THE VIGENÈRE CIPHER

Many people are generally acquainted with the concept of a substitution cipher. Its most familiar form, the Monoalphabetic Substitution Cipher (MASC), works by replacing characters from the original, non-encrypted message (the plaintext) with other characters in accordance with a pre-established key. As the name suggests, MASCs are substitution ciphers that only use a single alphabet. The replacement can be viewed as a one-to-one correspondence between the original alphabet and a ciphertext alphabet:

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

We would take each letter in our plaintext in turn, locating it in the upper alphabet and replacing it with the corresponding letter from the lower alphabet. In this way, the lower alphabet corresponds to the notion of a key: CWEIGUJMZBPOAHQRSDLXTVKYFN.

Using the above example, we would encrypt “Shall we meet at noon” as LMCOO KG AGGX CX HQQH (by tradition we often capitalize all of the ciphertext, and typically we’d disguise the spacing as well).

You’ll likely have already noticed that each plaintext letter is always mapped to the same ciphertext letter, which means the frequency of any particular letter in the original version of the message is preserved in the enciphered version. This is why, in spite of having a key-space of $26! \approx 2^{88}$, this cipher is easily broken.

Although variations on the MASC saw widespread historical use (think of our discussion of Mary, Queen of Scots), early cryptographers struck upon the crucial insight that there is no need to limit the cipher to a single alphabet.

Indeed, if we allow the mapping of each letter in the message to rotate among several different cipher alphabets, we can disguise (or “flatten”) the letter frequency in the ciphertext. To help us remember all these different alphabets, we can even use a keyword or phrase that establishes their ordering. Proceeding in this way, we arrive at a Polyalphabetic Substitution Cipher (PASC) – the most famous example being the Vigenère Cipher.

As an example, let’s say we choose the keyword WINTER and wish to encipher the same message as before: “Shall we meet at noon”.

Working it through on paper, we’d begin by creating a grid of alphabets, with the regular alphabet across the top and our keyword running down the first column. The alphabets then appear on successive rows, beginning with the letter of the keyword:

	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
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
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
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
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
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
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

We begin with the 'W' row and work our way down, repeating the rotation if the message is longer than the keyword. So to encipher "Shall we meet at noon", we'd start by locating the 'S' in the regular alphabet across the top, then find the letter beneath it in the 'W' row: 'O'. Then for 'h', we'd start with 'H' on the top (remember that case doesn't matter) and find the entry where that column is intersected by the 'I' row: 'P'. Continuing in this way, we get: OPNEP NA URXX RP VBHR. Adopting uniform spacing to hide word boundaries, we have: OPNEP NAURX XRPVB HR.

Notice how the same letter in the plaintext often appears as different letters in the ciphertext: 'e' first becomes 'A', then 'R', then 'X'. Working back in the other direction, a given letter in the ciphertext can stem from different letters in the plaintext: 'P' first came from 'h', then from 'l'. Even an obvious pattern word like "noon", which would otherwise be easily guessable, is much better disguised.

Although this cipher dominated the landscape as the cutting-edge encryption method for several centuries, insightful cryptanalysts eventually recognized weaknesses and began to develop attacks. These attacks were based on the fact that although the Vigenère does indeed obscure the link between a plaintext letter and its ciphertext mapping(s), subtle patterns and connections may still be observed.

One possible attack, which came to be known as the Kasiski test, attempts to identify repeated encryptions of the same letters that happen to be mapped using the same alphabets. In other words, we can hope that some number of words were repeated in the plaintext, and that the spacing between these words happens to line up with the repetition of the key. If this occurs, the distance between the repetitions will be a multiple of the length of the key.

A different attack was developed in the early twentieth century by cryptanalyst William Friedman. Known as the **Index of Coincidence method**, this attack calculates the probability that two randomly selected letters from a text will be the same.

For example, using a text of length N, the chances that both letters will be A could be calculated as P(letter 1 is A) * P(letter 2 is A). So we would have:

$$\frac{(Frequency\ of\ A)}{N} * \frac{(Frequency\ of\ A) - 1}{N - 1}$$

Thinking beyond one letter to the entire alphabet, we must sum the probabilities for all the letters:

$$Index\ of\ Coincidence = \frac{\sum_{i=A}^{Z} F_i(F_i - 1)}{N(N-1)}$$

As described above, the strength of Vigenère comes from the "flattening" effect that the cipher exerts on the frequency distribution of the plaintext letters. In using multiple alphabets, the cipher is decreasing the chance that two randomly selected letters will be the same: the more alphabets, the greater the flattening. *So in measuring this flattening effect, the Index of Coincidence is giving us a hint about the number of alphabets in use!*

The expected Index of Coincidence for different key lengths can be calculated. Although the precise values will vary with the length of the text under consideration (and of course with the language), the following are sample values for a long text in English[1]:

Keyword Length	Expected Value of IC
1	.0660
2	.0520
3	.0473
4	.0449
5	.0435
6	.0426
7	.0419
8	.0414
9	.0410
10	.0407

Think for a moment about the two possible extreme cases. Choosing a key length of one would simply result in a Caesar Cipher, completely preserving all of the letter-frequency structure of the underlying language. At the other extreme, if we were looking at a text composed of completely random letters (i.e., no underlying language structure at all), we would approach a limit of approximately .0385 (because each letter would be equally likely, having a 1 in 26 chance of appearing at any position).

So we can use the results of the IC calculation to make an educated guess as to the extent of the "flattening" effect imposed on the underlying message, which itself is a direct result of the encipherer's choice of key length. In doing so, we can split the ciphertext letters into groupings, based on our guess of the key length; if our guess was correct, each member of a grouping would have been mapped from the same alphabet, from amongst all the rotating alphabets in play.

[1] Adapted from *Secret History* by Craig P. Bauer (CRC Press 2013).

Let's look at the example above, where "Shall we meet at noon" became OPNEP NAURX XRPVB HR. As an attacker, if we correctly suspect that the key length is six, we could group the letters as follows:

O	P	N	E	P	N	A	U	R	X	X	R	P	V	B	H	R
1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5

We would suspect, in other words, that 'O', 'A', and the third 'P' were all encrypted with the same alphabet:

O	P	N	E	P	N	**A**	U	R	X	X	R	**P**	V	B	H	R
1	2	3	4	5	6	**1**	2	3	4	5	6	**1**	2	3	4	5

Similarly, we would suspect that the first 'P', 'U', and 'V' were encrypted using another alphabet:

O	**P**	N	E	P	N	A	**U**	R	X	X	R	P	**V**	B	H	R
1	**2**	3	4	5	6	1	**2**	3	4	5	6	1	**2**	3	4	5

...and so on with all the letters of the ciphertext. Note that each grouping is an equivalence class under modular addition, using the length of the key as the modulus.

Given a sufficiently long ciphertext, we could now construct a table of the groupings. Since each grouping was enciphered using its own alphabet, we could also compute the Index of Coincidence for the groupings as a check on our guess of the key length. If we guessed correctly, the groupings are likely to have an index that is close to that of English (0.0660).

Perhaps even more significantly, each grouping represents its own small instance of a Caesar Cipher! With a normal Caesar Cipher, of course, we could just try 25 possibilities and be done – eventually one of our attempts would result in a recognizable message. Here, that wouldn't work, because we wouldn't necessarily be able to tell when we had succeeded. But we can still use our reliable weapon: frequency analysis.

The catch is that each grouping may represent a fairly small sample space, whereas frequency analysis works best with a large sample. One approach to this problem is to look for the shift that maximizes the frequency of the three most common English letters: E, A, and T. The letters A and E are four letters apart in the alphabet, while A and T are 19 letters apart. So we can cycle through each grouping, adding the frequencies of the letters that occur at these intervals. The maximal sum is our likely shift – and the letter that was mapped from A is the letter of the key that enciphered this grouping.

Let's work through an example with a larger text, to demonstrate how this approach can crack a Vigenère cipher. Imagine we have come across the following ciphertext:

APJJZ SJCUH FPPJY GHTTP AJOTV UWANH FEBNL SHTTP WZWST DHPFG VOBMT LPPJI JEUNM ARMBT
QKNGK WWSNG YAOLL TANTK WSMJT LPPJF OWAZI GJBMX DWZLX JAVIU MPPNL HNMXX FPUFC
WOBDL YNISW XWBMX JSPNE WDMBT KWJTR YKQSZ LKMFM SJMLZ SJLGK WWSNG YEBFV UKZIB
FCBTM ZAISV AAVYI JWKYB UAPFI HAVJW LKKZM GJMTY ZEAKB FCMWL ODMWX MLWSM ZAMRI
WNWWA AONFM ZAZUN THQXA WZISX VEKYV GIUFG VEVLT DHPNL KQJOX UPAZI GJOWX SPXJG SHBNX
KPWGK WWSYA WOUFE DAZJG VKNYA WEZJZ YOBMX HAWUE WOWMB YDTDK WOMSM WZBMB
KHIBM ZWBTN JDQXM GNQJL LATQN KPPJK WDIAX TAMSL ATZJU WHTNH FOZFB KALTG LDIYT UYWZG
LSPJK WEVTG WAUUX JKZQH KPPNL DENJT FZISH LDMWA AOKWH OJBMX KAKNO AHKTF EKBNH FOEJK
WYWSL LWVYE QBWRX FPMIU QPPJF GJIWV ZOWKU DANZL UQISW ODMSM ZAGBX JAYZX DHMIM
ZAMCB DAAFE OWGXY DALKH JNMKN YABTM ZWBJF HEZJB LEAHH ELCYX VPPFM WHMAX FPPTN KWVII
WNATG KDIAX SPAJO WNIQM AIMXL MBNJK WZLJT LDZFM ZAZYA SJAZU EEBYH TNMFD LDMNK WCOXT
LPPJL EWTQX JAVIF SJGMN FZZJW DWZLX NKTZF WOPFO WXMJG HQJQB KDMIN HKVYA AOKTG LNWAX
JOGGN LPPJU GKSXH XPPJU ACMSW AWVXA SRMGX WJTTG YBWWU AZLJG SJLYA WSPTE WLIWM
QNMSW WNMIB FYIUT THMGR DWETY ZKTIB FCMRI DKGRX FPAIN JEVLM ZAKTN JOMTY LDMXX LNWZU
DAAYA WAUUX JKZXH XXTJY MOKFW AZNWX IQMSM DUMCI GOBZE SPMGR LDMNK SIJFL KWLTK
KWKHN KEVLN KKNRT CEVLT KYPNL EEVWX DEONH FXGTY XAVIB FCILT AJAYT XQVIT EAVYT DZWHM
JEVJH XKCWZ JAIYI JKXMX LHCXM JKONG LDMKB XPGKH MNBMV ZWXYX JKNYA WXTZG VAKWT DSPNV
ZEAYA WEZFE UKZFG LDQXA GSMAX JEAYA GQOMM LKJJT EAZJL LNING MLWSM ZABJQ LBWWM ZAETK
VOIWX LDMXX LDIYT DHBWN WXMQB WRMWL TNMFD LDMNK WCOXT LPPJV GJDJG AAVYX FZISW
ODQHA AOBMX UKVAX FEMSM WJLXX WIANG EUPZF THMTI AJQTG LKJJE WBBYH WRMWR EWVXV
GJAHB WJKJH JWBQX SOBNG LDMUH OAZTY LDMHA AANRT YEAYK SPMYH VABJK EEVJG GSBMX TEOJG
VEISX PETJL ZWDJY GQVIL GICHA UNMIB LEVYA WAUUX JKZTY THMKN KYCXV GQZYT FZATF MYPUK
ARIYX SOANL LWVHX SJLJG UKCWT YAUJG LBZTF LDMNK HWZYR ZAZJT LDWRX LDIYT THWTW QSIWA
SOJJX FYIWK AALTG TABBX WJBMX LSWJF HEZJL XKZXB PWVIM ZEZYR EKWSL OEBMO SNQTN KOCHV
WOAIN JEVLP ZEKMM AIMBX ZWDJE GOBKH JPGHT HEBFE KDQUL SJLFF MYPFZ JAIYX JJCRU WNWKL
EWTQX JRMXL WHAYH YABMX JSQYA LDQWM QPPTN KWVIH XKCWU WOBXX SIMST FZATE VEMWL
SJLYA WZIRT YAZJV WEDJW TUBMX WJMRR AOZJV CKVJW LKJJL GIMBA SPOWX SPMWM ZWVTN JOPTP
WRMWM ZAGMT NAVTP WMCNI HALFG MIMWH MONQX WPISW SNMON KPXWX HWZNG YPWRT
CAIIX KYMSM MLWSN KWVIA AOQRI WNQFE EWRJL LUXQT UEVLZ JAIYV GJNNW WJKJB FUWZK NWTTN
JWVIL LNMSZ LDPFL UKURT FZMIF WPWQT QPPNL SYKTN FPWKA AOIKY SEZXU WBWWX QKC

If we do not know the key, we could proceed as follows:

> Step 1: Compute the Index of Coincidence of the entire ciphertext so that we can make an educated guess as to the key length. In this example, the IC is 0.0444463.
>
> Step 2: Compare the Index of Coincidence to the expected values for the English language (see the table above). Here, the IC appears to correspond to a key length around four or five.

Step 3: Taking a guess at the key length, break the ciphertext into groupings based on that length. Let's say we choose a possible key length of five. We could imagine the ciphertext reorganized into columns, where the letters in each column were enciphered with the same letter of a five-letter key:

A	P	J	J	Z
S	J	C	U	H
F	P	P	J	Y
G	H	T	T	P
A	J	O	T	V
U	W	A	N	H
...	...	...	...	...

If we were correct in our guess of a key length of five, then the letters in the left-most column were all enciphered with the first letter of the key, the letters in the second column were all enciphered with the second letter of the key, etc.

Step 4: We can check our guess in a couple of ways. First, we can calculate the Index of Coincidence for each column. If we guessed correctly, then the IC for each column may be close to 0.0660, since each column (in isolation) was effectively enciphered with a key length of one. Rather than examine five new indices, we could just take the average (here, it's 0.0661905). This gives us more confidence that our guess may have been right.

Step 5: Taking each column in turn, try to identify the alphabetic shift (in the manner of a Caesar Cipher) that was used for that column. Normally we might apply frequency analysis to find which letter was mapped from E. As mentioned above, given the small sample size, it might be better to try to find the shift that would maximize not only E, but also the letters that would then need to correspond to A and T.

Visually:

(add up the frequencies of A, E, and T)

(add up the frequencies of B, F and U)

(add up the frequencies of C, G and V)

etc., for all shifts...

The "winning" shift is likely the one that actually enciphered that column. In that case, whatever plaintext letter corresponds to a ciphertext letter 'A' for that shift would be the next letter of the key.

In this manner, a candidate key can quickly be built and tested against the ciphertext. With the example above, the process produces a candidate key of SWIFT.

Attempting decryption with that key, we have the following recovered plaintext:

ITBEGANUPONTHEFOLLOWINGOCCASIONITISALLOWEDONALLHANDSTHATTHEPRIMITIVEWAYOFBREAKI
NGEGGSBEFOREWEEATTHEMWASUPONTHELARGERENDBUTHISPRESENTMAJESTYSGRANDFATHERWHIL
EHEWASABOYGOINGTOEATANEGGANDBREAKINGITACCORDINGTOTHEANCIENTPRACTICEHAPPENEDTOC
UTONEOFHISFINGERSWHEREUPONTHEEMPERORHISFATHERPUBLISHEDANEDICTCOMMANDINGALLHISS
UBJECTSUPONGREATPENALTIESTOBREAKTHESMALLERENDOFTHEIREGGSTHEPEOPLESOHIGHLYRESENTE
DTHISLAWTHATOURHISTORIESTELLUSTHEREHAVEBEENSIXREBELLIONSRAISEDONTHATACCOUNTWHEREI
NONEEMPERORLOSTHISLIFEANDANOTHERHISCROWNTHESECIVILCOMMOTIONSWERECONSTANTLYFOM
ENTEDBYTHEMONARCHSOFBLEFUSCUANDWHENTHEYWEREQUELLEDTHEEXILESALWAYSFLEDFORREFUG
ETOTHATEMPIREITISCOMPUTEDTHATELEVENTHOUSANDPERSONSHAVEATSEVERALTIMESSUFFEREDDEA
THRATHERTHANSUBMITTOBREAKTHEIREGGSATTHESMALLERENDMANYHUNDREDLARGEVOLUMESHAVE
BEENPUBLISHEDUPONTHISCONTROVERSYBUTTHEBOOKSOFTHEBIGENDIANSHAVEBEENLONGFORBIDDE
NANDTHEWHOLEPARTYRENDEREDINCAPABLEBYLAWOFHOLDINGEMPLOYMENTSDURINGTHECOURSEOF
THESETROUBLESTHEEMPERORSOFBLEFUSCADIDFREQUENTLYEXPOSTULATEBYTHEIRAMBASSADORSACC
USINGUSOFMAKINGASCHISMINRELIGIONBYOFFENDINGAGAINSTAFUNDAMENTALDOCTRINEOFOURGRE
ATPROPHETLUSTROGINTHEFIFTYFOURTHCHAPTEROFTHEBLUNDECRALWHICHISTHEIRALCORANTHISHO
WEVERISTHOUGHTTOBEAMERESTRAINUPONTHETEXTFORTHEWORDSARETHESETHATALLTRUEBELIEVER
SBREAKTHEIREGGSATTHECONVENIENTENDANDWHICHISTHECONVENIENTENDSEEMSINMYHUMBLEOPIN
IONTOBELEFTTOEVERYMANSCONSCIENCEORATLEASTINTHEPOWEROFTHECHIEFMAGISTRATETODETERM
INENOWTHEBIGENDIANEXILESHAVEFOUNDSOMUCHCREDITINTHEEMPEROROFBLEFUSCUSCOURTANDS
OMUCHPRIVATEASSISTANCEANDENCOURAGEMENTFROMTHEIRPARTYHEREATHOMETHATABLOODYWA
RHASBEENCARRIEDONBETWEENTHETWOEMPIRESFORSIXANDTHIRTYMOONSWITHVARIOUSSUCCESSDU
RINGWHICHTIMEWEHAVELOSTFORTYCAPITALSHIPSANDAMUCHAGREATERNUMBEROFSMALLERVESSELS
TOGETHERWITHTHIRTYTHOUSANDOFOURBESTSEAMENANDSOLDIERSANDTHEDAMAGERECEIVEDBYTHE
ENEMYISRECKONEDTOBESOMEWHATGREATERTHANOURSHOWEVERTHEYHAVENOWEQUIPPEDANUMER

OUSFLEETANDAREJUSTPREPARINGTOMAKEADESCENTUPONUSANDHISIMPERIALMAJESTYPLACINGGREATCONFIDENCEINYOURVALOURANDSTRENGTHHASCOMMANDEDMETOLAYTHISACCOUNTOFHISAFFAIRSBEFOREYOU

Since the resulting text is clearly in English, we know we have succeeded. If the candidate key and/or the resulting plaintext were gibberish, we would try again with a different key length.

Although the Vigenère cipher is no longer considered secure, it reigned supreme for several hundred years and is therefore of significant historical importance. More directly for our purposes, analysis of the strengths and weaknesses of such a cipher contributes to our understanding of fundamental principles of cryptography that still apply today.

The output from a Vigenère cipher program is provided below, to help you see how the attack works with different messages and keys.

Sample output:

```
***  Welcome to the Vigenere Cipher program.  ***


MAIN MENU:

1) Encrypt with key
2) Decrypt with key
3) Attempt decryption without key
4) Quit

Selection: 3


Enter the ciphertext: APJJZ SJCUH FPPJY GHTTP AJOTV UWANH FEBNL SHTTP WZWST DHPFG VOBMT LPPJI
JEUNM ARMBT QKNGK WWSNG YAOLL TANTK WSMJT LPPJF OWAZI GJBMX DWZLX JAVIU MPPNL HNMXX FPUFC
WOBDL YNISW XWBMX JSPNE WDMBT KWJTR YKQSZ LKMFM SJMLZ SJLGK WWSNG YEBFV UKZIB FCBTM ZAISV
AAVYI JWKYB UAPFI HAVJW LKKZM GJMTY ZEAKB FCMWL ODMWX MLWSM ZAMRI WNWWA AONFM ZAZUN THQXA
WZISX VEKYV GIUFG VEVLT DHPNL KQJOX UPAZI GJOWX SPXJG SHBNX KPWGK WWSYA WOUFE DAZJG VKNYA
WEZJZ YOBMX HAWUE WOWMB YDTDK WOMSM WZBMB KHIBM ZWBTN JDQXM GNQJL LATQN KPPJK WDIAX TAMSL
ATZJU WHTNH FOZFB KALTG LDIYT UYWZG LSPJK WEVTG WAUUX JKZQH KPPNL DENJT FZISH LDMWA AOKWH
OJBMX KAKNO AHKTF EKBNH FOEJK WYWSL LWVYE QBWRX FPMIU QPPJF GJIWV ZOWKU DANZL UQISW ODMSM
ZAGBX JAYZX DHMIM ZAMCB DAAFE OWGXY DALKH JNMKN YABTM ZWBJF HEZJB LEAHH ELCYX VPPFM WHMAX
FPPTN KWVII WNATG KDIAX SPAJO WNIQM AIMXL MBNJK WZLJT LDZFM ZAZYA SJAZU EEBYH TNMFD LDMNK
WCOXT LPPJL EWTQX JAVIF SJGMN FZZJW DWZLX NKTZF WOPFO WXMJG HQJQB KDMIN HKVYA AOKTG LNWAX
JOGGN LPPJU GKSXH XPPJU ACMSW AWVXA SRMGX WJTTG YBWWU AZLJG SJLYA WSPTE WLIWM QNMSW WNMIB
FYIUT THMGR DWETY ZKTIB FCMRI DKGRX FPAIN JEVLM ZAKTN JOMTY LDMXX LNWZU DAAYA WAUUX JKZXH
XXTJY MOKFW AZNWX IQMSM DUMCI GOBZE SPMGR LDMNK SIJFL KWLTK KWKHN KEVLN KKNRT CEVLT KYPNL
EEVWX DEONH FXGTY XAVIB FCILT AJAYT XQVIT EAVYT DZWHM JEVJH XKCWZ JAIYI JKXMX LHCXM JKONG
LDMKB XPGKH MNBMV ZWXYX JKNYA WXTZG VAKWT DSPNV ZEAYA WEZFE UKZFG LDQXA GSMAX JEAYA GQOMM
LKJJT EAZJL LNING MLWSM ZABJQ LBWWM ZAETK VOIWX LDMXX LDIYT DHBWN WXMQB WRMWL TNMFD LDMNK
WCOXT LPPJV GJDJG AAVYX FZISW ODQHA AOBMX UKVAX FEMSM WJLXX WIANG EUPZF THMTI AJQTG LKJJE
WBBYH WRMWR EWVXV GJAHB WJKJH JWBQX SOBNG LDMUH OAZTY LDMHA AANRT YEAYK SPMYH VABJK EEVJG
GSBMX TEOJG VEISX PETJL ZWDJY GQVIL GICHA UNMIB LEVYA WAUUX JKZTY THMKN KYCXV GQZYT FZATF
MYPUK ARIYX SOANL LWVHX SJLJG UKCWT YAUJG LBZTF LDMNK HWZYR ZAZJT LDWRX LDIYT THWTW QSIWA
SOJJX FYIWK AALTG TABBX WJBMX LSWJF HEZJL XKZXB PWVIM ZEZYR EKWSL OEBMO SNQTN KOCHV WOAIN
JEVLP ZEKMM AIMBX ZWDJE GOBKH JPGHT HEBFE KDQUL SJLFF MYPFZ JAIYX JJCRU WNWKL EWTQX JRMXL
```

```
WHAYH YABMX JSQYA LDQWM QPPTN KWVIH XKCWU WOBXX SIMST FZATE VEMWL SJLYA WZIRT YAZJV WEDJW
TUBMX WJMRR AOZJV CKVJW LKJJL GIMBA SPOWX SPMWM ZWVTN JOPTP WRMWM ZAGMT NAVTP WMCNI HALFG
MIMWH MONQX WPISW SNMON KPXWX HWZNG YPWRT CAIIX KYMSM MLWSN KWVIA AOQRI WNQFE EWRJL LUXQT
UEVLZ JAIYV GJNNW WJKJB FUWZK NWTTN JWVIL LNMSZ LDPFL UKURT FZMIF WPWQT QPPNL SYKTN FPWKA
AOIKY SEZXU WBWWX QKC


Index of Coincidence for entire ciphertext: 0.0444463

Reference Table for English:

Key Length     IoC

1              0.0660
2              0.0520
3              0.0473
4              0.0449
5              0.0435
6              0.0426
7              0.0419
8              0.0414
9              0.0410
10             0.0407


What key length would you like to try?
Enter length (0 to return to Main Menu): 4


Index of Coincidence for suggested key length of 4: 0.0442812
Possible key: WWWW

Attempting decryption with possible key:

ETNNDWNGYLJTTNCKLXXTENSXZYAERLJIFRPWLXXTADAWXHLTJKZSFQXPTTNMNIYRQEVQFXUORKOAAWRKCESPPXERXOAWQN
XPTTNJSAEDMKNFQBHADPBNEZMYQTTRPLRQBBJTYJGASFHPCRMWABAFQBNWTRIAHQFXOANXVCOUWDPOQJQWNQPDWNPKOAAW
RKCIFJZYODMFJGFXQDEMWZEEZCMNAOCFYETJMLEZNAPOODQKNQXCDIEOFJGQAPSHQABQPAWQDEQVMARAAEESRJQDEDYRXL
UBEADMWBZIOCZKMYJKZIZPXHLTRPOUNSBYTEDMKNSABWTBNKWLFRBOTAKOAAWCEASYJIHEDNKZORCEAIDNDCSFQBLEAYIA
SAQFCHXHOASQWQADFQFOLMFQDAFXRNHUBQKRUNPPEXUROTTNOAHMEBXEQWPEXDNYALXRLJSDJFOEPXKPHMCXYCADKPWTNO
AIZXKAEYYBNODULOTTRPHIRNXJDMWLPHQAEESOALSNFQBOEORSELOXJIOFRLJSINOACAWPPAZCIUFAVBJTQMYUTTNJKNMA
ZDSAOYHERDPYUMWASHQWQDEKFBNECDBHLQMQDEQGFHEEJISAKBCHEPOLNRQORCEFXQDAFNJLIDNFPIELLIPGCBZTTJQALQ
EBJTTXROAZMMAREXKOHMEBWTENSARMUQEMQBPQFRNOADPNXPHDJQDEDCEWNEDYIIFCLXRQJHPHQROAGSBXPTTNPIAXUBNE
ZMJWNKQRJDDNAHADPBROXDJASTJSABQNKLUNUFOHQMRLOZCEESOXKPRAEBNSKKRPTTNYKOWBLBTTNYEGQWAEAZBEWVQKBA
NXXKCFAAYEDPNKWNPCEAWTXIAPMAQURQWAARQMFJCMYXXLQKVHAIXCDOXMFJGQVMHOKVBJTEMRNIZPQDEOXRNSQXCPHQBB
PRADYHEECEAEYYBNODBLBBXNCQSOJAEDRABMUQWQHYQGMKSFDIWTQKVPHQROWMNJPOAPXOOAOLROIZPROORVXGIZPXOCTR
PIIZABHISRLJBKXCBEZMFJGMPXENECXBUZMXIEZCXHDALQNIZNLBOGADNEMCMNOBQBPLGBQNOSRKPHQOFBTKOLQRFQZDAB
CBNORCEABXDKZEOAXHWTRZDIECEAIDJIYODJKPHUBEKWQEBNIECEKUSQQPONNXIEDNPPRMRKQPAWQDEFNUPFAAQDEIXOZS
MABPHQBBPHMCXHLFARABQUFAVQAPXRQJHPHQROAGSBXPTTNZKNHNKEEZCBJDMWASHULEESFQBYOZEBJIQWQANPBBAMERKI
YTDJXLQXMENUXKPONNIAFFCLAVQAVIAZBZKNELFANONLNAFUBWSFRKPHQYLSEDXCPHQLEEERVXCIECOWTQCLZEFNOIIZNK
KWFQBXISNKZIMWBTIXNPDAHNCKUZMPKMGLEYRQMFPIZCEAEYYBNODXCXLQOROCGBZKUDCXJDEXJQCTYOEVMCBWSERPPAZL
BWNPNKYOGAXCEYNKPFDXJPHQROLADCVDEDNXPHAVBPHMCXXLAXAUWMAEWSNNBJCMAOEEPXKXEFFBANFQBPWANJLIDNPBOD
BFTAZMQDIDCVIOAWPSIFQSWRUXROSGLZASEMRNIZPTDIOQQEMQFBDAHNIKSFOLNTKLXLIFJIOHUYPWNPJJQCTJDNEMCBNN
GVYARAOPIAXUBNVQBPALECLCEFQBNWUCEPHUAQUTTXROAZMLBOGAYASFBBWMQWXJDEXIZIQAPWNPCEADMVXCEDNZAIHNAX
YFQBANQVVESDNZGOZNAPONNPKMQFEWTSABWTQAQDAZXRNSTXTAVQAQDEKQXREZXTAQGRMLEPJKQMQALQSRUBATMWAWRQSR
OTBABLADRKCTAVXGEMMBOCQWQQPAWROAZMEESUVMARUJIIAVNPPYBUXYIZPDNEMCZKNRRAANONFJYADORAXXRNAZMPPRQW
DPHTJPYOYVXJDQMJATAUXUTTRPWCOXRJTAOEESMOCWIDBYAFAABUOG


What key length would you like to try?
Enter length (0 to return to Main Menu): 5
```

```
Index of Coincidence for suggested key length of 5: 0.0661905
Possible key: SWIFT

Attempting decryption with possible key:

ITBEGANUPONTHEFOLLOWINGOCCASIONITISALLOWEDONALLHANDSTHATTHEPRIMITIVEWAYOFBREAKINGEGGSBEFOREWEE
ATTHEMWASUPONTHELARGERENDBUTHISPRESENTMAJESTYSGRANDFATHERWHILEHEWASABOYGOINGTOEATANEGGANDBREAK
INGITACCORDINGTOTHEANCIENTPRACTICEHAPPENEDTOCUTONEOFHISFINGERSWHEREUPONTHEEMPERORHISFATHERPUBL
ISHEDANEDICTCOMMANDINGALLHISSUBJECTSUPONGREATPENALTIESTOBREAKTHESMALLERENDOFTHEIREGGSTHEPEOPLE
SOHIGHLYRESENTEDTHISLAWTHATOURHISTORIESTELLUSTHEREHAVEBEENSIXREBELLIONSRAISEDONTHATACCOUNTWHER
EINONEEMPERORLOSTHISLIFEANDANOTHERHISCROWNTHESECIVILCOMMOTIONSWERECONSTANTLYFOMENTEDBYTHEMONAR
CHSOFBLEFUSCUANDWHENTHEYWEREQUELLEDTHEEXILESALWAYSFLEDFORREFUGETOTHATEMPIREITISCOMPUTEDTHATELE
VENTHOUSANDPERSONSHAVEATSEVERALTIMESSUFFEREDDEATHRATHERTHANSUBMITTOBREAKTHEIREGGSATTHESMALLERE
NDMANYHUNDREDLARGEVOLUMESHAVEBEENPUBLISHEDUPONTHISCONTROVERSYBUTTHEBOOKSOFTHEBIGENDIANSHAVEBEE
NLONGFORBIDDENANDTHEWHOLEPARTYRENDEREDINCAPABLEBYLAWOFHOLDINGEMPLOYMENTSDURINGTHECOURSEOFTHESE
TROUBLESTHEEMPERORSOFBLEFUSCADIDFREQUENTLYEXPOSTULATEBYTHEIRAMBASSADORSACCUSINGUSOFMAKINGASCHI
SMINRELIGIONBYOFFENDINGAGAINSTAFUNDAMENTALDOCTRINEOFOURGREATPROPHETLUSTROGINTHEFIFTYFOURTHCHAP
TEROFTHEBLUNDECRALWHICHISTHEIRALCORANTHISHOWEVERISTHOUGHTTOBEAMERESTRAINUPONTHETEXTFORTHEWORDS
ARETHESETHATALLTRUEBELIEVERSBREAKTHEIREGGSATTHECONVENIENTENDANDWHICHISTHECONVENIENTENDSEEMSINM
YHUMBLEOPINIONTOBELEFTTOEVERYMANSCONSCIENCEORATLEASTINTHEPOWEROFTHECHIEFMAGISTRATETODETERMINEN
OWTHEBIGENDIANEXILESHAVEFOUNDSOMUCHCREDITINTHEEMPEROROFBLEFUSCUSCOURTANDSOMUCHPRIVATEASSISTANC
EANDENCOURAGEMENTFROMTHEIRPARTYHEREATHOMETHATABLOODYWARHASBEENCARRIEDONBETWEENTHETWOEMPIRESFOR
SIXANDTHIRTYMOONSWITHVARIOUSSUCCESSDURINGWHICHTIMEWEHAVELOSTFORTYCAPITALSHIPSANDAMUCHAGREATERN
UMBEROFSMALLERVESSELSTOGETHERWITHTHIRTYTHOUSANDOFOURBESTSEAMENANDSOLDIERSANDTHEDAMAGERECEIVEDB
YTHEENEMYISRECKONEDTOBESOMEWHATGREATERTHANOURSHOWEVERTHEYHAVENOWEQUIPPEDANUMEROUSFLEETANDAREJU
STPREPARINGTOMAKEADESCENTUPONUSANDHISIMPERIALMAJESTYPLACINGGREATCONFIDENCEINYOURVALOURANDSTREN
GTHHASCOMMANDEDMETOLAYTHISACCOUNTOFHISAFFAIRSBEFOREYOU


What key length would you like to try?
Enter length (0 to return to Main Menu): 0


MAIN MENU:

1) Encrypt with key
2) Decrypt with key
3) Attempt decryption without key
4) Quit

Selection: 4
```

```
***  Welcome to the Vigenere Cipher program.  ***


MAIN MENU:

1) Encrypt with key
2) Decrypt with key
3) Attempt decryption without key
4) Quit

Selection: 3
```

```
Enter the ciphertext: WLPHZ UEGUE GSCTE EISCG FQTJL PWPVK OAYIY WVVTG RWASR SOSKM XKRAE KSSFB
UQNTD VPQFV DVWIX OKBEE WSFGY QSCDP PUIMY RBIDG YWNRD ROHNQ NXOIO OELHV VYDIR TLLSE WSWIC
RZEDT CCSUH HLBUI NVPEE SUBHR IMCSS CRAWF CWXPT YBEYR KPEFR JEFRL INQGP CWBHR LRNOE LEFFI
YHCQG UWWTB KPEYL PTSJW FFLPG SIKAH JLEHY MBHEF WSJBH NWJWO JPEQD RODRA SRGMY CLZGY DWDSJ
WUEFL LWIAB RLRRV ZAPNW IYHJM MOUEN SUINQ FECSJ AEQXW COKPE EWLLB JCBZL XESUB OOHWL HLXOA
DROHY MRRZE DHYIT YXBFF ZWUFD JESIL IAQIC OKUOF SLPFV EHRQX SCLOH GUYYG XZAPH JFZCG FEHIZ
TKPEG UEXAV TSBIT CSTQS VRR


Index of Coincidence for entire ciphertext: 0.0413844

Reference Table for English:

Key Length     IoC

1              0.0660
2              0.0520
3              0.0473
4              0.0449
5              0.0435
6              0.0426
7              0.0419
8              0.0414
9              0.0410
10             0.0407


What key length would you like to try?
Enter length (0 to return to Main Menu): 8


Index of Coincidence for suggested key length of 8: 0.0658381
Possible key: DELORWAN

Attempting decryption with possible key:

THETIYETRAVELXERFORSOUTWILLBEOONVENIEZTTOSPEAWOFHIMWAEEXPOUNDUNGARECOZDITEMATFERTOUSHUSPALEGRQ
YEYESSHANEANDTWUNKLEDANPHISUSUAXLYPALEFMCEWASFLGSHEDANDMNIMATEDFHEFIREBGRNTBRIGTTLYANDTTESOFTR
APIANCEOFFHEINCANPESCENTLUGHTSINTTELILIESAFSILVEROAUGHTTHQBUBBLESFHATFLASTEDANDPAESEDINOUDGLAS
SESAURCHAIREBEINGHIEPATENTSQMBRACEDMNDCARESEEDUSRATTERTHANSGBMITTEDFOBESATUBONANDTHQREWASTHMTL
UXURIAUSAFTERPINNERATYOSPHEREIHENTHOUSHTRUNSGDACEFULLKFREEOFTTETRAMMEXSOFPRECUSION


What key length would you like to try?
Enter length (0 to return to Main Menu): 0


MAIN MENU:

1) Encrypt with key
2) Decrypt with key
3) Attempt decryption without key
4) Quit

Selection: 2


Enter a key consisting of alphabetic characters: Delorian
```

```
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

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 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
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
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
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
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
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
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


Enter a message to be decrypted: WLPHZ UEGUE GSCTE EISCG FQTJL PWPVK OAYIY WVVTG RWASR SOSKM
XKRAE KSSFB UQNTD VPQFV DVWIX OKBEE WSFGY QSCDP PUIMY RBIDG YWNRD ROHNQ NXOIO OELHV VYDIR
TLLSE WSWIC RZEDT CCSUH HLBUI NVPEE SUBHR IMCSS CRAWF CWXPT YBEYR KPEFR JEFRL INQGP CWBHR
LRNOE LEFFI YHCQG UWWTB KPEYL PTSJW FFLPG SIKAH JLEHY MBHEF WSJBH NWJWO JPEQD RODRA SRGMY
CLZGY DWDSJ WUEFL LWIAB RLRRV ZAPNW IYHJM MOUEN SUINQ FECSJ AEQXW COKPE EWLLB JCBZL XESUB
OOHWL HLXOA DROHY MRRZE DHYIT YXBFF ZWUFD JESIL IAQIC OKUOF SLPFV EHRQX SCLOH GUYYG XZAPH
JFZCG FEHIZ TKPEG UEXAV TSBIT CSTQS VRR

Decrypting...

Recovered plaintext:
THETIMETRAVELLERFORSOITWILLBECONVENIENTTOSPEAKOFHIMWASEXPOUNDINGARECONDITEMATTERTOUSHISPALEGRE
YEYESSHONEANDTWINKLEDANDHISUSUALLYPALEFACEWASFLUSHEDANDANIMATEDTHEFIREBURNTBRIGHTLYANDTHESOFTR
ADIANCEOFTHEINCANDESCENTLIGHTSINTHELILIESOFSILVERCAUGHTTHEBUBBLESTHATFLASHEDANDPASSEDINOURGLAS
SESOURCHAIRSBEINGHISPATENTSEMBRACEDANDCARESSEDUSRATHERTHANSUBMITTEDTOBESATUPONANDTHEREWASTHATL
UXURIOUSAFTERDINNERATMOSPHEREWHENTHOUGHTRUNSGRACEFULLYFREEOFTHETRAMMELSOFPRECISION


MAIN MENU:

1) Encrypt with key
2) Decrypt with key
3) Attempt decryption without key
4) Quit

Selection: 4
```