MATH 195: CRYPTOGRAPHY
HOMEWORK #1

Problem 2.1. *What is the message embedded in the following:*

3rd March

Dear George,
Greetings to all at Oxford. Many thanks for your
letter and for the Summer examination package.
All Entry Forms and Fees Forms should be ready
for final despatch to the syndicate by Friday
20th or at the very latest, I'm told, by the 21st.
Admin has improved here, though there's room
for improvement still; just give us all two or three
more years and we'll really show you! Please
don't let these wretched 16+ proposals destroy
your basic O and A pattern. Certainly this
sort of change, if implemented immediately,
would bring chaos.

Sincerely yours,

Problem 2.2. *The purpose of this problem is to show the unbreakability of the one-time pad. Suppose that we are using a Vigenère scheme with* 27 *characters in which the twenty-seventh character is the space character, but with a one-time key that is as long as the message. Given the ciphertext*

```
ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
```

find the key that yields the following plaintext:

```
MR MUSTARD WITH THE CANDLESTICK IN THE HALL
```

and find another key that yields the following plaintext:

```
MISS SCARLET WITH THE KNIFE IN THE LIBRARY
```

Comment on the result.

Problem 2.3. *In one of Dorothy Sayers' mysteries, Lord Peter is confronted with the message:*

I thought to see the fairies in the fields, but I saw only the evil
elephants with their black backs. Woe! how that sight awed me! The
elves danced all around and about while I heard voices calling clearly.
Ah! how I tried to see–throw off the ugly cloud–but no blind eye of a
mortal was permitted to spy them. So then came minstrels, having gold

Date: January 29, 2002.
2.1–2.6.

trumpets, harps and drums. These played very loudly beside me, breaking that spell. So the dream vanished, whereat I thanked Heaven. I shed many tears before the thin moon rose up, frail and faint as a sickle of straw. Now though the Enchanter gnash his teeth vainly, yet shall he return as the spring returns. Oh, wretched man! Hell gapes, Erebus now lies open. The mouths of Death wait on thy end.

He also discovers the key to the message, which is a sequence of integers:

```
787656543432112343456567878878765654343211234345656787887876565443321 1234
```

(a) *Decrypt the message. [Hint: What is the largest integer value?]*
(b) *If the algorithm is known but not the key, how secure is the scheme?*
(c) *If the key is known but not the algorithm, how secure is the scheme?*

Problem 2.4. *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. [Hints:

(1) *As you know, the most frequently occurring letter in English is* e. *Therefore, the first or second (or perhaps third?) most common character in the message is likely to stand for* e. *Also* e *is often seen in pairs (e.g.,* meet, fleet, speed, seen, been, agree, *etc.). Try to find a character in the ciphertext that decodes to* e.
(2) *The most common word in English is* the. *Use this fact to guess the characters that stand for* t *and* h.
(3) *Decipher the rest of the message by deducing additional words.]*

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

Problem 2.5. *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. The particular scheme discussed in this problem is from one of the best suspense novels involving secret codes,* Talking to Strange Men, *by Ruth Rendell. Work this problem without consulting that book.*

Consider the following message:

```
SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
```

This ciphertext 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 he headlights of the cars.

A simple substitution cipher was used.

(a) *What is the encryption algorithm?*
(b) *How secure is it?*

(c) *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?*

Problem 2.6. *In one of his cases, Sherlock Holmes was confronted with the following message:*

534 C2 13 127 36 31 4 7 21 41
DOUGLAS 109 293 5 37 BIRLSTONE
26 BIRLSTONE 9 127 171

Although Watson was puzzled, Holmes was able immediately to deduce the type of cipher. Can you?