Table of Contents


```
title: Readme.markdown
author: Moritz Haslhofer (e0025215@student.tuwien.ac.at)
categories: secintro, SS2012
```

Content

- **Readme.markdown**
  plaintext version of this document
- **Readme.html**
  html version of this document
- **Uebung1.pdf**
  this document
- **cyphertext.txt**
  encrypted message
- **symbcounter.pl**
  perl program, that counts the frequency of symbols
- **xxx_round.pl**
  Different versions of the mapping table, documenting the progress of my iterative search.

Caesars wordsalad

Frequency Analsysis as basic idea: If every input symbol s in the cypher is mapped to a fixed output symbol c(s), the propability p(s) of s occuring in any given message of the language should correlate to the propability p(c(s)) occuring in ceasars message.

Step 1

Find the propability of any given english letter occuring in a english message:

http://en.wikipedia.org/wiki/Letter_frequency

Step 2

I wrote a perl script, that counts the occurance of a symbol in a message, and prints the letter, count, and propability of that symbol to stdout.

```
#!/bin/perl -w

my %seen = ();
my $total = 0;

while( <STDIN> ){
    while ($_ =~ /(.)/g) {
    $seen{$1}++;
    $total++;
    }
}

print "symbol | frequency | probability\n";
print "-------|-----------|------------\n";
foreach my $symbol (keys(%seen)) {
    print pack("A9",$symbol) . " | " . pack("A9", $seen{$symbol}) . " | " .
  (100.00 * $seen{$symbol}/$total) . "\n";
}
```

Result:

symbol	frequency	probability
w	5	0.3424
a	153	10.4794
r	42	2.8767
:	1	0.0684
d	24	1.6438
,	24	1.6438
x	75	5.1369
j	2	0.1369
y	83	5.6849
u	1	0.0684
h	26	1.7808
k	18	1.2328
g	38	2.6027
.	5	0.3424
;	3	0.2054
f	89	6.0958
t	30	2.0547
i	85	5.8219
e	29	1.9863
n	21	1.4383
	252	17.260
m	63	4.3150
v	26	1.7808
s	50	3.4246
l	106	7.2602
c	71	4.8630
b	12	0.8219
q	15	1.0273
z	1	0.0684
o	110	7.5342

The " " (blank) is the most frequent symbol. I guessed that it is, in fact the blank symbol in the message.

The next most frequent symbol is "a" - if the message is indeed in english, and the frequencies are not that disturbed, that could correspond to "e" in the message.

Step 3 - naive substitution

I created a simple map, where i assigned each symbol in my table the symbol of the english language frequency table, that had the same rank.

The resulting map was:

```
#!/bin/perl -w
%map = (
" " => " ",
"a" => "E",
"o" => "T",
"l" => "A",
"f" => "O",
"i" => "I",
"y" => "N",
"x" => "S",
"c" => "R",
"m" => "H",
"s" => "D",
"r" => "L",
"g" => "U",
"t" => "C",
"e" => "M",
"h" => "F",
"v" => "Y",
"d" => "W",
"," => "G",
"n" => "P",
"k" => "B",
"q" => "V",
"b" => "K",
"w" => "X" );

while( <STDIN> ){
    while ($_ =~ /(.)/g) {
    if( exists($map{$1}) ){
        print $map{$1};
    }
    else {
        print "#";
    }
    }
    print "\n";
}
```

using that maping, the message transformed into:

LAEHASG NAPIOC DEUAYED TVR DAYH IO TNAT KUALEG BELAFHE NE NAD AOTILIKATED
TNATG IO TNE OATFSAU LRFSHE RM EPEOTHG HFLN VRFUD BE TNE LRODFLT RM
PESLIOCETRSIXG UEAPEH TNE ASWY FODES KSETEOHE RM SAIHIOC SELSFITH AOD
LAPAUSY# NE KUALEH BSFTFHG A YRFOC WAOG IO LRWWAOD RM TNEHE MRSLEH# NE
CIPEH NIW IOHTSFLTIROH TNAT TNE LAPAUSY HNRFUDSAOCE AH EXTEOHIPEUY AH
KRHHIBUE IO AUU DISELTIROH# TNAT NE VRFUD EXEST NIWHEUM ORT TR BE ABHEOT
MSRW TNE LAWK UROCES TNAO TNSEE DAYH# NAPIOC ASSAOCED TNEHE WATTESHG NE
WASLNEH TR PIEOOA BY AH UROC #RFSOEYH AH NE LAOG VNEO NIH RVO HRUDIESH DID
ORT EXKELT NIW# MIODIOC TNESE A MSEHN BRDY RM LAPAUSYG VNILN NE NAD HEOT RO
TR TNAT KUALE HEPESAU DAYH BEMRSEG WASLNIOC IOLEHHAOTUY OICNT AOD DAYG NE
ADPAOLED SAKIDUY TNSRFCN TNE TESSITRSY RM TNEAEDFI IOTR TNAT RM TNE
UIOCROEHG IO VNILN TVR UECIROH VESE VIOTESIOCG TNATG IM AOY KUAO AMMELTIOC
NIH RVO HAMETY HNRFUD NAPE BEEO RSCAOI#ED BY TNE AEDFIG NE WICNT DEMEAT IT
BY TNE SAKIDITY RM NIH WRPEWEOTH# VNEO NE ASSIPED TNESEG NE HEODH
IOMRSWATIRO TR TNE SEHT RM TNE UECIROHG AOD CATNESH AUU NIH ASWY IOTR ROE
KUALE BEMRSE IOTEUUICEOLE RM NIH ASSIPAU LRFUD BE AOORFOLED TR TNE ASPESOI#
PESLIOCETRSIXG RO NEASIOC TNIH LISLFWHTAOLEG UEADHBAL# NIH ASWY IOTR TNE
LRFOTSY RM TNE BITFSICEH# AOD AMTES WASLNIOC MSRW IT TR CESCRPIAG A TRVO RM
TNE BRIIG VNRW LAEHAS NAD HETTUED TNESE AMTES DEMEATIOC TNEW IO TNE
NEUPETIAO VASG AOD NAD SEODESED TSIBFTASY TR TNE AEDFIG NE DETESWIOED TR
ATTAL# IT#

Step 4 - Tweaking the table

Iteration 1

I couldnt yet read the text, but some familiar patterns emerged.

The string "TNE" for example was repeated often, and could very well be "THE".
So i tried swapping N and H in my map.

The resulting text was ... astonishingly promising:

*LAENASG HAPIOC DEUAYED TVR DAYN IO THAT KUALEG BELAFNE HE HAD AOTILIKATED
THATG IO THE OATFSAU LRFSNE RM EPEOTNG NFLH VRFUD BE THE LRODFLT RM
PESLIOCETRSIXG UEAPEN THE ASWY FODES KSETEONE RM SAINIOC SELSFITN AOD
LAPAUSY# HE KUALEN BSFTFNG A YRFOC WAOG IO LRWWAOD RM THENE MRSLEN# HE
CIPEN HIW IONTSFLTIRON THAT THE LAPAUSY NHRFUD SAOCE AN EXTEONIPEUY AN
KRNNIBUE IO AUU DISELTIRON# THAT HE VRFUD EXEST HIWNEUM ORT TR BE ABNEOT
MSRW THE LAWK UROCES THAO THSEE DAYN# HAPIOC ASSAOCED THENE WATTESNG HE
WASLHEN TR PIEOOA BY AN UROC #RFSOEYN AN HE LAOG VHEO HIN RVO NRUDIESN DID
ORT EXKELT HIW# MIODIOC THESE A MSENH BRDY RM LAPAUSYG VHILH HE HAD NEOT RO
TR THAT KUALE NEPESAU DAYN BEMRSEG WASLHIOC IOLENNAOTUY OICHT AOD DAYG HE
ADPAOLED SAKIDUY THSRFCH THE TESSITRSY RM THE AEDFI IOTR THAT RM THE
UIOCROENG IO VHILH TVR UECIRON VESE VIOTESIOCG THATG IM AOY KUAO AMMELTIOC
HIN RVO NAMETY NHRFUD HAPE BEEO RSCAOI#ED BY THE AEDFIG HE WICHT DEMEAT IT
BY THE SAKIDITY RM HIN WRPEWEOTN# VHEO HE ASSIPED THESEG HE NEODN
IOMRSWATIRO TR THE SENT RM THE UECIRONG AOD CATHESN AUU HIN ASWY IOTR ROE
KUALE BEMRSE IOTEUUICEOLE RM HIN ASSIPAU LRFUD BE AOORFOLED TR THE ASPESOI#
PESLIOCETRSIXG RO HEASIOC THIN LISLFWNTAOLEG UEADN BAL# HIN ASWY IOTR THE
LRFOTSY RM THE BITFSICEN# AOD AMTES WASLHIOC MSRW IT TR CESCRPIAG A TRVO RM
THE BRIIG VHRW LAENAS HAD NETTUED THESE AMTES DEMEATIOC THEW IO THE
HEUPETIAO VASG AOD HAD SEODESED TSIBFTASY TR THE AEDFIG HE DETESWIOED TR
ATTAL# IT#*

Iteration 2

Some words THAT, THE, BE ... looked good, others where nearly correct.

"IO" could be "IS" and DEUAYED could be DELAYED

swapping N for S and U to L i got:

*UAESANG HAPIOC DELAYED TVR DAYS IO THAT KLAUEG BEUAFSE HE HAD AOTIUIKATED
THATG IO THE OATFNAL URFNSE RM EPEOTSG SFUH VRFLD BE THE URODFUT RM
PENUIOCETRNIXG LEAPES THE ANWY FODEN KNETEOSE RM NAISIOC NEUNFITS AOD
UAPALNY# HE KLAUES BNFTFSG A YRFOC WAOG IO URWWAOD RM THESE MRNUES# HE
CIPES HIW IOSTNFUTIROS THAT THE UAPALNY SHRFLD NAOCE AS EXTEOSIPELY AS
KRSSIBLE IO ALL DINEUTIROS# THAT HE VRFLD EXENT HIWSELM ORT TR BE ABSEOT
MNRW THE UAWK LROCEN THAO THNEE DAYS# HAPIOC ANNAOCED THESE WATTENSG HE
WANUHES TR PIEOOA BY AS LROC #RFNOEYS AS HE UAOG VHEO HIS RVO SRLDIENS DID
ORT EXKEUT HIW# MIODIOC THENE A MNESH BRDY RM UAPALNYG VHIUH HE HAD SEOT
RO TR THAT KLAUE SEPENAL DAYS BEMRNEG WANUHIOC IOUESSAOTLY OICHT AOD DAYG
HE ADPAOUED NAKIDLY THNRFCH THE TENNITRNY RM THE AEDFI IOTR THAT RM THE
LIOCROESG IO VHIUH TVR LECIROS VENE VIOTENIOCG THATG IM AOY KLAO AMMEUTIOC
HIS RVO SAMETY SHRFLD HAPE BEEO RNCAOI#ED BY THE AEDFIG HE WICHT DEMEAT IT BY
THE NAKIDITY RM HIS WRPEWEOTS# VHEO HE ANNIPED THENEG HE SEODS IOMRNWATIRO
TR THE NEST RM THE LECIROSG AOD CATHENS ALL HIS ANWY IOTR ROE KLAUE BEMRNE
IOTELLICEOUE RM HIS ANNIPAL URFLD BE AOORFOUED TR THE ANPENOI#
PENUIOCETRNIXG RO HEANIOC THIS UINUFWSTAOUEG LEADS BAU# HIS ANWY IOTR THE
URFOTNY RM THE BITFNICES# AOD AMTEN WANUHIOC MNRW IT TR CENCRPIAG A TRVO
RM THE BRIIG VHRW UAESAN HAD SETTLED THENE AMTEN DEMEATIOC THEW IO THE
HELPETIAO VANG AOD HAD NEODENED TNIBFTANY TR THE AEDFIG HE DETENWIOED TR
ATTAU# IT#*

Iteration 3

still not perfect, but more combinations emerged:

KRSSIBLE could very well mean "POSSIBLE" making K<->P and R<->O my next choice

yielding:

*UAESANG HAKIRC DELAYED TVO DAYS IR THAT PLAUEG BEUAFSE HE HAD ARTIUIPATED
THATG IR THE RATFNAL UOFNSE OM EKERTSG SFUH VOFLD BE THE UORDFUT OM
KENUIRCETONIXG LEAKES THE ANWY FRDEN PNETERSE OM NAISIRC NEUNFITS ARD
UAKALNY# HE PLAUES BNFTFSG A YOFRC WARG IR UOWWARD OM THESE MONUES# HE
CIKES HIW IRSTNFUTIORS THAT THE UAKALNY SHOFLD NARCE AS EXTERSIKELY AS
POSSIBLE IR ALL DINEUTIORS# THAT HE VOFLD EXENT HIWSELM ROT TO BE ABSERT
MNOW THE UAWP LORCEN THAR THNEE DAYS# HAKIRC ANNARCED THESE WATTENSG HE
WANUHES TO KIERRA BY AS LORC #OFNREYS AS HE UARG VHER HIS OVR SOLDIENS DID
ROT EXPEUT HIW# MIRDIRC THENE A MNESH BODY OM UAKALNYG VHIUH HE HAD SERT OR
TO THAT PLAUE SEKENAL DAYS BEMONEG WANUHIRC IRUESSARTLY RICHT ARD DAYG HE
ADKARUED NAPIDLY THNOFCH THE TENNITONY OM THE AEDFI IRTO THAT OM THE
LIRCORESG IR VHIUH TVO LECIORS VENE VIRTENIRCG THATG IM ARY PLAR AMMEUTIRC
HIS OVR SAMETY SHOFLD HAKE BEER ONCARI#ED BY THE AEDFIG HE WICHT DEMEAT IT BY
THE NAPIDITY OM HIS WOKEWERTS# VHER HE ANNIKED THENEG HE SERDS IRMONWATIOR
TO THE NEST OM THE LECIORSG ARD CATHENS ALL HIS ANWY IRTO ORE PLAUE BEMONE
IRTELLICERUE OM HIS ANNIKAL UOFLD BE ARROFRUED TO THE ANKENRI#
KENUIRCETONIXG OR HEANIRC THIS UINUFWSTARUEG LEADS BAU# HIS ANWY IRTO THE
UOFRTNY OM THE BITFNICES# ARD AMTEN WANUHIRC MNOW IT TO CENCOKIAG A TOVR
OM THE BOIIG VHOW UAESAN HAD SETTLED THENE AMTEN DEMEATIRC THEW IR THE
HELKETIAR VANG ARD HAD NERDENED TNIBFTANY TO THE AEDFIG HE DETENWIRED TO
ATTAU# IT#*

Iteration 4

i guess:

HIWSELM -> himself
HE CIKES HIW -> HE LIKES HIM

yielding
W<->M
C<->L

*UAESANG HAKIRL DECAYED TVO DAYS IR THAT PCAUEG BEUAFSE HE HAD ARTIUIPATED
THATG IR THE RATFNAC UOFNSE OW EKERTSG SFUH VOFCD BE THE UORDFUT OW
KENUIRLETONIXG CEAKES THE ANMY FRDEN PNETERSE OW NAISIRL NEUNFITS ARD
UAKACNY# HE PCAUES BNFTFSG A YOFRL MARG IR UOMMARD OW THESE WONUES# HE
LIKES HIM IRSTNFUTIORS THAT THE UAKACNY SHOFCD NARLE AS EXTERSIKECY AS
POSSIBCE IR ACC DINEUTIORS# THAT HE VOFCD EXENT HIMSECW ROT TO BE ABSERT
WNOM THE UAMP CORLEN THAR THNEE DAYS# HAKIRL ANNARLED THESE MATTENSG HE
MANUHES TO KIERRA BY AS CORL #OFNREYS AS HE UARG VHER HIS OVR SOCDIENS DID
ROT EXPEUT HIM# WIRDIRL THENE A WNESH BODY OW UAKACNYG VHIUH HE HAD SERT
OR TO THAT PCAUE SEKENAC DAYS BEWONEG MANUHIRL IRUESSARTCY RILHT ARD DAYG
HE ADKARUED NAPIDCY THNOFLH THE TENNITONY OW THE AEDFI IRTO THAT OW THE
CIRLORESG IR VHIUH TVO CELIORS VENE VIRTENIRLG THATG IW ARY PCAR AWWEUTIRL
HIS OVR SAWETY SHOFCD HAKE BEER ONLARI#ED BY THE AEDFIG HE MILHT DEWEAT IT BY
THE NAPIDITY OW HIS MOKEMERTS# VHER HE ANNIKED THENEG HE SERDS IRWONMATIOR
TO THE NEST OW THE CELIORSG ARD LATHENS ACC HIS ANMY IRTO ORE PCAUE BEWONE
IRTECCILERUE OW HIS ANNIKAC UOFCD BE ARROFRUED TO THE ANKENRI#
KENUIRLETONIXG OR HEANIRL THIS UINUFMSTARUEG CEADS BAU# HIS ANMY IRTO THE
UOFRTNY OW THE BITFNILES# ARD AWTEN MANUHIRL WNOM IT TO LENLOKIAG A TOVR
OW THE BOIIG VHOM UAESAN HAD SETTCED THENE AWTEN DEWEATIRL THEM IR THE
HECKETIAR VANG ARD HAD NERDENED TNIBFTANY TO THE AEDFIG HE DETENMIRED TO
ATTAU# IT#*

Iteration 5

i guess:

ARD -> AND

yielding:

R <-> N

Iteration 6

THE ARMY FNDER PRETENSE OW -> The army under pretense of
UAESAR HAD SETTCED THERE AWTER DEWEATINL -> Caesar had settled there after defeating

F -> U
U -> C
C -> L
L -> G
W -> F
G -> W

*CAESARW HAKING DELAYED TVO DAYS IN THAT PLACEW BECAUSE HE HAD ANTICIPATED
THATW IN THE NATURAL COURSE OF EKENTSW SUCH VOULD BE THE CONDUCT OF
KERCINGETORIXW LEAKES THE ARMY UNDER PRETENSE OF RAISING RECRUITS AND
CAKALRY# HE PLACES BRUTUSW A YOUNG MANW IN COMMAND OF THESE FORCES# HE
GIKES HIM INSTRUCTIONS THAT THE CAKALRY SHOULD RANGE AS EXTENSIKELY AS
POSSIBLE IN ALL DIRECTIONS# THAT HE VOULD EXERT HIMSELF NOT TO BE ABSENT FROM
THE CAMP LONGER THAN THREE DAYS# HAKING ARRANGED THESE MATTERSW HE
MARCHES TO KIENNA BY AS LONG #OURNEYS AS HE CANW VHEN HIS OVN SOLDIERS DID
NOT EXPECT HIM# FINDING THERE A FRESH BODY OF CAKALRYW VHICH HE HAD SENT ON
TO THAT PLACE SEKERAL DAYS BEFOREW MARCHING INCESSANTLY NIGHT AND DAYW HE
ADKANCED RAPIDLY THROUGH THE TERRITORY OF THE AEDUI INTO THAT OF THE
LINGONESW IN VHICH TVO LEGIONS VERE VINTERINGW THATW IF ANY PLAN AFFECTING
HIS OVN SAFETY SHOULD HAKE BEEN ORGANI#ED BY THE AEDUIW HE MIGHT DEFEAT IT BY
THE RAPIDITY OF HIS MOKEMENTS# VHEN HE ARRIKED THEREW HE SENDS INFORMATION
TO THE REST OF THE LEGIONSW AND GATHERS ALL HIS ARMY INTO ONE PLACE BEFORE
INTELLIGENCE OF HIS ARRIKAL COULD BE ANNOUNCED TO THE ARKERNI#
KERCINGETORIXW ON HEARING THIS CIRCUMSTANCEW LEADS BAC# HIS ARMY INTO THE
COUNTRY OF THE BITURIGES# AND AFTER MARCHING FROM IT TO GERGOKIAW A TOVN OF
THE BOIIW VHOM CAESAR HAD SETTLED THERE AFTER DEFEATING THEM IN THE
HELKETIAN VARW AND HAD RENDERED TRIBUTARY TO THE AEDUIW HE DETERMINED TO
ATTAC# IT#*

Iteration 7

CAKALRY -> CAVALARY
GIKES -> GIVES
HAKING -> HAVING

K -> V

Iteration 8

VOULD -> WOULD

V -> W
W->,

EKENTSW -> EVENTS

*CAESAR, HAVING DELAYED TWO DAYS IN THAT PLACE, BECAUSE HE HAD ANTICIPATED
THAT, IN THE NATURAL COURSE OF EVENTS, SUCH WOULD BE THE CONDUCT OF
VERCINGETORIX, LEAVES THE ARMY UNDER PRETENSE OF RAISING RECRUITS AND
CAVALRY# HE PLACES BRUTUS, A YOUNG MAN, IN COMMAND OF THESE FORCES# HE
GIVES HIM INSTRUCTIONS THAT THE CAVALRY SHOULD RANGE AS EXTENSIVELY AS
POSSIBLE IN ALL DIRECTIONS# THAT HE WOULD EXERT HIMSELF NOT TO BE ABSENT
FROM THE CAMP LONGER THAN THREE DAYS# HAVING ARRANGED THESE MATTERS, HE
MARCHES TO VIENNA BY AS LONG #OURNEYS AS HE CAN, WHEN HIS OWN SOLDIERS DID
NOT EXPECT HIM# FINDING THERE A FRESH BODY OF CAVALRY, WHICH HE HAD SENT ON
TO THAT PLACE SEVERAL DAYS BEFORE, MARCHING INCESSANTLY NIGHT AND DAY, HE
ADVANCED RAPIDLY THROUGH THE TERRITORY OF THE AEDUI INTO THAT OF THE
LINGONES, IN WHICH TWO LEGIONS WERE WINTERING, THAT, IF ANY PLAN AFFECTING HIS
OWN SAFETY SHOULD HAVE BEEN ORGANI#ED BY THE AEDUI, HE MIGHT DEFEAT IT BY THE
RAPIDITY OF HIS MOVEMENTS# WHEN HE ARRIVED THERE, HE SENDS INFORMATION TO
THE REST OF THE LEGIONS, AND GATHERS ALL HIS ARMY INTO ONE PLACE BEFORE
INTELLIGENCE OF HIS ARRIVAL COULD BE ANNOUNCED TO THE ARVERNI#
VERCINGETORIX, ON HEARING THIS CIRCUMSTANCE, LEADS BAC# HIS ARMY INTO THE
COUNTRY OF THE BITURIGES# AND AFTER MARCHING FROM IT TO GERGOVIA, A TOWN OF
THE BOII, WHOM CAESAR HAD SETTLED THERE AFTER DEFEATING THEM IN THE HELVETIAN
WAR, AND HAD RENDERED TRIBUTARY TO THE AEDUI, HE DETERMINED TO ATTAC# IT#*

Iteration 9

.,:; map to themselves j -> K

*CAESAR, HAVING DELAYED TWO DAYS IN THAT PLACE, BECAUSE HE HAD ANTICIPATED
THAT, IN THE NATURAL COURSE OF EVENTS, SUCH WOULD BE THE CONDUCT OF
VERCINGETORIX, LEAVES THE ARMY UNDER PRETENSE OF RAISING RECRUITS AND
CAVALRY: HE PLACES BRUTUS, A YOUNG MAN, IN COMMAND OF THESE FORCES; HE GIVES
HIM INSTRUCTIONS THAT THE CAVALRY SHOULD RANGE AS EXTENSIVELY AS POSSIBLE IN
ALL DIRECTIONS; THAT HE WOULD EXERT HIMSELF NOT TO BE ABSENT FROM THE CAMP
LONGER THAN THREE DAYS. HAVING ARRANGED THESE MATTERS, HE MARCHES TO
VIENNA BY AS LONG #OURNEYS AS HE CAN, WHEN HIS OWN SOLDIERS DID NOT EXPECT
HIM. FINDING THERE A FRESH BODY OF CAVALRY, WHICH HE HAD SENT ON TO THAT
PLACE SEVERAL DAYS BEFORE, MARCHING INCESSANTLY NIGHT AND DAY, HE ADVANCED
RAPIDLY THROUGH THE TERRITORY OF THE AEDUI INTO THAT OF THE LINGONES, IN WHICH
TWO LEGIONS WERE WINTERING, THAT, IF ANY PLAN AFFECTING HIS OWN SAFETY
SHOULD HAVE BEEN ORGANI#ED BY THE AEDUI, HE MIGHT DEFEAT IT BY THE RAPIDITY OF
HIS MOVEMENTS. WHEN HE ARRIVED THERE, HE SENDS INFORMATION TO THE REST OF
THE LEGIONS, AND GATHERS ALL HIS ARMY INTO ONE PLACE BEFORE INTELLIGENCE OF
HIS ARRIVAL COULD BE ANNOUNCED TO THE ARVERNI. VERCINGETORIX, ON HEARING THIS
CIRCUMSTANCE, LEADS BACK HIS ARMY INTO THE COUNTRY OF THE BITURIGES; AND
AFTER MARCHING FROM IT TO GERGOVIA, A TOWN OF THE BOII, WHOM CAESAR HAD
SETTLED THERE AFTER DEFEATING THEM IN THE HELVETIAN WAR, AND HAD RENDERED
TRIBUTARY TO THE AEDUI, HE DETERMINED TO ATTACK IT.*

Done - 9 iterations

About the cypher

i couldn't find a simple *key* that would allow me to create the transformation table. So i would have to provide the whole table to someone, who wanted to decrypt messages.

I would descripe the cypher as a **simple substitution cipher** where the following table is the *key*:

```
%map = (
" " => " ",
"a" => "E",
"o" => "T",
"l" => "A",
"f" => "N",
"i" => "I",
"y" => "H",
"x" => "R",
"c" => "O",
"m" => "S",
"s" => "D",
"r" => "C",
"g" => "L",
"t" => "G",
"e" => "F",
"h" => "U",
"v" => "Y",
"d" => "M",
"," => ",",
"n" => "V",
"k" => "B",
"q" => "W",
"b" => "P",
"w" => "X",
"j" => "K",
"." => ".",
":" => ":",
";" => ";");
```

Each imput symbol *s* from the message is mapped to a single symbol *c(s)* in the cyphered message. The mapping is fixed - the function described by the map is bijective.

Deciphered Text

CAESAR, HAVING DELAYED TWO DAYS IN THAT PLACE, BECAUSE HE HAD ANTICIPATED
THAT, IN THE NATURAL COURSE OF EVENTS, SUCH WOULD BE THE CONDUCT OF
VERCINGETORIX, LEAVES THE ARMY UNDER PRETENSE OF RAISING RECRUITS AND
CAVALRY: HE PLACES BRUTUS, A YOUNG MAN, IN COMMAND OF THESE FORCES; HE GIVES
HIM INSTRUCTIONS THAT THE CAVALRY SHOULD RANGE AS EXTENSIVELY AS POSSIBLE IN
ALL DIRECTIONS; THAT HE WOULD EXERT HIMSELF NOT TO BE ABSENT FROM THE CAMP
LONGER THAN THREE DAYS. HAVING ARRANGED THESE MATTERS, HE MARCHES TO
VIENNA BY AS LONG #OURNEYS AS HE CAN, WHEN HIS OWN SOLDIERS DID NOT EXPECT
HIM. FINDING THERE A FRESH BODY OF CAVALRY, WHICH HE HAD SENT ON TO THAT
PLACE SEVERAL DAYS BEFORE, MARCHING INCESSANTLY NIGHT AND DAY, HE ADVANCED
RAPIDLY THROUGH THE TERRITORY OF THE AEDUI INTO THAT OF THE LINGONES, IN WHICH
TWO LEGIONS WERE WINTERING, THAT, IF ANY PLAN AFFECTING HIS OWN SAFETY
SHOULD HAVE BEEN ORGANI#ED BY THE AEDUI, HE MIGHT DEFEAT IT BY THE RAPIDITY OF
HIS MOVEMENTS. WHEN HE ARRIVED THERE, HE SENDS INFORMATION TO THE REST OF
THE LEGIONS, AND GATHERS ALL HIS ARMY INTO ONE PLACE BEFORE INTELLIGENCE OF
HIS ARRIVAL COULD BE ANNOUNCED TO THE ARVERNI. VERCINGETORIX, ON HEARING THIS
CIRCUMSTANCE, LEADS BACK HIS ARMY INTO THE COUNTRY OF THE BITURIGES; AND
AFTER MARCHING FROM IT TO GERGOVIA, A TOWN OF THE BOII, WHOM CAESAR HAD
SETTLED THERE AFTER DEFEATING THEM IN THE HELVETIAN WAR, AND HAD RENDERED
TRIBUTARY TO THE AEDUI, HE DETERMINED TO ATTACK IT.