Bachelor Informatica

Universiteit van Amsterdam

Information and Communication

Codebreaking for Traditional Cipher Systems

Abe Wiersma

10433120

7th February 2016

Supervisor(s): Christian Schaffner

Signed:

Abstract

In a time where Traditional Cipher systems have little to no value in keeping your secrets safe from others, what is their value in comparison to modern cryptography? This paper describes the breaking of several traditional ciphers, with the choices and tools used to get a decoded plain text.

Contents

CHAPTER 1

Introduction

The first cipher in recorded history was found in a tomb in Egypt[1] around 2000 B.C. A master scribe, in a town called Menet Khufu, sketched for the first time a hieroglyphic cipher using simple symbol substitutions. It might not have been to make the text unreadable, but to convey a sense of dignity and authority. The cipher text though is the first example of deliberate transformation of a piece of text. In the centuries that follow as the Egyptian civilization thrived, these transformations became more and more complicated.

In other civilizations cryptology also arose independently, but mostly died with the collapses of these civilizations. Sometimes cryptology would survive embedded in literature but more was lost than retained.

After being used decoratively, ciphers started getting used to transport secrets like war movements or government secrets. Only when the renaissance started in the western world, the knowledge of cryptology began taking leaps forward and cryptology was developed further than 'simple' substitution ciphers. Ciphers proclaimed to be unbreakable that were developed during this period failed to hold up long after computers where developed. The breaking of Enigma (a poly-alphabetic cipher) by the English during the second World War is a good example of this.

How hard is it for me, a computer science student with little beforehand cryptography experience, to break a few ciphers that have made for the course Information Theory at the Institute for Logic, Language and Computation in Amsterdam? When explaining how the cipher was broken is finished, traditional and modern cryptography will be related to each other.

CHAPTER 2

Breaking Traditional Ciphers

Where the early Egyptian ciphers could be broken just by looking at them a bit longer[1], later ciphers became harder and harder to crack by hand. Where early code breaking machines were made with one goal cipher, I have to my disposal the Internet and the high level computer language Python, which are the tools I used to break these ciphers:

- Subsitution cipher
- Permutation cipher
- Subsitution and Permutation cipher
- Polyalphabetic cipher

In this paper the theory behind the Ciphers is discussed first an Example is given, and then a cipher made from a plain text from project Gutenberg and a unknown ciphering is broken. After which the flaws of the cipher in particular are discussed.

2.1 Substitution Cipher

A substitution cipher replaces characters of a plain text with the characters of a cipher text, following a fixed replacement system. The characters may be encoded from single characters to single cipher characters, but one can encode to many or many can encode to one, also. For example $A \rightarrow BC$ and $AB \rightarrow C$. A receiver can decipher the text by performing the inverse substitution.

Example
A nice example of a substitution cipher is the Caesar cipher, in which a regular latin alphabet is shifted n places to encode a plaintext.

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:	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	a

This cipher can encode a plaintext to be unreadable at first glance:

plaintext:	defend	the	east	wall	of	the	castle
ciphertext:	efgfoe	uif	fbtu	xbmm	pg	uif	dbtumf

But if you think about the cipher for a bit longer you can see that there are only 26 possible shifts, which is so small that you can manage to write out the possibilities by hand. The result is that the only security comes from the obscurity of the cipher.

Luckily though not all substitution ciphers are this simple to decrypt, substitution ciphers can permute, shift and replace the characters of a cipher alphabet to obscure a cipher text.

Problem
A substitution problem was provided as part of an old Information Theory course by Mathias Winther Madsen. For this course he made several cipher texts from Gutenberg plain text. For each of them the information of origin language and cipher type was provided with the cipher.

As a substitution cipher Mathias provided with this cipher text:

```
RVRZF19;:-P:8OP-8RHP8:PL1P19RP-LYY8 DP19RZRP;HPLPZL;YOLFPH RRWP;:P19RPH1;ZZ
;:-P8EP19RPS;:WCP:81PYRHHP19L:P;:P19RPS8VRSR:1P8EP19RP78W;RHP8EPSR:DP19RPH8N
;LYPL:WP 8Y;1;NLYP LHH;8:HP9LVRPLNMI;ZRWPHIN9P;:1R:H;1FCPL:WP7RR:PH8PO;
WRYFPW;EEIHRWCP19L1P19R;ZP;:RV;1L7YRPZRHIY1HPLZRPLYS8H1P;SSRW;L1RYFP
Z8WINRWDP19RP RZ;8WP8EPHRRWA1;SRPL:WP9LZVRH1P9LHP7RN8SRPLHPH98Z1P;:P 8Y;1;
NLYPLHP;1P;HP;:PL-Z;NIY1IZLYPYL78IZDPLPH;:-YRPFRLZP7Z;:-HP;1HPL  Z8 Z;
L1RPEZI;1HP18PSL1IZ;1FP;:P19RPS8ZLYPLHP;:P19RP 9FH;NLYPO8ZYWDPR;-91
FPFRLZHPRYL HRWP;:PZ8SRPEZ8SP19RP1;SRPO9R:P19RP 8Y;1;NLYP LHH;8:HPORZRPE;
ZH1PH1;ZZRWP7FP1;7RZ;IHP-ZLNN9IHCP7RE8ZRP;1HPI:ZIYFPN;1;KR:HPORZRPE;:
LYYFPHI7WIRWP7FP19RPLZ1CP8ZPWRN;SL1RWP7FP19RPNZIRY1FP8EP8N1LV;IHDPR:-YL:WPI:
WRZOR:1PH;XPFRLZHP8EPN;V;YPOLZPL:WPHIEERZ;:-CP7RE8ZRP19RPLS7;1;8:PL:WPSLW:
RHHP8EP19RPY8:-P LZY;LSR:1PORZRPRX RYYRWP7FP19RP IZ-RP8EP Z;
WRCP8ZPNZIH9RWP7FP19RPHO8ZWP8EPNZ8SORYYBP1ORYVRPFRLZHPRYL HRWP7R1ORR:P19RPN8
:V8NL1;8:P8EP19RPH1L1RHA-R:RZLYP;:P,U.GCPL:WP19RPRX1;:N1;8:P8EP19RPY;NR:
HRP8EP19RPEZR:N9PZRV8YI1;8:P7FP19RPLZSP8EP:L 8YR8:DP7I1CP8:P19;HP8NNLH;8:CP
;:P8:RPFRLZCPLYYCP;:P19RPSRL:1;SRPL1PYRLH1CP9LHP7RR:PLNN8S Y;
H9RWDPRZRP19RPYRLVRHCPO9;N9PI:E8YWRWP;:PH Z;:-PLS;WH1P19RP8VRZ19Z8OP8EP19Z8:
RHCPL:WP19RP1ZL:H 8Z1HP8EPZRV8YI1;8:;H1HP8VRZP19RPO8ZYWCP9LWPELYYR:P;:PLI1IS
:CP19RP LHH;8:HPO9;N9P9LWPN8:VIYHRWPSL:T;:WPORZRPNZIH9RWPE8ZP19RP1;SRCPL:
WP19RP1Z;IS 9HP8EPWRS8NZLNFPORZRPLZZRH1RWDPLP1RZZ;7YRPZRLN1;8:P9LWPHR1P;:
QPRX RZ;R:NRP8EPHIEERZ;:-P9LWPW8:RP;1HPO8ZTQPL:WPHO;E1PLHP19RPH9LWRHP8EP
:;-91P7RE8ZRP19RPZLFHP8EP19RPLHNR:W;:-PHI:CP9LWPW;HL  RLZRWP19RPERZSR:1
P8EPZRV8YI1;8:P7RE8ZRP19RPLZ8IHRWP;:W;-:L1;8:P8EP19RPI:N8ZZI 1RWP LZ1P8EPSL:
T;:WDP19RPHLSRP LHH;8:HPSLFPL-L;:PLZ;HRQP19RPHLSRPWRYIH;8:HPL-L;:PH
ZRLWCPLHPH;:PH Z;:-HPI PLEZRH9P;:PHINNRHH;VRP-R:RZL1;8:HP8EPSR:QP7I1PORPT:8
OP19RPZRHIY1DP19RFPO;YYCPY;TRP19RPOLFHP8EP19RPI:Z;-91R8IHCP7RPL-L;:PNZIH9RWD
```

Listing 2.1: Substitution Cipher provided by Mathias

If the cipher type was unknown, it would've been possible to deduce it by looking at the frequency table. Conversely if the origin language were unknown, but the cipher type was known; by looking at the frequency table the similarities between the English language and the table would be apparent.

Gutenberg frequency table[2]

Character	Frequency in %
e	12.58
t	9.085
a	8.000
o	7.591
i	6.920
n	6.904
s	6.340
h	6.237
r	5.959
d	4.317
l	4.057
u	2.841
c	2.575
m	2.560
f	2.350
w	2.224
g	1.982
y	1.900
p	1.795
b	1.535
v	0.981
k	0.739
x	0.179
j	0.145
q	0.117
z	0.079

Listing 2.2: Frequency table of numerous collected works in the Gutenberg library. [2]

Substitution frequency table

Character	Frequency in %
p	16.86
r	10.83
1	6.723
;	6.296
l	6.083
h	5.869
:	5.763
8	5.336
z	5.336
9	4.268
w	3.361
y	3.201
i	2.401
e	2.401
n	2.187
s	1.867
	1.814
f	1.440
o	1.387
-	1.334
7	1.334
c	1.173
v	0.907
d	0.640
t	0.266
x	0.213
q	0.213
a	0.106
.	0.053
,	0.053
k	0.053
b	0.053
u	0.053
g	0.053
m	0.053

Listing 2.3: Frequency table of the substitution Cipher.

As seen in the frequency tables 2.2 and 2.3 the alphabet of the cipher text is quite a lot bigger than the Gutenberg frequency reference I used. This causes the English alphabet to increase from 26 characters to 35 in this case, because of usage of punctuation marks.
Space is the most used character in the English language so I replaced the P, with a space. Then in the English language the letter e is second most common, so I replaced the R with an e.

```
eVeZF19;:- :8O -8eH 8: L1 19e -LYY8 D 19eZe ;H L ZL;YOLF H eeW ;: 19e H1;ZZ
;:- 8E 19e S;:WC :81 YeHH 19L: ;: 19e S8VeSe:1 8E 19e 78W;eH 8E Se:D 19e H8N
;LY L:W  8Y;1;NLY  LHH;8:H 9LVe LNMI;ZeW HIN9 ;:1e:H;1FC L:W 7ee: H8 O;WeYF
W;EEIHeWC 19L1 19e;Z ;:eV;1L7Ye ZeHIY1H LZe LYS8H1 ;SSeW;L1eYF  Z8WINeWD 19e
  eZ;8W 8E HeeWA1;Se L:W 9LZVeH1 9LH 7eN8Se LH H98Z1 ;:  8Y;1;NLY LH ;1 ;H
;: L-Z;NIY1IZLY YL78IZD L H;:-Ye FeLZ 7Z;:-H ;1H L  Z8 Z;L1e EZI;1H 18 SL1IZ
;1F ;: 19e S8ZLY LH ;: 19e  9FH;NLY O8ZYWD e;-91F FeLZH eYL HeW ;: Z8Se EZ8S
 19e 1;Se O9e: 19e  8Y;1;NLY  LHH;8:H OeZe E;ZH1 H1;ZZeW 7F 1;7eZ;IH -
ZLNN9IHC 7eE8Ze ;1H I:ZIYF N;1;Ke:H OeZe E;:LYYF HI7WIeW 7F 19e LZ1C 8Z WeN;
SL1eW 7F 19e NZIeY1F 8E 8N1LV;IHD e:-YL:W I:WeZOe:1 H;X FeLZH 8E N;V;Y OLZ L
:W HIEEeZ;:-C 7eE8Ze 19e LS7;1;8: L:W SLW:eHH 8E 19e Y8:-  LZY;LSe:1 OeZe eX
 eYYeW 7F 19e  IZ-e 8E  Z;WeC 8Z NZIH9eW 7F 19e HO8ZW 8E NZ8SOeYYB 1OeYVe
FeLZH eYL HeW 7e1Oee: 19e N8:V8NL1;8: 8E 19e H1L1eHA-e:eZLY ;: ,U.GC L:W 19e
 eX1;:N1;8: 8E 19e Y;Ne:He 8E 19e EZe:N9 ZeV8YI1;8: 7F 19e LZS 8E :L 8Ye8:D
7I1C 8: 19;H 8NNLH;8:C ;: 8:e FeLZC LYYC ;: 19e SeL:1;Se L1 YeLH1C 9LH 7ee:
LNN8S Y;H9eWD eZe 19e YeLVeHC O9;N9 I:E8YWeW ;: H Z;:- LS;WH1 19e 8VeZ19Z8O
8E 19Z8:eHC L:W 19e 1ZL:H 8Z1H 8E ZeV8YI1;8:;H1H 8VeZ 19e O8ZYWC 9LW ELYYe:
;: LI1IS:C 19e  LHH;8:H O9;N9 9LW N8:VIYHeW SL:T;:W OeZe NZIH9eW E8Z 19e 1;
SeC L:W 19e 1Z;IS 9H 8E WeS8NZLNF OeZe LZZeH1eWD L 1eZZ;7Ye ZeLN1;8: 9LW He1
 ;:Q eX eZ;e:Ne 8E HIEEeZ;:- 9LW W8:e ;1H O8ZTQ L:W HO;E1 LH 19e H9LWeH 8E
:;-91 7eE8Ze 19e ZLFH 8E 19e LHNe:W;:- HI:C 9LW W;HL  eLZeW 19e EeZSe:1 8E
ZeV8YI1;8: 7eE8Ze 19e LZ8IHeW ;:W;-:L1;8: 8E 19e I:N8ZZI 1eW  LZ1 8E SL:T;:
WD 19e HLSe  LHH;8:H SLF L-L;: LZ;HeQ 19e HLSe WeYIH;8:H L-L;: H ZeLWC LH H
;: H Z;:-H I  LEZeH9 ;: HINNeHH;Ve -e:eZL1;8:H 8E Se:Q 7I1 Oe T:8O 19e
ZeHIY1D 19eF O;YYC Y;Te 19e OLFH 8E 19e I:Z;-91e8IHC 7e L-L;: NZIH9eWD
```

Listing 2.4: Substitution Cipher provided by Mathias, with p and r replaced

At this step some patterns become visible as words mostly have the right length, and trigrams can be spotted. A Trigram is a combination of three characters making up part of or a whole word. The most common trigram in the English language is ‘the’, so ‘19e’, a Trigram found often in this cipher text, is probably corresponding to ‘the’.

```
eVeZFth;:- :8O -8eH 8: Lt the -LYY8 D theZe ;H L ZL;YOLF H eeW ;: the Ht;ZZ
;:- 8E the S;:WC :8t YeHH thL: ;: the S8VeSe:t 8E the 78W;eH 8E Se:D the H8N
;LY L:W  8Y;t;NLY  LHH;8:H hLVe LNMI;ZeW HINh ;:te:H;tFC L:W 7ee: H8 O;WeYF
W;EEIHeWC thLt the;Z ;:eV;tL7Ye ZeHIYtH LZe LYS8Ht ;SSeW;LteYF  Z8WINeWD the
  eZ;8W 8E HeeWAt;Se L:W hLZVeHt hLH 7eN8Se LH Hh8Zt ;:  8Y;t;NLY LH ;t ;H
;: L-Z;NIYtIZLY YL78IZD L H;:-Ye FeLZ 7Z;:-H ;tH L  Z8 Z;Lte EZI;tH t8 SLtIZ
;tF ;: the S8ZLY LH ;: the  hFH;NLY O8ZYWD e;-htF FeLZH eYL HeW ;: Z8Se EZ8S
 the t;Se Ohe: the  8Y;t;NLY  LHH;8:H OeZe E;ZHt Ht;ZZeW 7F t;7eZ;IH -
ZLNNhIHC 7eE8Ze ;tH I:ZIYF N;t;Ke:H OeZe E;:LYYF HI7WIeW 7F the LZtC 8Z WeN;
SLteW 7F the NZIeYtF 8E 8NtLV;IHD e:-YL:W I:WeZOe:t H;X FeLZH 8E N;V;Y OLZ L
:W HIEEeZ;:-C 7eE8Ze the LS7;t;8: L:W SLW:eHH 8E the Y8:-  LZY;LSe:t OeZe eX
 eYYeW 7F the  IZ-e 8E  Z;WeC 8Z NZIHheW 7F the HO8ZW 8E NZ8SOeYYB tOeYVe
FeLZH eYL HeW 7etOee: the N8:V8NLt;8: 8E the HtLteHA-e:eZLY ;: ,U.GC L:W the
 eXt;:Nt;8: 8E the Y;Ne:He 8E the EZe:Nh ZeV8YIt;8: 7F the LZS 8E :L 8Ye8:D
7ItC 8: th;H 8NNLH;8:C ;: 8:e FeLZC LYYC ;: the SeL:t;Se Lt YeLHtC hLH 7ee:
LNN8S Y;HheWD eZe the YeLVeHC Oh;Nh I:E8YWeW ;: H Z;:- LS;WHt the 8VeZthZ8O
8E thZ8:eHC L:W the tZL:H 8ZtH 8E ZeV8YIt;8:;HtH 8VeZ the O8ZYWC hLW ELYYe:
;: LItIS:C the  LHH;8:H Oh;Nh hLW N8:VIYHeW SL:T;:W OeZe NZIHheW E8Z the t;
SeC L:W the tZ;IS hH 8E WeS8NZLNF OeZe LZZeHteWD L teZZ;7Ye ZeLNt;8: hLW Het
 ;:Q eX eZ;e:Ne 8E HIEEeZ;:- hLW W8:e ;tH O8ZTQ L:W HO;Et LH the HhLWeH 8E
:;-ht 7eE8Ze the ZLFH 8E the LHNe:W;:- HI:C hLW W;HL  eLZeW the EeZSe:t 8E
ZeV8YIt;8: 7eE8Ze the LZ8IHeW ;:W;-:Lt;8: 8E the I:N8ZZI teW  LZt 8E SL:T;:
WD the HLSe  LHH;8:H SLF L-L;: LZ;HeQ the HLSe WeYIH;8:H L-L;: H ZeLWC LH H
;: H Z;:-H I  LEZeHh ;: HINNeHH;Ve -e:eZLt;8:H 8E Se:Q 7It Oe T:8O the
ZeHIYtD theF O;YYC Y;Te the OLFH 8E the I:Z;-hte8IHC 7e L-L;: NZIHheWD
```

Listing 2.5: Substitution Cipher provided by Mathias, 'the' trigram identified

I used a mixture of substitution and filling to make sense piece by piece.

```
e_e__th___ ___ __e_ __ _t the _______ the_e __ _ _______ __ee_ __ the
_t______ __ the _____ __t _e__ th__ __ the ___e_e_t __ the ____e_ __ _e__
the ______ ___ ____t____ ________ h__e ______e_ ___h __te___t__ ___ _ee_ __
___e__ ______e__ th_t the__ __e__t___e _e___t_ __e _____t ___e___te__
______e__ the _e____ __ _ee__t__e ___ h___e_t h__ _e___e __ _h__t __
____t____ __ _t __ __ _______t____ _______ _ _____e _e__ ______ _t_
_________te ____t_ t_ __t___t_ __ the _____ __ __ the _h______ ______ e__ht_
 _e___ e____e_ __ ___e ____ the t__e _he_ the ____t____ ________ _e_e ____t
_t___e_ __ t__e____ _____h___ _e___e _t_ ______ __t__e__ _e_e _______
_____e_ __ the __t_ __ _e____te_ __ the ___e_t_ __ __t______ e______
___e__e_t ___ _e___ __ _____ ___ ___ ____e_____ _e___e the ____t___ ___
____e__ __ the ____ _______e_t _e_e e__e__e_ __ the ____e __ ____e_ __
____he_ __ the _____ __ _____e___ t_e__e _e___ e____e_ _et_ee_ the
_______t___ __ the _t_te___e_e___ __ _____ ___ the e_t___t___ __ the ___e__e
 __ the __e__h _e____t___ __ the ___ __ _____e___ __t_ __ th__ _________ __
__e _e___ ____ __ the _e__t__e _t _e__t_ h__ _ee_ _________he__ e_e the
_e__e__ _h__h ______e_ __ ______ _____t the __e_th___ __ th___e__ ___ the
t_______t_ __ _e____t_____t_ __e_ the ______ h__ ____e_ __ __t____ the
________ _h__h h__ _______e_ _______ _e_e ____he_ ___ the t__e_ ___ the
t_____h_ __ _e_______ _e_e ___e_te__ _ te_____e _e__t___ h__ _et ___
e__e__e__e __ ____e____ h__ ___e _t_ _____ ___ ____t __ the _h__e_ __ ___ht
_e___e the ____ __ the ___e_____ ____ h__ ______e__e_ the _e__e_t __
_e____t___ _e___e the _____e_ _______t___ __ the ________te_ ___t __
________ the ___e ________ ___ _____ _____e_ the ___e _e_______ _____ ___e___
 __ ___ _______ __ ___e_h __ ____e____e _e_e__t____ __ _e__ __t _e ____ the
_e___t_ the_ _____ ___e the ____ __ the _____hte____ _e _____ ____he__
```

Listing 2.6: Plaintext(decrypted),'the' trigram identified

At this point multiple vowels and consonants can be substituted because of incomplete words like the_e th__ th_t, and frequencies fitting these substituting vowels and consonants.

Switching between substitution and mixing, more words like i_, and _tirri__, and ha_e seem to fit common English words. And so piece by piece an English text is retrieved:

```
everything now goes on at the gallop. there is a railway speed in the
stirring of the mind, not less than in the movement of the bodies of men.
the social and political passions have acquired such intensity, and been so
widely diffused, that their inevitable results are almost immediately
produced. the period of seed-time and harvest has become as short in
political as it is in agricultural labour. a single year brings its
appropriate fruits to maturity in the moral as in the physical world. eighty
 years elapsed in rome from the time when the political passions were first
stirred by tiberius gracchus, before its unruly citizens were finally
subdued by the art, or decimated by the cruelty of octavius. england
underwent six years of civil war and suffering, before the ambition and
madness of the long parliament were expelled by the purge of pride, or
crushed by the sword of cromwell: twelve years elapsed between the
convocation of the states-general in 1789, and the extinction of the license
 of the french revolution by the arm of napoleon. but, on this occasion, in
one year, all, in the meantime at least, has been accomplished. ere the
leaves, which unfolded in spring amidst the overthrow of thrones, and the
transports of revolutionists over the world, had fallen in autumn, the
passions which had convulsed mankind were crushed for the time, and the
triumphs of democracy were arrested. a terrible reaction had set in;
experience of suffering had done its work; and swift as the shades of night
before the rays of the ascending sun, had disappeared the ferment of
revolution before the aroused indignation of the uncorrupted part of mankind
. the same passions may again arise; the same delusions again spread, as sin
 springs up afresh in successive generations of men; but we know the result.
 they will, like the ways of the unrighteous, be again crushed.
```

Listing 2.7: Plaintext(solution): BLACKWOOD'S MAGAZINE, Jan. 1845

The complete cipher alphabet that was found is:

```
Plain:   abcdefghiklmnopqrstuvwxyz ,-.1789:;
Cipher:  -:,.fy9suzaqcwp;rmk7vdxlrp1g8tbohni
```

Vulnerabilities
The problem with this cipher is that with frequency analysis and knowledge of English words, these texts can be decoded fast. This is because the character frequency distribution remains similar to the original one.

2.2 Permutation Cipher

A Permutation Cipher is a Cipher that scrambles characters of a plain text in blocks of a fixed length. The Permutation cipher is part of the transposition cipher family. Transposition ciphers permute characters using a bijective function to encode and decode using the inverse function.

Example
An example of a permutation cipher in which a piece of plain text is encoded with the key: *5406312*. The key encodes blocks of 7 characters long.

```
Plain:   This is a test
Cipher:  iis hTs stea t
```

Problem
The permutation problem was provided by Mathias Winther Madsen. This cipher again finds it's origin from the Gutenberg library.

```
INTBUI BRETHMH ESTIFE, RPIEA C ORPRY UNTT, ITASES BA HRTHO EN HLYGOUTERSDUNY, BDOOFN OE M NSEE S
ALL OFSTIERPA HATT, GHANCA YF DOE ITY SNAOUT OS QHE TF NTIOSUETND A, E THTHANIS  REREFORO HORTWM
NNTEO COG FNDIHN TIR ETATSE HHICW, T NOS I  BEO TEECTFEFHY TBD SEANME  ICHH WN COETHITUTISTEITS ON
HAS LFEVIDOPRSTHI D.CNVIO CLN, OTIP IMGON SEDSREHN TOUPOATINE  AND N,OERWTIN  ASNVEEWER ITTTH I
WYVER HEWAMER F  OFKORI BRETHIH MSTIV HA,NDM COGINOO CTE  IDECINHH TTWIIASSPE C INSONTNT EIDYARTPO
IVISI D  INSON REEFA  TE,AST  INSHASCESOPRM TIF OURODPE E THDCEGRANT STND AE SUOUTORYLICO P,ICHH
WBR AO FQ A EOV TERRUAEA C OF RY,UNTW NOSHAFEN E BDOWELOLI THN ITOUNCS TBY  RYEGOV HE,ENTMRNAD LN
AOD TEUDKE SH T  BYSIEO WHETHELIB LER PALRATON  TYTCON HE NT.EINERIVPDEHF TOD HATCWE ODS RWO EN,MF
R PAETHAS HETIECOM VES ASO TO THEUMTOF  SE GS.NHICANIGORC SOR OA CHLIAV HAENGMECOBE WHE TE  CRY-
ARTFAC OFN, INIOOAD ESTGHANCF YF DOE  TY.SNAT NAETH  ISNIOGLON NONDRE ERID WECHOBLO THRY ABD IS
FEMI INGTGHE THRFORD OE RHE WH TS ROEITPBY  E, IESTARNIVIRSTTOR FG TMAS HET BEYERHN TEWERTUASE HND
AT  VEROANEILIMFA BUT S, WAS ITS LETNOOHORTS DLY HUG DEDIIV THE BY  OFYCRIE BH"TE TH,LL OLEH WAL,
LBIHNOT NDT BUGINIE BH TT" A,LLIE TN OD AN,MEOAT H TEFRE"F  ADER-TE CHDANNCOR APNT AA"  ER.HOT
IALCSO,NGEACHATERL AONS OTICOLIPF EHAV Y,CUS H T  TOEOM THE BEOAT EGR CTSEBJDCH IWHTDE IIVINAT HED
AN;ONTS IA, E EVS IPHE TR OCY IOLSPPOOF TON IITEEPRRO HT TNSEUONDCE GOF  CTERNMEOVEAS  NTUNEOORRFIT
  S,,OWSLOLN A S ARSSAEECEONSCY ,NCEEQUTAT H TNMAI HETFORF EHF TOS YARTPE EPOSP ODO ATD RISTNMIAON
IATHYS ALWE BEEAVCSIN N,SHE TE SRESPUP  OFNIOB REETH IONLEL5174 INFO ET, WT, CFE  INNHETOSIPOP ,
ANIO NGEACHEGEN INI OPLRAAN, ONIE WH,NDON PIN O, TRWE RRYA CHT CATHNE IGANEEFF TOABY  CTEANGH CL
POF OH. TYICLLD OE NOF  AWIRE UATLTILSS E OPN I.IONTRANTIOC AED RN A IONTACAE MLRU ND;INK  INDANF
EFETHFS OTORERTIA PAUTUMS  TOYLLNPLAPSU ACHET IER HOTROWEPN U FOA, NTIOANDI LAS IAOR FD RNTIEN
GHANCE OF POE TY ACLIDATET SDRIOE P AND S,EALT AN,IONTRAE GRS AFAS  ATG NIMRODTO  HT  IN,AYI
OPETHANS ONIIPOL NDTOF  CYIRUL HETPAR NGHN TIY  AMESE ATE ASTEIFFDT IT TNRE .  SME
```

Listing 2.8: Permutation Cipher provided by Mathias

Gutenberg frequency table[2]

Character	Frequency in %
e	12.58
t	9.085
a	8.000
o	7.591
i	6.920
n	6.904
s	6.340
h	6.237
r	5.959
d	4.317
l	4.057
u	2.841
c	2.575
m	2.560
f	2.350
w	2.224
g	1.982
y	1.900
p	1.795
b	1.535
v	0.981
k	0.739
x	0.179
j	0.145
q	0.117
z	0.079

Listing 2.9: Frequency table of numerous collected works in the Gutenberg library. [2]

Permutation frequency table

Character	Frequency in %
	17.95
e	9.210
t	8.458
o	7.236
n	6.672
i	6.203
a	6.015
h	4.699
s	4.464
r	4.464
c	2.772
d	2.678
f	2.584
l	2.302
p	1.926
,	1.785
y	1.691
u	1.503
g	1.315
b	1.315
w	1.315
m	1.268
v	0.892
.	0.375
”	0.187
k	0.140
q	0.140
-	0.093
;	0.093
4	0.046
7	0.046
5	0.046
1	0.046
j	0.046

Listing 2.10: Frequency table of the permutation cipher.

When looking at the frequencies2.92.10 it can be seen that the English frequencies are intact and it follows that the cipher text is a form of a transposition cipher.

An online tool[1] was found for convenient columnar switching of a cipher text. Because the text starts with two spaces this implies the text starts with two words followed by spaces. Using the tool and slowly increasing the block size of the permutation, at a block size of seven the solution was found. The words in the first block are “but in ”.

Solution

```
but in the british empire, for a century past, it has been thoroughly
understood, by men of sense of all parties, that a change of dynasty is out
of the question, and that there is no reform worth contending for in the
state, which is not to be effected by the means which the constitution
itself has provided. this conviction, long impressed upon the nation, and
interwoven as it were with the very framework of the british mind, having
come to coincide with the passions incident to party divisions in a free
state, has in process of time produced the strange and tortuous policy which
, for above a quarter of a century, has now been followed in this country by
 the government, and lauded to the skies by the whole liberal party on the
continent. deprived of the watchwords of men, the parties have come to
assume those of things. organic or social change have become the war-cry of
faction, instead of change of dynasty. the nation is no longer drenched with
 blood by armies fighting for the red or the white rose, by parties striving
 for the mastery between the stuart and hanover families, but it was not
less thoroughly divided by the cry of "the bill, the whole bill, and nothing
 but the bill," at one time, and that of "free-trade and cheap corn" at
another. social change, alterations of policy, have thus come to be the
great objects which divide the nation; and, as it is ever the policy of
opposition to represent the conduct of government as erroneous, it follows,
as a necessary consequence, that the main efforts of the party opposed to
administration always have been, since the suppression of the rebellion in
1745, to effect, when in opposition, a change in general opinion, and, when
in power, to carry that change into effect by a change of policy. the old
law of nature is still in operation. action and reaction rule mankind; and
in the efforts of parties mutually to supplant each other in power, a
foundation is laid for an entire change of policy at stated periods, and an
alteration, as great as from night to day, in the opinions and policy of the
 ruling party in the same state at different times.
```

Listing 2.11: Plaintext(solution): Essays Political Historical vol. 3, page 292

The key for the permutation cipher is 5641230.

[1] http://tholman.com/other/transposition/

Vulnerabilities
With enough computer power every 'anagram' at every block size can theoretically be calculated and matched with an English dictionary to have anagrams match legitimate words, thus the code can be brute forced. In practice, with large block sizes, this is pretty hard. A cipher text can easily be matched with several plain texts that follow an English dictionary.

2.3 Substitution and Permutation cipher

This cipher combines the previous Substitution and Permutation ciphers in one.

Problem
This problem was again provided by Mathias Winther Madsen. The cipher is from the Gutenberg library.

```
QUJTZJQG?DIZJUOUZQ?QZS'?.ZJ'-!FI!TJF?"J-QUJTJIUF!.JE?Q"DJU"FO'ZTZU?ZDJJL?FU.
JO-FIT!Z!!IISJ-FM'AIT-ZJ?Z!QJJ"'IZ.J'..TZIJ!TS'QJJWUX'TZIJF?IFAJAUIZJI!
ILJJMTIFFULB?SQI?JU?FZ!ZJT"IZJTZ?DJI-ILJ'I!ZJ'IFQUJTJTZI?.JQZ;!?APJ'FIGJI-!
MUO"?JTJ.FI'S"IJQQZ?JTZDJ?ZUITJJQJ'TTDQJZ"?FIJX'JIATZ-IJF'JZ'O'SQ'J.Q;JZZERJ
'KJ"DF?JFZITJ-!IT!OFZIJMT"I?DQJI!O!QJ"FIO'-KJJ"JXZX?KJ'ITJMDQ-DJI'TOJVI!U?"!
KJL?FUZJ?"FUZFFOUTAJLZUTDJQUJTJXX?UBJWT-F'JDQU!.UJFQ"JFIJ'D'ZJI?!IFUQ?
LUTAJZF?"JE!.'JMTQ?JA?JFIAL?UJ"UZ'?Z.'JJF"FMUAJIXTJIP"''Q'ZAJI!ZDJ"IXTSUJZW-
JQUUJQ'QVAIXJKU"JI'ZU!KSQTZIJIISFQJTDUJIFJ'TS'Z'JDXV?JPUJFISITJZJ'T'SQ'!'
YXTJIWAM-J!FQ'ITDFU"AJQ?JDJUXII!J".IBJAZ'!"JIITQIQ!VJF''UQ?USS"IJF'ZJT-K"
JUQU?!SLQXOJ.I!?LTSDJ?MI?S!JQIQ"QI"FJ?JLF!'SXO?Z?J"KIZBIIJ-KJ'-!FUJJ-JIQTZ''
XTS!AQJW?T!JWJQPU!IQ"QUAUJTJI.S.?F'?UZ-XMIZ"FJ?J"UJ?QJI.TQJZSXIU."F'JZ'
FIUTQJ.FF'UJSFIIS'!A.JITJZJQ!ZU.F?"JM"?JTJIB!IFQIV"JI!"U?J.U'JKJIQZJLAFUJII
"?I"FUBHJOWZF??UX"FJ?J,U?XI!IIDJQX'?J'AF?JJZZQL.JUITJZZQ!IKQJ'JDZ'Z!UJIT!V'V
?UZ'?KVO'JFUTQJFF'"SJWZJSO!'LILF?"JIZUZXJFJIIXID!J"I"XJIZTILUIK-J"J"AF'OQ!?I
'ZJJIJIZIQ!UJITIUF!.F'SJ"'A!JI?A"JI?TVJIJM?-VTJ'"FJ"QIVJFZ''?TBJ'UTAJIJQZ?
JSJTITJ.UIUTZIJF-J'!U.TOZOVQ'JXWQJZ!JZUOK?DQJZ!?J.J..IU"ZFJI!TZJUDIIF!LDJTMI
'FDJ'XIZ.JXXJ?JJIDTZSZTI!IFQ"I.'JJQJISF'UBSF'J"'IZTZIJ.JM?Z."JI"FZSIIZFUJJ"
IQX?KZ?ZJ-UTFS?TZIJLQUL"JIS.?!SJTXOILJ!??JF'ZFF'UJZFJISJ"VF?QUI?!Z!T'D?X"J-
ITJJWJ"Z?TFIJP?JQQUTJZ??ITZIJZZR!IJZU-AIJ.Z'JQJSITX'Y'TA'M'!"FJ?JJQT?DFUL"
UQUJTJISJ?.TJUFU?TFJQJE?Q"ZJT"FTLJO''K-J?J.D'JI"!F'JXQO.U!ZUVF?"JQ!Z'
QJFJILFMIJB!JQF?DKJ?D'"IJTZZJIFUMQJ!?J"QF?UKFK'X?'JLJW""OTJ?W!QUM!!'TJDJJ"K?
TJFLIIFULBUAUJTJIB!J?IQBJ-JIX!IOZ!SIQJZMIJXQXU"'J'Z!IJB'MAJUT!VIAUFULQQ'
VFOJAUJTJJIFTZQIQSIJ-'ZUI!ZJ.FUL!UZF'UJQUJTJA'M'!J'QZJJP.IIJAL'!ZJT"'.J'Z?
BUIL!QQJIFVJ!FU!IJ-?J"!F?FIZVIISMF?UTSDJTJIMT''JZJTSJOA!?II.DJ'M"J"FXOKJIZ'Q
?UIJ'JK-XFUI?Z!.'J"UTQJA..I'J"IJ"FJ""F?OLQQUJ"QIZ''XTSXIX.YWQJD'FJ'ITZJTMD.I
'!IJM?I!IQM'!"FJ?JI"J?AJQDUTZJ'-?"!Q?DITJZJ!'M'"JF"UJLFJU'SUTTDJITTJ?JL"?
JFZU?FISJ'ZFIO'TZIJ!IRSIJUZ'?!?JFQF'VUJ""IJZFLFIU.'J.Q!ITJZJQ-M'K'TJDJIU"!SQ
?JJMVJ?IT"IJQQAIMTZ'LMCJ'TOZJUTIZJJC? ..J'"FD'IXXUTAJ"ZFUOJTZIJX?QDJ-AUJTJIZ
!FIITJZJQOI'TITFJWJMT-!BIID'DJ?M!TZIJQXF-'J"?JXJJ'"TDFJ'"UVOKJZ"UJ?!EAJUTM!J
'.O'LTZ!LIJTJITFIKJI"?IB"?TJFQUJU"QJ'S?I!LJX?O.F?FAJZJ''I"!Q?DAUMTJJISTJ"XJO
'JZK'F.JIZO"JUXII!QZQJ"ZIQIQIJ'AUJTJIV?V?X?AJ!JZKQ'IPF''!!?ZITJWT"IZQUJI!
JIXXKAIIAM"JI!ZJTFUUA"JI'J.ZQQUJTJM-J'HZ?JTZJZ?OKDIJ.J!OQ'T"?JTJV?QXIQJU"
IJITSFI.XJIX?XJZITJZJZIS!DF"IIT'J.QQIFJ'JVV'OQJ"ZIQIKJJ'XUZOL.'JJ-.
IZTZDCTJWZJTZ?CMJFIQJ?ITZJ'"UAUQTJM.JXIQOZACJIZKJ.JIITFULXI.'JJQJADUTQJZ'TQ"
JF?BFU'S"IJZSZJT.'!SUJIJM?IAZJT"F.I'!ITJ?I!'FZJQITJZJQFS'SQOF'UJQ'QIFUFJ.
FISS''ZJJIVV'OQTJUZ!UJJNAFF'?SU.FJZFUJJ"TJI-AJZZ!?VOKJ'"UJ?!MACUTJIQTJM"JU?
TJIQ?''PZJ'I!LJ?JFILIF"J"J-ZKJTJ?IT?JF"FIX"J"ITAZJ!S'?JZJTQQ?XDJIJJJWF
```

Listing 2.12: Permutation & Substitution Cipher provided by Mathias

Gutenberg frequency table[2]

Character	Frequency in %
e	12.58
t	9.085
a	8.000
o	7.591
i	6.920
n	6.904
s	6.340
h	6.237
r	5.959
d	4.317
l	4.057
u	2.841
c	2.575
m	2.560
f	2.350
w	2.224
g	1.982
y	1.900
p	1.795
b	1.535
v	0.981
k	0.739
x	0.179
j	0.145
q	0.117
z	0.079

Listing 2.13: Frequency table of numerous collected works in the Gutenberg library. [2]

Permutation frequency table

Character	Frequency in %
J	17.70
I	10.25
Z	6.642
’	6.496
T	5.985
F	5.802
?	5.620
U	5.583
Q	5.364
”	4.525
!	4.379
.	2.445
X	2.226
S	2.189
A	1.970
D	1.897
O	1.642
M	1.569
L	1.532
-	1.423
K	1.204
V	1.058
W	0.620
B	0.620
P	0.291
C	0.218
E	0.182
R	0.109
Y	0.109
H	0.072
;	0.072
G	0.072
,	0.036
	0.036
N	0.036

Listing 2.14: Frequency table of the permutation and substitution cipher.

Finding the solution is a process of small increments just like with the Substitution cipher. Frequency analysis of the Cipher text gives the following tables 2.132.14, with a total of 35 different characters.

Space is the most used character in the English language so I replaced the J, with a space. Then in the English language the characters e and t are most frequent, so I and Z are replaced.

```
QU Tt QG?Det UOUtQ?QtS'?.t '-!Fe!T F?" -QU T eUF!. E?Q"D U"FO'tTtU?tD  L?FU.
 O-FeT!t!!eeS -FM'AeT-t ?t!Q  "'et. '..Tte !TS'Q  WUX'Tte F?eFA AUet e!eL
MTeFFULB?SQe? U?Ft!t T"et Tt?D e-eL 'e!t 'eFQU T Tte?. Qt;!?AP 'FeG e-!MUO"?
 T .Fe'S"e QQt? TtD ?tUeT  Q 'TTDQ t"?Fe X' eATt-e F' t'O'SQ' .Q; ttER 'K "
DF? FteT -!eT!OFte MT"e?DQ e!O!Q "FeO'-K  " XtX?K 'eT MDQ-D e'TO Ve!U?"!K L?
FUt ?"FUtFFOUTA LtUTD QU T XX?UB WT-F' DQU!.U FQ" Fe 'D't e?!eFUQ?LUTA tF?"
E!.' MTQ? A? FeAL?U "Ut'?t.'  F"FMUA eXT eP"''Q'tA e!tD "eXTSU tW- QUU Q'
QVAeX KU" e'tU!KSQTte eeSFQ TDU eF 'TS't' DXV? PU FeSeT t 'T'SQ'!'YXT eWAM-
!FQ'eTDFU"A Q? D UXee! ".eB At'!" eeTQeQ!V F''UQ?USS"e F't T-K" UQU?!SLQXO .
e!?LTSD ?Me?S! QeQ"Qe"F ? LF!'SXO?t? "KetBee -K '-!FU  - eQTt''XTS!AQ W?T! W
 QPU!eQ"QUAU T e.S.?F'?Ut-XMet"F ? "U ?Q e.TQ tSXeU."F' t'FeUTQ .FF'U SFeeS
'!A. eT t Q!tU.F?" M"? T eB!eFQeV" e!"U? .U' K eQt LAFU ee"?e"FUBH OWtF??UX"
F ? ,U?Xe!eeD QX'? 'AF?  ttQL. UeT ttQ!eKQ ' Dt't!U eT!V'V?Ut'?KVO' FUTQ FF
'"S Wt SO!'LeLF?" etUtX F eeXeD! "e"X etTeLUeK- " "AF'OQ!?e't  e eteQ!U
eTeUF!.F'S "'A! e?A" e?TV e M?-VT '"F "QeV Ft''?TB 'UTA e Qt? S TeT .UeUTte
F- '!U.TOtOVQ' XWQ t! tUOK?DQ t!? . ..eU"tF e!Tt UDeeF!LD TMe'FD 'Xet. XX ?
 eDTtStTe!eFQ"e.'  Q eSF'UBSF' "'etTte . M?t." e"FtSeetFU  "eQX?Kt?t -UTFS?
Tte LQUL" eS.?!S TXOeL !?? F'tFF'U tF eS "VF?QUe?!t!T'D?X" -eT  W "t?TFe P?
QQUT t??eTte ttR!e tU-Ae .t' Q SeTX'Y'TA'M'!"F ?  QT?DFUL"UQU T eS ?.T UFU?
TF Q E?Q"t T"FTL O''K- ? .D' e"!F' XQO.U!tUVF?" Q!t'Q F eLFMe B! QF?DK ?D'"e
 Ttt eFUMQ !? "QF?UKFK'X?' L W""OT ?W!QUM!!'T D  "K?T FLeeFULBUAU T eB! ?eQB
 - eX!eOt!SeQ tMe XQXU"' 't!e B'MA UT!VeAUFULQQ'VFO AU T  eFTtQeQSe -'tUe!t
.FUL!UtF'U QU T A'M'! 'Qt  P.ee AL'!t T"'. 't?BUeL!QQ eFV !FU!e -? "!F?
FetVeeSMF?UTSD T eMT'' t TS OA!?ee.D 'M" "FXOK et'Q?Ue ' K-XFUe?t!.' "UTQ A
..e' "e "F ""F?OLQQU "Qet''XTSXeX.YWQ D'F 'eTt TMD.e'!e M?e!eQM'!"F ? e" ?A
QDUTt '-?"!Q?DeT t !'M'" F"U LF U'SUTTD eTT ? L"? FtU?FeS 'tFeO'Tte !eRSe Ut
'?!? FQF'VU ""e tFLFeU.' .Q!eT t Q-M'K'T D eU"!SQ?  MV ?eT"e QQAeMTt'LMC '
TOt UTet  C? .. '"FD'eXXUTA "tFUO Tte X?QD -AU T et!FeeT t QOe'TeTF W MT-!
BeeD'D ?M!Tte QXF-' "? X  '"TDF '"UVOK t"U ?!EA UTM! '.O'LTt!Le T eTFeK e"?
eB"?T FQU U"Q 'S?e!L X?O.F?FA t '!e"!Q?DAUMT  eST "X O' tK'F. etO" UXee!QtQ
"teQeQe 'AU T eV?V?X?A ! tKQ'ePF'!!?teT WT"etQU e! eXXKAeeAM" e!t TFUUA" e'
.tQQU T M- 'Ht? Tt t?OKDe . !OQ'T"? T V?QXeQ U"e eTSFe.X eX?X teT t teS!DF"
eeT' .QQeF ' VV'OQ "teQeK  'XUtOL.'  -.etTtDCT Wt Tt?CM FeQ ?eTt '"UAUQT M.
XeQOtAC etK . eeTFULXe.'  Q ADUTQ t'TQ" F?BFU'S"e tSt T.'!SU e M?eAt T"F.e'!
eT ?e!'Ft QeT t QFS'SQOF'U Q'QeFUF .FeSS''t  eVV'OQT Ut!U  NAFF'?SU.F tFU  "
T e-A tt!?VOK '"U ?!MACUT eQT M" U?T eQ?''Pt 'e!L ? FeLeF" " -tK T ?eT? F"
FeX" "eTAt !S'? t TQQ?XD e   WF
```

After applying the partial decoding, it is time to unscramble using the online tool[2] that was also used in the previous permutation cipher. From the length of the cipher text a few possible permutation block sizes are possible. Block sizes in permutation ciphers are whole divisors, the text has a length of 2740, so possible block sizes are: [1, 2, 4, 5, 10, 20, 137, 274, 548, 685,

[2] http://tholman.com/other/transposition/

1370]. Using again frequency research and seeing that the most common first letter of a word is a t and the most common last letter of a word is an e[2], it follows it is best to find the permutation that holds to this rule the best.

A block size of two fails to remove multiple spaces behind each other, so a block size of two is discarded. Permutations with a block size of 4 either have multiple spaces, or single t's in them. At a block size of 5 a anagram was found that fulfills the above rule and does not have the problem of multiple spaces or singleton t's. The anagram looks like this:

```
tTUQ D?Q GOUte Q?tUQ.?St'!- t' TeF!- ?F" TUQ .!UeF"QE ?F" DUtT'Ot D?UtUFL ?F
- .O!tTe! Se!eA'F-M tTe- Qt?!te" '.. .'! tTe QST''XW UF tTe Ae?F tUAe L!
eeFeM T?BUFL ?QSe!t?UFe" tT?t tTe- De!e L'Fe t' TUQ .?tTe!;Q t' A?Pe eFGOU!-
M T?" S'F.eQQe" tT?t Ut D?Q Te DT' T?" Qt'XeF tTe A'Fe- 'Ot '. QS'tt;Q K'RE
?F" DTeF tTe- !etO!Fe"M Te D?Q QO!!'OF"e" K- ?XX tTe K'-QM DT' De!e OVK!?U"
UFL ?F" t?OFtUFL TUA DUtT TUQ BUXX?F-W TUQ 'DF .!UeF"Q t'' De!e ?L?UFQt TUAE
 ?F"M .!'A QT?Ae ?F" ?LUt?tU'F '. AUF"M Te X''Pe" A'Qt D!etSTe"X-W Ut UQ UAV
'QQUKXe t' "eQS!UKe tTe QSeFe DTUST F'D t''P VX?Se UF tTe QST''XY!''AW TeF!-
M DT'Qe AUF" D?Q !eXUeBe" .!'A tTe "eV!eQQU'F 'SS?QU'Fe" K- tTUQ "UQL!?Se.OX
 ST?!LeM D?Q S?!eQQe" ?F" S'FL!?tOX?te" K- eBe!- K'- UF tTe QST''XW A!QW T
?!!UQ PUQQe" TUA ?..eStU'F?teX-M ?F" Q?U" QTe .eXt S'F.U"eFt '. TUQ UFF'
SeFSe .!'A tTe .U!QtM ?F" T?" FeBe! "eQV?U!e" '. UtQ KeUFL A?"e eBU"eFtW
HOXU?F? ?F" eXU,? De!e ?XQ' ?A'FLQt tTe .U!Qt t' KeQt'D tTeU! ?VV!'K?tU'F OV
'F TUQ S'F"OStW Le'!Le ?F" XUttXe Fe" De!e "eXULTte" Ke-'F" Ae?QO!e t' Qee
tTeU! .!UeF" 'FSe A'!e A?"e T?VV-M ?F" T'Ve" Q''F t' T?Be TUA ?Q tTe STUe.
UF tTeU! -'OtT.OX QV'!tQW KOt Ut D?Q .?! "U..e!eFt DUtT L!eeFeM DT' F'D .eXt
 ?XX tTe D!etSTe"FeQQ '. 'Fe S'FBUSte" '. tTe.tM ?F" "eteSte" UF K?QeX- ?tt?
STUFL tTe "UQL!?Se.OX ST?!Le t' ?F UFF'SeFt ?F" V!?UQeD'!tT- X?"W Te T?" t?
PeF TUQ Qe?t ?t tTe eRt!eAUt- '. tTe QST''XY!''AM ?F" D?Q TU"UFL TUQ .?Se UF
 TUQ T?F"QE ?F" tT'OLT ? K'- '. D'F"e!.OX QVU!UtQ ?F" Qt!'FL Fe!BeM D?Q F'D
K?tTe" UF te?!QM ?F" Q'KKUFL ?X'O"W "!W T?!!UQM DT' T?" KeeF LUBUFL TUA ? Be
!- QeBe!e XeStO!eM QtUXX Qt''" 'Be! TUAM UAV!eQQUFL OV'F TUA tTe FeSeQQUt-
'. !etU!UFL UFt' TUQ !''AM t' QeeP .!'A L'" tT?t .'!LUBeFeQQ UF V!?-e! ?F" !
eVeFt?FSeM DTUSTM Te t'' AOST .e?!e"M D'OX" F't Ke e?QUX- 'Kt?UFe" .!'A TUQ
'..eF"e" ?F" "UQLOQte" QST''XY.eXX'DQW Te F'DM tTe!e.'!eM ?!'QeM ?F" A?"e
TUQ D?- t'D?!"Q tTe "''!M UF "'UFL DTUST Te T?" ?L?UF t' eFS'OFte! tTe eReS
!?tU'FQ ?F" V'UFte" .UFLe!Q '. tTe K'-QM DT' S!Ue"M ?Q Te V?QQe" tTeAM CL'M
tT'O tTUe. C ?F" .'XX'De" TUA OFtUX tTe- Q?D TUA eFte! tTe T'OQeW TeF!-M T'
DeBe!M D?Q tTe 'FX- X?" DT' "U" F't OVK!?U" TUAE .'!M tT'OLT L!eeFe T?" KeT?
Be" UF Q' "UQL!?Se.OX ? A?FFe! t'D?!"Q TUAM Te S'OX" F't KOt .eeX "UQt!eQQe"
 t' Qee TUA ?VVe?! ?XA'Qt K!'PeFTe?!te"W Te QtUXX !eAeAKe!e"M UF tTe AU"Qt
'. TUQ H'-M tT?t KOt ? .eD T'O!Q T?" eX?VQe" QUFSe Te .eXt ?XX tTe D!etSTe"
FeQQ '. 'Fe QOVV'Qe" t' Ke LOUXt- '. tTe.tW CDT?t tTeFMC Te Q?U" t' TUAQeX.M
 CAOQt Ke tTe .eeXUFLQ '. TUA DT' Qt?F"Q S'FBUSte" '. tTe S!UAeM ?F" tTe!e
.'!e T?Q F't tTe S'FQSU'OQFeQQ '. UFF'SeFSe t' QOVV'!t TUAN U S?FF't .UF" UF
 A- Te?!t t' OVK!?U" TUAMC Te Q?U"M ?Q Te t''P Le'!Le ?F" Fe" K- tTe T?F" ?F
" Xe" tTeA ?S!'QQ tTe X?DFW
```

From here we start filling in letters like with the substitution cipher. The first step is identifying the 'the' trigram and most common word in the English language, tTe fills is the most common trigram in the cipher text so tTe is most probably the.

```
thUQ D?Q GOUte Q?tUQ.?St'!- t' heF!- ?F" hUQ .!UeF"QE ?F" DUth'Ot D?UtUFL ?F
- .O!the! Se!eA'F-M the- Qt?!te" '.. .'! the QSh''XW UF the Ae?F tUAe L!
eeFeM h?BUFL ?QSe!t?UFe" th?t the- De!e L'Fe t' hUQ .?the!;Q t' A?Pe eFGOU!-
M h?" S'F.eQQe" th?t Ut D?Q he Dh' h?" Qt'XeF the A'Fe- 'Ot '. QS'tt;Q K'RE
?F" DheF the- !etO!Fe"M he D?Q QO!!'OF"e" K- ?XX the K'-QM Dh' De!e OVK!?U"
UFL ?F" t?OFtUFL hUA DUth hUQ BUXX?F-W hUQ 'DF .!UeF"Q t'' De!e ?L?UFQt hUAE
 ?F"M .!'A Qh?Ae ?F" ?LUt?tU'F '. AUF"M he X''Pe" A'Qt D!etShe"X-W Ut UQ UAV
'QQUKXe t' "eQS!UKe the QSeFe DhUSh F'D t''P VX?Se UF the QSh''XY!''AW heF!-
M Dh'Qe AUF" D?Q !eXUeBe" .!'A the "eV!eQQU'F 'SS?QU'Fe" K- thUQ "UQL!?Se.OX
 Sh?!LeM D?Q S?!eQQe" ?F" S'FL!?tOX?te" K- eBe!- K'- UF the QSh''XW A!QW h
?!!UQ PUQQe" hUA ?..eStU'F?teX-M ?F" Q?U" Qhe .eXt S'F.U"eFt '. hUQ UFF'
SeFSe .!'A the .U!QtM ?F" h?" FeBe! "eQV?U!e" '. UtQ KeUFL A?"e eBU"eFtW
HOXU?F? ?F" eXU,? De!e ?XQ' ?A'FLQt the .U!Qt t' KeQt'D theU! ?VV!'K?tU'F OV
'F hUQ S'F"OStW Le'!Le ?F" XUttXe Fe" De!e "eXULhte" Ke-'F" Ae?QO!e t' Qee
theU! .!UeF" 'FSe A'!e A?"e h?VV-M ?F" h'Ve" Q''F t' h?Be hUA ?Q the ShUe.
UF theU! -'Oth.OX QV'!tQW KOt Ut D?Q .?! "U..e!eFt DUth L!eeFeM Dh' F'D .eXt
 ?XX the D!etShe"FeQQ '. 'Fe S'FBUSte" '. the.tM ?F" "eteSte" UF K?QeX- ?tt?
ShUFL the "UQL!?Se.OX Sh?!Le t' ?F UFF'SeFt ?F" V!?UQeD'!th- X?"W he h?" t?
PeF hUQ Qe?t ?t the eRt!eAUt- '. the QSh''XY!''AM ?F" D?Q hU"UFL hUQ .?Se UF
 hUQ h?F"QE ?F" th'OLh ? K'- '. D'F"e!.OX QVU!UtQ ?F" Qt!'FL Fe!BeM D?Q F'D
K?the" UF te?!QM ?F" Q'KKUFL ?X'O"W "!W h?!!UQM Dh' h?" KeeF LUBUFL hUA ? Be
!- QeBe!e XeStO!eM QtUXX Qt''" 'Be! hUAM UAV!eQQUFL OV'F hUA the FeSeQQUt-
'. !etU!UFL UFt' hUQ !''AM t' QeeP .!'A L'" th?t .'!LUBeFeQQ UF V!?-e! ?F" !
eVeFt?FSeM DhUShM he t'' AOSh .e?!e"M D'OX" F't Ke e?QUX- 'Kt?UFe" .!'A hUQ
'..eF"e" ?F" "UQLOQte" QSh''XY.eXX'DQW he F'DM the!e.'!eM ?!'QeM ?F" A?"e
hUQ D?- t'D?!"Q the "''!M UF "'UFL DhUSh he h?" ?L?UF t' eFS'OFte! the eReS
!?tU'FQ ?F" V'UFte" .UFLe!Q '. the K'-QM Dh' S!Ue"M ?Q he V?QQe" theAM CL'M
th'O thUe. C ?F" .'XX'De" hUA OFtUX the- Q?D hUA eFte! the h'OQeW heF!-M h'
DeBe!M D?Q the 'FX- X?" Dh' "U" F't OVK!?U" hUAE .'!M th'OLh L!eeFe h?" Keh?
Be" UF Q' "UQL!?Se.OX ? A?FFe! t'D?!"Q hUAM he S'OX" F't KOt .eeX "UQt!eQQe"
 t' Qee hUA ?VVe?! ?XA'Qt K!'PeFhe?!te"W he QtUXX !eAeAKe!e"M UF the AU"Qt
'. hUQ H'-M th?t KOt ? .eD h'O!Q h?" eX?VQe" QUFSe he .eXt ?XX the D!etShe"
FeQQ '. 'Fe QOVV'Qe" t' Ke LOUXt- '. the.tW CDh?t theFMC he Q?U" t' hUAQeX.M
 CAOQt Ke the .eeXUFLQ '. hUA Dh' Qt?F"Q S'FBUSte" '. the S!UAeM ?F" the!e
.'!e h?Q F't the S'FQSU'OQFeQQ '. UFF'SeFSe t' QOVV'!t hUAN U S?FF't .UF" UF
 A- he?!t t' OVK!?U" hUAMC he Q?U"M ?Q he t''P Le'!Le ?F" Fe" K- the h?F" ?F
" Xe" theA ?S!'QQ the X?DFW
```

There are a few more words that can be found because of deducing the character h. Words like th?t and thUQ and hUQ, so ?,U and Q are replaced by a, i and s.

```
this Das GOite satis.aSt'!- t' heF!- aF" his .!ieF"sE aF" Dith'Ot DaitiFL aF
- .O!the! Se!eA'F-M the- sta!te" '.. .'! the sSh''XW iF the AeaF tiAe L!
eeFeM haBiFL asSe!taiFe" that the- De!e L'Fe t' his .athe!;s t' AaPe eFGOi!-
M ha" S'F.esse" that it Das he Dh' ha" st'XeF the A'Fe- 'Ot '. sS'tt;s K'RE
aF" DheF the- !etO!Fe"M he Das sO!!'OF"e" K- aXX the K'-sM Dh' De!e OVK!ai"
iFL aF" taOFtiFL hiA Dith his BiXXaF-W his 'DF .!ieF"s t'' De!e aLaiFst hiAE
 aF"M .!'A shaAe aF" aLitati'F '. AiF"M he X''Pe" A'st D!etShe"X-W it is iAV
'ssiKXe t' "esS!iKe the sSeFe DhiSh F'D t''P VXaSe iF the sSh''XY!''AW heF!-
M Dh'se AiF" Das !eXieBe" .!'A the "eV!essi'F 'SSasi'Fe" K- this "isL!aSe.OX
 Sha!LeM Das Sa!esse" aF" S'FL!atOXate" K- eBe!- K'- iF the sSh''XW A!sW ha
!!is Pisse" hiA a..eSti'FateX-M aF" sai" she .eXt S'F.i"eFt '. his iFF'SeFSe
 .!'A the .i!stM aF" ha" FeBe! "esVai!e" '. its KeiFL Aa"e eBi"eFtW HOXiaFa
aF" eXi,a De!e aXs' aA'FLst the .i!st t' Kest'D thei! aVV!'Kati'F OV'F his S
'F"OStW Le'!Le aF" XittXe Fe" De!e "eXiLhte" Ke-'F" AeasO!e t' see thei! .!
ieF" 'FSe A'!e Aa"e haVV-M aF" h'Ve" s''F t' haBe hiA as the Shie. iF thei!
-'Oth.OX sV'!tsW KOt it Das .a! "i..e!eFt Dith L!eeFeM Dh' F'D .eXt aXX the
D!etShe"Fess '. 'Fe S'FBiSte" '. the.tM aF" "eteSte" iF KaseX- attaShiFL the
 "isL!aSe.OX Sha!Le t' aF iFF'SeFt aF" V!aiseD'!th- Xa"W he ha" taPeF his
seat at the eRt!eAit- '. the sSh''XY!''AM aF" Das hi"iFL his .aSe iF his haF
"sE aF" th'OLh a K'- '. D'F"e!.OX sVi!its aF" st!'FL Fe!BeM Das F'D Kathe"
iF tea!sM aF" s'KKiFL aX'O"W "!W ha!!isM Dh' ha" KeeF LiBiFL hiA a Be!- seBe
!e XeStO!eM stiXX st''" 'Be! hiAM iAV!essiFL OV'F hiA the FeSessit- '. !eti!
iFL iFt' his !''AM t' seeP .!'A L'" that .'!LiBeFess iF V!a-e! aF" !
eVeFtaFSeM DhiShM he t'' AOSh .ea!e"M D'OX" F't Ke easiX- 'KtaiFe" .!'A his
'..eF"e" aF" "isLOste" sSh''XY.eXX'DsW he F'DM the!e.'!eM a!'seM aF" Aa"e
his Da- t'Da!"s the "''!M iF "'iFL DhiSh he ha" aLaiF t' eFS'OFte! the eReS!
ati'Fs aF" V'iFte" .iFLe!s '. the K'-sM Dh' S!ie"M as he Vasse" theAM CL'M
th'O thie. C aF" .'XX'De" hiA OFtiX the- saD hiA eFte! the h'OseW heF!-M h'
DeBe!M Das the 'FX- Xa" Dh' "i" F't OVK!ai" hiAE .'!M th'OLh L!eeFe ha"
KehaBe" iF s' "isL!aSe.OX a AaFFe! t'Da!"s hiAM he S'OX" F't KOt .eeX "ist!
esse" t' see hiA aVVea! aXA'st K!'PeFhea!te"W he stiXX !eAeAKe!e"M iF the Ai
"st '. his H'-M that KOt a .eD h'O!s ha" eXaVse" siFSe he .eXt aXX the D!
etShe"Fess '. 'Fe sOVV'se" t' Ke LOiXt- '. the.tW CDhat theFMC he sai" t'
hiAseX.M CAOst Ke the .eeXiFLs '. hiA Dh' staF"s S'FBiSte" '. the S!iAeM aF"
 the!e.'!e has F't the S'FsSi'OsFess '. iFF'SeFSe t' sOVV'!t hiAN i SaFF't .
iF" iF A- hea!t t' OVK!ai" hiAMC he sai"M as he t''P Le'!Le aF" Fe" K- the
haF" aF" Xe" theA aS!'ss the XaDFW
```

From here word by word the solution was found. Character substitutions were found by replacing words like GOite, satis.aSt'!-, Das, and Dith'Ot to quite, satisfactory, was and without.

```
this was quite satisfactory to henry and his friends; and without waiting
any further ceremony, they started off for the school. in the mean time
greene, having ascertained that they were gone to his father's to make
enquiry, had confessed that it was he who had stolen the money out of scott'
s box; and when they returned, he was surrounded by all the boys, who were
upbraiding and taunting him with his villany. his own friends too were
against him; and, from shame and agitation of mind, he looked most
wretchedly. it is impossible to describe the scene which now took place in
the school-room. henry, whose mind was relieved from the depression
occasioned by this disgraceful charge, was caressed and congratulated by
every boy in the school. mrs. harris kissed him affectionately, and said she
 felt confident of his innocence from the first, and had never despaired of
its being made evident. juliana and eliza were also amongst the first to
bestow their approbation upon his conduct. george and little ned were
delighted beyond measure to see their friend once more made happy, and hoped
 soon to have him as the chief in their youthful sports. but it was far
different with greene, who now felt all the wretchedness of one convicted of
 theft, and detected in basely attaching the disgraceful charge to an
innocent and praiseworthy lad. he had taken his seat at the extremity of the
 school-room, and was hiding his face in his hands; and though a boy of
wonderful spirits and strong nerve, was now bathed in tears, and sobbing
aloud. dr. harris, who had been giving him a very severe lecture, still
stood over him, impressing upon him the necessity of retiring into his room,
 to seek from god that forgiveness in prayer and repentance, which, he too
much feared, would not be easily obtained from his offended and disgusted
school-fellows. he now, therefore, arose, and made his way towards the door,
 in doing which he had again to encounter the execrations and pointed
fingers of the boys, who cried, as he passed them, "go, thou thief " and
followed him until they saw him enter the house. henry, however, was the
only lad who did not upbraid him; for, though greene had behaved in so
disgraceful a manner towards him, he could not but feel distressed to see
him appear almost brokenhearted. he still remembered, in the midst of his
joy, that but a few hours had elapsed since he felt all the wretchedness of
one supposed to be guilty of theft. "what then," he said to himself, "must
be the feelings of him who stands convicted of the crime, and therefore has
not the consciousness of innocence to support him? i cannot find in my heart
 to upbraid him," he said, as he took george and ned by the hand and led
them across the lawn.
```

Listing 2.15: Plaintext(solution): "The Friends; Or the Triumph of Innocence Over False Changes: A Tale, Founded on Facts." page 80

The complete cipher alphabet that was found is:

```
Plain:   abcdefghijklmnopqrstuvwxyz '"!?.-;,
Cipher:  ?ks"i.ltuhpxaf'vg!qzobdr-,j;c nwyem
```

Vulnerabilities
The problem with this cipher is that the frequencies of the English language have not been obscured, so with frequency analysis and knowledge of the English language the text can still be deciphered. There is the difficulty of the permutation, but again with the frequency of characters at the beginning and the end of a word the right anagram can easily be found.

2.4 Poly-Alphabetic cipher

A poly-alphabetic cipher uses multiple alphabets to encode and decode a plain text into a cipher text. The first official poly-alphabetic cipher is the Alberti cipher which was invented by Leon Battista Alberti $\sim$ 1467. First official because there are claims that an Arabian scientist first described a poly-alphabetic cipher 600 years before Alberti[3]. Alberti used two rotating metal disks on top of each other to have multiple alphabets for multiple indexes. From figure 2.1 can be seen that the disk allows for 24 different characters to match to a single character.

Figure 2.1: An example of an Alberti cipher disk in which the g is matched to an A.

Alberti cipher example
As with figure 2.1 the inner g is used as an index. Say someone wants to encode something about the war: "The war shall...". As can be seen from the cipher disk we do not have access to the full Latin alphabet, so we have to be a little inventive. For convenience we will encode from Italian:"La guerra si farà" First we set the index g to A, which we will have to note in the cipher. The first letter in the cipher is an A. Then we encode "la guerra" with this alphabet.

```
Plaintext:   _laguerra
Ciphertext:  Azgthpmmg
```

Then comes the second part "si farà" which we will encode with index g on Q.

```
Plaintext:   _sifara
Ciphertext:  Qlfiyky
```

Which gives the full ciphertext: AzgthpmmgQlfiyky

The problem with this encryption is that it relies heavily on the secrecy of the method of encoding. Given that the method of encoding is known, to break a cipher text only 24 possible alphabets would have to be tried.

The Vigènere cipher is another notable example of a poly-alphabetic cipher because of it's similarity to the problem cipher text given by Mathias Winther Madsen. The Vigènere cipher was first described by Giovan Battista Bellaso $\sim$ 1553 and earned the description 'le chiffre indéchiffrable' for being unbreakable for $\sim$ 300 years. Unlike the Alberti cipher, the cipher uses a key that is outside the cipher text, and does not rely on the safekeeping of the encoding scheme. The Vigènere cipher uses multiple Caesar shifted alphabets to encode plain text switching alphabets every character according to a predetermined key, when the key is fully traversed the key is reused. Like with another cipher, the Trithemius cipher(circa. 1518), the Vigènere cipher uses the Tabula Recta, a table with the 26 possible Caesar shifted alphabets. The Tabula Recta can be seen in figure 2.2.

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

Figure 2.2: The Tabula Recta first used in the Trithemius cipher, and then in the Vigènere cipher.

Vigènere cipher example
The war is starting and you do not want the enemy to know, so our message is: "the war starts...". Our key is banana. Using the Tabula Recta the message is encoded, spaces are subtracted to further diffuse the message.
Plaintext:
`THEWARSTARTS...`
KEY(BANANA):
`BANANABANANA...`
Ciphertext:
`UHRWNRTTNRGS...`

This cipher works pretty well for short messages but with longer messages and a key that is relatively short, repetitions in the cipher text are common. With this fact the key size can be estimated, after which for every index of the key frequency analysis can be applied.

Problem

Now that information about poly-alphabetic cipher has been read, we should be able to crack Mathias his cipher.

```
QBRYXGELP;CJ FIOBIBIR.FL-BLFBXUKRLGIEKDTANRWLSKOL'XAJ GVKOLBGBOY'FN'LUUN-PCFX,LLSVJ'QGEKPZR.JAZCGCT'F
.CBI AFTIMXIW-SQFBISKJ,IHL;ZXREZVIZC'XC;EYZZWNK'KFVZLPZGJ,TF.;FIMNEWA,NRD;PECTRFVFIPSVLLEXN-,ERA-
LSUGHD'RAKJIXAJAZHE,';;EZVIXBHOI SRLXIELPIHS,V-CAKLZFGFHCUTNLXREG,TF'L' ,JJR-CVZTZ,HJ,;;EYPEZS'
PIDFJWXCWQNTRNIW-HERYZREL,RFWZNSUREPRF.;NIRXJRZCTJVCDUJ';UE;TIQ.ZF-FWZNSZK;';H.;RIXAJYZ;EKPCSQFBIZEOZ
-ZTJB-ZRJ'PFLEPZHS-PKFBILCUVSPEREZVIZKMLPUAED;PEZVIPAIXXGAJFGCGZAMFTLPIUKRDCUE'W-GAJP;ZWRPRFCF.
QUAILLSU'P IECTRFVR,;,AMLLZ;JQ-UKJ,IMXHR UTFLPZGVPKFTL'AP.JY-F.CBISKUPTRAKL'XNRLRDSOY'.EG,
CCBZZIQBRYIONI IZKKLRSVRD;PS;FLU;JYGGX-FIZKKLVCAC.IAXGPCYELPIXNKL;UQFZIUKRPCRN;T-;EZTIR.FLUU.CIPFX,
LLSVJWLSA,LGIF;WXZRJ.LZTJV-UR;TVFX,LEDK,DRUKVPIHXJPTHAI.XZRJ.GFTLPIMXHR ZB',;MAJ'PFU;TRFX,LZGJJZA,A-
OISTJAZHELDTFBI.-GT;';FTZLTUTJQ-IX-PIR.C.ISKKDJS;Q, FNIL-BNHR UEZVISKRPVCBR IZKKLRUQZ.XDKJ.LZTJ.LUETD
;PE,,;MBFBIQXQIRFCFLQURELQDGRYHFX,L-OSE,'SXIOIZVJ,;FNKBXRBZTZ,E',PUDQ,C;HJYGQAUPCYELPIMNQF-;E'
PECARLTABFFIDFJYXHEZA;FVFI-MT;';FTZLUUEKDTANRWLU;JD;FTLPIRGCD;FX,LTSGJZXM.CZRLE;TIZ;ZR'SKOL'XB'LEDS-F
-F.FLUUR;PJU;JYXOVFIPFTZLUUETP-ABIHIR.FLTSTQ,'SXILQURELXGEL,;;IJ,'FXIW-FDQ,C;BIHIZDCD;HTJ,;.E;T'UG-
XSRBZTIDFJ.LUE,D;ZRJB-,BUPC.EZVIR.FLAGS'XZ,EG,CCNI.MFNIBIAGZKX;BIHIXBHLQSTLL'XAJN-ZK'LGIERPTRBIHI,X-
BIHTCT UJ FI;AU''SXIL'DELDTFWCXTUMJ.LVVNLLZ;JTGRE'DCFG;WLZGKL'ZYFTISTJD;RXJYXHELPZ;ER'IIXEIGQECTIST;T
-CN- IUKRDCURMLRSF,PCUKRLPCXHL-STLPCFTLPIDKFLTVDOPTRAKLU.ELP;CJNLGCERYZRE'PECARIHFT-,;HU;.'U;J.GF.;NI
 A'DRUERY-FLZZ'MSEIXHEY I,X-BIHTCT UJNLTDUFLTRNRPIAGZQ UU'LGIEU,TREH,VGBRXCUECTRFBHRGCTCTEUEHDVXTJ.
LUKJYZWAJQ-UKJFG,QFBKFN'LXRE'XUHA.X-GTE IRGCTTAB-PRYECI FNE';PECTRFCF.QUAIL'XAJZGZ;'L'XNRLXREG,TF;
FVXGBRP .E'XSAX'PRFTLPI.XQTVFYIDVXTJ,;;ELDTFV.XXCAJAGVRKLWZYFL'XA;ZIABEHCSUCH-YETD;P 'L-OB'FZCBFFIQA-
PIMXIF'ZKRIHFUFP'SKOLZG;JZ-MA;KXGDJP;RA-.ZSKHP;REZVIHTCT UJ FI,BFX'UKCT'HHJ,TF'FI FN'L'XAJ''XA-LQZJJ,
UDSROIDCUDGVVE MFKFD'XA-L'XAJ';UE'DRUEI'CFTLPIDTLPCF;CZ-;ER'IXBI.IDFJD'HESXCAX'PIDFJPTABZTZPAJ'CF;FF'
SKC.XDKBL;DGJ -REK,CU;J.GF;;FS,NMLZGJJX;;SFLLZVRPISKJRZCT;TVFTZLSVG'X-FBRFIHAVZ-REG,HLE;.IZR''I AV,
WUEIPEUV',C.E,'CFTLPWFTZLG VFZJUEFK-CJJRGHV;Q UESZ-MNQ.XDKJD;FTLPIONR.-CEZVIMXUPCSKOLAAERY-SGJ.
CZBEFMFXIPIIGZNIZKZ.LUGBLZG;NLXGERYXHEG,HYERY-FBITGMAI.IMNQF-FX,L'XB'
LCZTLPCFNHXTSKOLVZUFLGIEVZGHVPRACLZF-HEG,TFLFZWSTRPRFTZLVDEQTWDRFF'U;JXSDKJYXHEG,HLERY-FGZX'UERYZRE'
DCFG;WLZGKLLZ;JWLDVFTICAIB-CAKLXREIPEUV',C.E,'CF.;NTUR,LZG;JFFVB-PIRXJ.CUNKLSZTLFIZKKLU.,G,HHEQF-;
EVYXUFE I JJR-ZVCT'FFCZWUG'LZG;JFLUASSLUGKPCHMJ,'FT;N-HHJ,PRA-LZF.F,J.E,, ,EZVICN;TMFVQWLFX,L'XA'
PIZVJAGVKKL'XGZXVXERY-FRZAI,J;TVFQCI UJ'LQDSEBI AV'WUEGYG,RMLXOLCFTZCEPMFUCEXGDJD'FKFPRISELPDGJ'ACESD
 PG;NTFTZLZQN;.IR.FLRCN;TXGDJ'PFTLPIIRZ'RFBI.GFTLPICBUPCHHJ'CFTZLWZYFL DKOLRUTZXCHER'IMXHPIVLZTIR.
FLGR.FZIHBKPKFFZZIR.;FICACFGGHJD'F.CBICACWLU;JA-,RJ, DKOLXGTZLGMTZQ-CEYPPDGFL'XAMLLZ;JRZHVFBIR.-'AP.J
.LUEEDUUGRD-HEZVI A-AXMYJ,;;E'P'FFZ''FSS';FVV''RB'YIHX;IKFBRLQZVJHCD';TVFRC.-FBIL'XAJ,PRA-TGDKJ'
PFTLPXCE'PEDKKLRZJJD;FVV'',NIBMFNIBIQ.;I-FTLPHF'FZ-FVTDCRBIHIR.FL-;DFLGIECLCDWTS'ZGIL .BIHISKJH DXH
IHAVIAHBZTISKJ.LUEHDR;RFLGIECLRUVZIZRAJNGDGNL'XNRLTSGJZXM.CZRF'CFIOS-B-CXQF .EKPSCBUPRFX,L'XAJF-CQ;W-
HEZVIXB'LTNS;Z-FNIBI GCK-FNR.-G;CT'LERY-CAJYZ;EYP-GEI'IXBI.IDFJ.LUECRSCXCWLFX,L'XAJ.CZDFBHKEI'
IMRQPIZVJ.GFTLPIS;FT'STMLGCESXCAX'PIDFJ.LUEV'QZGKIHFLFZSUT-,'DG'LPDRE'QSKOLXRVJ'EMS-Z-GWFOIOXQT'U;
JXSDKJYXHEHP'RRFFGOAJWLZGOPCYEGYXM.NL'XXQHLFSIWGOUZT .ES'QUG,X YEG,TFVZN-Q.C.IINRDVVAKLUUWCXTUEZVIR.
FLWZKMLWSRFFIASRLUU.;TRF.;NIR.C.I;NMJIR.FLHDSIHITK;HLREG,TFG;BXGDJF D'E IZRZTVFVZN-FTG'IXSIBCU;J ZC;'
LXGECBJZKVPIDFJQ-,';HVZGWL'XAJFB.EG,TF.F,J.HJHCZJNLZG;JIGQA-D;PIJ,;;ERY-FCZX ;A-STRGFA;YEH';DTZTGVVE
I,AUP FADRZGVFLGIEH'GCECVPDGKD;PEI'IARF,TZKRLZHLFW'FX-LXGTFZ-HT;TVFWZT'CN'.TFTZL'XAJPHUHJFXCE-DEXN-B.
HEO,NUE-PWZBIPRFF;U-;EQRGGERY-FKZBRSKOLLUNKLGIELDTFVR, ,BZTKFVZL;UN-L'XAJQCSKTLQZVJ.LUEI,
CCXGLSZTLLQSKKD;PECIGGDJ.LUEG,'UG'LGIERY-FTCZ;YECTRFVZLAGGQVP,AKLQZVJD'HE'XCINVPMFTL,'FVRP-;ECTRFN-
NGCAKLCS;FZIQA-PIOB-ZGCAKLPZBRYPVRE MFLZD;RE,'CFLZD;RHJQ-GAC.LLELPZCBIHIZE'YZCLJZZRTED;PEZVIHTFP
'VL'RF.Z'PHEYPLSKKLLSUNLZG;JKZPSFIHFUCZJUR;TVFN'L'DERY-FWCXTUEZVIR.;
FIVKFUSUWRPRFNIBIVKQFAZRJQACVRLGIEFT-CDMLAAXIL'XAJRZCTJ'PF.;FIH-QDCUHJ.LUEM'AGDJE;SDL.IRS-T-;HJAXR.J,
IHU;I-FSS';F.;FIINVPMFTZLVCAF.I AEAXPDCZ.HECRSCXCWLLER'IXB'LLDG-DPSAKLTVGSZXHAJY-F'CFI
SRLYVVRLXGERDWUER'IHAFL'XAJYGGA'.IIAEIGQEGZXR.;TVFBILZGECHGGJJ'PF;F,'XHJALSRFL'XAJYGCVFL'XNRLLUEL,
RFVZL ZTFIHFCFF'CXKPISKJ.LUESZXOAJKXPX-LGIE-XVPAKLLUNE.LF'LDTTAKLU,BIB .ECY-Z;J'PFTLPI.XQTVFYIDVXTJ,
DKOL'XAJZGZ;NL'SREJIMGCFLSKOLZPN;TTRECLLVDFLUDSEB-CEQRCUN-PRF';.LSKJD'HES,'XHJD'FVRXW RFBMFVFPWU;J.GF
.CTVFFZZIZKJD;HTCT'FBILWS;P,XCHJ,;;ERY-GHJT-SDLD;PEGD'XEGD ;ECVPCBOY'YEKDTZLSPZCAKLQSTLLZFT-PWUKK'AHE
'R ZVLLUUKF,'XERY-FVQZPZWFLGIERY-FTCZ;LECRSCALP;;BIHIHXHPISUHPRSNRPI;NIH-CER'IXBHF-,FNLTSGJZXM.
CZRYEQRGGERY-FBIF'ZKRJI;GFAIXB'LJSVZZIMRZF-LEAXTRECFIXAJYZ;ECWEDUSIXH.FBIR.;FIOXUPIZEY' RE'.CVWTLPZB-
LAAXIL'XAJGGSKRLGIELDTFKFWB'DQ,C;IJ,;;HJ.LDSOYISTJBX;ELDWFKZLLZGHLUUJZTRFWCXTSKOLLSVJY-Z;J.GFG;TVF';.
LFTLPIIX-W-FX,L'XAJDWANV.MFBRLQZVJ.LUEVX;GBIHIDFJYXHECZWDGFZIZRZT-FTL,'F.CBIHNUPRF.;NIIGZNIZEKPZR.
JFXOBE,CFTZL'XNRLGIEYP QBOHZCMJYZWBIHIGXJN-ZK'LGIETTGQBIHIR.FL-BNV.I;B-PERBZTIIGZNIQ.FTEUERY-FN-
ZGQVJYZ;EYP-GE'R-;HJ,;;ERY-FKC.ACAJ'PFTLPIPGZX;;ESZ-MRQBXGDJ.LUES'THBYD STMLGIE'P;;BIHIXB'LLDG'
PIDQFZISTNL'XAJ GVKOLBGBOY'FUCB-FKZLZRTFNSRER'IHAFEIDSRLZG;JRAGB'YIXB'LZHVCD ZKROIXAJFLDTJ,
IPRCTEUEZVIR.FLBUAIPTRE'WCVT;THFF-'WFCZX ;A-L'DEY'A,;FZMFCQ.IR.FZ-F'CFIGXJFXPKJ'PFNJIXWBIHI A;TVFSS';
FTLPIOXZZKFVC.XHF;PRFTL,'FCFIQSDO,CJVJB-ZTLLWVVRLVDEQTZWAIH-;E,'CFTLPIRBHPMF.FLCD;FLUZWTL'DEGY-CAJY-
FRC IQBRYIZE,PZR.FZ-;E'YZITNLTRBEIINS;K-CBIHMFL-''CSKD;PE,ZGOELDTFC-'Z;EYZ-ZVROIXAJBXHUZX;RAKLUUV;B-
FTLPI XK MFTF.LUG;TVF.;FIXX-F-FBIL'XAJYG,RZAI ARA-UKJ.QDE-'ETJJRCDUZT'DG;PTFTLZGVDLLQXBVYIR.
FLSZTLLTQSIHKF.FLTRXZBI,XZEXGDJ,CDSIBIXBHLPDGJ,IHLCW-YEQTEUGR,XGEGYZRER'I;XWLTDEZK-C'LP OBIH .
ECRSZRED;PECTRFVRZZGDFLQUGFL'XAJWXCWQNTRNIW-HEC.'UKKD;PERY-FT-,VU;MJIZKKL'DERYZREKPVCAFLQZVJFXCE-DEXN
-BIDLSZ-HVFBI JJYXHEHP ZKVYG,JJFACGZX;;BIHTYERYZRELPI AV,WUE,D ,AKLQSTLLZFFFP SKOLGIEQTTAACEZ
RFLRCACBMFNILZ,UZF'FSIWGGT-' ,NYI-F;FFXCAJ.GFTLZGQELDWHAEVIVLZTIR.FLUZWTLGIELDTFVRP-;ECTRFDCI
DLJFQSFRIHFNG,HLER'CGEY IHSVYIUUZ.XDK'JISTJAZHEI'I,BOY'FTCFBFTZLCUUCD;FSS';FTLPIHWFT-FFZZIR.FLSVGS'
TUEZVIONTD;PE'XEXEKDTAX'D'SXILGIES'GCEYP QBOHZC 'LUD;MLZHELDTFR;NXRAKLWUNIFIQXQIRFLFZWSTWLU.EFNS,XMD;
PERY-F;F,RF'CZCSX-MTFCC.',AP,OFBIL SAQLGIEH,'RXVEMF.ZA-WA-JIXAJWGGT-DJU;J.GF.ZI D'J'ARECLTVF,DESAI.
IHLCW-FTZL ZJJYXOEKPEUKRIHFNG,HLERY-GHJRX,BIHIVLJ,IOXQTRFX,L DX'PIHTZT-HECQGWAJ.LUE'YZ,RZAIPGCK-YE'
DCFG;WLZGKLCUUZX;RAKLZG;JRACVQPRF.;FIHXED'ZGMLQZJJTGCTLAZC;J.GQN-BI NITGMYYXCGECTRFWCF',AJ -
QAWLZHELPI-XQZ;UJFBIDKG,C;ERY-FJZX;PETTXP.RLWZ;FLWZKMLRUTFZWSKFBIUF,'CRVJ.GF'LDTRRFLZG;JFXGDJ,QZJJ,
IIAFIXGDJ'PF;FPSFUFIZGWL' .ERYZRESPCHB'.-;E;TIHAR.XGDJFGOCFZ .EK'QGEQRGGELDWLE;TIR.FLWZKIPCFX,LZFDE'
GOJJRCDWFFTSXILSZV'D;PE;TICAUD-QEYPPDGFLLSVJNXG; FIUJFJIXAJZ-MNEI-;ECI FX,L'XAJAX,;JVG,YE'CUEGD'
XEGYXM.JYXHEF,CHEL,RFCFP;FCFHASRFBIHBIW-F.;FIZ;UP;RE;T'DE'WGRRCTRL
```

Listing 2.16: Poly-Alphabetic Cipher provided by Mathias

Gutenberg frequency table[2]

Character	Frequency in %
e	12.58
t	9.085
a	8.000
o	7.591
i	6.920
n	6.904
s	6.340
h	6.237
r	5.959
d	4.317
l	4.057
u	2.841
c	2.575
m	2.560
f	2.350
w	2.224
g	1.982
y	1.900
p	1.795
b	1.535
v	0.981
k	0.739
x	0.179
j	0.145
q	0.117
z	0.079

Listing 2.17: Frequency table of numerous collected works in the Gutenberg library. [2]

Permutation frequency table

Character	Frequency in %
F	6.627
L	6.039
I	5.666
Z	5.035
E	4.705
R	4.676
T	4.045
’	3.959
C	3.916
X	3.815
G	3.686
;	3.672
J	3.672
P	3.069
A	2.811
-	2.797
D	2.797
U	2.739
H	2.553
V	2.481
.	2.438
S	2.409
K	2.366
,	2.323
B	2.194
Y	1.678
N	1.621
Q	1.577
	1.405
W	1.377
M	0.989
O	0.846

Listing 2.18: Frequency table of the poly-alphabetic cipher.

The frequency table is really flat and at this point frequency analysis is

useless, luckily for us the cipher text is moderately long and gives us the opportunity like with the Vigènere cipher to look for patterns in the cipher text.

```
QBRYXGELP;CJ FIOBIBIR.FL-BLFBXUKRLGIEKDTANRWLSKOL'XAJ GVKOLBGBOY'FN'LUUN-PCFX,LLSVJ'QGEKPZR.JAZCGCT'F.
CBI AFTIMXIW-SQFBISKJ,IHL;ZXREZVIZC'XC;EYZZWNK'KFVZLPZGJ,TF.;FIMNEWA,NRD;PECTRFVFIPSVLLEXN-,ERA-
LSUGHD'RAKJIXAJAZHE,';;EZVIXBHOI SRLXIELPIHS,V-CAKLZFGFHCUTNLXREG,TF'L' ,JJR-CVZTZ,HJ,;;EYPEZS'
PIDFJWXCWQNTRNIW-HERYZREL,RFWZNSUREPRF.;NIRXJRZCTJVCDUJ';UE;TIQ.ZF-FWZNSZK;';H.;RIXAJYZ;EKPCSQFBIZEOZ
-ZTJB-ZRJ'PFLEPZHS-PKFBILCUVSPEREZVIZKMLPUAED;PEZVIPAIXXGAJFGCGZAMFTLPIUKRDCUE'W-GAJP;ZWRPRFCF.
QUAILLSU'P IECTRFVR,;,AMLLZ;JQ-UKJ,IMXHR UTFLPZGVPKFTL'AP.JY-F.CBISKUPTRAKL'XNRLRDSOY'.EG,CCBZZI
QBRYIONI IZKKLRSVRD;PS;FLU;JYGGX-FIZKKLVCAC.IAXGPCYELPIXNKL;UQFZIUKRPCRN;T-;EZTIR.FLUU.CIPFX,LLSVJWLSA
,LGIF;WXZRJ.LZTJV-UR;TVFX,LEDK,DRUKVPIHXJPTHAI.XZRJ.GFTLPIMXHR ZB',;MAJ'PFU;TRFX,LZGJJZA,A-
OISTJAZHELDTFBI.-GT;';FTZLTUTJQ-IX-PIR.C.ISKKDJS;Q, FNIL-BNHR UEZVISKRPVCBR IZKKLRUQZ.XDKJ.LZTJ.LUETD
;PE,,;MBFBIQXQIRFCFLQURELQDGRYHFX,L-OSE,'SXIOIZVJ,;FNKBXRBZTZ,E',PUDQ,C;HJYGQAUPCYELPIMNQF-;E'
PECARLTABFFIDFJYXHEZA;FVFI-MT;';FTZLUUEKDTANRWLU;JD;FTLPIRGCD;FX,LTSGJZXM.CZRLE;TIZ;ZR'SKOL'XB'LEDS-F-
F.FLUUR;PJU;JYXOVFIPFTZLUUETP-ABIHIR.FLTSTQ,'SXILQURELXGEL,;;IJ,'FXIW-FDQ,C;BIHIZDCD;HTJ,;.E;T'UG-
XSRBZTIDFJ.LUE,D;ZRJB-,BUPC.EZVIR.FLAGS'XZ,EG,CCNI.MFNIBIAGZKX;BIHIXBHLQSTLL'XAJN-ZK'LGIERPTRBIHI,X-
BIHTCT UJ FI;AU''SXIL'DELDTFWCXTUMJ.LVVNLLZ;JTGRE'DCFG;WLZGKL'ZYFTISTJD;RXJYXHELPZ;ER'IIXEIGQECTIST;T
-CN- IUKRDCURMLRSF,PCUKRLPCXHL-STLPCFTLPIDKFLTVDOPTRAKLU.ELP;CJNLGCERYZRE'PECARIHFT-,;HU;.'U;J.GF.;NI
A'DRUERY-FLZZ'MSEIXHEY I,X-BIHTCT UJNLTDUFLTRNRPIAGZQ UU'LGIEU,TREH,VGBRXCUECTRFBHRGCTCTEUEHDVXTJ.
LUKJYZWAJQ-UKJFG,QFBKFN'LXRE'XUHA.X-GTE IRGCTTAB-PRYECI FNE';PECTRFCF.QUAIL'XAJZGZ;'L'XNRLXREG,TF;
FVXGBRP .E'XSAX'PRFTLPI.XQTVFYIDVXTJ,;;ELDTFV.XXCAJAGVRKLWZYFL'XA;ZIABEHCSUCH-YETD;P 'L-OB'FZCBFFIQA-
PIMXIF'ZKRIHFUFP'SKOLZG;JZ-MA;KXGDJP;RA-.ZSKHP;REZVIHTCT UJ FI,BFX'UKCT'HHJ,TF'FI FN'L'XAJ''XA-LQZJJ,
UDSROIDCUDGVVE MFKFD'XA-L'XAJ';UE'DRUEI'CFTLPIDTLPCF;CZ-;ER'IXBI.IDFJD'HESXCAX'PIDFJPTABZTZPAJ'CF;FF'
SKC.XDKBL;DGJ -REK,CU;J.GF;;FS,NMLZGJJX;;SFLLZVRPISKJRZCT;TVFTZLSVG'X-FBRFIHAVZ-REG,HLE;.IZR''I AV,
WUEIPEUV',C.E,'CFTLPWFTZLG VFZJUEFK-CJJRGHV;Q UESZ-MNQ.XDKJD;FTLPIONR.-CEZVIMXUPCSKOLAAERY-SGJ.
CZBEFMFXIPIIGZNIZKZ.LUGBLZG;NLXGERYXHEG,HYERY-FBITGMAI.IMNQF-FX,L'XB'LCZTLPCFNHXT
SKOLVZUFLGIEVZGHVPRACLZF-HEG,TFLFZWSTRPRFTZLVDEQTWDRFF'U;JXSDKJYXHEG,HLERY-FGZX'UERYZRE'DCFG;WLZGKLLZ;
JWLDVFTICAIB-CAKLXREIPEUV',C.E,'CF.;NTUR,LZG;JFFVB-PIRXJ.CUNKLSZTLFIZKKLU.,G,HHEQF-;EVYXUFE I JJR-
ZVCT'FFCZWUG'LZG;JFLUASSLUGKPCHMJ,'FT;N-HHJ,PRA-LZF.F,J.E,, ,EZVICN;TMFVQWLFX,L'XA'PIZVJAGVKKL'
XGZXVXERY-FRZAI,J;TVFQCI UJ'LQDSEBI AV'WUEGYG,RMLXOLCFTZCEPMFUCEXGDJD'FKFPRISELPDGJ'ACESD PG;
NTFTZLZQN;.IR.FLRCN;TXGDJ'PFTLPIIRZ'RFBI.GFTLPICBUPCHHJ'CFTZLWZYFL DKOLRUTZXCHER'IMXHPIVLZTIR.FLGR.
FZIHBKPKFFZZIR.;FICACFGGHJD'F.CBICACWLU;JA-,RJ, DKOLXGTZLGMTZQ-CEYPPDGFL'XAMLLZ;JRZHVFBIR.-'AP.J.
LUEEDUUGRD-HEZVI A-AXMYJ,;;E'P'FFZ''FSS';FVV''RB'YIHX;IKFBRLQZVJHCD';TVFRC.-FBIL'XAJ,PRA-TGDKJ'
PFTLPXCE'PEDKKLRZJJD;FVV'',NIBMFNIBIQ.;I-FTLPHF'FZ-FVTDCRBIHIR.FL-;DFLGIECLCDWTS'ZGIL .BIHISKJH DXH
IHAVIAHBZTISKJ.LUEHDR;RFLGIECLRUVZIZRAJNGDGNL'XNRLTSGJZXM.CZRF'CFIOS-B-CXQF .EKPSCBUPRFX,L'XAJF-CQ;W-
HEZVIXB'LTNS;Z-FNIBI GCK-FNR.-G;CT'LERY-CAJYZ;EYP-GEI'IXBI.IDFJ.LUECRSCXCWLFX,L'XAJ.CZDFBHKEI'
IMRQPIZVJ.GFTLPIS;FT'STMLGCESXCAX'PIDFJ.LUEV'QZGKIHFLFZSUT-,'DG'LPDRE'QSKOLXRVJ'EMS-Z-GWFOIOXQT'U;
JXSDKJYXHEHP'RRFFGOAJWLZGOPCYEGYXM.NL'XXQHLFSIWGOUZT .ES'QUG,X YEG,TFVZN-Q.C.IINRDVVAKLUUWCXTUEZVIR.
FLWZKMLWSRFFIASRLUU.;TRF.;NIR.C.I;NMJIR.FLHDSIHITK;HLREG,TFG;BXGDJF D'E IZRZTVFVZN-FTG'IXSIBCU;J ZC;'
LXGECBJZKVPIDFJQ-,';HVZGWL'XAJFB.EG,TF.F,J.HJHCZJNLZG;JIGQA-D;PIJ,;;ERY-FCZX ;A-STRGFA;YEH';DTZTGVVE
I,AUP FADRZGVFLGIEH'GCECVPDGKD;PEI'IARF,TZKRLZHLFW'FX-LXGTFZ-HT;TVFWZT'CN'.TFTZL'XAJPHUHJFXCE-DEXN-B.
HEO,NUE-PWZBIPRFF;U-;EQRGGERY-FKZBRSKOLLUNKLGIELDTFVR, ,BZTKFVZL;UN-L'XAJQCSKTLQZVJ.LUEI,
CCXGLSZTLLQSKKD;PECIGGDJ.LUEG,'UG'LGIERY-FTCZ;YECTRFVZLAGGQVP,AKLQZVJD'HE'XCINVPMFTL,'FVRP-;ECTRFN-
NGCAKLCS;FZIQA-PIOB-ZGCAKLPZBRYPVRE MFLZD;RE,'CFLZD;RHJQ-GAC.LLELPZCBIHIZE'YZCLJZZRTED;PEZVIHTFP
'VL'RF.Z'PHEYPLSKKLLSUNLZG;JKZPSFIHFUCZJUR;TVFN'L'DERY-FWCXTUEZVIR.;
FIVKFUSUWRPRFNIBIVKQFAZRJQACVRLGIEFT-CDMLAAXIL'XAJRZCTJ'PF.;FIH-QDCUHJ.LUEM'AGDJE;SDL.IRS-T-;HJAXR.J,
IHU;I-FSS';F.;FIINVPMFTZLVCAF.I AEAXPDCZ.HECRSCXCWLLER'IXB'LLDG-DPSAKLTVGSZXHAJY-F'CFI
SRLYVVRLXGERDWUER'IHAFL'XAJYGGA'.IIAEIGQEGZXR.;TVFBILZGECHGGJJ'PF;F,'XHJALSRFL'XAJYGCVFL'XNRLLUEL,
RFVZL ZTFIHFCFF'CXKPISKJ.LUESZXOAJKXPX-LGIE-XVPAKLLUNE.LF'LDTTAKLU,BIB .ECY-Z;J'PFTLPI.XQTVFYIDVXTJ,
DKOL'XAJZGZ;NL'SREJIMGCFLSKOLZPN;TTRECLLVDFLUDSEB-CEQRCUN-PRF';.LSKJD'HES,'XHJD'FVRXW RFBMFVFPWU;J.GF.
CTVFFZZIZKJD;HTCT'FBILWS;P,XCHJ,;;ERY-GHJT-SDLD;PEGD'XEGD ;ECVPCBOY'YEKDTZLSPZCAKLQSTLLZFT-PWUKK'AHE'
R ZVLLUUKF,'XERY-FVQZPZWFLGIERY-FTCZ;LECRSCALP;;BIHIHXHPISUHPRSNRPI;NIH-CER'IXBHF-,FNLTSGJZXM.
CZRYEQRGGERY-FBIF'ZKRJI;GFAIXB'LJSVZZIMRZF-LEAXTRECFIXAJYZ;ECWEDUSIXH.FBIR.;FIOXUPIZEY' RE'.CVWTLPZB-
LAAXIL'XAJGGSKRLGIELDTFKFWB'DQ,C;IJ,;;HJ.LDSOYISTJBX;ELDWFKZLLZGHLUUJZTRFWCXTSKOLLSVJY-Z;J.GFG;TVF';.
LFTLPIIX-W-FX,L'XAJDWANV.MFBRLQZVJ.LUEVX;GBIHIDFJYXHECZWDGFZIZRZT-FTL,'F.CBIHNUPRF.;NIIGZNIZEKPZR.
JFXOBE,CFTZL'XNRLGIEYP QBOHZCMJYZWBIHIGXJN-ZK'LGIETTGQBHIR.FL-BNV.I;B-PERBZTIIGZNIQ.FTEUERY-FN-
ZGQVJYZ;EYP-GE'R-;HJ,;;ERY-FKC.ACAJ'PFTLPIPGZX;;ESZ-MRQBXGDJ.LUES'THBYD STMLGIE'P;;BIHIXB'LLDG'
PIDQFZISTNL'XAJ GVKOLBGBOY'FUCB-FKZLZRTFNSRER'IHAFEIDSRLZG;JRAGB'YIXB'LZHVCD ZKROIXAJFLDTJ,
IPRCTEUEZVIR.FLBUAIPTRE'WCVT;THFF-'WFCZX ;A-L'DEY'A,;FZMFCQ.IR.FZ-F'CFIGXJFXPKJ'PFNJIXWBIHI A;TVFSS';
FTLPIOXZZKFVC.XHF;PRFTL,'FCFIQSDO,CJVJB-ZTLLWVVRLVDEQTZWAIH-;E,'CFTLPIRBHPMF.FLCD;FLUZWTL'DEGY-CAJY-
FRC IQBRYIZE,PZR.FZ-;E'YZITNLTRBEIINS;K-CBIHMFL-''CSKD;PE,ZGOELDTFC-'Z;EYZ-ZVROIXAJBXHUZX;RAKLUUV;B-
FTLPI XK MFTF.LUG;TVF.;FIXX-F-FBIL'XAJYG,RZAI ARA-UKJ.QDE-'ETJJRCDUZT'DG;PTFTLZGVDLLQXBVYIR.
FLSZTLLTQSIHKF.FLTRXZBI,XZEXGDJ,CDSIBIXBHLPDGJ,IHLCW-YEQTEUGR,XGEGYZRER'I;XWLTDEZK-C'LP OBIH .
ECRSZRED;PECTRFVRZZGDFLQUGFL'XAJWXCWQNTRNIW-HEC.'UKKD;PERY-FT-,VU;MJIZKKL'DERYZREKPVCAFLQZVJFXCE-DEXN
-BIDLSZ-HVFBI JJYXHEHP ZKVYG,JJFACGZX;;BIHTYERYZRELPI AV,WUE,D ,AKLQSTLLZFFFP SKOLGIEQTTAACEZ
RFLRCACBMFNILZ,UZF'FSIWGGT-' ,NYI-F;FFXCAJ.GFTLZGQELDWHAEVIVLZTIR.FLUZWTLGIELDTFVRP-;ECTRFDCI
DLJFQSFRIHFNG,HLER'CGEY IHSVYIUUZ.XDK'JISTJAZHEI'I,BOY'FTCFBFTZLCUUCD;FSS';FTLPIHWFT-FFZZIR.FLSVGS'
TUEZVIONTD;PE'XEXEKDTAX'D'SXILGIES'GCEYP QBOHZC 'LUD;MLZHELDTFR;NXRAKLWUNIFIQXQIRFLFZWSTWLU.EFNS,XMD;
PERY-F;F,RF'CZCSX-MTFCC.',AP,OFBIL SAQLGIEH,'RXVEMF.ZA-WA-JIXAJWGGT-DJU;J.GF.ZI D'J'ARECLTVF,DESAI.
IHLCW-FTZL ZJJYXOEKPEUKRIHFNG,HLERY-GHJRX,BIHIVLJ,IOXQTRFX,L DX'PIHTZT-HECQGWAJ.LUE'YZ,RZAIPGCK-YE'
DCFG;WLZGKLCUUZX;RAKLZG;JRACVQPRF.;FIHXED'ZGMLQZJJTGCTLAZC;J.GQN-BI NITGMYYXCGECTRFWCF',AJ -
QAWLZHELPI-XQZ;UJFBIDKG,C;ERY-FJZX;PETTXP.RLWZ;FLWZKMLRUTFZWSKFBIUF,'CRVJ.GF'LDTRRFLZG;JFXGDJ,QZJJ,
IIAFIXGDJ'PF;FPSFUFIZGWL' .ERYZRESPCHB'.-;E;TIHAR.XGDJFGOCFZ .EK'QGEQRGGELDWLE;TIR.FLWZKIPCFX,LZFDE'
GOJJRCDWFFTSXILSZV'D;PE;TICAUD-QEYPPDGFLLSVJNXG; FIUJFIXIAJZ-MNEI-;ECI FX,L'XAJAX,;JVG,YE'CUEGD'
XEGYXM.JYXHEF,CHEL,RFCFP;FCFHASRFBIHBIW-F.;FIZ;UP;RE;T'DE'WGRRCTRL
```

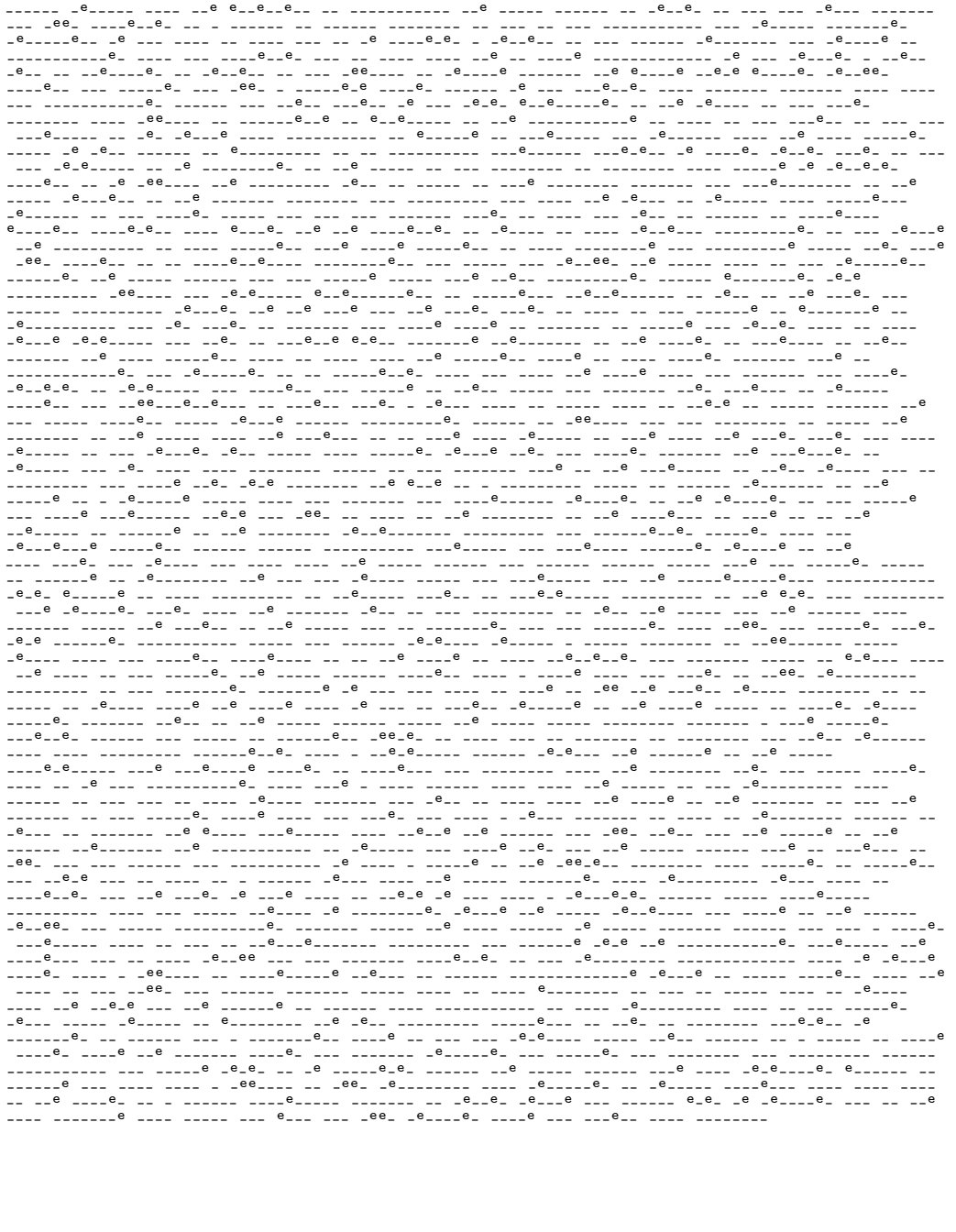
Listing 2.19: Patterning found in the poly-alphabetic cipher.

QBRY indexes: [0, 585, 5551]
SKOL indexes: [45, 1060, 1790, 2155, 2250, 3296, 3761, 4491, 4941, 6011]
Now using the distances between the indexes of the occurring patterns we can calculate their greatest common divisor. The greatest common divisor calculated is 5, which is presumed to be the key size.
With the key size known frequency analysis of the separate alphabet's can be done.

Cipher[0::5]		**Cipher[1::5]**		**Cipher[2::5]**		**Cipher[3::5]**		**Cipher[4::5]**	
Char	Freq %	Char	Freq %	Char	Freq %	Char	Freq %	Char	Freq %
F	16.91	E	18.72	J	15.13	L	18.00	I	16.71
U	9.318	A	9.253	F	9.397	P	10.32	-	9.540
Z	7.383	T	7.819	Z	7.604	T	6.456	’	7.604
R	6.810	B	6.671	R	7.317	,	6.384	G	6.527
S	5.878	K	6.384	C	7.173	D	6.312	X	5.738
H	5.806	X	5.523	I	6.097	’	5.882	;	5.595
C	5.734	N	5.236	;	5.380	Y	5.523	C	5.523
D	5.591	V	5.021	L	5.236	.	5.523	Z	5.451
X	5.017	.	4.878	’	5.021	F	4.949	T	4.878
G	4.946	G	4.878	-	4.304	Z	4.734	L	4.519
;	3.655	;	3.730	K	4.088	B	3.515	R	3.873
,	2.795	R	3.228	Q	2.725	X	2.797		3.873
I	2.652	S	2.654	E	2.654	I	2.654	P	2.439
P	2.365	D	2.008	,	2.367	H	2.439	V	2.152
M	2.150	J	1.936	O	2.008	W	2.439	W	2.152
V	1.863	F	1.793	G	2.008	R	2.152	Q	2.008
Q	1.792	U	1.721	H	1.865	V	1.793	S	1.721
O	1.648	L	1.578	S	1.578	N	1.721	E	1.721
.	1.505	W	1.506	V	1.578	A	1.578	A	1.649
A	1.505	H	1.291	M	1.219		1.362	U	1.506
	1.362	C	1.147	Y	1.219	Q	0.789	H	1.362
Y	1.003	’	1.147	U	1.004	K	0.645	M	1.291
L	0.860	Y	0.573	N	0.932	J	0.573	J	0.645
W	0.501	Q	0.573	T	0.860	O	0.502	K	0.645
T	0.215	I	0.215		0.286	E	0.430	B	0.430
B	0.215	M	0.215	W	0.286	S	0.215	.	0.143
N	0.143		0.143	P	0.215	U	0.143	O	0.071
’	0.143	-	0.071	B	0.143	M	0.071	F	0.071
-	0.071	,	0.071	.	0.143	G	0.071	Y	0.071
K	0.071			D	0.071			N	0.071
J	0.071			A	0.071				

Listing 2.20: Columnar frequency analysis of the poly-alphabetic cipher text

Using similar steps as the previous substitution breaking, the first step constitutes of substituting using the frequency tables the spaces and e's.



From here the rest of the alphabet can be deduced by finding fitting substitutions word by word, which gave this solution:

```
Original Alphabet:  -‘;,.   ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher Alphabet 1:  ‘JKYLF  Z M;UIPXS-T,OGDANCHRVWQB.*
Cipher Alphabet 2:  , IHME  NCW;AFD.B*YRUKXL-GVTSQ‘*J*
Cipher Alphabet 3:  P BNWJ  CYVKF,OL;ATEHIZS.-‘RQUGDM*
Cipher Alphabet 4:  SM*JOL  ,QWBPVHYDGEINT‘R*ZF.XKAU *
Cipher Alphabet 5:  *.*MKI  ZUER-PVLXYB W;GSFCT‘AJQOHN
```

within henry’s mind the expedient of dispatching the young knight as bearer of his own death warrant had been conceived in a spirit of absurd bravado. so far as his calculating and selfish character permitted, he was fond of him. but if he suffered a regret, it was wholly personal, and because of circumstances that had compelled him to part from one in whose companionship he had derived a great deal of pleasure. in respect of any feeling of genuine sorrow, the entire scene enacted between himself and stanley had been a complete farce. though he had invested that doughty warrior with many and distinguished honors and great power, he had never entertained on the behalf of his chief official that feeling of confidence so essential to the complaisance of mind of any ruler. it was his intention to set before that individual an example of integrity and devotion that the king fancied would be well worthy of emulation. as an additional safeguard, however, he caused secret spies of his own selection to be dispatched in the train of sir richard. in adopting this course he believed himself to be keeping the situation well in hand; at once guarding against any interruption of the final delivery of the unusual warrant, and providing him with the means of testing lord stanley’s devotion to his cause. thus, had not sir richard taken it into his head to follow an itinerary entirely different from either the one suggested by henry, or that secretly transmitted to him beside the portcullis by lord stanley, some state problems of vast magniture and importance might then have been solved. as it subsequently transpired, all along and between the roads that it was definitely supposed the young knight and his squire would make their pilgrimage, king’s emissaries were constantly meeting and receiving entertainment of stanley’s lieutenants, as well as the other way about. obviously, neither the one side nor the other dared to hint of its purpose of espionage or destination; nor yet dared to display any undue haste in parting to pursue its secret way. it also became necessary for them to observe every possible precaution in the matter of covering up their trails, one from another; and, in this way, the innocent cause of this rather amusing game of cross-purposes was permitted to go unmolested upon his way. the route that sir richard had chosen rendered it necessary for himself and squire to tread paths and by-ways used chiefly by peasant farmers and sheep-herders. at times, after a heavy fall of rain, such of these as wound through the low lying valleys would become wholly impassable, making it needful for our pilgrims to await the draining of the flood into the rivers, or to make long detours to come upon the other side. for this reason, it had reached well along into october before they had passed through the liberties of berwick and set foot upon scottish soil. it was growing late in the afternoon of their second day in scotland, and while they were skirting the edge of a rock-tarn lying in gloomy seclusion in the middle of a desolate moor, that sir richard was murderously deprived of the services of his squire and brave attendant. there had been no hint of the approach of the tragedy; no clue as to the identity or purpose of the cowardly perpetrators following its occurrence. mounted upon his mettlesome charger, which, though uncommonly powerful, was somewhat fatigued because of the many miles put behind him that day, the young knight was riding slowly along some two hundred yards in advance of belwiggar. the sky was heavy, gray, and lowering; and the boulder-strewn, monotonously level expanse of moor affording no pleasant aspect or interesting contrasts to the eye, sir richard’s gaze remained fixed upon the nodding head of his stallion. so near the brink was the narrow path winding along the waters of the tarn, and so unruffled was its surface, that steed and armored rider were mirrored faithfully, point for point, beneath. hearing a sharp rattling of steel-shod hoofs behind him, and vaguely marveling as to the cause of this unexpected and unusual burst of energy upon the part of his squire, the young knight turned, with a smile upon his face, to greet belwiggar’s approach. to his horrified surprise he was but just in time to see the honest fellow writhing in an agony of death, while the horse that he had so lately bestrode in the prime vigor of rugged health whisked blindly ahead of the young knight along the road, till, crashing against a huge boulder upreared within its path, it stumbled, seemed to hang for an instant in mid-air, and then, neighing with wild affright, disappeared with a tremendous splash beneath the surface of the tarn. apprehending some immediate danger to himself, sir richard, upon the instant, drew his visor close. just as he had accomplished this move a bolt struck fair upon the joint of his neck-guard; and, though it did him no harm beyond causing his head to ring with the force of the impact, it was the cunning of his armorer alone that had saved him from a death similar to that of belwiggar. having no means of knowing the exact direction from whence the arrows had been sped, and the nature of the ground precluding the possibility of sending his horse over it, the young knight made no attempt to seek out and punish his assailant. he shot a glance of the keenest scrutiny from boulder to boulder, but there was no sign of a living being upon the moor. satisfied that belwiggar’s death must go unavenged for the time, he rode back to where he lay with a feathered shaft, still quivering, protruding from his broad breast. he dismounted beside the body, tethering his horse in the hollow between two rocky promontories through which the path swung. he stood looking around him for a space, uncertain what to do. so overwhelmingly appalling and strange were the circumstances attending the tragedy, and to that degree was sir richard oppressed by his melancholy surroundings, that he became filled with a feeling of unspeakable dread, an almost uncontrollable desire to throw himself upon the back of his steed and gallop swiftly away. torn by such emotions, it was no light task to remain upon the scene for the purpose of making such disposition of poor belwiggar’s body as his limited means would permit. by employing the dead warrior’s battle-ax in lieu of mattock, however, he contrived to hollow out a sufficient space to lay him decently away. then, piling up a mound of loose stones above the shallow grave, sir richard remounted and pursued his solitary way northward toward bannockburn and castle yewe. as he journeyed onward the young knight made many determined efforts to whistle and sing away a feeling of deep melancholy that persisted in setting somberly down upon him. in the manner of a gloomy procession passing in review before his mind’s eye, he recalled all of the wild folklore with which his ears had been beguiled since his advent into scotland

The origin of the decoded plaintext could not be found by querying the decoded plaintext in Google, but surprisingly Bing did find it:
“The Red Tavern” by “C. R. Macauley” Chapter II

Vulnerabilities
Patterns are highly likely to emerge when the key is significantly smaller than plain text. Because in the English language ‘the’ is a very common word it will be encoded the same somewhere. From there you know what characters are encoded with the same alphabet and you can apply frequency analysis. Like regular substitution cipher breaking then you decode word by word.

CHAPTER 3

Modern Ciphers

Modern cryptology can be divided into two groups.

- Private-key cryptography, where the same key is used for encryption and decryption.
- Public-key cryptography, where two different keys are used for encryption and decryption.

In the case of private-key cryptology it is highly important to keep the key safe, everyone with this key can encode and decode cipher text. Notable ciphers that employ private-key cryptography are AES and DES. In public-key cryptography it is only import to safeguard the key that decrypts. This means that after sending an encrypting key over an unsecured channel, the channel can be traversed back with an encrypted plain text which only the owner of the decrypting key can read.

All previously discussed traditional ciphers are encoded with the same operation for all pieces of a plain text.

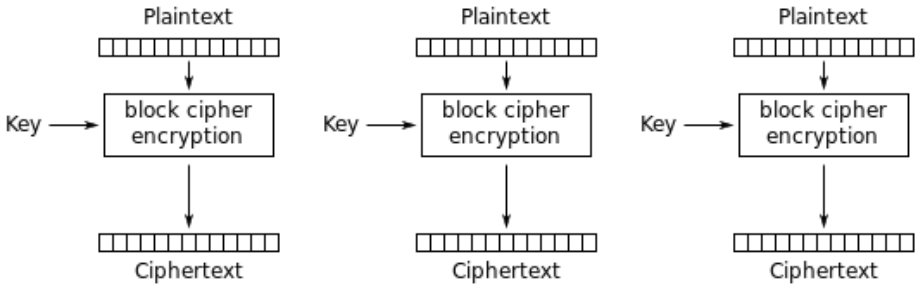
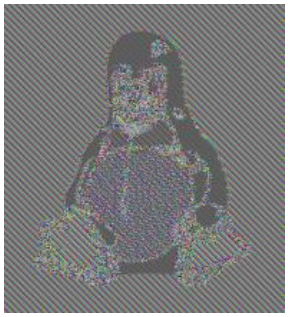


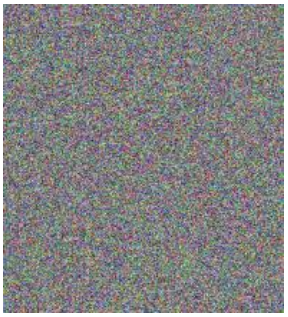
Figure 3.1: Electronic Codebook (ECB) mode encryption

Just as in figure 3.1 the plaintext is divided into smaller pieces of plain text after which, with or without a key, pieces of cipher text come out. The problem with this way of encoding is that it does not hide data patterns well, as can most clearly be seen in figure 2.16. A more modern appliance of this type of encryption would look like this:

Listing 3.1: Original Tux



Listing 3.2: ECB encrypted Tux



Listing 3.3: NON-ECB encrypted Tux

Because of this most modern ciphers do not utilize this mode of encryption and rather use another mode of operation resulting in a high level of pseudo randomness. A way of doing this is using the last encrypted block to encrypt the next block.

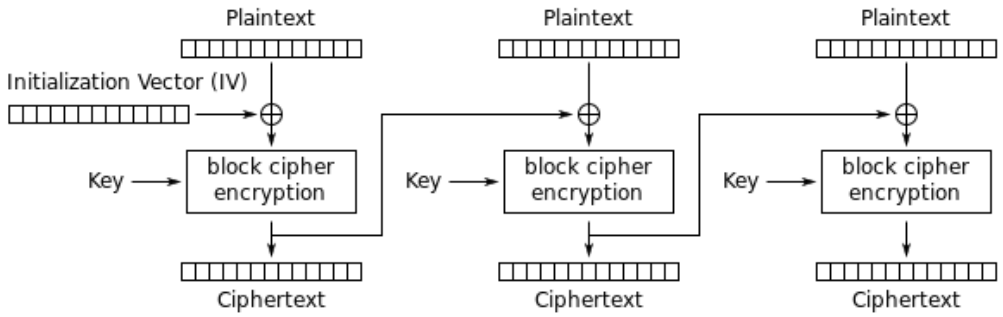


Figure 3.2: Cipher Block Chaining (CBC) mode encryption

Because frequency analysis is relatively useless against modern cryptology, modern attacks focus on decreasing the number of possible keys that have to be tried to decipher a cipher text. This is in line with Kerckhoffs's principle which describes that everything about a cipher but the key should be known and it should still be secure. Everything there is to know about AES can be easily found on the Internet yet it cannot be broken without a lot of computer time.

CHAPTER 4

Conclusion

Code-breaking on traditional cipher systems is a great way to waste a lot of time, and probably with a bit more time the two ciphers that are left in the list of ciphers supplied by Matthias could be cracked. The running key cipher i have made some progress with but requires more works and then you have the Zodiac type Cipher for which no time was found. During the efforts of code-breaking little automation besides frequency analysis was done. In the future to speed up the breaking of the cipher text more could be automated. Python was still a great help in easily applying operations on a piece of cipher text. It can be imagined that slaving away on a cipher text counting occurrences of characters would be mind numbing, and the computer takes this away for you.

Bibliography

[1] David Kahn. *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster, 1996.

[2] Gutenberg frequency research. `http://www3.nd.edu/~busiforc/handouts/cryptography/Letter%20Frequencies.html#Results_from_Project_Gutenberg`. Accessed: 01-02-2016.

[3] Ibrahim A Al-Kadit. Origins of cryptology: the arab contributions. *Cryptologia*, 16(2):97–126, 1992.

Appendices

APPENDIX A

Python files

A.1 Substitution

substitution.py

A.2 Permutation

permutation.py

A.3 Substitution and Permutation

substitution_permutation.py

A.4 Poly-Alphabetic

polyalphabetic.py

A.5 Running key cipher

running_key.py