CISS451: Cryptography

O.R. Oyedeji (February 7, 2025)

Contents

Chapter 1

Classical ciphers

1.1 Classical ciphers: instructions

1. At my website, in the Tutorials section, you'll find `latex.pdf`. Post LaTeX questions in CCCS discord.
2. In `thispreamble.tex`, change `AUTHOR` and `SHORTAUTHOR` to your name.
3. To speed up compilation, in `chap-classical-ciphers.tex`, you might want to comment out some sections using `%`.
4. Rewrite the contents of this chapter in your own words, otherwise your book is considered plagiarized. (You probably want to make a copy of this directory.) Note that you need not rewrite the questions in the exercises. You may retain the chapter and section organization (and their titles).
5. Every cipher in my notes must be present in your notes. You can add extra ciphers not found in my notes. (Example: enigma, playfair, etc.)
6. For each cipher, have a complete definition of each cipher and then have at least one example on encryption and decryption. Include definitions of terms. Your example(s) must be different from the examples in my notes.
7. You must write in proper English and using proper mathematical style.
8. Think of your notes as the only notes you can use in an open-book test or open-book final exam. Therefore you need not include historical or pedagogical remarks (but that's up to you).
9. Solve as many exercises as you can. The exercises are stored in directory `exercises`. For instance if you see `\input{exercises/abc/main.tex}`, this means the question of this exercise is stored in `\input{exercises/abc/question.tex}` and the answer should be written in `\input{exercises/abc/answer.tex}`
10. In terms of writing style, technically speaking, in formal writings, you should not use personal noun like "I". Instead, "we" should be used.

For instance instead of saying

"I will now prove my theorem."

you should write

"We will now prove the (or our) theorem."

I use "I" just to make my notes informal. For your book, you should use the formal writing style.

11. When you are done with this chapter, comment out this section of instructions.

The subtitle: Stuff that you should not use anymore.

However some of these old stuff is important because their ideas are used in modern-day cryptography.

Here we go ...

1.2 Shift cipher debug: classical-cipher-shift-cipher.tex

So first of all we need to establish is the mathematical representation of a cryptosystem.

A cryptosystem is made up of an Encrytpion function E(x, k) which usually requires a plaintext and a key to create a cipher text, and a decryption function D(x, k) which requires a ciphertext and a decryption key.

The feature of a good cryptosystem is then D(E(x), k) = x for a symmetric cipher so assuming is the domain for plaintext and the ciphertext is P and C so there is a bijection on the funtion $E : P \to C$ so that means that $D = E^{-1}$.

The Shift cipher is the general cipher name of the earliest cipher called the ceaser cipher. so how the cipher goes is that the key would be the amount of letters a character in the plaintext would shift hence the name shift cipher.

The encryption function would look like this $E(x, k) = x + k$. So in the actual cryptosystem the alphabets are in a domain of $\mathbb{Z} \pmod{26}$ so the encryption function will look like this $E(x, k) = x + k \pmod{26}$ and the decryption function would look like this $D(x, k) = x-k$ this is because to decryption would have to reverse the operation of the encryption. The is basically the trend of how most of the ciphers go we basically find the reverse of the encryption process

Now for an example lets assume we are trying to encrypt a message with the shift cipher. Assume our plaintext is s = "i am a really good boy i promise" and our key is shift by 3 first we would want to cleanup the plaintext by removing the spaces and only considering lowercase characters then we take all the letters one by one and shift all by the key 3 and also taking their mod 26. Then we consider the numerical representation of letters

i.e

$$a \to 0$$
$$b \to 1$$
$$c \to 2$$

and so on

So when shifting the letter when we have the first letter i the numeric representation of i is 8.

So applying the encryption function on i would be $8 + 3 = 11 \pmod{26}$ and in the cipher text the letter would be l

Applying this encryption process the ciphertext will look like this

`"ldpdjrrgerblsurplvh".`

1.3 Attacking the shift cipher debug: classical-cipher-attacking-shift-cipher.tex

Now its time to attack the shift cipher. When attacking a cipher one common method is to do a brute force search with powerful technologies, today we could search through huge key spaces in seconds, for example the key space of a shift cipher is 26 beacause you could shift each letter 26 different ways. So for our computers today brute force might be a quick method but the goal of having an optimizing technique is to learn how to make a heuristic approach to breaking ciphers.

So using heuristics we would need to have a public information theory fact i.e we look at the most commonly occuring letters in the English alphabets which is e. So with this we look at the most occuring letter in our cipher text then we can deduce that that letter is corresponding to the most occuring letter in the English language.

So we compute the relative shift of both letters if we assume that was encrypted to that letter.

Remember this works best for long cipher texts, with longer cipher texts the better and the more spread out the probabilities are.

The following is a table of probabilities for each letter used in English.

Letter	Probability
e	0.127
t	0.091
a	0.082
o	0.075
i	0.070
n	0.067
s	0.063
h	0.061
r	0.060
d	0.043
l	0.040
c	0.028
u	0.028
m	0.024
w	0.023
f	0.022
g	0.020
y	0.020
p	0.019
b	0.015
v	0.010
k	0.008
j	0.002
x	0.001
q	0.001
z	0.001

Here are the frequencies of the 2-grams (of course not all 2-grams, just the top few):

2-gram	Probability
th	0.0271
he	0.0233
in	0.0203
er	0.0178
an	0.0161
re	0.0141
es	0.0132
on	0.0132
st	0.0125
nt	0.0117
en	0.0113
at	0.0112
ed	0.0108
nd	0.0107
to	0.0107
or	0.0106
ea	0.0100
ti	0.0099
ar	0.0098
te	0.0098
ng	0.0089
al	0.0088
it	0.0088
as	0.0087
is	0.0086
ha	0.0083
et	0.0076
se	0.0073
ou	0.0072
of	0.0071

and the 3-grams:

3-gram	Probability
the	0.0181
and	0.0073
ing	0.0072
ent	0.0042
ion	0.0042
her	0.0036
for	0.0034
tha	0.0033
nth	0.0033
int	0.0032
ere	0.0031
tio	0.0031
ter	0.0030
est	0.0028
ers	0.0028
ati	0.0026
hat	0.0026
ate	0.0025
all	0.0025
eth	0.0024
hes	0.0024
ver	0.0024
his	0.0024
oft	0.0022
ith	0.0021
fth	0.0021
sth	0.0021
oth	0.0021
res	0.0021
ont	0.0020

and the 4-grams:

4-gram	Probability
tion	0.31
nthe	0.27
ther	0.24
that	0.21
ofth	0.19
fthe	0.19
thes	0.18
with	0.18
inth	0.17
atio	0.17
othe	0.16
tthe	0.16
dthe	0.15
ingt	0.15
ethe	0.15
sand	0.14
sthe	0.14
here	0.13
thec	0.13
ment	0.12
them	0.12
rthe	0.12
thep	0.11
from	0.10
this	0.10
ting	0.10
thei	0.10
ngth	0.10
ions	0.10
andt	0.10

1.4 Affine cipher debug: classical-cipher-affine-cipher.tex

With the knowledge from shift cipher and how easy it is to break a shift cipher so we could do better. So how can we complicate this by adding more keys So the premise of the affine cipher is having two keys instead of one key we could have like 2.

So we could represent this cipher in a mathematical expression E(x, (a, b)) = ax + b $\pmod{26}$ with keys being a and b.

This cipher is totally fine so far but lets try to come up with the decryption function.

So if the cipher text x' is x' = ax + b $\pmod{26}$
Then the plain text x will be x = x' $\cdot a^{-1} - b \cdot a^{-1} \pmod{26}$

What does the above imply. It implies for the a part of the key it has to have an inverse in order for the cryptosystem to work. So the key space of this cipher would be cardinality of the set of invertible numbers $\phi(26)$ which are the numbers co prime to 26 multiplied by 26.
Keyspace K = $\phi(26) \cdot 26$ which is larger than the keyspace of the shift cipher.

1.5 Attacking Affine Cipher

So Attacking this cipher is basically similar to the shift cipher i.e using the probabilities of letters. So with this information we can construct a system of equations if we find the what e (this most frequent letter) is encrypted to and what the t (the second most frequent letter) is encrypted to we construct a system of equation and solve for a and b.

So assuming we want to decrypt

```
fflqlghsfbqiwldqbgsklkhslmklybeyoklophsoleqgyldlilhyzslksbnqglhsy
fnlhmgfgslpmqllhsflulnsflylolqphsfllygsdlillhmklsosklkhslsibmvksk
lylnfvfsnqgmlypsklphslehqbslqxlhsflksjdlipleykllqplphyplhslxsbply
lolsgqpmqlfywmllpqlbqzslxqflifslslunbsfdlubblsgqpmqlktlylnlphyplq
lslvyfpmiubyfbotfesfslydhqffslplpqlhmkliqbntlvfsimksldupl yngmfydb
oldybylisnlgmlndldsfeyktlilpywslmptlphslgqkplvsfxsiplfsykqlmlclyl
nlqdksfzmlclgyihmlslphypfphsleqfbnlhyklkssltlduplyklylbqzsflhsleq
ubnlhyzslvbyisnlhmgksbxlmllyfxybkslvqkmpmqldldsllszsflkvqwslqxlph
slkqxpsflvykkmqlktlkyzslemphlylcmdsfylnlylklssfdllhsolesfslyngmfy
dbslphmlcklxqflphslqdksfzsfnsjisbbslplxqffnfyemlclphslzsmblxfqglg
```

```
slmklgqpmzsklylnlyipmqlkdlzuplxqflphslpfymlsnffsykqlsflpqlyngmplk
uihlmlpfukmqlklmlpqlhmklqellnsbmiypslylnlxmlsbofynrukpsnlpsgvsfyg
slpleyklpqlmlpfqnuislylnmkpfyipmlclxyipqflehmihlgmchpfphfqelylnqu
dpluvqllybblhmklgslpyblfskubpkdlyfmplmllylkslkmpmzsfmlkpfugslptlq
flylifyiwlmllqlslqxlhmklqellhmchyvqesflbslksktlequbnllqpfdslgqfsl
nmkpufdmlclphyllylkpfqlclsgqpmqllmllyllypufslkuihlyklhmkdlulnfosp
lphsfsleykldupqlsleqgyllpqlhmgtlylnlphypleqgylleyklphslbypslifsl
sfunbsftlqxlnudmquklylnlauskpmqlydbslgsgqfodf
```

we first have to get the frequency of the letters and get the highest frequent letter for this case that would be s appering 116 times and the second most frequent is p with 80 apperence this is done with a computer ofcourse. With that information we can construct the system of equation.

$$s = a \cdot e + b \pmod{26}$$
$$p = a \cdot t + b \pmod{26}$$

which is

$$18 = a \cdot 4 + b \pmod{26}$$
$$15 = a \cdot 19 + b \pmod{26}$$

then you solve and get a as 5 and b as 24.
Then the decrypted message will be:

```
tosherlockholmessheisalwaysthewomanihaveseldomheardhimmentionheru
nderanyothernameinhiseyessheeclipsesandpredominatesthewholeofhers
exitwasnotthathefeltanyemotionakintoloveforireneadlerallemotionsa
ndthatoneparticularlywereabhorrenttohiscoldprecisebutadmirablybal
ancedmindhewasitakeitthemostperfectreasoningandobservingmachineth
attheworldhasseenbutasaloverhewouldhaveplacedhimselfinafalseposit
ionheneverspokeofthesofterpassionssavewithagibeandasneertheywerea
dmirablethingsfortheobserverexcellentfordrawingtheveilfrommensmot
ivesandactionsbutforthetrainedreasonertoadmitsuchintrusionsintohi
sowndelicateandfinelyadjustedtemperamentwastointroduceadistractin
gfactorwhichmightthrowadoubtuponallhismentalresultsgritinasensiti
veinstrumentoracrackinoneofhisownhighpowerlenseswouldnotbemoredis
turbingthanastrongemotioninanaturesuchashisandyettherewasbutonewo
```

`mantohimandthatwomanwasthelateireneadlerofdubiousandquestionablem`
`emory`

1.6 Vigenère cipher debug: classical-cipher-vigenere-cipher.tex

To understand Vignere cipher you have to know what monoalphabetic and polyalphabetic ciphers are.

monoalphabetic ciphers are ciphers where each letters are mapped to a single character, example shift cipher and affine cipher. monoalphabetic ciphers

polyalphabetic ciphers are ciphers that could be mapped to different character. polyalphabetic ciphers

So you might be wondering how can you have a letter map to multiple characters, thats where vignere cipher comes in.

The premise of the Vignere cipher is to divide the plaintext and perform different shift ciphers on the amount of strings your plaintext is divided to.

Lets talk about the division of string and the key.
So the way the string is divided is based on the size of the string.
Assuming my plaintext is $x_1x_2x_3x_4x_5x_6\cdots$ and my key is $k_1k_2k_3k_4$. To divide this string we look at the size of the key which is 4 so all the strings will look like this.

$$s_1 = x_1x_5x_9x_{13}\cdots$$

$$s_2 = x_2x_6x_{10}x_{14}\cdots$$

$$s_3 = x_3x_7x_{11}x_{15}\cdots$$

$$s_4 = x_4x_8x_{12}x_{16}\cdots$$

Then encrypt it would be performing a shift cipher on all the strings with corresponding k's, so s_1 will be encrypted using k_1 and s_2 will be encypted using k_2 and so on.

The keyspace of the cipher is 26^l where l is the size of the plaintext.

Example 1.6.1. Given a String

```
I want to start by saying that I love you so much.
Being with you has been one of the greatest adventures
of my life and I will always hold you in my heart. I'm
sorry that things didn't work out the way we wanted them
to. We both tried our best, but at the end of the day,
trust was broken and there really isn't much we can do.
```

```
I hope you know that despite everything, I don't regret
being with you, nor do I regret giving you a second chance
after what you did. I know you meant it when you said you
were sorry and I know you tried your best to make things
right. I truly appreciate your effort. I am so honored to
have been a part of your life at all. You gave me so much
even when you had little to give. You were patient and kind
and never stopped trying to make me happy. You've taught me
to be a better, more understanding, and more open minded
person. You gave me a love that I will always remember and
for that, I am eternally grateful.
```

using key times divide and encrypt.

the first string s_1 would be

```
itratlouitheogevrmewlhoytrandrtynhwhdetefasbnheiuciyotieiogeiuorv
ochawoiyawoderdwrosaiitacyfiheaeroflgecnydliupnkneprtepuueaeerdne
mdogeeiasmntarye
```

second string s_2

```
wotyhoucnhanfrseeyaiwouhirtgnkhwteetosaetytraeascahowdtrnnritniei
uoafhukonhuyrriyiutkngrpiofaodvntuelashwolevwatidrpyompvgtbrusido
ipnaatwlrbdhmngf
```

third string s_3

```
asbiavshgysotetnslnlaliemytstoeeembruttnhtwonrlnhnouteeygtenhortn
anntadnutesoeykoerteghupauomnteaorayvoehuiteetannseimeyehoemntnmp
neyvlhiweefaearu
```

fourth string s_4

```
ntynteobwobnhaatoidlydnasthdwuwwdtoirbtderakdeltwdpkhsetirtgyregg
sdcetiominausanudbotstlrtrrsoobpfltoemvehtoyrindetdnahyttbtodagoe
droeoalamrottlal
```

and the fifth string s_5

```
tasgiymeiueeetduffiasymrohiiotaatotebuhodusetrymeoenapvhdebwodgiy
ecerydwetyiwonotyemhriyeeetorheayiaumuenatgoeedavotgkaoametrenarn
esumvtlyearielt
```

So Encrypting all the strings are whith the key times $shift(s_i, k_i)$

$shift(s_1, t)$:

```
bmktmehnbmaxhzxokfxpeahrmktgwkmrgapawxmxytlugaxbnvbrhmbxbhzxbnhko
hvatphbrtphwxkwpkhltbbmtvrybaxtxkhyezxvgrwebnigdgxikmxinnxtxxkwgx
fwhzxxbtlfgmtkrx
```

$shift(s_2, i)$

```
ewbgpwckvpivnzammgiqewcpqzbovspebmmbwaimbgbzimiakipwelbzvvzqbvqmq
cwinpcswvpcgzzqgqcbsvozxqwniwldvbcmtiapewtmdeibqlzxgwuxdobjzcaqlw
qxviibetzjlpuvon
```

$shift(s_3, m)$

```
menumhetskeafqfzexzxmxuqykfefaqqqyndgffztfiazdxztzagfqqksfqztadfzm
zzfmpzgfqeaqkwaqdfqstgbmgayzfqmadmkhaqtgufqqfmzzequyqkqtaqyzfzybzq
khxtuiqqrmqmdg
```

$shift(s_4, e)$

```
rxcrxisfasfrleexsmhpchrewxlhayaahxsmvfxhiveohipxahtolwixmvxkcvikkw
hgixmsqmreyweryhfsxwxpvxvvwssftjpxsiqzilxscvmrhixhrelcxxfxsheksihv
sisepeqvsxxpep
```

$shift(s_5, s)$

```
lskyaqewamwwwlvmxxaskqejgzaaglsslglwtmzgvmkwljqewgwfshnzvwtogvyaqw
uwjqvowlqaogfglqwezjaqwwwlgjzwsqasmemwfslygwwvsnglycsgsewljwfsjfwk
menldqwsjawdl
```

Then joining all those string together we have

```
bemrlmwexskbncktgurympmxaewhiqhcesenktfwbvsaampksmaiefwxvarwhnflwz
zqelxafevomzxmkmesxfgxmxxizhapqxpseemckawxhqhcurerpqejmqywgkzkxztb
flagoehawvfagksaylmpqasreqasgbqhlamyxgpmnslabdmwwwgvtxaffmmifxzxmz
hgybtivtgfvmlbiekuzaowgizhlamdijxixpqbazxenktawvizhgbpatwrwgofhefl
smlqwhbbqinxzkxzbvsmvhvfvwzzqxtxqzkobbtcgnvavvhqdiykmfkaoqzkqhcmww
vwzhuaizgwtnfijppmxqhcpmvbszsorwgqwtvfmlppqrqhceeawgayoxzqwgkzkefw
qwrgpgaylkqqhqhcdfwlbfsetsqxzbvswjbotxamzgpqtxbvwvqmxwrwgvwynavlbi
ywgawzsjxlfsztdqfwxvmtskbajqhcdpaymmxsetksmzihiexaaqmvpqzwgetifrwg
lswtuxlemfsybdqcgneqvwiifmwgbmrvdqzhsglzinxzexgixqhlkgurymwyecxuql
sixkcgndqxsnotxexbafwtjqxlxzysjxczhwkafefwqzksglysjxwbiffqzhwwxqvk
```

```
hvksmzihiexixsnxbtelbeupdttieqlzqqwfjqvsglrsjmpmxatuqxwkvmpdrodelx
ngp
```

1.7 Attacking Vignere cipher

So The first step of breaking this cipher is to determine the length of the string. Now like how we did for shift cipher we use a public information theory fact that is the sum of the square of all the frequency is approximately 0.065 in the english language this is denoted by I(s) which is the probabilty of choosing two random letters to be the same.
So the goal is to find length where each division of the string are approximately 0.065.

$$I(s) = \sum_{i=0}^{25} p_i^2$$

Example 1.7.1. Given a string

```
bemrlmwexskbncktgurympmxaewhiqhcesenktfwbvsaampksmaiefwxvarwhnflwz
zqelxafevomzxmkmesxfgxmxxizhapqxpseemckawxhqhcurerpqejmqywgkzkxztb
flagoehawvfagksaylmpqasreqasgbqhlamyxgpmnslabdmwwwgvtxaffmmifxzxmz
hgybtivtgfvmlbiekuzaowgizhlamdijxixpqbazxenktawvizhgbpatwrwgofhefl
smlqwhbbqinxzkxzbvsmvhvfvwzzqxtxqzkobbtcgnvavvhqdiykmfkaoqzkqhcmww
vwzhuaizgwtnfijppmxqhcpmvbszsorwgqwtvfmlppqrqhceeawgayoxzqwgkzkefw
qwrgpgaylkqqhqhcdfwlbfsetsqxzbvswjbotxamzgpqtxbvwvqmxwrwgvwynavlbi
ywgawzsjxlfsztdqfwxvmtskbajqhcdpaymmxsetksmzihiexaaqmvpqzwgetifrwg
lswtuxlemfsybdqcgneqvwiifmwgbmrvdqzhsglzinxzexgixqhlkgurymwyecxuql
sixkcgndqxsnotxexbafwtjqxlxzysjxczhwkafefwqzksglysjxwbiffqzhwwxqvk
hvksmzihiexixsnxbtelbeupdttieqlzqqwfjqvsglrsjmpmxatuqxwkvmpdrodelx
ngp
```

we need to find the key

computing the I(s) value of 10 different string length

```
Average I-value       keyLength
-------------------- -----------
0.0720190990494878          5
0.05674947924604988         9
0.05595853205769283         8
0.053815997799514285        7
0.0523394211228767          6
```

```
0.05027720641212229          4
0.04814645463936731          3
0.04680577532250629          2
0.04603145033973668          1
```

The closest value to 0.065 is key length 5 so we can assume that the key length is 5.

The next step is getting the relative shift of all the different strings. So the Theory is that we calculate the shift relative to the first string.

$k_1k_2k_3k_4k_5$ so the relative shift of the first string to the other strings would be given as

$k_2 = k_1 + sft_1 \pmod{26}$ and so on. We rotate the first string against the second string so the amount of rotations would give us the relative shift but the rotation that when we perform M(s_i, s_j) would be approximately 0.065.

This is to simulate I(s) so M(s_i, s_j) would be

$$\sum_{l=0}^{26} p_l p_{l+k_i-k_j}$$

$k_i - k_j$ is the relative shift.

Because if you shifted it back well you get almost the same probabilities of both strings.

Performing the above method

```
Index of key      M value      Relative Shift
-------------     -------      --------------
            1     0.05920                  11
            2     0.06788                   7
            3     0.06061                  15
            4     0.07052                   1
```

The equation for relative shift would be

$$k_1 - k_2 = 11 \pmod{26}$$

$$k_2 = k_1 - 11 \pmod{26}$$

$$k_2 = k_1 + 15 \pmod{26}$$

This means if $k_1 = 0$ then $k_2 = 15$ i.e if $k_1 = a$ then $k_2 = p$

Our key according to relative shift is [0, 15, 19, 11, 25]

with this information when we scan k_1 to be a - z we find that the key are as follows.

```
aptlz
bquma
crvnb
dswoc
etxpd
fuyqe
gvzrf
hwasg
ixbth
jycui
kzdvj
laewk
mbfxl
ncgym
odhzn
peiao
qfjbp
rgkcq
shldr
times
ujnft
vkogu
wlphv
xmqiw
ynrjx
zosky
```

To get k_1 we use frequency analysis on s_1 we see that the most frequent letter is x and the relative shift from x to e is 19 and that is relative shift from a to t so k_1 is the letter t.

When the k_1 is the letter t the key string would look like this

```
times
```

Using the assumed key to decrypt the ciphertext we get

```
iwanttostartbysayingthatiloveyousomuchbeingwithyouhasbeenoneoftheg
reatestadventuresofmylifeandiwillalwaysholdyouinmyheartimsorrythat
thingsdidntworkoutthewaywewantedthemtowebothtriedourbestbutattheen
dofthedaytrustwasbrokenandtherereallyisntmuchwecandoihopeyouknowth
atdespiteeverythingidontregretbeingwithyounordoiregretgivingyouase
condchanceafterwhatyoudidiknowyoumeantitwhenyousaidyouweresorryand
iknowyoutriedyourbesttomakethingsrightitrulyappreciateyoureffortia
msohonoredtohavebeenapartofyourlifeatallyougavemesomuchevenwhenyou
hadlittletogiveyouwerepatientandkindandneverstoppedtryingtomakemeh
appyyouvetaughtmetobeabettermoreunderstandingandmoreopenmindedpers
onyougavemealovethatiwillalwaysrememberandforthatiameternallygrateful
```

1.8 Substitution cipher debug: classical-cipher-substitution-cipher.tex

The substition cipher is a bit tricky to break, i will explain the premise of this cipher is that you have all the alphabets map to different alphabets. For example a could be mapped to e and f could be mapped to d and so on. The encryption is trivial but the decrytpion is difficult.

Example 1.8.1. The goal is to decrypt the following ciphertext (i.e., you need to compute the plaintext) and also to discover the key used. The substitution cipher is used.

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewm
hmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehq
ermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtx
lajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatlj
mwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqq
evjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlh
jggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamt
liammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqt
xltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmloji
akexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvat
kkmxnmh
```

Solution. The top few 1–gram frequencies of the ciphertext are

```
1gram: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30 ...
```

The gap between the frequency of `m` and `t` is extremely large. Therefore we suspect that part of the encryption is `e->m`. The rest, at least up to `x` are most probably from `t, a, o, i, n, s, h, r`:

$$\{\texttt{t, a, o, i, n, s, h, r}\} \to \{\texttt{t, q, h, j, e, i, a, x}\}$$

We can try different possible assignments on the above 8 letters to 8 letters, but that's $8! = 40320$ which is too big. At this point we have

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
-e--------------------e--------------e-----------e-e----------------------------e--e-e-----e--------

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
--------e-e------e-----e---e-e----------e---e-------e-----------e-------------e----e------e---------

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
-----------------e-----------e---e-------------e----------------e-e--e----e-----e---------e----e----

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
--ee-e--ee------------e---------e-----------------e-e--e----e----------------e-----e---e--ee----e---

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
---e--e-----------e---e-----e---e----e-----------------e--------------------e----e---------e----e---

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
------------------e---------------e----e----e------------------e------e----e--------e-----------e-e-

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
-------------------------------e----------e---e-e----ee-e--e-e---e-------e---e-------------e----e---

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
e--------------e------e--------e---e----------e--------e-----e-----e--e-e--e---e-------------------e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
--e-----e--e----e---e------e---------------e-e---------------------------e--------------------------

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e---e-------------e---------e-------------e---------e--e-

ciphertext
2-grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
         tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3-grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
         feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
plaintext
1-grams: e t a o i n s h r
2-grams: th he in er an re ed on es st en at to nt ha nd
         ou ea ng as or ti is et it ar te se hi of
3-grams: the ing and her ere ent tha nth was eth for dth
```

We now look at 2-grams and 3-grams.

The common 2-grams are `th, he, in, er, an, re, ed, on, es, st`. Since we are assuming `e->m`, `mh` is either from `er` or `ed` or `es`. Note that `er` and `re` are common 2-grams. We also note that `mh` and `hm` are high frequency 2-grams in the ciphertext. Note further that `ere` is a common 3-gram and `mhm` is also a common 3-gram in the ciphertext. We suspect that `h->r`. Therefore we now have

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
-e------r-----------r-e------r-------e-----------ere---------------------r------e--ere-----e------r-

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
--------e-e------e-r---e---e-e---------re--re---r---e-------r---e--------r----er---er-----er--------

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
-----------------e-----------e--re-------------e---------------re-e--e----e-----e--r------e--r-e----

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
--ee-er-ee------------e--------re-----------------e-er-e---re----------------e-----e---er-ee---re---

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
--re--e-----------er---e-----e---e----e-r---------------e----------r---------e--r-er---r----e----er--

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
------------------e---------------e----e----e----r-------------er-----e----e---r----e-----r-----ere-

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
-------r------------r----------er---------e--re-e----ee-e--ere---e-r-----er-re-------------er---e-r-

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er--r----------er-----er-------e--re----------er-------e-----e---rre--ere--e---er--r---------------e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
```

```
-re-----e--e----e---e--r---e--r-----------ere-----------------r---------e-------r--r---r-----------

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e---e------r-----re---------e----r-----r--e---r-----e--er

ciphertext
1grams: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30
2grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
        tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
        feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
plaintext
1grams: e t a o i n s h r
2grams: th he in er an re ed on es st en at to nt ha nd
        ou ea ng as or ti is et it ar te se hi of
3grams: the ing and her ere ent tha nth was eth for dth

e->m, r->h
```

Now we look for `the`. We have `the -> ??m`. The most commonly occurring ciphertext of this form is `iam`, `ewm`, `mhm`, `twm`. `mhm` is from `ere` which we already know so this is useless. So we are left with `iam`, `ewm`, `twm`. The frequency between `iam` and `ewm` is a huge 30% drop. So hopefully `the -> iam`. This means `t->i` and `h->a`. We have to take note of this since here we are creating two substitutions and the confidence is not as high. If we end up in a deadend, we will have to backtrack to this point. With the above two new substitutions, we have

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
-e--t---r-t-t--------r-e------r---t---e----------here---t-------------------r------e-tere-----e-t----r-

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
---t----e-e------e-r---e---e-e---------re--re---r---et-----tr---e--t--t--r---her---er-----er------t-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
--t----t---------e-----t-----e--re-t-----------e-----------------re-e--e----e-----e--r----t-e--r-e-t--

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
-heeher-ee------------e--------ret--t---t----t----eherhe-t-re-t-----t-------he-----e--her-ee-t-re---

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
--re-te-----------er--e---t-e---e----e-r--------------te--t-------r-------t-e--r-er---r--t-e--tter--

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
------------tt---he-------------e----e----e----r--------------her-----e-tt-e---r----e-----r----tere-

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
-------r--t---------rh--------her--------he--re-e--t-ee-e--ere---e-r-----er-re-t-----t--t-her---e-rh

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er--r-t-------her----ter-------e--re----------er-------e-t---e---rre--eret-e-t-er--rt--------------e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
-re----het-et---e--he--rt--e--r-----------here---t-------------rt--------e-------r--r---r-------h---

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e---e------r-t---re-------t-e--t-r-----r--e---r-----e--er
ciphertext
1grams: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30
2grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
        tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
        feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
plaintext
1grams: e t a o i n s h r
2grams: th he in er an re ed on es st en at to nt ha nd
        ou ea ng as or ti is et it ar te se hi of
3grams: the ing and her ere ent tha nth was eth for dth

e->m, r->h, t->i, h->a
```

`ent` is also a common plaintext trigram. This is encrypted as `m?i`. The only one that fits is `mqi` but the frequency of this is only 4 – so this is probably wrong.

Another high frequency plaintext 3-gram is `tha`. This would encrypt as `ia?`. We notice that `iam` has a high frequency. So perhaps `a->m`.

Now let's look at pairs of digrams.

`es,st` is a high frequency digram. This is encrypted as `m?,?i`. The only possibility is `mq,qi`. So we suspect `s->q`. This is what we have now:

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hes-t---r-t-t----h--r-eh-----r---t---e-h--h--s---ere---th----s---s-------r--s-s-e-tere-h-sse-ts---r-

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
---t----e-eh-s---e-r---e---e-e--s----s-re--re---rs--eth---str---e--t--t--rs---er---er-----ers-----t-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
-sth-s-t--sh-ss--e-h--ht-----es-re-th----h-ss--e---h-s----s----rese--eh-she----se--r---sthe--r-est-h

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
--ee-ersee------h-----e------s-reth-th-st--h-th---e-er-e-t-re-t-----t-----h--es----e---er-ee-t-re---

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
--reste-----sh----ersheh--the---e----e-r--h--h--ss----te--th---ss-r-------the--r-er---r--the--tters-

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
------s----stt-h--e-s-s-----------es---esh--e----r-------------erh-s-hesttheh--r--s-e-----r---stere-

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
-------r--t---------r------s---erh-s--ss--e--rehe--thee-es-ere---e-r-----er-re-t-----t--ts-er---e-r-

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er--r-t--------er---ster----h--es-re----sh----ers-----hest---e---rre--erethe-ther--rts--h---h--h---e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
-re-----ethet---es--e--rt--e--r---sh---s---ere---th---------h--rth-s-----e-------r--r---r-----------

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e---e------rst---ress-----the--t-r---s-r--ess-r-h---e--er

ciphertext
1grams: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30
2grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
        tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
        feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
        plaintext
1grams: e t a o i n s h r
2grams: th he in er an re ed on es st en at to nt ha nd
        ou ea ng as or ti is et it ar te se hi of
3grams: the ing and her ere ent tha nth was eth for dth

e->m, r->h, t->i, h->a, s->q
```

Note that `ti,is` is a common plaintext 2-gram. When encrypted, this is `i?,?q`. Unfortunately we can't find this pattern.

We now have enough substitutions to consider multiple cases of pairs of digrams.

Consider the common plaintext digram `aj,jq`. With what we have at this point, the encryption is `h?,?s -> aj,jq`. The possibilities for `h?,?s` are

- `he,es`: Therefore `e->j`, but `e` is already encrypted as `m`.
- `ha,as`: Therefore `a->j`.
- `hi,is`: Therefore `i->j`.

So we have `a->j` or `i->j`. Before we make a choice, let's consider more digrams.

Consider `h?,e?`. `h?,e?` might be encrypted as `at,mt`. Possibilities for `h?,e?`

- `hi,ei`: But `ei` is not common.
- `ha,ea`: Therefore `a->t`.

Therefore `a->t`.

Consider `h?,?r`. `h?,?r` might be encrypted to `at,th`. The only possibilities for `h?,?r` are

- `ha,ar`: Therefore `a->t`.
- `hi,ir`: But `ir` is not common.

Therefore `a->t`.

Consider `?s,e?`. `?s,e?` might be encrypted as `tq,mt`. The only possibility for `?s,e?` is `as,ea` which implies `a->t`.

`?s,e?` might be encrypted as `tq,th`. The only possibility for `?s,e?` is `as,ea` which implies `a->t`.

`e?,?r` might be encrypted to `mt,th`. The possibilities for `e?,?r` are

- `ed,rd`: But `rd` is not common.
- `es,sr`: But `sr` and `os` not common.
- `en,nr`: But `nr` is not common.
- `ea,ar`: Therefore `a->t`.
- `et,tr`: But `tr` is not common.

All in all, this case implies `a->t`.

From all the above cases, it seems that `a->t` and `i->j`. (The argument for `a->t` is stronger.) We now have

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hesati-ar-tati---hair-ehi--a-r-a-ta--e-hi-h-as---ere--ith----s-a-sa---ia-ra-sasie-tere-hisseats---r-

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
---t--a-e-ehisa--eara--e-a-e-e-as-i-as-re-are---rs--ethi--stra--e--t--t--rs---er---eri--a-ers--a-it-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
asthisit-ashissi-e-hi-ht-----es-reatha-a-hissi-ea--hisi---si---rese--ehishea--ase--r---sthe-ar-estih

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
a-ee-ersee-----ah--a--ei--ia-s-rethathist--hatha-ie-er-e-t-re-t----it-----ha-es-i--e---er-ee-tire--a

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
--reste-----sh----ersheha-the-a-ea---ear--hi-hiass--iate-itha-ass-ria-----the--r-er---ri-the-atters-

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
--a--asa---stt-ha-eas-s-i-i-------es-a-esha-e-a--ri---i--------erhis-hestthehair-as-e---iar--astere-

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
```

```
----i--r--ti-a------r-i---is---erhis-assi-e--rehea-thee-es-ere---e-ra----er-reat--a--t--ts-er---ear-

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er--riti-a-a---er--aster---ah--es-rea---sh----ersa--a-hest-i-ea-arre--erethe-ther-arts--hi--hi-ha--e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
are-a---etheta--esa-e--rt--e--r---sha--s---ere--ith------a--hairthisa--a-e----i--r-ari--r----i----i-

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e-a-e-----irsti--ressi----the--t-ri--s-r--ess-r-ha--e--er

ciphertext
1grams: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30
2grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
        tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
        feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
        plaintext
1grams: e t a o i n s h r
2grams: th he in er an re ed on es st en at to nt ha nd
        ou ea ng as or ti is et it ar te se hi of
3grams: the ing and her ere ent tha nth was eth for dth

e->m, r->h, t->i, h->a, s->q, a->t, i->j
```

At this point we can already see (possibly) "`he sat`" at line one and "`that his`" at line 4 and "`his -hest the hair`" at line 4 – perhaps "`chest`" is the second word?

Next, we try `tx,jx`. `a?,i?` might be encrypted as `tx,jx`. The possibilities for `a?,i?` are

- `an,in`: Therefore `n->x`.
- `ar,ir`: But `ir` is not common.

We get

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hesatinar-tatin--hair-ehin-a-r-a-ta--e-hi-h-as---ere--ith----s-a-san--ia-ra-sasientere-hisseats--nr-

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
-n-t--a-e-ehisa--earan-e-a-e-e-as-i-as-re-are---rs--ethin-stran-e--tn-t--rs---er---erin-a-ers-na-it-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
asthisit-ashissi-e-hi-ht----nes-reatha-a-hissi-ean-hisi---sin--resen-ehishea--asen-r---sthe-ar-estih

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
a-ee-erseen---nah--an-ein-ia-s-rethathist--hatha-ie-er-ent-re-t---nit-----ha-es-i--e---er-eentire--a

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
n-reste--n--sh----ersheha-the-a-ean--ear--hi-hiass--iate-ithanass-rian----the--r-er---ri-the-atters-

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
--a--asa---stt-ha-eas-s-i-i-n-----es-a-esha-e-an-ri---in----n--erhis-hestthehair-as-e---iar--astere-

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
---nin-r-ntina--n---r-in--is---erhis-assi-e--rehea-thee-es-ere---e-ra--n-er-reat--a--t--ts-er---ear-

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er--riti-a-an--er--aster---ah--es-rea---sh----ersan-a-hest-i-ea-arre--erethe-ther-arts--hi--hi-ha--e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
are-a---etheta--esa-e--rt--en-r---shan-s---ere--ith--n---a--hairthisan-a-e----in-r-arin-r----in---i-

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e-a-e-----irsti--ressi-n--then-t-ri--s-r--ess-r-ha--en-er

ciphertext
1grams: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30
2grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
        tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
        feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
        plaintext
1grams: e t a o i n s h r
2grams: th he in er an re ed on es st en at to nt ha nd
```

```
        ou ea ng as or ti is et it ar te se hi of
3grams: the ing and her ere ent tha nth was eth for dth

e->m, r->h, t->i, h->a, s->q, a->t, i->j, n->x
```

The beginning of the plaintext now reads "`he sat in a`." We now look at `xl`,`ml` and `ex`,`eh`.

`n?`,`e?` might be encrypted as `xl`,`ml`. The possibilities for `n?`,`e?` are

- `nt`,`et`: But `t` is already assigned.
- `nd`,`ed`: Therefore implies `d->l`.
- `ng`,`eg`: But `eg` is not common.

`?n`,`?r` might be encrypted as `ex`,`eh`. The possibilities for `?n`,`?r` are

- `in`,`ir`: But `i` is already assigned.
- `an`,`ar`: But `a` is already assigned.
- `on`,`or`: This implies `o->e`.
- `en`,`er`: But `e` is already assigned.

Adding `d->l` and `o->e`, we get

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hesatinarotatin--hair-ehinda-roadta--e-hi-h-as-o-ered-ith-oo-s-a-sanddia-ra-sasienteredhisseats--nro

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
-ndto-a-e-ehisa--earan-e-ade-e-as-i-as-re-ared-orso-ethin-stran-e--tnot-orsoo-er-o-erin-a-ersona-it-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
asthisit-ashissi-e-hi-htoo-ones-reatha-a-hissi-eandhisi--osin--resen-ehishead-asenor-o-sthe-ar-estih

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
a-ee-erseen--onah--an-ein-ia-s-rethathisto-hathadie-er-ent-redtodonit-o--dha-es-i--edo-er-eentire--a

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
ndrestedon--sho--dershehadthe-a-eand-eard-hi-hiasso-iate-ithanass-rian----the-or-er--oridthe-atterso

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
--a--asa--osttoha-eas-s-i-iono----es-adesha-edandri---in-do-no-erhis-hestthehair-as-e---iar--astered

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
do-nin-rontina-on---r-in--is-o-erhis-assi-e-oreheadthee-es-ere---e-ra--nder-reat--a--t--ts-er---ear-

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er--riti-a-and-er--aster---ah--es-reado-sho--dersanda-hest-i-ea-arre--eretheother-artso-hi--hi-ha--e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
areda-o-etheta--esa-e-ort-oenor-o-shands-o-ered-ith-on---a--hairthisanda-e--o-in-roarin-r----in--oi-

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e-ade-----irsti--ressiono-thenotorio-s-ro-essor-ha--en-er

ciphertext
1grams: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30
2grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
        tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
        feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
        plaintext
1grams: e t a o i n s h r
2grams: th he in er an re ed on es st en at to nt ha nd
        ou ea ng as or ti is et it ar te se hi of
3grams: the ing and her ere ent tha nth was eth for dth

e->m, r->h, t->i, h->a, s->q, a->t, i->j, n->x, d->l, o->e
```

The beginning reads "`he sat in a rotatin--hair-ehinda-road...`" which is very likely "`he sat in a rotating chair-ehinda-road...`", giving us `g->n` and `c->v`. This gives us

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hesatinarotatingchair-ehinda-roadta--e-hich-asco-ered-ith-oo-s-a-sanddiagra-sasienteredhisseats--nro

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
-ndto-ace-ehisa--earance-ade-egas-i-as-re-ared-orso-ethingstrange--tnot-orsoo-er-o-eringa-ersona-it-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
asthisit-ashissi-e-hichtoo-ones-reatha-a-hissi-eandhisi--osing-resencehishead-asenor-o-sthe-argestih

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
a-ee-erseen--onah--an-eingia-s-rethathisto-hathadie-er-ent-redtodonit-o--dha-es-i--edo-er-eentire--a

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
ndrestedon--sho--dershehadthe-aceand-eard-hichiassociate-ithanass-rian----the-or-er--oridthe-atterso

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
--ac-asa--osttoha-eas-s-iciono----es-adesha-edandri---ingdo-no-erhischestthehair-as-ec--iar--astered

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
do-nin-rontina-ongc-r-ing-is-o-erhis-assi-e-oreheadthee-es-ere---egra--ndergreat--ac-t--ts-er-c-ear-

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er-critica-and-er--aster---ah-ges-reado-sho--dersandachest-i-ea-arre--eretheother-artso-hi--hicha--e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
areda-o-etheta--esa-e-ort-oenor-o-shandsco-ered-ith-ong--ac-hairthisanda-e--o-ingroaringr----ing-oic

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
e-ade-----irsti--ressiono-thenotorio-s-ro-essorcha--enger

ciphertext
1grams: m:116 t:95 q:75 h:74 j:68 e:65 i:59 a:59 x:53 l:40 k:34 g:30
2grams: mh:25 ia:20 hm:20 aj:19 wm:18 at:16 am:16 tq:15 mq:15 xn:14
        tx:14 mt:14 jx:14 xl:12 qi:12 jq:12 th:11 ml:10 ex:10 eh:10
3grams: wmh:11 ajq:11 jxn:10 iam:10 txl:9 hml:7 ewm:7 mhm:6 otq:5 mhq:5
        feh: 5 twm: 4 qqj: 4 oaj: 4 mth:4 mqi:4 mia:4 jva:4 imh:4 iat:4
        plaintext
1grams: e t a o i n s h r
2grams: th he in er an re ed on es st en at to nt ha nd
        ou ea ng as or ti is et it ar te se hi of
3grams: the ing and her ere ent tha nth was eth for dth

e->m, r->h, t->i, h->a, s->q, a->t, i->j, n->x, d->l, o->e, g->n, c->v
```

Near the middle of the first line, "`-hich-asco-ered-ith`" is probably "`which-asco-eredwith`" giving us `w->o`.

On the second line "`orso-ethingstrange-`" is probably "`or something strange-`", giving us `m->r`.

On the third line "`sthe-argestiha-ee-erseen`" is probably "`s the largest i have ever seen`." This gives us `l->k` and `v->w`.

At this point we have

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hesatinarotatingchair-ehinda-roadta-lewhichwascoveredwith-oo-sma-sanddiagramsasienteredhisseats--nro

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
-ndto-acemehisa--earancemademegas-iwas-re-ared-orsomethingstrange--tnot-orsoover-oweringa-ersonalit-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
asthisitwashissi-ewhichtoo-ones-reathawa-hissi-eandhisim-osing-resencehisheadwasenormo-sthelargestih

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
aveeverseen--onah-man-eingiams-rethathisto-hathadievervent-redtodonitwo-ldhavesli--edovermeentirel-a
```

```
xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
ndrestedonm-sho-ldershehadthe-aceand-eardwhichiassociatewithanass-rian--llthe-ormer-loridthelatterso

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
-lac-asalmosttohaveas-s-iciono--l-es-adesha-edandri--lingdownoverhischestthehairwas-ec-liar-lastered

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
downin-rontinalongc-rvingwis-overhismassive-oreheadthee-eswere-l-egra--ndergreat-lac-t--tsver-clearv

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er-criticalandver-master--lah-ges-reado-sho-ldersandachestli-ea-arrelweretheother-artso-himwhicha--e

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
areda-ovetheta-lesave-ortwoenormo-shandscoveredwithlong-lac-hairthisanda-ellowingroaringr-m-lingvoic

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
emade--m--irstim-ressiono-thenotorio-s-ro-essorchallenger

e->m, r->h, t->i, h->a, s->q, a->t, i->j, n->x, d->l, o->e, g->n, c->v, w->o, m->r,
l->k, v->w
```

At the third line "`hisim-osing-resencehisheadwasenormo-sthelargestihaveeverseen`" is probably "`his imposing presence his head was enormous the largest i have ever seen`" giving us `p->g` and `u->b`.

At line 7, "`hismassive-orehead`" is "`his massive forehead`" giving us `f->f`.

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hesatinarotatingchair-ehinda-roadta-lewhichwascoveredwith-oo-smapsanddiagramsasienteredhisseatspunro

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
undtofacemehisappearancemademegaspiwaspreparedforsomethingstrange-utnotforsooverpoweringapersonalit-

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
asthisitwashissi-ewhichtoo-ones-reathawa-hissi-eandhisimposingpresencehisheadwasenormousthelargestih

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
aveeverseenuponahuman-eingiamsurethathistophathadieverventuredtodonitwouldhaveslippedovermeentirel-a

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
ndrestedonm-shouldershehadthefaceand-eardwhichiassociatewithanass-rian-ulltheformerfloridthelatterso

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
-lac-asalmosttohaveasuspicionof-luespadeshapedandripplingdownoverhischestthehairwaspeculiarplastered

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
downinfrontinalongcurvingwispoverhismassiveforeheadthee-eswere-luegra-undergreat-lac-tuftsver-clearv

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
er-criticalandver-masterfulahugespreadofshouldersandachestli-ea-arrelweretheotherpartsofhimwhichappe

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
areda-ovetheta-lesavefortwoenormoushandscoveredwithlong-lac-hairthisanda-ellowingroaringrum-lingvoic

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
emadeupm-firstimpressionofthenotoriousprofessorchallenger

e->m, r->h, t->i, h->a, s->q, a->t, i->j, n->x, d->l, o->e, g->n, c->v, w->o, m->r,
l->k, v->w, p->g, u->b, f->f
```

The beginning "`hesatinarotatingchair-ehinda-roadta-le`" is "`he sat in a rotating chair behind abroad table`" giving us `b->u`.

At line 5, "`restedonm-shoulder`" is "`rested on my shoulder`" giving us `y->s`.

At line 8, "`shouldersandachestli-ea-arrel`" is "`shoulders and a chest like a barrel`, giving us `k->c`.

At line 3, "`itwashissi-ewhichtookonesbreathaway`" is "`it was his size which took ones breath away`" giving us `z->p`.

We now have

```
amqtijxtheitijxnvatjhumajxltuhetlitukmoajvaotqvewmhmlojiaueecqrtgqtxlljtnhtrqtqjmximhmlajqqmtiqgbxhe
hesatinarotatingchairbehindabroadtablewhichwascoveredwithbooksmapsanddiagramsasienteredhisseatspunro

bxlieftvmrmajqtggmthtxvmrtlmrmntqgjotqghmgthmlfehqermiajxnqihtxnmubixeifehqeewmhgeomhjxntgmhqextkjis
undtofacemehisappearancemademegaspiwaspreparedforsomethingstrangebutnotforsooverpoweringapersonality

tqiajqjiotqajqqjpmoajvaieecexmquhmtiatotsajqqjpmtxlajqjrgeqjxnghmqmxvmajqamtlotqmxehrebqiamkthnmqija
asthisitwashissizewhichtookonesbreathawayhissizeandhisimposingpresencehisheadwasenormousthelargestih

twmmwmhqmmxbgextabrtxumjxnjtrqbhmiatiajqiegatiatljmwmhwmxibhmlielexjioebklatwmqkjggmlewmhrmmxijhmkst
aveeverseenuponahumanbeingiamsurethathistophathadieverventuredtodonitwouldhaveslippedovermeentirelya

xlhmqimlexrsqaebklmhqamatliamftvmtxlumthloajvajtqqevjtimojiatxtqqshjtxubkkiamfehrmhfkehjliamktiimhqe
ndrestedonmyshouldershehadthefaceandbeardwhichiassociatewithanassyrianbulltheformerfloridthelatterso

uktvctqtkreqiieatwmtqbqgjvjexefukbmqgtlmqatgmltxlhjggkjxnleoxewmhajqvamqiiamatjhotqgmvbkjthgktqimhml
blackasalmosttohaveasuspicionofbluespadeshapedandripplingdownoverhischestthehairwaspeculiarplastered

leoxjxfhexijxtkexnvbhwjxnojqgewmhajqrtqqjwmfehmamtliammsmqomhmukbmnhtsbxlmhnhmtiuktvcibfiqwmhsvkmthw
downinfrontinalongcurvingwispoverhismassiveforeheadtheeyeswerebluegrayundergreatblacktuftsveryclearv

mhsvhjijvtktxlwmhsrtqimhfbktabnmqghmtlefqaebklmhqtxltvamqikjcmtuthhmkomhmiameiamhgthiqefajroajvatggm
erycriticalandverymasterfulahugespreadofshouldersandachestlikeabarrelweretheotherpartsofhimwhichappe

thmltuewmiamitukmqtwmfehioemxehrebqatxlqvewmhmlojiakexnuktvcatjhiajqtxltumkkeojxnhethjxnhbrukjxnwejv
aredabovethetablesavefortwoenormoushandscoveredwithlongblackhairthisandabellowingroaringrumblingvoic

mrtlmbgrsfjhqijrghmqqjexefiamxeiehjebqghefmqqehvatkkmxnmh
emadeupmyfirstimpressionofthenotoriousprofessorchallenger

e->m, r->h, t->i, h->a, s->q, a->t, i->j, n->x, d->l, o->e, g->n, c->v, w->o, m->r,
l->k, v->w, p->g, u->b, f->f, b->b, y->s, k->c, z->p
q->q, x->x, j->j
```

Note that `q,x,j` were not used in the plaintext. We have added `q->q, x->x, j->j` to the substitution key. The following is the plaintext with spaces inserted (puncuations not restored):

> he sat in a rotating chair behind a broad table which was covered with books maps and diagrams as i entered his seat spun round to face me his appearance made me gasp i was prepared for something strange but not for so overpowering a personality as this it was his size which took ones breath away his size and his imposing presence his head was enormous the largest i have ever seen upon a human being i am sure that his tophat had i ever ventured to don it would have slipped over me entirely and rested on my shoulders he had the face and beard which i associate with an assyrian bull the former florid the latter so black as almost to have a suspicion of blue spade shaped and rippling down over his chest the hair was peculiar plastered down in front in a long curving wisp over his massive forehead the eyes were blue gray under great black tufts very clear very critical and very masterful a huge spread of shoulders and a chest like a barrel were the other parts of him which appeared above the table save for two enormous hands covered with long black hair this and a bellowing roaring rumbling voice made up my first impression of the

notorious professor challenger

□

The following programs are helpful (so go ahead and write them):

(a) Code to print the top 1-grams, 2-grams, 3-grams. The 1-grams will help determine the character that `e` is encrypted to. The trigrams might help determine what `the` is encrypted to.
(b) Given a character `c`, code that computes character(s) `d` such that `cd` and `dc` occurs most frequently. So if you suspect `e` is encrypted to `r`, your code will print all `x` such that `rx` and `xr` is common will be helpful in decoding `x`.
(c) Given a collection of common 2-grams (in plaintext), a partially specified substitution, compute pairs of commonly ocurring digrams of the form `xy,xz` or `xy,zx` or `xy,yz` or `xy,zy` (i.e., there are three distinct characters in the pairs of digrams) where two of the characters have already been decrypted and the remaining one has not and has not been assigned to a plaintext character.
(d) Instead of the above where there are two digrams, listing 4-grams where the decryption of 3 are known and one is unknown is also useful.

Index

Bibliography