Cryptography of the Vigenère Cipher

Simple substitution ciphers, Caesar ciphers, multiplicative ciphers, and affine ciphers are all examples of **monoalphabetic ciphers** – only one ciphertext alphabet is used.

> Even if the original word lengths are concealed and the substitution alphabet is random, it is possible to find a solution by using frequency data, repetition patterns and information about the way letters combine with one another. What makes the solution possible is the fact that a given plain language letter is always represented by the same cipher letter. As a consequence, all the properties of plain language such as frequencies and combinations are carried over into the cipher and may be utilized for solution. In effect we could say that all such properties are invariant except that the names of the letters have been changed.
>
> It would seem then that one way to obtain greater security would be to use more than one alphabet in enciphering a message. The general system could be one that uses a number of different alphabets for encipherment, with an understanding between correspondents of the order in which the alphabets are to be used. Sinkov, Abraham, *Elementary Cryptanalysis: A mathematical approach*, Mathematical Association of America, 1968.

A simple scheme would be to have two cipher alphabets and alternate between them during encryption. Such a scheme is an example of a **polyalphabetic cipher** a cipher in which there is more than one ciphertext alphabet and a rule that describes how to use them. For example, our ciphertext alphabets might be a Caesar cipher with additive key 3 and a Caesar cipher with additive key 5. Our enciphering rule is that we will use the Caesar cipher alphabet with additive key 3 to encrypt the first plaintext letter, the Caesar cipher alphabet with additive key 5 to encrypt the second plaintext letter, the Caesar cipher alphabet with additive key 3 to encrypt the third plaintext letter, the Caesar cipher alphabet with additive key 5 to encrypt the fourth plaintext letter, etc. Our rule is to alternate between the two alphabets beginning with the Caesar cipher with additive key 3.

For example, we will encrypt the plaintext message Northern Kentucky University:

The key

```
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

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
```

Plaintext and ciphertext

```
n o r t h e r n k e n t u c k y u n i v e r s i t y
Q T U Y K J U S N J Q Y X H N D X S L A H W V N W D
```

Notice that two of the ns are encrypted with Q and two with S. Two rs are encrypted with U and one with W. Two ts are encrypted with Y and one with W. Etc. But, for example, because of the spacing of the plaintext letters, both of the ys are encrypted as D.

For the inverse process – decryption – there are two Hs, but one has been substituted for plaintext c and the other for plaintext e.

Because two ciphertext letters correspond to each plaintext letter, this scheme will tend to balance frequencies, and it is memorable.

We might balance frequencies even better if we have several cipher alphabets and rotate among them according to some scheme to which the correspondents have agreed. We will examine a classic example of such a method – the Vigenère cipher.

The Cryptographer

Blaise de Vigenère (1523 – 1596)

Vigenère was not a nobleman. The "de" in his name simply indicates that his family came from the village of Vigenère or Viginaire. He himself was born in the village of Saint-Pourçain, about halfway between Paris and Marseilles, on April 15, 1523. At 17, he was taken from his studies and sent to court and, five years later, to the Diet of Worms as a very junior secretary. This gave him an initiation into diplomacy, and his subsequent travels through Europe broadened his experience. At 24, he entered the service of the Duke of Nevers, to whose house he remained attached the rest of his life, except for periods at court and as a diplomat. In 1549, at 26, he went to Rome on a two-year diplomatic mission.

It was here that he was first thrown into contact with cryptology, and he seems to have steeped himself in it. He read the books of Trithemius [1462 – 1516], Belaso [? - ? but known to have published in 1553 a booklet in which he proposed a polyalphabetic cipher], Cardano [1501 – 1576], and Porta [1535 – 1615], and the unpublished manuscript of Alberti [1404 – 1472]. He evidently conversed with the experts of the papal curia … . … in 1566 he was sent again to Rome as secretary to King Charles IX. Here he renewed his acquaintance with the cryptographic experts, and this time seems to have been admitted to their chambers … . Finally in 1570, at 47, Vigenère quit the court for good, turned over his annuity of 1,000 livres a year to the poor of Paris, married the much younger Marie Varé, and devoted himself to writing.

He turned out some 20-odd books before he died of throat cancer in 1596. … [The] book which is constantly cited by workers in its field is his *Traicté des Chiffres*, which was written in 1581 … .

It is a curious work. In its more than 600 pages, it distilled not only much of the cryptographic lore of Vigenère's day … but a hodgepodge of other topics.

> … [The] *Traicté* is reliable in its cryptographic information. Vigenère was scrupulous in assigning credit for material from other authors and quoted them accurately and with comprehension.
>
> Among the numerous ciphers that Vigenère discussed … were polyalphabetics. Each of his used a Trithemius-like tableau [which he improved by adding mixed alphabets on the sides. He also improved upon the autokey system of Cardano. Vigenère's system] works well and affords fair guarantees of security … .
>
> In spite of Vigenère's clear exposition of his devices, both were entirely forgotten and only entered the stream of cryptology late in the 19th-Century after they were reinvented. Writers on cryptology then added insult to injury by degrading Vigenère's system into one more elementary.
>
> This system is … more susceptible to solution than Vigenère's original. Nevertheless, a legend grew up that this degenerate form of Vigenère's work was the indecipherable cipher par excellence, a legend so hardy that as late as 1917, more than a half century after it had been exploded, the Vigenère was touted as "impossible of translation" in a journal as respected as *Scientific American*. Kahn, David, *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*, Scribner, 1996.

The method we shall study below is the corrupted version of the cipher that now bears Vigenère 's name. His original cipher was more secure than this.

The Vigenère Square

The Vigenère cipher is based upon a square that consists of the 26 Caesar cipher alphabets; this is in fact the square used by Trithemius [1462 – 1516].

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	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	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	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	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
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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

The Cipher

The key to this method of encryption is a memorable word or phrase. Let us use the name of the French mathematician *Galois* (1811 – 1832) as our key to encipher `Northern Kentucky University`.

The letters of the keyword determine the alphabets used to encrypt:

> The first letter of the keyword is *g*; so, the first letter of the message is encrypted using row *g* of the table. Plaintext `n` corresponds to ciphertext `T`.
>
> The second letter of the keyword is *a*; so, the second letter of the message is encrypted using row *a* of the table. Row *a* corresponds to a shift of 0 – plaintext; so, plaintext `o` corresponds to ciphertext `O`.
>
> The third letter of the keyword is *l*; so, the third letter of the message is encrypted using row *l* of the table. Plaintext `r` corresponds to ciphertext `C`.
>
> The fourth letter of the keyword is *o*; so, the fourth letter of the message is encrypted using row *o* of the table. Plaintext `t` corresponds to ciphertext `H`.
>
> The fifth letter of the keyword is *i*; so, the fifth letter of the message is encrypted using row *i* of the table. Plaintext `h` corresponds to ciphertext `P`.
>
> The sixth and last letter of the keyword is *s*; so, the sixth letter of the message is encrypted using row *s* of the table. Plaintext `e` corresponds to ciphertext `W`.
>
> Now we returned to the beginning of the keyword. The first letter of the keyword is *g*; so, the seventh letter of the message is encrypted using row *g* of the table. Plaintext `r` corresponds to ciphertext `X`.
>
> Etc.

Here are the keyword, plaintext, and ciphertext messages:

```
g a l o i s g a l o i s g a l o i s g a l o i s g a
n o r t h e r n k e n t u c k y u n i v e r s i t y
T O C H P W X N V S V L A C V M C F O V P F A A Z Y
```

Notice that the four ns are encrypted as T, N, V, and F. The three rs are encrypted as C, X, and F. The three ts are encrypted as H, L, and Z.

But, notice that because of the spacing of the plaintext letters, the two ks are each encrypted with row *l* as V.

For the inverse process – decryption – A represents u, s, and i. V represents both k and v.

Etc.

Ideally, a different alphabet could be used to encrypt each letter of the plaintext message. (Of course, there are only 26 possible shifts.)

Both the sender and receiver of a message need a Vigenère square. So, it is possible that someone could discover the method of encryption. But, the keyword need not be written; so, the key can remain secure even if the method is known.

Here is another example. Let us use the keyword *magic* to encrypt the following message.

```
Alberti's cipher disk founded polyalphabeticity.
```

The first letter of the keyword is *m*; so, the first letter of the message is encrypted using row *m* of the table. Plaintext a corresponds to ciphertext M.

The second letter of the keyword is *a*; so, the second letter of the message is encrypted using row *a* of the table. Plaintext l corresponds to ciphertext L.

The third letter of the keyword is *g*; so, the third letter of the message is encrypted using row *g* of the table. Plaintext `b` corresponds to ciphertext `H`.

The fourth letter of the keyword is *i*; so, the fourth letter of the message is encrypted using row *i* of the table. Plaintext `e` corresponds to ciphertext `M`.

The fifth letter of the keyword is *c*; so, the fifth letter of the message is encrypted using row *c* of the table. Plaintext `r` corresponds to ciphertext `T`.

Now we returned to the beginning of the keyword. The first letter of the keyword is *m*; so, the sixth letter of the message is encrypted using row *m* of the table. Plaintext `t` corresponds to ciphertext `F`.

Etc.

The encryption process cycles through the letters of the keyword as many times as are necessary to encyrpt each letter of the plaintext message. The process rotates among five alphabets – those whose rows correspond to the letters *m*, *a*, *g*, *i*, *c*.

```
abcdefghijklmnopqrstuvwxyz
MNOPQRSTUVWXYZABCDEFGHIJKL
ABCDEFGHIJKLMNOPQRSTUVWXYZ
GHIJKLMNOPQRSTUVWXYZABCDEF
IJKLMNOPQRSTUVWXYZABCDEFGH
CDEFGHIJKLMNOPQRSTUVWXYZAB
```

(It would not be wise to leave such a key "lying around" because the first column would reveal the keyword. "Leaving around" the complete Vigenère square reveals the method but not the keyword.)

Here is the encrypted message:

```
MLHMT   FIYKK   BHKZF   USQNQ   GNJMF   BORGC
XPNID   QTOKK   FY
```

Rotating among the five alphabets tends to equalize the frequencies of ciphertext letters and makes frequency analysis more challenging (but not impossible). The more alphabets that are used (i.e., the longer the keyword or phrase) the more the frequencies can be equalized.

Here is a plaintext message:

```
It is all but impossible to draw a distinction between Bletchley Park’s
work on wartime Germany and its growing work on the Soviet Union in the
nineteen forties.  Knowledge of wartime Germany required the tracking
of events on the eastern front and involved learning as much as
possible about the Soviet effort.  British intelligence began to value
the Germans for their knowledge of the Soviet Union as soon as Ultra
came onstream.  German messages used to send their own Sigint summaries
about the Soviet Union back to Berlin were, in turn, intercepted by the
British.  This “second-hand” Signit proved to be London’s best source
on the performance of Soviet forces.  As early as nineteen forty-three
the Joint Intelligence Committee – Britains’ highest intelligence
authority – was able to produce detailed and accurate reports on the
capabilities of the Soviet Air Force, based upon Luftwaffe Sigint
material.
```

After encrypting it with a Vigenère cipher using the keyphrase *Northern Kentucky Univeristy*, the ciphertext message is:

```
vhzlh pcoex vfjqc qcotz xfvzt unrzl amepd mbgvg duyrv wpvlk ajrmg tyojj
yvxhh ykpnv uzkvj utllo ewpxj tbsjb higml xwixy wahtv sknum fasrg aypsl
ygmzr wgzmg rgbgv acrnk rhzyk pnvuz kvjut llfvj bmirn xuxnt kaevv bswwd
xlggf galvr kwgxl pppia bvrua vomyj vwsir exmaz uuwsw uintf kabzy sruvy
kgrif hpkor ysnjv ktzbr vgybu xvyvm txheo zytii xfnie srhyx niizk rfyit
dfyvz frfot xbtsf yalvf yzvxn wxgia inwfg vtqhz kkhgr zosal ntoyg tmmqr
fuxqf oxxzy jrnxb lypnr brqms nfabe vbklb qdnbm rludy sngpz wfnqx rhbzh
ufrpu xbuyt vghjm mizfb npawe mlvtr zxrwv adfyo zdxzk pmfvg jxjse qreaw
mkqlc gxmsm wlmmo schuh facfr lnuys lpmjr kzmic etfkt eepos slixs cnswm
gvkil cnfcr hwevx igxyp pmlgg oliwm mfrxf buxza diyec iolwr kjqda bmcrp
ibaez aclvz bgcrc abzpc aoxlp srnal fesxl puukz frbjt iglna rrvmh mcrne
awuem slnbz vvhwk rfcem oitnz eobfk dgyfw axywa htvsk tpvwb bgruu uoboc
wiplx bpyst vlpkz adqnm ytsyf
```

(This message was encrypted with software that may be downloaded from http://faculty.goucher.edu/blewand/cryptomath/)

Here are the plaintext frequencies:

```
a     1111111111111111111111111111111111111111111111111
b     1111111111111111111
c     11111111111111111111
d     11111111111111111111
e     11111111111111111111111111111111111111111111111111111111111111111
      1111111111111111111111111111
f     11111111111111111
g     1111111111111111111
h     1111111111111111111111111
i     1111111111111111111111111111111111111111111111111111111111111111
j     1
k     1111111
l     11111111111111111111111111
m     11111111111111111
n     1111111111111111111111111111111111111111111111111111111111111111
o     11111111111111111111111111111111111111111111111111111111111
p     1111111111
q     1
r     111111111111111111111111111111111111111111111111
s     11111111111111111111111111111111111111111111111111
t     11111111111111111111111111111111111111111111111111111111111111111
      11111111111
u     1111111111111111111
v     11111111111
w     1111111111111
x
y     1111111
z
```

Here are the ciphertext frequencies:

```
A     11111111111111111111111111111111
B     11111111111111111111111111111111
C     11111111111111111111
D     111111111111
E     1111111111111111111111
F     11111111111111111111111111111111111
G     11111111111111111111111111111111
H     111111111111111111111
I     111111111111111111111111111
J     111111111111111111
K     1111111111111111111111111111
L     11111111111111111111111111111111111
M     111111111111111111111111111111111111
N     111111111111111111111111111111
O     111111111111111111111
P     1111111111111111111111111111
Q     111111111111
R     11111111111111111111111111111111111111111111
S     1111111111111111111111111111
T     1111111111111111111111111111
U     1111111111111111111111111111
V     1111111111111111111111111111111111111111111
W     1111111111111111111111111111
X     1111111111111111111111111111111111111
Y     1111111111111111111111111111111111
Z     1111111111111111111111111111111111
```

A balanced frequency analysis is a clue that a Vigenère cipher might have been used.

Kahn, in *The Codebreakers*, reports that the Vigenère cipher was commonly used by the Confederacy during the Civil War. He states that only three keyphrases were used throughout the war – `Manchester Bluff`, `Complete Victory`, and `Come Retribution`.

Lewis Carroll

Charles Dodgson (Lewis Carroll, 1832 – 1898) created several ciphers. In 1868 he invented the Alphabet-Cipher. Dodgson's cipher is just the Vigenère cipher with the "usual" key.

```
  ABCDEFGHIJKLMNOPQRSTUVWXYZ

A abcdefghijklmnopqrtsuvwxyz A
B bcdefghijklmnopqrstuvwxyza B
C cdefghijklmnopqrstuvwxyzab C
D defghijklmnopqrstuvwxyzabc D
E efghijklmnopqrstuvwxyzabcd E
F fghijklmnopqrstuvwxyzabcde F
G ghijklmnopqrstuvwxyzabcdef G
H hijklmnopqrstuvwxyzabcdefg H
I ijklmnopqrstuvwxyzabcdefgh I
J jklmnopqrstuvwxyzabcdefghi J
K klmnopqrstuvwxyzabcdefghij K
L lmnopqrstuvwxyzabcdefghijk L
M mnopqrstuvwxyzabcdefghijkl M
N nopqrstuvwxyzabcdefghijklm N
O opqrstuvwxyzabcdefghijklmn O
P pqrstuvwxyzabcdefghijklmno P
Q qrstuvwxyzabcdefghijklmnop Q
R rstuvwxyzabcdefghijklmnopq R
S stuvwxyzabcdefghijklmnopqr S
T tuvwxyzabcdefghijklmnopqrs T
U uvwxyzabcdefghijklmnopqrst U
V vwxyzabcdefghijklmnopqrstu V
W wxyzabcdefghijklmnopqrstuv W
X xyzabcdefghijklmnopqrstuvw X
Y yzabcdefghijklmnopqrstuvwx Y
Z zabcdefghijklmnopqrstuvwxy Z

  ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

Dodgson notes about his cipher:

> In Sending a message, write the key-word over it, letter for letter, repeating it as often as may be necessary: the letters of the key-word will indicate which column is to be used in translating each letter of the message, the symbols for which should be written underneath: then copy out the symbols only, and destroy the first paper. It will now be impossible for any one, ignorant of the key-word, to decipher the message, even with the help of the table.

Dodgson was wrong about the security of his cipher; the 1917 *Scientific American* article was also wrong. The Vigenère cipher had been solved before either of these publications. It is possible that Charles Babbage (1792 – 1871) solved the cipher, but he did not publish it. Friedrich Kasiski (1805 – 1881) did publish a solution; in 1863 Kasiski published a 95-page volume *Die Geheimschriften und due Dechiffrir-kunst*, a volume that received little attention at the time. We will take up Kasiski's solution in the next section.

Exercises

1. Here is a message encrypted with a Vigenère cipher with keyword *ultra*.

```
NSXLS   HLOPT   OCGVD   NZWRY   NZGJN   WCMFC   LPTKE
UYXCE   WEKFN   CNFRC   BTGVT   BLMTO   UWWHU   CNDCY
LPTUE   HTZDA
```

1a. Do a frequency analysis of the ciphertext.
1b. Decrypt the message.

2. Encrypt the following message using a Vigenère cipher with keyword *packers*. Then do a frequency analysis of the ciphertext.

```
While the autokey was a brilliant idea, Cardano formulated
it defectively.
```

3. Here is an example of Vigenère's autokey system. We will encrypt (a portion of) the message of exercise 2. The key is a single letter, say, *K*.

The first letter of plaintext is encrypted with the alphabet in row `K` – the row of the keyletter. Plaintext `w` becomes ciphertext `G`.

The second letter of plaintext is encrypted with the alphabet in the row of the first plaintext letter `w`. Plaintext `h` becomes ciphertext `D`.

The third letter of plaintext is encrypted with the alphabet in the row of the second plaintext letter `h`. Plaintext `i` becomes ciphertext `P`.

Etc.

Key	K	W	H	I	L	E	T
Plaintext	w	h	i	l	e	t	h
Ciphertext	G	D	P	T	P	X	A

Complete the encryption of the message.

4. The following message has been encrypted with the autokey scheme discussed in exercise 3 with keyletter *C*. Decrypt the message.

```
RDFKT   SXFMQ   ESSCT    PNIHZ   ZUOAL   KVWLL   GBGAL
FPCYN   HJZLK   BDDAD    TBXVR   RLGZB   HBA
```

5. Compare using "the usual" Vigenère cipher with the autokey scheme described in exercise 3. Which is easier to encrypt? Decrypt? What are potential problems with encryption? Decryption? Etc.

6. Use the Vigenère square given earlier to encrypt the message `Diffie and Hellman proposed a solution to the key exchange problem` using as much of the key phrase "Even in the blackout you could sense the size of the place. The mansion was still the same, and so were the huts, but these were now just a fraction of the overall site," as needed. The phrase appears on page 46 of the October 1996 Ballatine paperback version of Robert Harris' novel *Engima* (and is describing Bletchley Park); it begins line 4. If both sender and receiver had a copy of the book, the key could, for example, be exchanged as 464.

7. Use the Vigenère square given earlier and as much of the random key phrase

```
GUJDTWVDXUVEADPYCBKTNUPEJSAOPFNEELCQGKJNUJUPYUAFEJZPOGLRWHYL
CETNQMVIYAMXHUIPEOZAMVRLVHSNFQYNTBMIDIXCMSMGGUJYIMNDZWARNB
```

as needed to encrypt the message `There is a growing concern that computers now constitute, or will soon constitute, a dangerous threat to individual privacy.` It's not a very memorable key phrase, is it?

8. On the next page is a Vigenère square with rows that are random alphabets. Use that square and the keyword *Cardano* to encrypt the message `The flaw that led to the decryption of Enigma messages was not due to the design of the machine itself.`

	abcdefghijklmnopqrstuvwxyz
A	FGXSOYQEALPWBZCTIHJNMVRDKU
B	SLOJQBYVZDCTKMHGFNHAUWPRXE
C	PJUWKSACVFBZDMTOXIYLQGERHN
D	QNMXSYGZJLCKBUIRPOVWHDFEAT
E	SRBKMTCGYHFOVWAZDNILPXQJEU
F	ROENAYHSFGVPTMQBWXLCIZJDUK
G	OQPMNSVKUIGBEJHDWCXYRTFZAL
H	XWUYRDKGBFASZIPQCLOEJMNTVH
I	HJMVKSZGFDCAUIXLPTNQBYROEW
J	DWMHTZVGBXSEUAFNQYRLCJKIPO
K	VFUJDZRNMSLYHQGWAOIPXCETBK
L	ATIPUNVCHXJBFYRGODLQSZKWEM
M	JYETAHKQPNBSCXRLUZOFIWVMGD
N	IFUDJOGXVYRCLBTWMQPNZHSKAE
O	ZDHCVFBLKENWIQXUAOJPYRSMGT
P	YDZHNTCJLMRQFGBAPVUXEOSKIW
Q	YXTODRJLGMFQAUCVXZHKPSNBIE
R	XBJDTSHGCEUMOFLPYNVZWIKQAR
S	AWBCGETYZULFDJOQPMKXRVINHS
T	THJPMULSIDZCQBREAOFVKYNGWX
U	HKLUEZCFIDWJPNYRMXGTVQSBAO
V	FMKXAZJQRDLNCWHSOPIBTYGEVO
W	SATXZGOVFDCNMJLHEPBKIYRUWQ
X	DLUWXRHQCTFVZKGSOIEJMBYAPN
Y	HDBMRQYSVWPAUTOXNFVCLKJEIG
Z	DXBCTGKMJHQOWZUNIPSFRYLVEA

9. Vigenère used a square like the following that scrambled the alphabets in the left column and on the top row:

ytbmkaqouwjlizrfgxdvcshpen

Z	ABCDEFGHIJKLMNOPQRSTUVWXYZ
R	BCDEFGHIJKLMNOPQRSTUVWXYZA
E	CDEFGHIJKLMNOPQRSTUVWXYZAB
A	DEFGHIJKLMNOPQRSTUVWXYZABC
I	EFGHIJKLMNOPQRSTUVWXYZABCD
X	FGHIJKLMNOPQRSTUVWXYZABCDE
N	GHIJKLMNOPQRSTUVWXYZABCDEF
P	HIJKLMNOPQRSTUVWXYZABCDEFG
C	IJKLMNOPQRSTUVWXYZABCDEFGH
M	JKLMNOPQRSTUVWXYZABCDEFGHI
G	KLMNOPQRSTUVWXYZABCDEFGHIJ
B	LMNOPQRSTUVWXYZABCDEFGHIJK
Y	MNOPQRSTUVWXYZABCDEFGHIJKL
D	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
S	PQRSTUVWXYZABCDEFGHIJKLMNO
H	QRSTUVWXYZABCDEFGHIJKLMNOP
K	RSTUVWXYZABCDEFGHIJKLMNOPQ
L	STUVWXYZABCDEFGHIJKLMNOPQR
U	TUVWXYZABCDEFGHIJKLMNOPQRS
T	UVWXYZABCDEFGHIJKLMNOPQRST
J	VWXYZABCDEFGHIJKLMNOPQRSTU
V	WXYZABCDEFGHIJKLMNOPQRSTUV
F	XYZABCDEFGHIJKLMNOPQRSTUVW
Q	YZABCDEFGHIJKLMNOPQRSTUVWX
W	ZABCDEFGHIJKLMNOPQRSTUVWXY

Vigenère also recommended long key phrases, but use a short one – *Trithemius* and the table above to encrypt the message `The telegraph made cryptography what it is today`.

10. Re-encrypting a Vigenère cipher with another Vigenère cipher results in a Vigenère cipher, but the key is likely to be a random string of letters.

10a. A message is encrypted with a Vigenère cipher using the keyword *Norse* and then encrypted again with a Vigenère cipher using keyword *maths*. What is the key to the re-encrypted message?

10b. A message is encrypted with a Vigenère cipher using the keyword *Kahn* and then encrypted again with a Vigenère cipher using keyword *Kentucky*. What is the key to the re-encrypted message?

10c. A message is encrypted with a Vigenère cipher using the keyword *Friedman* and then encrypted again with a Vigenère cipher using keyword *Sinkov*. What is the key to the re-encrypted message?

10d. A message is encrypted with a Vigenère cipher using the keyword *Norse* and then encrypted again with a Vigenère cipher using keyword *Kentucky*. What is the key to the re-encrypted message?

10e. A message is encrypted with a Vigenère cipher using the keyword *Enigma* and then encrypted again with a Vigenère cipher using keyword *uboat*. What is the key to the re-encrypted message?

10f. A message is encrypted with a Vigenère cipher using the keyword *Ultra* and then encrypted again with a Vigenère cipher using keyphrase *Bletchley Park*. What is the key to the re-encrypted message?

10g. A message is encrypted with a Vigenère cipher using the keyword *Turing* and then encrypted again with a Vigenère cipher using keyword *Welchman*. What is the key to the re-encrypted message?

11a. A message is encrypted with a Vigenère cipher using the keyword having length 6 and then encrypted again with a Vigenère cipher using keyword having length 6. What is the length of the key to the re-encrypted message?

11b. A message is encrypted with a Vigenère cipher using the keyword having length 5 and then encrypted again with a Vigenère cipher using keyword having length 10. What is the length of the key to the re-encrypted message?

11c. A message is encrypted with a Vigenère cipher using the keyword having length 6 and then encrypted again with a Vigenère cipher using keyword having length 9. What is the length of the key to the re-encrypted message?

11d. A message is encrypted with a Vigenère cipher using the keyword having length 7 and then encrypted again with a Vigenère cipher using keyword having length 8. What is the length of the key to the re-encrypted message?

12. A message is encrypted with a Vigenère cipher using the keyword *codebreaker* and then encrypted again with a Caesar cipher with additive key 8. What is the resulting cipher? What is the key?

13. A message is encrypted with keyword cipher with key *cryptography* and then encrypted again with a Vigenère cipher with keyword *England*. Has the security been increased?

14. It is possible, by remembering several short keywords, to effectively encipher with a long key. Consider the following encryption. The plaintext was first encrypted with a Vigenère cipher with keyword *history* and then encrypted again with a Vigenère cipher with keyword *Enigma* and then encrypted again with a Vigenère cipher with keyword *black*. What is the length of the keyphrase for the resulting Vigenère cipher?