HONS 195N: CRYPTOGRAPHY
HOMEWORK # 3

Problem 1. The following ciphertext was generated using a simple substitution algorithm:

```
53ddc305))6*;4826)4d.)4d);806*;48c8p60))85;;]8*;:d*8c83
(88)5*c;46(;88*96*?;8)*d(;485);5*c2:*d(;4956*2(5*-4)8p8*
;4069285);)6c8)4dd;1(d9;48081;8:8d1;48c85;4)485c528806*81
(d9;48;(88;4(d?34;48)4d;161;:188;d?;
```

Decrypt the message. *[Warning: The resulting message is in English but may not make much sense on a first reading.]*

Problem 2. A disadvantage of the general substitution 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 following ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
itwasdisclosedyesterdaythatseveralinformalbut

VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
directcontactshavebeenmadewithpolitical

EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
representativesofthevietconginmoscow
```

Determine the keyword.

Problem 3. One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Typically, at least in spy novels, the first sentence of a book serves as the key. Consider the following ciphertext:

SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA

It was produced using the first sentence of *The Other Side of Silence* (a book about the spy Kim Philby):

The snow lay thick on the steps and the snowflakes driven by
the wind looked black in the headlights of the cars.

A simple substitution cipher was used.

(a) Decrypt the message.

(b) How secure is this cryptosystem compared to a more general substitution cipher? To make the key distribution problem simple, both parties can agree to use the first or last sentence of a book as the key. To change the key, they simply need to agree on a new book. The use of the first sentence would be preferable to the use of the last. Why?