MATH 75: Cryptography **Spring 2022**

PSET 1 — April 8, 2022

Prof. Asher Auel ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***The Code Book*** by **Simon Singh**.
(b) ***The Algorithm Design Manual*** by **Steven S. Skiena**.
(c) ***grokking algorithms: An illustrated guide for programmers and other curious people*** by **Aditya Y. Bhargava**

Problems

1. What is the message embedded in the following?

> 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.

Since **all** it was unlikely that the message was encrypted since every word in the message is correct. I next looked at the words at corresponding positions in each sentence, and discovered:

your package ready Friday 21st. room three. Please destroy this immediately.

2. In one of Dorothy Sayers' mysteries, Lord Peter is confronted with the following 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
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:

```
787656543432112343456567878878765654343211234345656787887876565443321123 4
```

(a) Decrypt the message. *Hint. What is the largest integer value?*

The largest integer value is 8, and there are no 0 values, suggesting that the scheme runs from 1 to 8. Using this strategy, I wrote a program that split the message into 8 lists of letters. Here is the resultant matrix:

```
ITFNDWEHHAWAWECOBEOLRISOLUDOPDECTIRAREEYEGLRSEKNNETRAICRONGTNAUSTRAPSOOEO
TOATSOVATCOTELEUOIIILTEFYTERETMARNURUPRBBTLEHAEIYFHOINKAUCNELLRPUENENPUAN
HSIHBNINHKESDVDNUHCNYREFCNYTROSMEGMPMLYERHSAETDSTOISLTLWGHAEYLNRRTHSOETTT
OEREULLTEBHIMEADTEEGAITTLOEAMSOELGPSSALSEAOMDIHHERNEAAENHASTYHAINCEEWNHHH
UEIFTYESIAOGESLAWASCHEHHOBOLIPTMSOEATYOIATTVWTEEAEMUNSOOTNHHEESNSHLRLTSWY
GTEIITLWRCWHTDLNHRCLHDREULFWTYHIHLTNHEUDKSHAHHADRTOPDAFWHTHVTRTGOELEIHOAE
HHSESHEIBKTTHAADIDAEOTOUDIAATTENADSDEDDEIPENEAVMSHOFFSSTEEIASEHRHDGBEEFIN
TEILAEPTLSHAENRALVLAWOWGBNMSEHNSVTHDSVLMNEDIRNEABENRAITHERSIHTEEWMAUSMDTD
```

Using the key to pick out rows for each letter position, I picked out the following letters:

```
hesittethbetweenthecherubimstheisles
maybegladthereofastheriversinthesouth
```

When spaced out properly, the above reads:

```
He sitteth between the cherubims the isles
may be glad thereof as the rivers in the south
```

(b) If the algorithm is known, but not the key, how secure is this encryption scheme?

(c) If the key is known, but not the algorithm, how secure is this encryption scheme?

3. The message

`ofoxdryeqrsgkvudrbyeqrdrofkvvoiypdrocrknygypnokdrspokbxyofsv`

was encrypted using a shift cipher. Decrypt the message.

I wrote a program implementing the basic mechanics of shift ciphers.

Running the text through the program, I got the following message (added spaces to make it easier to read):

even though i walk through the valley of the shadow of death i fear no evil

4. The following message was encrypted using a simple substitution cipher:

```
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. *Hint. Use frequency analysis: consider e, ee, the, ...*

5. For fun, take a stab at this problem. 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 immediately able to deduce the type of cipher. Can you?