

Code Makers and Code Breakers From Julius Caesar To Alan Turing And Beyond IV

An Introduction To Some Mathematics and Linguistics Used to Crack Secret Ciphers

How Does One Begin To Crack a Cipher?

Single Most Important Tool:
Frequency Count of Characters

The percentage of occurrence of any particular letter, its **Characteristic Frequency**, will not vary widely from one plaintext message to the next.

Consequence: **Monoalphabetic Ciphers Are Not Secure**

Plaintext Example
Opening Chapter of *Anna Karenina*

A	331	E	515
B	57	T	380
C	83	H	332
D	200	A	331
E	515	I	324
F	107	N	308
G	94	O	307
H	332	S	281
I	324	R	219
J	2	D	200
K	27	L	163
L	163	U	117
M	88	F	107
N	308	W	100
O	307	G	94
P	75	M	88
Q	4	Y	85
R	219	C	83
S	281	P	75
T	380	B	57
U	117	V	45
V	45	K	27
W	100	Q	4
X	4	X	4
Y	85	J	2
Z	0	Z	0

Characters Counted: 4248

How can we get rid of the tell tale fingerprints of the characteristic frequencies?

Blaise de Vigenère (1523 - 1596)



Giovan Battista Bellaso (1553)

ALLECCELLEN. ET
honoratiss. Sig. il S. Giro-
lamo Ruscelli,

GIOVAN BATTISTA BELLASO.



A MOLTI anni, che io incomincio à dar'opera à gli studi, &
à conuersare tra persone grandi, habendo veduto in quanta stima;
et di quanta importanza sia la bellissima professione di scriuer segres-
so per via di quelle che universalmente chiamano Cifre, io con l'in-
clinatione datami dalla natura di nō hauer maggior diletto che l'im-
parare, son uenuto di continuo esercitandomi intorno à tal professione; & habendo
ritrouati molti modi, che à persone d'ingegno mostrauano di non dispiacere, mi oc-
corse in questa ultima fide uiscante di ritrouarmi l'ingegnosamente generale dell'illustriss.
& Reuerendiss. Cardinal Durante, nello Stato di Camerino.

POLYALPHABETIC SUBSTITUTIONS

POLYALPHABETIC SUBSTITUTIONS

keyword: VERMONT

V E R M O N T V E R M O N T V E R
M I D D L E B U R Y C O L L E G E

V	E	R	M	O	N	T	V	E	R	M	O	N	T	V	E	R
22	5	18	13	15	14	20	22	5	18	13	15	14	20	22	5	18
13	9	4	4	12	5	2	21	18	25	3	15	12	12	5	7	5
M	I	D	D	L	E	B	U	R	Y	C	O	L	L	E	G	E

22	5	18	13	15	14	20	22	5	18	13	15	14	20	22	5	18
13	9	4	4	12	5	2	21	18	25	3	15	12	12	5	7	5
35	14	22	17	27	19	22	43	23	43	16	30	26	32	27	12	23
9	14	22	17	1	19	22	17	23	17	16	4	26	6	1	12	23
I	N	V	Q	A	S	V	Q	W	Q	P	D	Z	F	A	L	W

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

MIDDLEBURYCOLLEGE

INVQASVQWQPDZFALW

OBSERVE:

D has been encrypted as **V** and as **Q**

L has been encrypted as **A** and **Z** and as **F**

E has been encrypted as **S** and **A** and as **W**

Ciphertext **A** came from **L** and **E**

Ciphertext **W** came from **R** and **E**

The resulting frequency distribution will be much flatter.

Frequency Data

A	331	<i>A</i>	<i>202</i>
B	57	<i>B</i>	<i>179</i>
C	83	<i>C</i>	<i>180</i>
D	200	<i>D</i>	<i>116</i>
E	515	<i>E</i>	<i>100</i>
F	107	<i>F</i>	<i>159</i>
G	94	<i>G</i>	<i>196</i>
H	332	<i>H</i>	<i>202</i>
I	324	<i>I</i>	<i>160</i>
J	2	<i>J</i>	<i>178</i>
K	27	<i>K</i>	<i>119</i>
L	163	<i>L</i>	<i>145</i>
M	88	<i>M</i>	<i>125</i>
N	308	<i>N</i>	<i>204</i>
O	307	<i>O</i>	<i>140</i>
P	75	<i>P</i>	<i>135</i>
Q	4	<i>Q</i>	<i>118</i>
R	219	<i>R</i>	<i>137</i>
S	281	<i>S</i>	<i>249</i>
T	380	<i>T</i>	<i>159</i>
U	117	<i>U</i>	<i>158</i>
V	45	<i>V</i>	<i>148</i>
W	100	<i>W</i>	<i>269</i>
X	4	<i>X</i>	<i>131</i>
Y	85	<i>Y</i>	<i>191</i>
Z	0	<i>Z</i>	<i>148</i>

Characters Counted: 4248

Tolstoy with Vigenère Cipher

Keyword: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

ICSTDLHURVTQFOGURDEUGEHCDFVFTBYSNHXYIQMZ
WAOZKNHCWMNXIOKWWTCUEJIPHRFNJYAGARWPGM
CPPIYXOVVRXETRCQBFFLETOEMTSFVKIBOMMQKOPV
GREMWKYYPEYSTIGKYXHHVMGLEPOGHPAGAJJXLHN
UTLKZKDKCRLRESCSYBLGSEMGAEDHISGNWEOCZRG
HYELAYDNCYLIMADRIYOMQKOMABDKEUXXOKECQH
UEESJAPJDDTRQDKCVGIOCLMMLJXLRLLOUBQODMZSW
ELKXQDPEFHMUJLWUUZQCSZZBTPVWSBLNDXBMOXN
DWYKKQBQBPQQONIRFWHJPLLKYUJHLZYIWNLZQKXV
VLAYHOBJUETDXXFRSBQOXQZPTHJGYNCAFPEANKOC
FTKPXEDQUCATNWKYKWFLEUMNBGTTZKRYFEBTXJV
NXLTLBPROOKQXMKOWDCPRRZIJYSMNCAOCVATPRW
JTZMRXETRWGBZNBHBPLEDTIGUESJAPJDETRGIHRQI
YJLICARPWJLYZVONDSQEPNSYSGWZEKMYJPQLFJT
WAOTZPCBCFFPCODLLDAOQWLJXAPJXETRMIXVEXGW
AOQNFUJHJFSPTHKYPUCJIVZHFYKCRGEPDOSSYRGBD
SQJWUUUAWHJPICZVFJHVTCUZXYXFUSWKJTTHYDXB
MOUDHISGAPXWPRBFIXIWXXVUPRGEDJLPXLVAKYIV
ZSQCDHPZNQFDHPWVIYNLMWQWUFVVMWKHZOPOT
ASTHPQKKERDSFUSWELKXEZAMCQAOFZVTZLBXKQDV
SCTRKDCICECQTPNRSPUBBOYCMASLIZLNUOELLEOSJ
HVVNLUJXNABYWQUOTFFAAMEFUJHHFEIMOYCQIOH
JRLWCIJBPSINGWLJQPBLRPZZOXTRFWNCBZMCIODR
MGKORFPZJOGDZFNZCNBCCAZUDJYKYBQOBGNFGUC
HKCIYBQSEQCQEWQHLHOGUGQWESDHHNGVQSIWCD
WMKDIBMLXYSSYELAYAWPFHOOCEPJCVZUNHAXSJFR
LACNQPSZLIQXVYNHBRCLFRWVXKGVFJYHGMTIGPSW
TPVPXZFVBWYJOBZZOYCCRPQPFZZVVCRPXROIXVJVI
QAOCSPHDMSNPABDFPLVTJLJGYKSCQHJUVXTAAE

Frequency Data

A	141	C	185
B	146	Q	181
C	185	S	178
D	149	R	176
E	163	K	175
F	160	I	174
G	160	V	174
H	139	W	173
I	174	X	172
J	165	L	171
K	175	P	171
L	171	Y	168
M	145	O	167
N	152	J	165
O	167	Z	165
P	171	E	163
Q	181	F	160
R	176	G	160
S	178	N	152
T	152	T	152
U	146	D	149
V	174	B	146
W	173	U	146
X	172	M	145
Y	168	A	141
Z	165	H	139

The Vigenère Cipher in Literature



Jules Verne, *La Jangada*, *Eight Hundred Leagues on the Amazon* (1881)

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

The man who held in his hand the document of which this strange assemblage of letters formed the concluding paragraph remained for some moments lost in thought.

It contained about a hundred of these lines, with the letters at even distances, and undivided into words. It seemed to have been written many years before, and time had already laid his tawny finger on the sheet of good stout paper which was covered with the hieroglyphics.

On what principle had these letters been arranged? He who held the paper was alone able to tell. With such cipher language it is as with the locks of some of our iron safes—in either case the protection is the same. The combinations which they lead to can be counted by millions, and no calculator's life would suffice to express them.

ADA LOVELACE

CHARLES BABBAGE

THE VIGENÈRE CYPHER



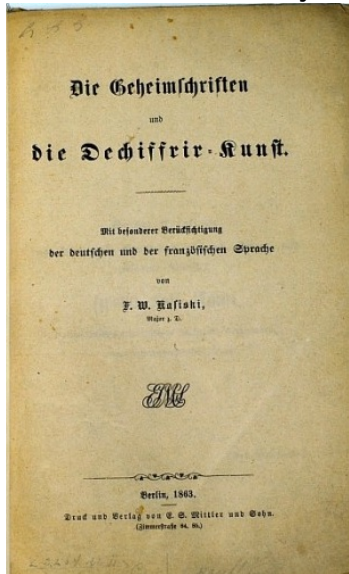
Charles Babbage

December 16, 1791 - October 18, 1871



Major Friedrich Wilhelm Kasiski

November 29, 1805 - May 22, 1881



M	A	P	L	E	M	A	P	L	E	M	A	P	L	E
13	1	16	12	5	13	1	16	12	5	13	1	16	12	5
M	I	D	D	L	E	B	U	R	Y	C	O	L	L	E
13	9	4	4	12	5	2	21	18	3	15	12	12	5	7
Z	J	T	P	Q	R	C	K	D	D	P	P	B	X	J

Detecting a Polyalphabetic Cipher

A monoalphabetic cipher has greater variation among frequencies of the individual letters



William Friedman (1930)
Index of Coincidence

Index of Coincidence

$$\sum_{i=A}^Z \frac{f_i(f_i - 1)}{N(N - 1)}$$

f_i = frequency of letter i

N = number of characters in message

Number of Alphabets	Expected IC
1	.066
2	.052
5	.044
10	.041
26	.038

How To Crack a Vigenère Cipher

- 1) Determine the Length L of the Keyword
- 2) Split Message into L Pieces, Determine Each Shift

Determine Length L of the Keyword

To encipher, we can repeat the keyword over the message:

V	E	R	M	O	N	T	V	E	R	M	O	N	T	V	E
M	I	D	D	L	E	B	U	R	Y	C	O	L	L	E	G

or write the message under a single copy of the keyword:

V	E	R	M	O	N	T
M	I	D	D	L	E	B
U	R	Y	C	O	L	L
E	G	E				

V	E	R	M	O	N	T
M	I	D	D	L	E	B
U	R	Y	C	O	L	L
E	G	E				

V	E	R	M	O	N	T
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21

V	E	R	M	O	N	T
M	I	D	D	L	E	B
U	R	Y	C	O	L	L
E	G	E				

V	E	R	M	O	N	T
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21

SUPPOSE **MIDDLEBURY** OCCURS TWICE IN THE MESSAGE, BOTH TIMES STARTING IN COLUMN 5, UNDER THE "**O**". THEN IT WILL BE ENCIPHERED THE SAME WAY BOTH TIMES AS **BWXZQWOJFS**

THE DISTANCE BETWEEN THE STARTING "**M**'s" WILL BE A MULTIPLE OF THE LENGTH OF THE KEYWORD

V E R M O N T

 M I D
D D L E B U R
Y

 M I D
D D L E B U R
Y

Hence we examine the ciphertext for the repetition of strings and determine the distances between the repeated occurrence of the same string of letters.

Some of the repetitions will occur by "chance" and will represent different plaintext, but a long string which repeats is very likely to be the encipherment of the same plaintext.

The length of the keyword will then be a factor of the distances.

German	Schubfachprinzip
French	principe des tiroirs
Polish	zasada szufladkowa
Hungarian	katulyaelv
Danish	Skuffeprincippet
Chinese	抽屉原理

German	Schubfachprinzip
French	principe des tiroirs
Polish	zasada szufladkowa
Hungarian	katulyaelv
Danish	Skuffeprincippet
Chinese	抽屉原理
English	Pigeonhole Principle



The pigeonhole principle: If n items are put into m containers, with $n > m$, then at least one container must contain more than one item.

Application of Pigeonhole Principle to Solve Vigenère Ciphers

Example: If the keyword is 7 letters long and **MIDDLEBURY**, or any other particular word, occurs 8 or more times in the plaintext, then at least two occurrences must begin under the same letter of the keyword.

Thus, there will be at least two repetitions of the same characters in the cipher text.

Repeated Sequence	Positions of First Letter	Interval
KGFDLRLZK	37, 184	$147 = 7 \times 7 \times 3$
KYEXSRSIQ	55, 132	$77 = 7 \times 11$

Solving a Vigenère

DDBCII MYMXSNUGTZEJWXYHHIDIJHJBFXUVQIHXTTOIHZGCTWVOIMCIHZHE
UDIHZFHTPQFJWJWBDZXIIMUJATQUGJXKETHEJWBEJXYCYBUSJYFQTM
BTZJWJISTFHRJWCUSSIMPWYEJWVHDBMRDZHTLNNXKNWJDWCEJXQHTF
NXHTOHQWOYHJXQGRMXJSAKEKIBTHKBHJHTOHYYHCFFQGRMSWFH
WTINEBJLHNRYUINHWHTOHSWYQSKOBBFLSWJMJDIYBXLBJUZCTFMKGJ
MWGNGLXXUWTIQQGMUJWXGEDYBUSMCILWCDZQYTUWIDIFHTCTQYCXN
UPIIVBTODINHWQFLRTIMJTJXIITZHLBJIMYIDZFIDKZUPWZKAFXLTWMQGN
YIWJWQEJLICNGRADCDPQUTNXWXPRVUGYIJWJFQHHCLXTOIEQYQHNHW
DKUBJYYRJYCJWFNQBSIJHMFUFTIZEGXJEGYCLTYLYRPMDDWGQSJNERTO
HIFHQBTLEJXFEDPCDVLFFQHCJWFNQBWOTTQSIIFGFTIUDSBUDIQLTXGQ
YJMJNYIIIWOJQJZEGJUMPSNECFGRANHWCDGFWNNXPYUCRZLJPNFUSTZ
JWNMVPNLFGTJEGYCECHBUPYYTDKZUPYOHTGSTXXMUBGFYCLHQIZLUS
JZEGRYTJSZYCNMXTIMUCYVUUTLUBDNYBJCDITNXXXVHTFNXXSAMDWFT
HHUHRJBQAKGQSJOFPXJWFNIDQUCTQSQCIODUFMXXTHQQQYJWFNTD
LMRPWEQIRYQHNBQAYVOIMYCLMSYXSNXXXQUPPJYENHWINGUDKJUPH
YXPAYDDIYBXLBJITJQHXPMPDNXTYCCTZHBTXMJDXJOBDMXPIIMXSNXTX
ODPSXTTXWQCYIDBNHUBHTTKIHBNNOPSXJWJLUUTLUHNHSTNWQCSIJ
EWILTFFEKJLJDJHJTNWQXSNXTXYVPLMTQFIETEUCIUOHNUCSJNUGRC
DTINEEWILTFPYAQUYCFHTWFNUIMYYSQYFAJUIJWYIDKNXTXYTPDMFATN
IWFPUXQUYSNHTJHNYDSMTPSAUGTOIQDXHJSEUCULEEMYXJMBXGYB
HFHTSWYQBXNEHJNCNGLEIMYHRQUHTSWUPSXJWJEYCLCDSJUTADBQIJ
NXTTHUPLUYCXNJWJIIJWJLQCICVZNHWTIQQGIVUPXNHJJUDSOOIFMYPR
MKQYFUUFFITFHTIWIYQRMVYHDZMJWNMTPDMXDZFTRQUHTSWURQIITQS
RTRYMTIOFPGIKIFJHDUBURDQXXHBIPDMJWFNEUJXMPWXIWIJCHHYBUBZ
LTTWYHHMUBAGYTXAYJWTOWWYMTDBHJDRSIDZF

DDBCIIIMYMXSNUGTZEJWXYHHIDIJHJBFXUVQIHXTTOIHZGCTWVOIMCIHZHE
UDIHZFHTPQFJWJWBDZXIIMUJATQUGJXKETHEJWBEJXYCYBUSJYFQTM
BTZJWJISTFHRJWCUSSIMPWYEJWVHDBMRDZHTLNNXKNWJDWCEJXQHTF
NXHTOHQWOYHJXQGRMXJSAKEKIHBTBKBJHJHTOHHYYHCFFQGRMSWFH
WTINEBJLHNRYUINHWHOTOHSWYQSKOBBFLSWJMDIYBXLBJUZCTFMKGJ
MWGNGLXXUWTIQGMUJWXGEDYBUSMCILWCDZQYTUWIDIFHTCTQYCXN
UPIIVBTODINHWQFLRTIMJTJXIITZHLBJIMYIDZFIDKZUPWZKAFLXTWMQGN
YIWJWQEJLICNGRADCDPQUTNXWXPRVUGYIJWJFQHHCLXTOIEQYQHNHW
DKUBJYYRJYCJWFNQBSIJHMUFTIZEGXJEGYCLTYLYRPMDDWGQSJNERTO
HIFHQBTLEJXFEDPCDVLQFQXHCJWFNQBWOTTQSIIFGFTIUDSBUDIQLTXGQ
YJMJNYIIIWOJQJZEGJUMPSNECFGRANHWCDGFWNNXPYUCRZLJPNFUSTZ
JWNMVPNLFGTJEGYCECHBUPYYTDKZUPYOHTGSTXXMUBGFYCLHQIZLUS
JZEGRYTJSZYCNMXTIMUCYVUUTLUBDNYBJCDITNXXXVHTFNXXSAMDWFT
HHUHRJBQAKGQSJOFPXJWFNIDQUCTQSQCIODUFMXXTHQQQYJWFNTD
LMRPWEQIRYQHNBAQYVOIMYCLMSYXSNXXXQUPPJYENHWINGUDKJUPH
YXPAYDDIYBXLBJITJQHXUMPDNXTYCCTZHBTXMJDXJOBDMXPIIMXSNXTX
ODPSXTTXWQCYIDBNHUBHTTKIHBNNOPXJWJLUUTLUHNHSTNWQCSIJ
EWILTFFEKJLJDJHJTNQXSNXTXYVPLMTQFIETEUCIUOHNUCSJNUGRC
DTINEEWILTFPYAQUYCFHTWFNUIMYYSSQYFAJUIJWYIDKNXTXYTPDMFATN
IWFPUXQUYSNHTJHNYDSMTPSAUGTOIQDXHJSEUCULEEMYSXJMBXGYB
HFHTSWYQBXNEHJNCNGLEIMYHRQUHTSWUPSXJWJEYCLCDSJUTADBQIJ
NXTTHUPLUYCXNJWJJIWJLQCICVZNHWTIQQGIVUPXNHJJUDSOOIFMYPR
MKQYFUUFFITFHTIWIYQRMVYHDMJWNMTPDMXDZFTRQUHTSWURQIITQS
RTRYMTIOFPGIKIFJHDUBURDQXXHBIPDMJWFNEUJXMPWXIWJCHHYBUBZ
LTTWYHHMUBAGYTXAYJWTOWWYMTDBHJDRSIDZF

Repeated Sequence	Gap
DIYBXLB	$572 = 2 \times 2 \times 11 \times 13$
QUHTSWU	$124 = 2 \times 2 \times 31$
CJWFNQB	$68 = 2 \times 2 \times 17$
RQUHTSW	$124 = 2 \times 2 \times 31$
IYBXLBJ	$124 = 2 \times 2 \times 11 \times 13$

So split text into four columns

Column 1

DIMUEYDJUHICOIEHTJBIJUKEEYUFEJSRUMEHRTXJEHXHYQXKHI

Column 2

DIXGJHIBVXHTIHUZPWDIAGEJJCSQBWTJSPJDDLKDJTHQHGJEBE

Column 3:

BMSTWHJFQQTZWMZDFQJZMTJTWXYJTTJFWSWWBZNNWXFTW

Column 4

CYNZXIHXIIOGVCHIHFWXUQXHBXBYMZIHCIYVMHNWCQNOOXMA

Step 4: Do a Frequency Count on Each Column and Determine Each Shift

Frequency count on column 1 gives
 Looks Like Cipher text **U** represents plaintext **E**
 Other possibilities for **E**: **J** and **Q** do not work out.

A	0		N	0	
B	9	***	O	5	*
C	8	**	P	0	
D	18	*****	Q	31	*****
E	25	*****	R	8	**
F	9	***	S	5	*
G	0		T	25	*****
H	25	*****	U	37	*****
I	25	*****	V	4	*
J	34	*****	W	10	***
K	7	**	X	19	*****
L	7	**	Y	18	*****
M	9	***	Z	0	

Thus **E** $\rightarrow$ **U** means $5 \rightarrow 21$ so the shift was 16.

The initial letter of the keyword is **P**

Similarly,

Shift for column 2 was 15 corresponding to **O**

Shift for column 3 is 5 corresponding to **E**

Shift for column 4 is 20 corresponding to **T**

P	O	E	T	
16	15	5	20	Encipher Shift
10	11	21	6	Decipher Shift
J	K	U	F	

To decipher: Use Vigenère with keyword **JKUF**

NOW IS THE WINTER OF FOUR DISCONTENT MADE GLORIOUS SUMMER
BY THIS SUN OF YORK AND ALL THE CLOUDS THAT LOWERED UPON
OUR HOUSE IN THE DEEP BOSOM OF THE OCEAN BURIED NOW ARE OUR
BROWS BOUND WITH VICTORIOUS WREATHS OUR BRUISED ARMS
HUNG UP FOR MONUMENTS OUR STERNAL ARMS CHANGED TO MERRY
MEETINGS OUR DREADFUL MARCHES TO DELIGHTFUL MEASURES
GRIM VISAGED WAR HAS THUS SMOOTHED HIS WRINKLED FRONT AND NOW
INSTEAD OF MOUNTING BARBED STEEDS TO FRIGHT THE SOULS
OF FEARFUL ADVERSARIES HE CAPERS NIMBLY IN A LADY'S CHAMBER
TO THE LASCIVIOUS PLEASING OF A LUTE BUT IT HAS NOT SHAPED
FOR SPORTIVE TRICKS NOR MADE TO COURT AN AMOROUS LOOKING
GLASS THAT AMRUDELY STAMPED AND WANTS LOVE'S MAJESTY TO
STRUT BEFORE A WANTED NAMBLING NYMPH IT HAS A CURTAILED
DO THUS FAIR PROPORTION CHEATED OFF A FEATURE BY DISSEMBLING
NATURE DEFORMED UNFINISHED SENT BEFORE MY TIME INTO THIS
BREATHING WORLD SCARCE HALF MADE UP AND THAT'S SOLAMEL
Y AND UNFASHIONABLE THAT DOGS BARK AT ME AS I HALT BY THEM
WHY IN THIS WEAK PIPING TIME OF PEACE HAVE NO DELIGHT TO PASS
AWAY THE TIME UNLESS TO SPY MY SHADOW IN THE SUN AND DES
CANTON MINE OWN DEFORMITY AND THEREFORE SINCE I CANNOT
PROVE A LOVER TO ENTERTAIN THESE FAIR WELLSPOKEN DAYS I AM
DETERMINED TO PROVE A VILLAIN AND THAT THE IDLE PLEASURES
OF THESE DAYS PLOT HAVE LAID IN INDUCTIONS DANGEROUS BY DR
UNKEN PROPHECIES LIBELS AND DREAMS TO SET MY BROTHER CLARE
NCE AND THE KING IN DEADLY HATE THE ONE AGAINST THE OTHER
AND IF KING EDWARD BE A TRUE AND JUST AS I AM SUBTLE FALSE
AND TREACHEROUS THIS DAY SHOULD CLARENCE CLOSELY BEMEWED
ABOUT A PROPHECY WHICH SAYS THAT OF EDWARD'S HEIR SHALL

