasdisclosedyesterdaythatseveralinformalbut

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
directcontactshavebeenmadewithpolitical

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
representativesofthevietconginmoscow
```

Determine the keyword.

Problem 2.8. *How many possible keys does a Playfair cipher have? Express your answer as an approximate power of* 2*.*

Problem 2.9. *We have shown that the Hill cipher succumbs to a known plaintext attack if sufficient plaintext-ciphertext pairs are provided. It is even easier to solve the Hill cipher if a chosen plaintext attack can be mounted. Describe such an attack.*

Date: February 5, 2002.
2.7–2.10.

Problem 2.10. *Let S be a (finite) set and $f : S \to S$ a bijective map. Show that there are maps $g, h : S \to S$ such that $f = g \circ h$ ad $g^2 = h^2 = \mathrm{id}_S$.*