Cryptology for Beginners

Stu Schwartz
Wissahickon High
Ambler, Pa 19002
sschwartz8128@verizon.net
www.mastermathmentor.com

This workbook requires the use of the Cipher System Excel spreadsheet. When opening the spreadsheet, be sure to enable macros.

Cryptology for Beginners

Stu Schwartz
sschwartz8128@verizon.net

1. Introduction and Terminology

Cryptology is defined as the science of making communication incomprehensible to all people except those who have a right to read and understand it. The study of cryptology consists of two parts:

- cryptography, which concerns itself with the secrecy system itself and its design, and
- cryptanalysis, which concerns itself with the breaking of the secrecy system above.

Most of us associate cryptography with the military, war, and secret agents. And, indeed, those areas have seen extensive use of cryptography. In World War II, for example, a great deal of effort was expended to create systems so that the high command could communicate with generals in the field over radio waves with the enemy not being able to decipher it. Even more time was spent in analyzing these messages and "breaking the code."

Today we need cryptology because of the everyday use of computers and the Internet. It is important for businesses to be able to protect the information in their computers. If you decide to buy a CD from Amazon.com using your credit card, it is important that no one but Amazon has the ability to read the file where your credit card number is stored. Electronic fund transfers have made privacy a great concern.

This booklet will help your understand some simple cryptography systems and teach you how to apply some techniques of cryptanalysis.

First, some terminology:

Code - a set of information that will allow words to be changed to other words or symbols, For instance, a code for the word "rifle" may be "escargot." That is not the type of cryptography that lends itself to analyze. The only way to decode a message is by having the set of words and their codes. If someone is able to get his hands on the codebook, then every secrecy message can be broken. We are interested in methods of cryptography that lend themselves to explainable techniques that can be performed to change a message into a secret one, and, more importantly, change back by people having the authorization and knowledge to do so.

Plaintext - the message that you wish to put into a secret form. Plaintext is usually written in all lower case letters without spaces. Numbers are written out and punctuation is ignored. So the message

"I will meet you at 5 PM in the mall" is written as:

iwillmeetyouatfivepminthemall

Another name for plaintext is called "clear." A message sent "in the clear" is sent without any attempt to alter it.

Cipher - the method for altering the plaintext

Ciphertext - the secret version of the plaintext. So the plain text:

iwillmeetyouatfivepminthemall may be changed to:

NBNQQRJJYDTZFYKNAJURNSYMJRFQQ

To make reading the ciphertext easier, the letters are usually written in blocks of 5. The above is:

NBNQQ RJJYD TZFYK NAJUR NSYMJ RFQQ

Encipher - changing from plaintext to ciphertext

Decipher - changing from ciphertext to plaintext

Key - information that will allow someone to encipher the plaintext and also decipher the ciphertext

Converting letters to numbers - as we learn techniques of cryptography, it is necessary to work in numerical form. Computers are used in cryptanalysis and computers work better with numbers than letters. The simplest method used in converting a letter to a number and vice versa is by using its position in the alphabet: a = 1, b = 2, ... z = 26. Here is a chart used for conversion. Save it. We will make extensive use of it.

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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

Note that both lower case and capital letters have the same numerical value. When we have the letter "m" in plaintext, it will be converted to the number 13. When we have the number letter "U", it will be converted to the number 21.

2. Monoalphabetic Substitution Ciphers

Don't let this difficult word upset you. In a monoalphabetic substitution cipher, every character in the plaintext message is replaced with a unique alternative character in the ciphertext message.

A type of monoalphabetic substitution cipher is a cryptogram, usually found on the newspaper puzzle page. You are given a message such as

NBNQQ RJJYDT ZFYKN AJURN SYMJR FQQ

and try to reconstruct the plaintext message. Cryptograms are created using a key (a = G, b = X, c = K, ...) People attempt to solve cryptograms by knowing which letters are more likely to occur in English phrases and letters which are likely to occur next to each other. We will look at these facts later. But, we will not examine cryptograms because there is no rule that can be followed that goes from plaintext to ciphertext and vice versa. It is like the code book described above. If someone gets the code book, he has the key.

A. The Additive (or shift) Cipher System

The first type of monoalphabetic substitution cipher we wish to examine is called the additive cipher. In this cipher method, each plaintext letter is replaced by another character whose position in the alphabet is a certain number of units away. We actually shift each letter a certain number of places over.

One of the first additive ciphers was used by Julius Caesar around 50 B.C. Each letter of the alphabet was replaced by the third letter following it. So, a is replaced by D, b is replaced by E, c is replaced by F, and so on.

The problem comes when we get to x. x is the 24th letter of the alphabet. If we add 3 to 24, we get 27. So we go back to the beginning of the alphabet and replace x with A, y with B, and z with c.

So once we add, if the number is greater than 26, we subtract 26 from it. The chart shows each letter in plaintext and its corresponding letter in cipher text.

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
position	1	2	3	4	5	6	7	8	9	10	11	12	13
add 3	4	5	6	7	8	9	10	11	12	13	14	15	16
position of cipher-text	4	5	6	7	8	9	10	11	12	13	14	15	16
Cipher text	D	E	F	G	H	I	J	K	L	M	N	O	P

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
position	14	15	16	17	18	19	20	21	22	23	24	25	26
add 3	17	18	19	20	21	22	23	24	25	26	27	28	29
position of cipher-text	17	18	19	20	21	22	23	24	25	26	1	2	3
Cipher text	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

So under an additive cipher with key equal to 3, the message “I would like a pizza” would become:

LZRXOGOLNHDSLCCD

To make reading of the ciphertext easier, we will use the convention of putting the letters in blocks of five. There is nothing sacrosanct about the number five. During World War II, the Germans used different numbers of letters in their blocks. The Luftwaffe used four and the German Army used three in their blocks, for example. So the ciphertext above will be written as:

LZRXO GOLNH DSLCC D

It is not necessary to use the number 3 as your additive key. You may choose any number from 1 to 26 as your additive key. If, for instance, you choose 22 as your additive key, your chart above would change to the following.

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
position	1	2	3	4	5	6	7	8	9	10	11	12	13
add 22	23	24	25	26	27	28	29	30	31	32	33	34	35
position of cipher-text	23	24	25	26	1	2	3	4	5	6	7	8	9
Cipher text	W	X	Y	Z	A	B	C	D	E	F	G	H	I

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
position	14	15	16	17	18	19	20	21	22	23	24	25	26
add 3	36	37	38	39	40	41	42	43	44	45	46	47	48
position of cipher-text	10	11	12	13	14	15	16	17	18	19	20	21	22
Cipher text	J	K	L	M	N	O	P	Q	R	S	T	U	V

So under an additive cipher with key equal to 22, the same message “I would like a pizza” would become **`ESKQH ZHEGA WJJLE VVW`** (when the spaces are added for reading ease)

Try your own. Encipher the message “The Eagles will win the Super Bowl“ using the additive key of 16. Complete the chart first.

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
position	1	2	3	4	5	6	7	8	9	10	11	12	13
add 16													
position of cipher-text													
Cipher text													

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
position	14	15	16	17	18	19	20	21	22	23	24	25	26
add 16													
position of cipher-text													
Cipher text													

The message is: ____

Although this is a very easy ciphering routine, it still takes time to encipher a message. That is where technology comes in. Open up the Excel spreadsheet called Cipher System. At the bottom, go to the first sheet named “additive.”

In this and all the ciphering systems on this spreadsheet, you can input a plaintext message and have it enciphered using the corresponding method and key. Since this is an additive cipher routine, you will input a plaintext message and additive key. Here are the particulars:

- Input the plaintext message in cell F2. The message must be in lower case letters and have no spaces. You may have a message of up to 120 characters. More than 120 characters will cause the extra characters to be deleted.

- Input the additive key in cell C9 (in the box). The number you input should be a number from 1 to 26, but in fact may be any whole number at all. If for instance, you use an additive key of 30, you are moving the letters 30 positions ahead which is like pushing them only 4 ahead.

Try some messages in cell F2 and try changing your additive key. You will see the enciphered message in red in the middle of the screen.

What would happen if your additive key was 26? _______________________________________

What other additive keys would give you the same result as adding 26? _______________________

So enciphering is fairly easy using this spreadsheet. Now. how about deciphering?

The easy way of thinking about deciphering a message is simply reversing the process. If we added 3 to encipher, we could simply subtract 3 to decipher. However, you will find that it is much easier to restrict ourselves to addition rather than talk about subtraction. Since adding 26 to the letter positions is the same as doing nothing, what number could we add to counterbalance the 3 we already added to encipher? __________

So with 3 in your enciphering key cell C9, type 23 in the deciphering key C29. You should go back to your original message.

Suppose you enciphered with 22, what would you decipher with? _________

In general, if *a* is your enciphering key, your deciphering key is the formula __________

Try some examples to prove to yourself that this works.

Now suppose you were told that the message **QUPCV OZGTM BAOMB IXQHH I** was enciphered using an additive cipher system. Could you decipher it?

Here's how: Go to cell O19 and type the cipher message above into that cell. You should be in all caps and have no spaces.

Now type different numbers into C29. One of them must work. There are only 26 you have to try. Try all 26 and prove to yourself that only one gives a message. Your deciphering additive key was _____.

If you wish to now send the message "I'm broke. Can you pay?" to the person who sent it to you, *using his same encrypting key*, what would be the encrypting additive key and what would the message be?

______ ____

Exercises: Assuming these were created with additive ciphers, find the key and encipher them. You can find these in the "data" worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell Itself, and then paste in the decoding section of the additive worksheet to save yourself a lot of typing.

1.ZNKIG XOCUA RJSUY ZROQK ZUNGB KOYGV UXYIN K

2.KVSBM CIUSH HVSOB GKSFH CDFCP ZSABW BSDZS OGSQO ZZAS

3.VGFLX GJYWL LGTMQ LZWLA UCWLK LGLZW UGFUW JL

4.UFCLR FCBCD CLQCZ JGRXC QUCUG JJRFP MUYQA PCCLN YQQ

5.JRCYN AGBIN PNGVB AVAOR EZHQN VAFGR NQBSS YBEVQ NGUVF
LRNE

B. Modular Arithmetic

In order to communicate in a better fashion, we now have to learn some math terminology. Back in grade school you learned to use a clock. You were taught that if it is currently 9 A.M. and you want the time 12 hours from now, you would know that the clock would read the same time. Now these times *are* different, but the clock wouldn't know that. So the clock would read the same 12 hours, 24 hours and any multiple of 12 hours in the future or the past, no matter what time it currently is.

You were taught this as "clock arithmetic." If it is 9 o'clock (doesn't matter whether A.M. or P.M.) and you want the time 5 hours from now, you would realize that 9 plus 5 = 14. Since there is no 14 o'clock, you could subtract 12 and get 2 o'clock.

If it is 9 o'clock and you are interested in the time 35 hours from now, you could find 9 + 35 = 44. Now continually subtract 12 until you get a number between 1 and 12. 44 - 12 = 32. 32 - 12 = 20. 20 - 12 = 8. So it will be 8 o'clock.

But suppose it is 9 o'clock and you are interested in the time 1,000 hours from now. Add 9 + 1,000 and you get 1,009. You could continually subtract 12, but that would become quite boring and tedious. There is an easier way.

Simply divide 12 into 1,009. We are not interested in the quotient. We are interested in the remainder.

$$\begin{array}{r} 84 \\ 12\overline{)1009} \\ \underline{1008} \\ 1 \end{array}$$

Since the remainder is 1, we can say that it will be 1 o'clock 1,000 hours after 9 o'clock.

To make this easier, we invent a terminology for this process. We called it a modular system.

So, when using the clock, we can add 12 or subtract 12 from any number and not change it, we can make statements like the following:

$13 \equiv 1 \bmod 12$, $25 \equiv 1 \bmod 12$, $37 \equiv 1 \bmod 12$, $-11 \equiv 1 \bmod 12$, $-23 \equiv 1 \bmod 12$ ...

We read the first statement as 13 is congruent (or equal) to 1 in modular system 12. What it also says is that 12 divides evenly (no remainder) 13 - 1.

The second statement $25 \equiv 1 \bmod 12$ says that 12 divides evenly into 25 - 1. The statement $-11 \equiv 1 \bmod 12$ says that 12 divides evenly into -11 - 1. (mod is read as "modulo")

When we use a modular system base 12, we wish to express our numbers using the smallest nonnegative numbers. So we wish to use the numbers 0 to 11 (unlike a clock, 1 to 12).

So we say that $12 \equiv 0 \bmod 12$ or 12 divides evenly into 12 - 0.

If you wish to change a number mod 12, you divide the number by 12 and look at the remainder. Some calculators (TI-89) actually have a mod key (located in the 2nd MATH 1: Number 9: mod menu). To find 77 mod 12, you would type in mod(77, 12). This can be a pain without a calculator that can take mods, but you can usually make things easier.

If you want to find 1234 mod 12, instead of dividing, you can think this way: 12 goes evenly into 1,200 so you can say $1234 \equiv 34 \bmod 12$. Now since $24 = 2 \times 12$, you can subtract 24 from 34. You get 10. So we conclude that $1234 \equiv 10 \bmod 12$.

If you want to find 185 mod 12, you may recall that $12^2 = 144$. So subtract 144 from 185 and you get 41. Since 41 is 5 more than 36 (3 • 12), you can conclude that $185 \equiv 5 \bmod 12$.

You can work in other modulo systems. If I want to find 79 mod 5, you can realize that 75 = 15 • 5. Subtract 75 from 79 and you realize that $79 \equiv 4 \bmod 5$.

If you wish to find 8024 mod 8, you realize that 8 goes evenly into 8,024. So $8024 \equiv 0 \bmod 8$.

Find the following:

129 mod 12 __________________ 444 mod 12 __________________

403 mod 3 __________________ 219 mod 7 __________________

5,245 mod 4 __________________ 719 mod 15 __________________

999 mod 9 __________________ 2,475 mod 6 __________________

In the ciphering systems we will use, it is natural to use a mod 26 system. 1 will correspond to A, 2 to B, 3 to C, ... Since in a mod 26 system, we use the numbers 0 to 25, there will be no number 26. $26 \equiv 0 \bmod 26$. So the number 0 will correspond to the letter Z.

Since we do a lot of calculations mod 26, here is a little routine that can make your work simpler if you have a TI-83 which, unfortunately, does not have a mod key. (the TI-89 does have one)

If you wish to find 75 mod 26, use these statements:

75 $\boxed{\text{STO}}$ X: X - 26 $\boxed{\text{MATH}}$ $\boxed{\text{NUM}}$ 5:int(X/26) $\boxed{\text{ENTER}}$

By continuing to press $\boxed{\text{2nd}}$ $\boxed{\text{ENTER}}$, you can back up to this statement and simply replace the 75 with whatever you wish to find mod 26. You can also change to a different mod by changing the two occurrences of the number 26 to whatever you want.

So, the additive system adds its key to every letter's number mod 26. If a plaintext letter is "f" and the key is 18. We take the position of "f" as 6 and add it to 18. We get 24 which corresponds to the letter "X."

If the plaintext letter is "r" and the key is 19, we add r's position as 18 and add 19 and get 37. We find 37 mod 26 which is 11 which corresponds to "K."

If the plaintext letter is "n" and the key is 12, we add n's position as 14 and add 12 and get 26. We find 26 mod 26 which is 0 which corresponds to "Z."

To reverse the process (decipher), we have to do the opposite process. If the key was 4, we added 4 to every plaintext position. To decipher, we need to subtract 4. But in modulo systems, we prefer not to use negatives. So realizing that $-4 \equiv 22 \bmod 26$, we add 22 to every letter position mod 26 in the ciphertext.

We will call the deciphering key the "additive inverse." The additive inverse of 4 is 22 mod 26.

If the key was 19, the decipher key is -19. But $-19 \equiv 7 \bmod 26$. So we add 7 to every letter position mod 26 in the ciphertext. So the additive inverse of 19 is 7 mod 26.

Find the following additive inverses of the following mod 26:

15: _________ 1: _________ 30: __________ 100: __________ 296: ___________

Note: it may seem that we are going to a lot of trouble to create a language for a process which seems fairly easy. Rest assured that there is a good reason to do so and we will spend a great deal of time working in mod 26. (Still, don't try to tell a policeman that if you are caught speeding at 93 mph, you were really going 15 mph because $93 \equiv 15 \bmod 26$!)

C. The Multiplicative Cipher

Now that we have tackled modulo systems, the multiplicative system should be easy. Instead of adding the key to the plaintext letter position, we simply multiply it. So our formula for our ciphertext *C* is based on the key *k* and the plaintext letter P:

$$C = k\text{P} \bmod 26$$

So, if our key is 3, the following table will show how to find the ciphertext:

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
position	1	2	3	4	5	6	7	8	9	10	11	12	13
multiply by 3	3	6	9	12	15	18	21	24	27	30	33	36	39
mod 26	3	6	9	12	15	18	21	24	1	4	7	10	13
Cipher text	C	F	I	L	O	R	U	X	A	D	G	J	M

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
position	14	15	16	17	18	19	20	21	22	23	24	25	26
multiply by 3	42	45	48	51	54	57	60	63	66	69	72	75	78
mod 26	16	19	22	25	2	5	8	11	14	17	20	23	0
Cipher text	P	S	V	Y	B	E	H	K	M	Q	T	W	Z

So, using the multiplicative key of 3, how would you encode, “The answer is seventeen.”?

____

Suppose our key was 11. Fill in the chart and encode the very same message. You may find that it is easier to find your answer mod 26 rather than actually multiply out. I would suggest having a calculator handy.

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
position	1	2	3	4	5	6	7	8	9	10	11	12	13
multiply by 11													
mod 26													
Cipher text													

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
position	14	15	16	17	18	19	20	21	22	23	24	25	26
multiply by 11													
mod 26													
Cipher text													

____

Go to your spreadsheet, change to the multiplicative sheet, and type in the plaintext in cell F2. Type the key in cell B10. Check to see if you are correct.

So far, there is no problem. But suppose our multiplicative key was 2? Here is the chart again.

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
position	1	2	3	4	5	6	7	8	9	10	11	12	13
multiply by 2	2	4	6	8	10	12	14	16	18	20	22	24	26
mod 26	2	4	6	8	10	12	14	16	18	20	22	24	26
Cipher text	B	D	F	H	J	L	N	P	R	T	V	X	Z

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
position	14	15	16	17	18	19	20	21	22	23	24	25	26
multiply by 2	28	30	32	34	36	38	40	42	44	44	48	50	52
mod 26	2	4	6	8	10	12	14	16	18	20	22	24	26
Cipher text	B	D	F	H	J	L	N	P	R	T	V	X	Z

Describe the problem created. ____

The message “hi” would be enciphered as “PR.” How would you end up deciphering it?

We say that the key 2 is unusable because 2 is not “invertible mod 26.” It turns out that all even numbers are also unusable because they contain no inverse. What is an inverse anyway?

We will define the inverse of a key *k*, a number k^{-1} such that $k \cdot k^{-1} = 1$ mod 26.

Think about it: Suppose our key *k* is 3. We start with the letter “a“ with has a position of 1. Multiply it by 3 and you get 3. Now, to decipher, you want to multiply it by something mod 26 which will get you back to 1. What is that number? ___________________.

It should be clear now why even numbers have no inverses. We start with the letter a with has a position of 1. Multiply it by 4 and you get 4. Now, to decipher, you want to multiply it by something mod 26 which will get you back to 1. Multiply 4 which is even by any number and you get an even number. Mod 26 it and you still get an even number. So you can never get back to 1.

Complete the chart. I give you the key *k*, and you find the inverse k^{-1}. It may take you some time.

key *k*	1	3	5	7	9	11	13	15	17	19	21	23	25
inverse k^{-1}													

You should have found that one number in the chart also does not have an inverse.

No matter how large the multiplicative key is, its inverse, if it has one, will be between 1 and 25.

As you use the multiplicative method sheet on the spreadsheet, notice that when you put your key in cell B10, the multiplicative inverse key appears automatically in cell B31. Also note that, if you attempt to put a key in of a number which has no inverse (even numbers or numbers divisible by 13, i.e., $\equiv 13 \bmod 26$) you will be so informed.

So if you put in a message in cell F2, it will be enciphered in red and then deciphered back in green below.

Try some examples on your own. Your message must be 120 or fewer characters, typed in lower case with no spaces. Your multiplicative key must be valid to be able to decipher it.

Suppose you were given this message and were told that it was created by a multiplicative cipher:

```
YQDIU   SOWJG   MGQQQ   TWPGF   UMGQX   BGTKY   FUUV
```

You wish to respond but how will you decipher it? Well, knowing that it was created by a multiplicative cipher is quite helpful. In additive ciphers, there were 25 numbers which could have been your additive key mod 26 (pretty senseless for your key to be zero). With multiplicative keys, there are only 11 possibilities (again, senseless for your key to be one). So type this message in cell Q20 and try your different keys in cell B10.

You wish to answer him with "No problem," using his inverse key as your key. What would your response be?

____

Exercises: The following ciphertexts were created with either additive or multiplicative ciphers methods. Decipher them and write the method and key. You can find these in the "data" worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell itself, and then paste in the decoding section of the appropriate worksheet to save yourself a lot of typing.

```
1.CIMOG FSXTS SIKDS OYCDD YCVRQ MEFSX TIVOC HNECV XO

2.KYVZE KVIEV KJZKV ZJNNN UFKDZ CBJYR BVUFK TFD

3.DLANA GIUQN AUDIL COCHD TDCHG QLDKL UHHAR IGJUD DAH

4.HESGD ONVDQ FNDRN TSADR TQDSN STQMN EEZKK ZOOKH ZMBDR

5.WQHWE QFWQF AQGRY DQLSY XQSGY NUKLV DVGFK VYARY NTKTT
```

D. The Affine Cipher

If you were given something written in ciphertext and asked to decipher it, it would be a daunting task. However, if you were told that it was created by an additive cipher, you would know that there are really only 25 possible shifts. If you were told that it was a multiplicative cipher, there are fewer possibilities, only 11. So if you were told that the cipher was created by either an additive or multiplicative cipher, there are only 36 possibilities. With the spreadsheet you have, that is child's play. 36, the worst case scenario, can be accomplished in minutes.

The question is: who would be crazy enough to tell you the actual type of cipher technique used? It defeats the problem of deciphering, doesn't it? This answer question is not as easy as it appears however. Later on, I will give good justification for actually telling you the method used to encipher.

However, it is clear that the additive and multiplicative methods are to easy to decipher. We will now examine the **affine cipher** method. Affine is a word that means "linear transformation." The affine method is really nothing more than a combination of the multiplicative and additive.

In the affine cipher system, we choose a multiplicative number *a* and and additive number *b*. If p is a plaintext number, then we define the cipher text number C = (*a*p + *b*) mod 26.

For instance, suppose we want to translate the plaintext message "yes" with an affine cipher system with *a* = 5 and *b* = 20. Here are the steps:

plaintext	y	e	s
position p	25	5	19
5p + 20	145	45	115
(5p + 20) mod 26	15	19	11
ciphertext	O	S	K

If we wanted to translate the plaintext "drink water" with an affine cipher system with *a* = 239 and *b* = 152, here are the steps:

plaintext	d	r	i	n	k	w	a	t	e	r
position p	4	18	9	14	11	23	1	20	5	18
239p + 152	1108	4454	2303	3498	2781	5649	391	4932	1347	4454
(239p + 152) mod 26	16	8	15	14	25	7	1	18	21	8
ciphertext	P	H	O	N	Y	G	A	R	U	H

However, if we wanted to translate the plaintext "an" with an affine cipher system with *a* = 2 and *b* = 8, here are the steps:

plaintext	a	n
position p	1	14
2p + 8	10	36
(2p + 8) mod 26	10	10
ciphertext	J	J

Obviously, we have a problem. There is no problem encoding but the decoding process will be impossible as the two J's translate to separate letters (a, and n). Hence some of the *a*'s and *b*'s will not have an inverse. Which are they?

Since, the *a* was the multiplicative number, the rules are the same as they were with the multiplication cipher system. That is: allowable values of *a* may not be any even number or congruent to 13 mod 26. So *a* may be the numbers 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25. There is no restriction on *b*.

As you can see, the number of possibilities in the affine system jumps dramatically. Since there are 12 possibilities for *a*, and 26 possibilities for *b*, there are 12 • 26 = 392 possibilities to try if we wish to decode a message.

Go to the spreadsheet, click on the affine method sheet at the bottom, and try to encode some messages. Put a message in F2, *a* = cell B10, and *b* in cell C10. Note that if *a* is not a legal number, you will be told so in cell B13, although it will appear that a translation will be accomplished. But it is illegal.

So now we come to the decoding process. In order to do so, we need to generate the inverse numbers of *a* and *b* which we will call *c* and *d.* This is not so easy. Let's try an example:

Let us suppose that p is the letter we wish to encode. We will use an *a* of 15 and *b* of 8. So the ciphertext position C will be 15p + 8 mod 26. From now on, we will use an equal sign instead of ≡ .

• To reverse the process, we must solve the equation:	$C = 15p + 8 \bmod 26$ (the encoding equation)
• Bring the 8 to the other side:	$C - 8 = 15p \bmod 26$
• Eliminate the negative 8 (add 26)	$C + 18 = 15p \bmod 26$
• We need to get p by itself. So multiply both sides by the inverse from the table. (there is no division process). The inverse of 15 is 7	$7(C + 18) = 1p \bmod 26$
• Multiply out	$7C + 126 = p \bmod 26$
• Find 126 mod 26	$p = 7c + 22 \bmod 26$
• Break the equation into *c* and *d*	$c = 7$, $d = 22$

In this spreadsheet, *c* and *d* are calculated for you in cells B27 and C27.

Let's try another one. p is the letter we wish to encode. We will use an *a* of 5 and *b* of 24. So the ciphertext position C will be 5p + 24 mod 26.

• To reverse the process, we must solve the equation:	$C = 5p + 24 \bmod 26$ (the encoding equation)
• Bring the 24 to the other side:	$C - 24 = 5p \bmod 26$
• Eliminate the negative 24 (add 26)	$C + 2 = 5p \bmod 26$
• We need to get p by itself. So multiply both sides by the inverse from the table. (there is no division process). The inverse of 5 is 21	$21(C + 2) = p \bmod 26$
• Multiply out	$21C + 42 = p \bmod 26$
• Find 42 mod 26	$p = 21c + 16 \bmod 26$
• Break the equation into *c* and *d*	$c = 21$, $d = 16$

This is not easy work. The spreadsheet accomplishes the work easily.

Exercises: Try the following by hand. You can certainly use the spreadsheet, but learning how to decipher requires you to be able to solve these modulo equations. So use the spreadsheet to see if you are correct. It does not matter what the plaintext message is.

1. $a = 1$, $b = 20$

2. $a = 9$, $b = 4$

3. $a = 19$, $b = 2$

4. $a = 25$, $b = 25$

5. $a = 29, b = 1$

6. $a = 101, b = 115$

Now, let’s make things a little more difficult. Suppose you were given this message:

```
RPIID XHIGGG MPOOH UIQVA GONIV QDXYI PQNII AEPRY IIWGOT T
```

The only thing you know is that it is created by an affine cipher. Where do you begin? You can type it into cell O19 (making sure an equally long message is in cell F2). Now what?

We can start with the fact that there are 392 possibilities for *a* and *b*. We can try them all. On the average, we will get the solution about the halfway mark or approximately after 200 trials. Assuming it takes 5 seconds to type your *a* and *b* values in and check to see if it is a correct solution, that is 1,000 seconds. So we would expect to get our solution by trial and error on the average of about 17 minutes. It could be as little as 5 seconds or as high as about 34 minutes though.

Here is a way that you could proceed and *possibly* get your answer much quicker:

Normal use of English words show that certain letters are much more likely to appear than others. The following chart shows the relative frequency of the letters of the English language:

plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m
relative frequency (%)	8.2	1.5	2.8	4.3	12.7	2.2	2.0	6.1	7.0	0.2	0.8	4.1	2.4

plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z
relative frequency	6.7	7.5	2.0	1.0	6.0	6.3	9.1	2.8	1.0	2.4	0.2	2.0	0.8

It is apparent that the letter “e” and the letter “t” are the hands-down winner for the letters most likely appear in a normal message.

Now look at the message above. Which letters seem to appear more than others?

There are 10 “I’s” and 5 “G’s”. If this message is normal, we would expect one of them to represent the letter “e.” So let’s start with the assumption that the letter “e“ is enciphered to the letter “I”.

Remember, our formula for enciphering is $C = a\text{p} + b \bmod 26$. The plaintext letter “e” will be 5 and the ciphertext letter ”I” will be 8. So plug those values in to the equation:

$$C = a\text{p} + b \bmod 26 \quad \text{or} \quad 9 = 5a + b \bmod 26$$

We can’t solve that. But we know that *a* can only be 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25.

Let *a* = 1: You get: 9 = 5 + b mod 26. That gets you to *b* = 3. Try *a* =1, *b* = 3 in the spreadsheet.

Let *a* = 3: You get: 9 = 15 + b mod 26. That gets you to *b* = -6 mod 26 or 20. Try *a* =3, *b* = 20.

Let *a* = 5: You get: 9 = 25 + b mod 26. That gets you to *b* = -16 mod 26 or 10. Try *a* =5, *b* = 10.

Let *a* = 7: You get: 9 = 35 + b mod 26. That gets you to *b* = -26 mod 26 or 0 Try *a* =7, *b* = 0.

Let *a* = 9: You get: 9 = 45 + b mod 26. That gets you to *b* = -36 mod 26 or 16. Try *a* =9, *b* = 16.

Let *a* = 11: You get: 9 = 55 + b mod 26. That gets you to *b* = -46 mod 26 or 6. Try *a* =11, *b* = 6.

BINGO!

Was this luck? Sure! What would have happened if you went through all your possibilities and didn't get an answer which gave a good plaintext message? Well, you might have retried it assuming that the letter "I" might have been translated from the letter "t" or you could take a look at those 5 "G"'s and hypothesize that it came from the letter "e."

A lot of work? Sure. People go through the work of coding messages simply to make sure that they cannot easily be decoded. Cryptologists spend many man hours trying to decipher messages and often work in teams so that none of the work is duplicated and careless errors are found. (Think of how upset someone would be if they actually had a correct *a* and *b* and didn't realize it?)

Also, remember that this method is based on the premise that the letter "e" or "t" are the most common letters in the plaintext. If the message is long, this is probably a good assumption. But if it is a shorter message, you are probably not on safe ground to make that assumption. So, as hard as it is to believe, it is probably easier to decipher a long message than a short one.

Exercises: Try to decipher the following messages if they are known to be created by the affine method. You can find these in the "data" worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell itself, and then paste in the decoding section of the additive worksheet to save yourself a lot of typing.

```
1.QPIFY EPKLX YYPRX XYSXX UXWSV IYRTS XIHPF YVNXH PFKYK
  ZWYPY SXOPP
```

```
2.AEKHF FYOKK FJKHK EOFUX OEUXO QYNAK LWFAT ATHFK HRYMA
  FHKUX ZMUOQ WCJUO FJKKU XZAKX YHKO
```

```
3.FVMHA FMCFL MZCYQ NQPFV MCGVQ QHNMO CTATM ZGQNF AYNMJ
  AHAZS MMZZQ ZFVAF GAICM JYFFQ DMZMT ZYNFM JGQCF YNSFV
  MGHID AHQFQ PKQNM U
```

```
4.NTYNC NSOGN XGNGQ NSNSN UIGEX GFNXG NGSMX GTUQZ TGQGF
  NQCNX SNXGM SFNSO GWKGQ NUCFQ
```

3. Polyalphabetic Substitution Ciphers

So far, the affine method of encrypting is the hardest to decipher. However, as we saw, there are 392 possibilities for a solution. By hand, it would take a while to go through them all, but with the speed of computers today, it takes microseconds. We need a better way.

Of course, we can extend the affine method. For instance, we can choose three numbers, *a*, *b*, and *c*, and multiply our plaintext message p by $a\text{p}^2 + b\text{p} + c \bmod 26$. Since there are 26 choices each for *a*, *b*, and *c*, there are initially 26^3 = 17,576 possibilities for decoding the ciphertext. Trial and error now takes more time.

But these can still be solved by using frequency data (which letters appear the most), repetition patterns (there are certain letters which appear together like “tt” and others that never appear together like “jj”), and information about the ways that letters combine with each other (“th” regularly appears in text while “vb“ never does).

So the way for a cryptographer to prevent the cryptanalyst success with these messages is to make the unit of enciphering a *group* of letters instead of just one.

In the monoalphabetic system, one letter in the plaintext *always* is replaced by one letter in the ciphertext. So an “e” is replaced by a “K.” In this system, the “e” is *always* replaced by the “K” making it susceptible for decryption.

So we create a **polyalphabetic** system in which a group of *n* plaintext letters is replaced by a unit of *n* ciphertext letters. For instance, if *n* = 2, the letters “th” might be replaced by “rk” while “te” might be replaced by “wm.” Despite the fact that each plaintext has the letter “t”, the ciphertext has completely different letters in it. That makes it much harder to decipher.

But before we go into a simple polyalphabetic system, we need to take a side journey to make our life easier. We need to look at integer matrices:

A. Integer matrices

Matrices were invented of Sir Arthur Cayley who lived in the nineteenth century. The array of numbers

$$\begin{pmatrix} 4 & 9 \\ 2 & 3 \end{pmatrix}$$

is an example of a 2×2 (two by two) matrix. It has two rows and two columns. It has four entries, row one has a 4 and 9 and row two has a 2 and 3. Usually, we refer to matrices as capital letters. So let

$$\mathbf{A} = \begin{pmatrix} 4 & 9 \\ 2 & 3 \end{pmatrix} \text{ and } \mathbf{B} = \begin{pmatrix} 6 & 5 \\ 10 & 7 \end{pmatrix}$$

We can add matrices easily by just adding their corresponding entries.

$$\mathbf{A} + \mathbf{B} = \begin{pmatrix} 4 & 9 \\ 2 & 3 \end{pmatrix} + \begin{pmatrix} 6 & 5 \\ 10 & 7 \end{pmatrix} = \begin{pmatrix} 4+6 & 9+5 \\ 2+10 & 3+7 \end{pmatrix} = \begin{pmatrix} 10 & 14 \\ 12 & 10 \end{pmatrix}$$

It should be apparent that $\mathbf{A}+\mathbf{B}=\mathbf{B}+\mathbf{A}$ (the commutative property).

Multiplication takes two forms: If you want to multiply a number *k* times a matrix, simply multiply every number in the matrix by *k*. Hence:

$$4\times\begin{pmatrix}5 & 8\\ 3 & 0\end{pmatrix}=\begin{pmatrix}20 & 32\\ 12 & 0\end{pmatrix} \text{ and } 9\times\begin{pmatrix}6 & 3\\ 8 & 2\\ 10 & 11\end{pmatrix}=\begin{pmatrix}54 & 27\\ 72 & 18\\ 90 & 99\end{pmatrix} \text{ and}$$

$$8\times\begin{pmatrix}4 & 6\\ 3 & 13\end{pmatrix}\bmod 26=\begin{pmatrix}32 & 48\\ 24 & 104\end{pmatrix}\bmod 26=\begin{pmatrix}6 & 22\\ 24 & 0\end{pmatrix}$$

But the rule for multiplication of 2×2 matrices is much more complex. If we want to multiply these two matrices, these are the steps:

$$\mathbf{A}\times\mathbf{B}=\begin{pmatrix}4 & 9\\ 2 & 3\end{pmatrix}\times\begin{pmatrix}6 & 5\\ 10 & 7\end{pmatrix}=\begin{pmatrix}4\times 6+9\times 10 & 4\times 5+9\times 7\\ 2\times 6+3\times 10 & 2\times 5+3\times 7\end{pmatrix}=\begin{pmatrix}114 & 83\\ 42 & 31\end{pmatrix}$$

Show that $\mathbf{A}\times\mathbf{B}\neq\mathbf{B}\times\mathbf{A}$

What we are doing is: multiplying each number in row 1 with each member in column 1 and adding them.

multiplying each number in row 1 with each member in column 2 and adding them.

multiplying each number in row 2 with each member in column 1and adding them.

multiplying each number in row 2 with each member in column 2 and adding them.

To multiply matrices $\mathbf{A}\times\mathbf{B}$, the number of columns in matrix **A** *must* be the same as the number of rows in row **B.** If this is not true, you cannot multiply the matrices. Remember this: **CARB** (Column A = Row B)

So we *can* multiply $\mathbf{A}\times\mathbf{B}=\begin{pmatrix}4 & 9\\ 2 & 3\end{pmatrix}\times\begin{pmatrix}5\\ 8\end{pmatrix}$ as the number of columns of **A** (2) is equal to the number of rows of **B** (2).

$$\mathbf{A}\times\mathbf{B}=\begin{pmatrix}4 & 9\\ 2 & 3\end{pmatrix}\times\begin{pmatrix}5\\ 8\end{pmatrix}=\begin{pmatrix}4\times 5+9\times 8\\ 2\times 5+3\times 8\end{pmatrix}=\begin{pmatrix}92\\ 34\end{pmatrix}$$

And we *can* multiply $\mathbf{A}\times\mathbf{B}=\begin{pmatrix}4 & 9\\ 2 & 3\end{pmatrix}\times\begin{pmatrix}5 & 8 & 3\\ 6 & 1 & 10\end{pmatrix}$ as the number of columns of **A** (2) is equal to the number of rows of **B** (2).

$$\mathbf{A}\times\mathbf{B}=\begin{pmatrix}4&9\\2&3\end{pmatrix}\times\begin{pmatrix}5&8&3\\6&1&10\end{pmatrix}=\begin{pmatrix}4\times5+9\times6&4\times8+9\times1&4\times3+9\times10\\2\times5+3\times6&2\times8+3\times1&2\times3+3\times10\end{pmatrix}=\begin{pmatrix}74&41&102\\28&19&36\end{pmatrix}$$

Thankfully, we do not need this type of multiplication in the next system we will study.

But we *cannot* multiply $\mathbf{A}\times\mathbf{B}=\begin{pmatrix}4&9\\2&3\end{pmatrix}\times\begin{pmatrix}6&5\\5&7\\10&1\end{pmatrix}$ as the number of columns of $\mathbf{A}$ (2) is equal to the number of rows of **B** (3).

As a final step, we can multiply matrices mod 26. That is the same type of multiplication just shown but all numbers in the final matrix are mod 26.

$$\text{So: } \mathbf{A}\times\mathbf{B}\bmod 26=\begin{pmatrix}4&9\\2&3\end{pmatrix}\times\begin{pmatrix}5\\8\end{pmatrix}=\begin{pmatrix}4\times5+9\times8\\2\times5+3\times8\end{pmatrix}=\begin{pmatrix}92\\34\end{pmatrix}\bmod 26=\begin{pmatrix}14\\8\end{pmatrix}$$

$$\mathbf{A}\times\mathbf{B}=\begin{pmatrix}4&9\\2&3\end{pmatrix}\times\begin{pmatrix}6&5\\10&7\end{pmatrix}=\begin{pmatrix}4\times6+9\times10&4\times5+9\times7\\2\times6+3\times10&2\times5+3\times7\end{pmatrix}=\begin{pmatrix}114&83\\42&31\end{pmatrix}\bmod 26=\begin{pmatrix}10&5\\16&5\end{pmatrix}$$

If you were asked to find $\mathbf{A}\times\mathbf{B}\bmod 26=\begin{pmatrix}114&299\\48&5\end{pmatrix}\times\begin{pmatrix}62&104\\81&90\end{pmatrix}$, rather than multiplying and adding first, it is easier to change all numbers to mod 26 first.

$$\begin{pmatrix}114&299\\48&5\end{pmatrix}\times\begin{pmatrix}62&104\\81&90\end{pmatrix}\bmod 26=\begin{pmatrix}10&13\\22&5\end{pmatrix}\times\begin{pmatrix}10&0\\3&12\end{pmatrix}=$$

$$\begin{pmatrix}10\times10+13\times3&10\times0+13\times12\\22\times10+5\times3&22\times0+5\times12\end{pmatrix}\bmod 26=\begin{pmatrix}139&156\\235&60\end{pmatrix}\bmod 26=\begin{pmatrix}9&0\\1&8\end{pmatrix}$$

Exercises: Perform these matrix multiplications mod 26

1. $15\times\begin{pmatrix}3&10\\1&6\end{pmatrix}\bmod 26$

2. $\begin{pmatrix}5&11\\3&6\end{pmatrix}\times\begin{pmatrix}4&9\\1&7\end{pmatrix}\bmod 26$

3. $\begin{pmatrix}23&17\\21&14\end{pmatrix}\times\begin{pmatrix}16&10\\25&9\end{pmatrix}\bmod 26$

4. $\begin{pmatrix}6&7\\8&4\end{pmatrix}\times\begin{pmatrix}2\\3\end{pmatrix}\bmod 26$

5. $\begin{pmatrix} 20 & 19 \\ 15 & 11 \end{pmatrix} \times \begin{pmatrix} 24 \\ 9 \end{pmatrix} \bmod 26$

6. $\begin{pmatrix} 79 & 100 \\ 55 & 80 \end{pmatrix} \times \begin{pmatrix} 2 & 32 \\ 50 & 91 \end{pmatrix} \bmod 26$

7. $\begin{pmatrix} 46 & 125 \\ 220 & 75 \end{pmatrix} \times \begin{pmatrix} 262 \\ 130 \end{pmatrix} \bmod 26$

B. The Hill Digraph Cipher

Now that we have an elementary idea of how to work with matrices, we are now ready to tackle a more sophisticated cipher system called the Hill Cipher. This system was invented in 1929 by an American mathematician, Lester S. Hill.

Here are the steps:
1. Choose a 2 by 2 matrix of numbers mod 26 to act as the key.
2. Take consecutive pairs of letters in the plaintext and convert to numbers mod 26.
3. Write these numbers in a 2 by 1 (2 rows, 1 column) matrix.
4. Multiply these two matrices mod 26.
5. Convert these numbers to ciphertext.

There are some added considerations to these steps which we will talk about later.

Here is an example: Let us convert the word “book” to a Hill Cipher.

Step 1: key = $\begin{pmatrix} 5 & 3 \\ 11 & 8 \end{pmatrix}$	Step 1: Key stays the same
Step 2: ”b” = 2, “0”= 15	Step 2: “o” = 15, “k” = 11
Step 3: $\begin{pmatrix} 2 \\ 15 \end{pmatrix}$	Step 3: $\begin{pmatrix} 15 \\ 11 \end{pmatrix}$
Step 4: $\begin{pmatrix} 5 & 3 \\ 11 & 8 \end{pmatrix} \times \begin{pmatrix} 2 \\ 15 \end{pmatrix} \bmod 26 = \begin{pmatrix} 3 \\ 12 \end{pmatrix}$	Step 4: $\begin{pmatrix} 5 & 3 \\ 11 & 8 \end{pmatrix} \times \begin{pmatrix} 15 \\ 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 19 \end{pmatrix}$
Step 5: 3 = “C”, 4 = “L”	Step 5: 4 = “D”, 19 = “S”

So, the word “book” gets converted to “CLDS”

Note that the letter “o” appears consecutively in the plaintext, but not in the ciphertext.

Blocking each letter of plaintext into 2 consecutive letters is called a *digraph model*. If there is an odd number of letters in the plaintext, you have to add an extra letter, usually at the end, usually an “x.”

You can group them into blocks of 3 consecutive letters is called a *trigraph model*. The greater the number of letters in a block, the harder it is to decipher the message.

Encode the message “Hi Ron” with the key $\begin{pmatrix} 12 & 7 \\ 7 & 5 \end{pmatrix}$. There will be 6 letters in the ciphertext.

To convert a plaintext message into ciphertext using the digraph model of the Hill system involves a lot of work. The spreadsheet that goes along with this document can encode plaintext very quickly. Go to the Hill Digraph Method sheet and input your message into cell F2 (no spaces, all lower case, 120 characters maximum).

You now need to input your key matrix. We will call the key matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and you input them in the box in cells B10, C10, B11, and D11. Not every matrix can create a ciphertext as we will see later. Experiment with some of them.

So, of course, the question becomes: how do you decipher a message that was encrypted by the digraph Hill method? It isn’t easy, nor should it be. But it can be done if you have the key.

First, realize that there are 26 numbers that could be *a*, *b*, *c*, and *d* (mod 26). So there are 26 permutations of 26^4 or 456,976 possible encryptions of a plaintext message.

To reverse the procedure, we need to find another matrix to multiply the ciphertext so that we get back to the original plaintext. We will call this new matrix *c*, *d*, *e*, and *f*. So by the same argument, there are 456,976 possible decryptions of a ciphertext message. We will reduce this number somewhat later. But if it took 5 seconds to check out each one (a gross underestimation), it would take 1.75 years to go through all of them.

Obviously we need to find this “inverse” key, the matrix *c*, *d*, *e*, and *f*, that will “undo” the original key *a*, *b*, *c*, and *d*. To accomplish this, we need to go back into matrix theory.

First, we define the *determinant* of a 2 by 2 matrix *a*, *b*, *c*, and *d* *ad* - *bc*. So the determinant of $\begin{pmatrix} 5 & 3 \\ 11 & 8 \end{pmatrix}$ is 5(8) - 3(11) = 7. The determinant of $\begin{pmatrix} 10 & 2 \\ 30 & 6 \end{pmatrix}$ is 10(6) - 2(30) = 0.

We will define the inverse of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ as another matrix $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is called the identity matrix. Without proving it, we will say that if matrix $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the inverse of **A** is $\mathbf{A}^{-1} = \dfrac{1}{ad - bc} \times \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Example: Suppose $\mathbf{A} = \begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix}$. So our inverse $\mathbf{A}^{-1} = \dfrac{1}{4(6) - 5(3)} \times \begin{pmatrix} 6 & -5 \\ -3 & 4 \end{pmatrix} = \begin{pmatrix} \dfrac{6}{9} & \dfrac{-5}{9} \\ \dfrac{-3}{9} & \dfrac{4}{9} \end{pmatrix}$

$$\text{So: } \begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix} \times \begin{pmatrix} \dfrac{6}{9} & \dfrac{-5}{9} \\ \dfrac{-3}{9} & \dfrac{4}{9} \end{pmatrix} = \begin{pmatrix} 4\left(\dfrac{6}{9}\right) + 5\left(\dfrac{-3}{9}\right) & 4\left(\dfrac{-5}{9}\right) + 5\left(\dfrac{4}{9}\right) \\ 3\left(\dfrac{6}{9}\right) + 6\left(\dfrac{-3}{9}\right) & 3\left(\dfrac{-5}{9}\right) + 6\left(\dfrac{4}{9}\right) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

But, unfortunately this will not work in mod 26. There are no fractions. We can make the process easier somewhat by this procedure:

1. Start with the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Mod 26 all numbers.
2. Find the determinant *ad* - *bc*. Mod 26 it. Since we want to divide by this number, we will find the inverse of this number mod 26. We did this earlier.

determinant *ad-bc*	1	3	5	7	9	11	15	17	19	21	23	25
inverse determinant	1	9	21	15	3	19	7	23	11	5	17	25

3. Change $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Mod 26 all numbers.
4. Multiply your inverse determinant by $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ mod 26 in step 3,
5. Mod 26 all numbers.

Example 1: find the inverse of $\begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix}$.

1. $\begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix}$ is already mod 26
2. *ad* - *bc* = 9. The inverse of 9 mod 26 is 3 (by the chart above)
3. $\begin{pmatrix} 6 & -5 \\ -3 & 4 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 6 & 21 \\ 23 & 4 \end{pmatrix}$
4. $3\begin{pmatrix} 6 & 21 \\ 23 & 4 \end{pmatrix} = \begin{pmatrix} 18 & 63 \\ 69 & 12 \end{pmatrix}$
5. $\begin{pmatrix} 18 & 63 \\ 69 & 12 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 18 & 11 \\ 17 & 12 \end{pmatrix}$

Note that $\begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix} \times \begin{pmatrix} 18 & 11 \\ 17 & 12 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 157 & 104 \\ 156 & 105 \end{pmatrix} \text{mod } 26 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Example 2: find the inverse of $\begin{pmatrix} 40 & 61 \\ 27 & 21 \end{pmatrix}$

1. $\begin{pmatrix} 40 & 61 \\ 27 & 21 \end{pmatrix} \bmod 26 = \begin{pmatrix} 14 & 9 \\ 1 & 21 \end{pmatrix}$
2. *ad* - *bc* = 285. 243 mod 26 = 25. The inverse of 25 mod 26 is 25 (by the chart above)
3. $\begin{pmatrix} 21 & -9 \\ -1 & 14 \end{pmatrix} \bmod 26 = \begin{pmatrix} 21 & 17 \\ 25 & 14 \end{pmatrix}$
4. $25\begin{pmatrix} 21 & 17 \\ 25 & 14 \end{pmatrix} = \begin{pmatrix} 525 & 425 \\ 625 & 350 \end{pmatrix}$
5. $\begin{pmatrix} 525 & 425 \\ 625 & 350 \end{pmatrix} \bmod 26 = \begin{pmatrix} 5 & 9 \\ 1 & 12 \end{pmatrix}$

This is a lot of work. Fortunately, the spreadsheet program will calculate the inverse automatically for you in cells B39, C39, B40 and C40. Also, remember that only odd numbers not equal to 13 mod 26 have inverses. So when you choose your matrix key, you must be sure that the determinant *ad* - *bc* is not an even number or divisible by 13. Of the 26^4 = 456,976 possible permutations of *ad* - *bc* mod 26, 299,728 of them are either even or divisible by 13. So there are total of 157,248 possible keys in the digraph Hill system. By trial and error, that is a lot of work. We will eventually make it easier.

Now you have a way to decipher. Using example 1 above, suppose the word you want to encipher is "go" using the key matrix $\begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix}$.

<u>To encipher:</u>

1. "g" = 7, "o" = 15
2. $\begin{pmatrix} 4 & 5 \\ 3 & 6 \end{pmatrix} \times \begin{pmatrix} 7 \\ 15 \end{pmatrix} \bmod 26 = \begin{pmatrix} 103 \\ 11 \end{pmatrix} \bmod 26 = \begin{pmatrix} 25 \\ 7 \end{pmatrix}$
3. 25 = "Y", 7 = "G"

<u>To decipher:</u>

1. "Y" = 25, "G" = 7
2. Inverse matrix is $\begin{pmatrix} 18 & 11 \\ 17 & 12 \end{pmatrix}$ (from above)
3. $\begin{pmatrix} 18 & 11 \\ 17 & 12 \end{pmatrix} \times \begin{pmatrix} 25 \\ 7 \end{pmatrix} \bmod 26 = \begin{pmatrix} 527 \\ 509 \end{pmatrix} = \begin{pmatrix} 7 \\ 15 \end{pmatrix}$
4. 7 = "g", 15 = "o"

Exercises: Find the inverses of the following matrix keys. You can check your answers using the spreadsheet Hill Digraph Method sheet.

1. $\begin{pmatrix} 5 & 7 \\ 7 & 10 \end{pmatrix}$

2. $\begin{pmatrix} 15 & 17 \\ 3 & 8 \end{pmatrix}$

3. $\begin{pmatrix} 7 & 15 \\ 5 & 4 \end{pmatrix}$

4. $\begin{pmatrix} 200 & 151 \\ 75 & 80 \end{pmatrix}$

Now comes the interesting (and hard) part. Let's suppose you received this message:

KMYEM UPAUO AHOJR YUKTT CACQC XXIYE DKSTQ ZXDAW

Let's also assume that you know it was created by a Hill digraph cipher system. (again, it may seem unlikely that you would know this, but we will see later that there is a reason that this information might be public knowledge). Still, where do you begin?

We know that there 157,248 possible combinations of *a*, *b*, *c*, and *d* mod 26. We can simply try them with the spreadsheet. Type **KMYEMUPAUOAHOJRYUKTTCACQCXXIYEDKSTQZXDAW** in cell N27 (make sure that there is a message at least that long in F2 - doesn't matter what). Now try some combinations of *a*, *b*, *c*, and *d* mod 26.

After a few trials (unless you were unbelievably lucky) you should be convinced that this is not the way to proceed. If you could get some help, it may make the process easier. 100 people working on this would give each person approximately 1,572 of them to try. Still, that would be expensive.

Of course, you could program the computer to run through them all. Still, you would have to examine each by sight to see the right answer which, hopefully, will pop out at you. That, still, is a good option. But we would like to solve it without use of a computer, except for checking the final answer.

But, again, where do you begin? So I will give you a clue. Suppose you know that the message is about Bob. This is not as farfetched as it sounds. Many times, a message is sent and the person receiving it has some idea what it is about. That knowledge is called a "*crib*." For us, it is a foothold into the key.

When the allies deciphered German messages during World War II, frequently they discovered cribs to help them. If a message came from a certain sector where Colonel Klink was commanding, it was normal that the message would mention who was sending it and hopefully, the word "Klink" might appear in the ciphertext.

So it might make sense that the word "Steve" might appear in the message above. We will start with that premise.

Let's assume that "Steve" appears at the beginning of the message, that is the first letter in the plaintext is "s" and the second is "t."

Then we are saying that via the enciphering process that the letters on top converted to the letters on the bottom: $\begin{matrix} \text{s} & \text{t} & \text{e} & \text{v} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \text{K} & \text{M} & \text{Y} & \text{E} \end{matrix}$. We are searching for variables *a*, *b*, *c*, and *d* mod 26 that could make this happen. The positions for "stev" are 19, 20, 5, and 22. The position for "KYME" are 11, 13, 25, and 5.

So these two equations must be true:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 19 \\ 20 \end{pmatrix} = \begin{pmatrix} 11 \\ 13 \end{pmatrix} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 5 \\ 22 \end{pmatrix} = \begin{pmatrix} 25 \\ 5 \end{pmatrix}$$

So let's write two equations from each:

$$\begin{array}{lcl}
19a+20b=11 \bmod 26 & \qquad & 5a+22b=25 \bmod 26 \\
19c+20d=13 \bmod 26 & \qquad & 5c+22d=5 \bmod 26
\end{array}$$

Now let's rearrange them.

$$\begin{array}{lcl}
19a+20b=11 \bmod 26 & \qquad & 19c+20d=13 \bmod 26 \\
5a+22b=25 \bmod 26 & \qquad & 5c+22d=5 \bmod 26
\end{array}$$

Let's solve each side independently. The rule are similar to simultaneous equations of normal algebra but, remember, there is no division. Whenever possible, mod 26 all numbers to make them small.

First, let's multiply the top equations by 5 and the bottom equations by 19.

$$\begin{array}{lcl}
5\left(19a+20b=11\right) \bmod 26 & \qquad & 5\left(19c+20d=13\right) \bmod 26 \\
19\left(5a+22b=25\right) \bmod 26 & \qquad & 19\left(5c+22d=5\right) \bmod 26 \\
 & & \\
95a+100b=55 \bmod 26 & \qquad & 95c+100d=65 \bmod 26 \\
95a+418b=475 \bmod 26 & \qquad & 95c+110d=95 \bmod 26
\end{array}$$

Let's mod 26 everything.

$$\begin{array}{lcl}
17a+22b=3 \bmod 26 & \qquad & 17c+22d=13 \bmod 26 \\
17a+2b=7 \bmod 26 & \qquad & 17c+2d=17 \bmod 26
\end{array}$$

Now subtract the two equations and mod 26 them

$$\begin{array}{lcl}
20b=-4 \bmod 26 & \qquad & 20d=-4 \bmod 26 \\
20b=22 \bmod 26 & \qquad & 20d=22 \bmod 26
\end{array}$$

These are the same equations. We only need to solve one of them. However, this is where things become tricky. Since these numbers are even, we have to be very careful. You could do it by trial and error. You can also multiply each side of the equation by an odd number. This can help as you will see.

If I multiply $20b = 22 \bmod 26$ by 3, I get $60b = 66 \bmod 26$ or $8b = 14 \bmod 26$. By inspection, it should be clear that $b = 5$. So, $d = 5$ as well.

Solve for a in one of the equations above. Solve for c in one of the equations above

$$\begin{array}{lcl}
17a+2b=7 \bmod 26 & \qquad & 17c+2d=17 \bmod 26 \\
17a+10=7 \bmod 26 & \qquad & 17c+10=17 \bmod 26 \\
17a=-3 \bmod 26 & \qquad & 17c=7 \bmod 26 \\
17a=23 \bmod 26 & \qquad &
\end{array}$$

To solve these multiply by the inverse of 17 = 23

$$\begin{array}{ll} 23\left(17a = 23\right)\bmod 26 & 23\left(17c = 7\right)\bmod 26 \\ a = 529\bmod 26 & c = 161\bmod 26 \\ a = 9 & c = 5 \end{array}$$

So we believe the solution matrix is $\begin{pmatrix} 9 & 5 \\ 5 & 5 \end{pmatrix}$. But, to our horror, the determinant of this matrix is even and hence this solution is impossible. *All that work for nothing!*

Ready to give up? If you were working alone, you very well may. But cryptologists usually work together. Maybe "Steve" appears starting with the second letter. But that would mean that the first letter would have to be a word like "I" or "A". "I Steve" or "A Steve doesn't make much sense. So let's start with the premise that "Stev" is the in position 3, 4, 5, and 6 of the plaintext and "YEMU" are in the 3rd, 4th, 5th and 6th letter of the ciphertext.

Then we are saying that via the enciphering process that the letters on top converted to the letters on the bottom: $\begin{matrix} \text{s} & \text{t} & \text{e} & \text{v} \\ \downarrow & \downarrow & \downarrow & \downarrow \\ \text{Y} & \text{E} & \text{M} & \text{U} \end{matrix}$. We are searching for variables a, b, c, and d mod 26 that could make this happen. The positions for "stev" are 19, 20, 5, and 22. The position for "YEMU" are 25, 5, 13, and 21.

So these two equations must be true:

$$\begin{array}{lcl} \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 19 \\ 20 \end{pmatrix} = \begin{pmatrix} 25 \\ 5 \end{pmatrix} & & \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 5 \\ 22 \end{pmatrix} = \begin{pmatrix} 13 \\ 21 \end{pmatrix} \\ 19a + 20b = 25\bmod 26 & & 5a + 22b = 13\bmod 26 \\ 19c + 20d = 5\bmod 26 & & 5a + 22d = 21\bmod 26 \\ & \text{rearranging} & \\ 19a + 20b = 25\bmod 26 & & 19c + 20d = 5\bmod 26 \\ 5a + 22b = 13\bmod 26 & & 5a + 22d = 21\bmod 26 \end{array}$$

These are the same types of equations we had on the last unsuccessful try. I will skip some steps by multiplying the top equation by 5 and the bottom equation by 19 and mod 26 them at the same time.

$$\begin{array}{ll} 17a + 22b = 21\bmod 26 & 17c + 22d = 25\bmod 26 \\ 17a + 2b = 13\bmod 26 & 17a + 2d = 9\bmod 26 \end{array}$$

subtracting

$$\begin{array}{ll} 20b = 8\bmod 26 & 20d = 16\bmod 26 \\ \text{by inspection, } b = 3 & \text{by inspection } d = 6 \end{array}$$

now plug in

$$\begin{aligned} 17a + 2b &= 13 \bmod 26 \\ 17a + 6 &= 13 \bmod 26 \\ 17a &= 7 \bmod 26 \end{aligned}$$

$$\begin{aligned} 17c + 2d &= 9 \bmod 26 \\ 17c + 12 &= 9 \bmod 26 \\ 17c &= -3 \bmod 26 \\ 17c &= 23 \bmod 26 \end{aligned}$$

Multiply both sides by the multiplicative inverse of 17 which is 23.

$$\begin{aligned} &23(17a = 7) \bmod 26 \\ &a = 161 \bmod 26 \\ &a = 5 \end{aligned}$$

$$\begin{aligned} &23(17c = 23) \bmod 26 \\ &c = 529 \bmod 26 \\ &c = 9 \end{aligned}$$

So we believe the solution is $\begin{pmatrix} 5 & 3 \\ 9 & 6 \end{pmatrix}$. The determinant is odd so it *is* possible. So go to your spreadsheet, and type it in to the key in cells B10, B11, C10, C11 and look below.

BINGO!

Was it worth it? That's up to you. But remember, this *is* supposed to be hard! The whole idea is secrecy.

Exercises: These will take time. Work slowly, preferably with someone. Resist the temptation to look at the answers in the back. You can find these in the "data" worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell itself, and then paste in the decoding section of the additive worksheet to save yourself a lot of typing.

1. Your math teacher, Mr. Schwartz takes this message off of you. He knows it was created by a Hill digraph cipher system.

   CMOWL KURLO DPPMM GROBD UTOTF YSNIL HQ

   The only clue that Mr. Schwartz has is that he suspects the message is about him.

2. (Harder) You suspect your boyfriend is seeing someone else. While he is getting his lunch, you notice this message in his notebook and you jot it down. You know that it was created by a Hill digraph cipher system.

   BQGIN CDMDN CXPSR XMYSX GZ

   The only clue that you have is that you heard him talking about the mall.

Finally, what do you do if you know the message came from a Hill digraph cipher system but have no crib? Can it be deciphered? The answer is "maybe." But it takes a great deal of time and trial and error. What you can do (hopefully)) is to reduce the 157,248 possible combinations of *a*, *b*, *c*, and *d* mod 26 to a manageable number.

Here is an example: You receive this message and know it came from a Hill digraph cipher system.

```
LXNYQ DUYDQ LXENL XCFJK IGDQU WIMDC LXBIK UPTFQ QQWBT
SUWMK TYLXO VKUKT HGRNY JDFWF WQGBV YATZS SSSEN TSUPW
QMCXU PTLXE NDEWQ YEHGO TQTCY RN
```

Where to begin? The first plan of attack is your knowledge of the English language.

There are certain digraphs (two letter combinations) that occur more than others. Here they are:

Number of Digraphs Expected in 2,000 Letters of English Text

th - 50	at - 25	st - 20
er - 40	en - 25	io = 18
on - 39	es - 25	le - 18
an - 38	of - 25	is - 17
re - 36	or - 25	ou - 17
he - 33	nt - 24	ar - 16
in - 31	ea - 22	as - 16
ed - 30	ti - 22	de - 16
nd - 30	to - 22	rt - 16
ha - 26	it - 20	ve - 16

There are also certain trigraphs (three letter combinations) that occur more than others. Here they are.

The 15 Most Common Trigraphs in the English Language

1 - the	6 - tio	11 - edt
2 - and	7 - for	12 - tis
3 - tha	8 - nde	13 - oft
4 - ent	9 has	14 - sth
5 - ion	10 - nce	15 - men

Let's concentrate on digraphs. Examine the ciphertext. Is there any digraph that occurs several times?

```
LXNYQ DUYDQ LXENL XCFJK IGDQU WIMDC LXBIK UPTFQ QQWBT
SUWMK TYLXO VKUKT YHALP WLXEZ PELXF AYXQG DEEML XDCQD
VSAPA PSSUW CMAZQ GINYA XQQIE AVSAP APSSU WCMAZ QGINY
AXQQI EA
```

If your eyes are sharp, you would have seen that the letter combination **LX** occurs 6 times. That's a lot!

Since the most common digraph in the English language is "th" by far, let's operate on the assumption that "th" in plaintext translated to "LX" in ciphertext. We don't make this assumption lightly because there is a lot of work attached to this assumption as you will see.

So there must be some *a*, *b*, *c*, and *d* in the key matrix that creates this phenomenon. Since "th" is represented by 20 and 8, and "LX" is represented by 12 and 24, the following must be true:

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 12 \\ 24 \end{pmatrix}$ and thus $20a + 8b = 12 \bmod 26$ and $20c + 8d = 24 \bmod 26$.

Here are all combinations of *a* and *b* for the expression 20*a* + 8*b* mod 26.

													b	**or**	**d**												
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
	0	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
	1	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12
	2	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6
	3	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0
	4	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20
	5	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14
	6	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8
	7	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2
	8	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22
	9	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16
	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10
	11	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4
a	**12**	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24
or	**13**	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
c	**14**	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12
	15	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6
	16	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0
	17	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20
	18	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14
	19	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8
	20	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2
	21	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22
	22	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16
	23	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10
	24	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4
	25	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24

To make this easier to read, we will only print the combinations where $20a + 8b = 12 \bmod 26$ and $20c + 8d = 24 \bmod 26$.

													b	**or**	**d**												
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
	0				24					12								24					12				
	1								24					12								24					12
	2				12								24					12								24	
	3			24					12								24					12					
	4							24					12								24					12	
	5			12								24					12								24		
	6		24					12								24					12						
	7						24					12								24					12		
	8		12								24					12								24			
	9	24					12								24					12							
	10					24					12								24					12			
a	**11**	12								24					12								24				
or	**12**					12								24					12								24
c	**13**				24					12								24					12				
	14								24					12								24					12
	15				12								24					12								24	
	16			24					12								24					12					
	17							24					12								24					12	
	18			12								24					12								24		
	19		24					12								24					12						
	20						24					12								24					12		
	21		12								24					12								24			
	22	24					12								24					12							
	23					24					12								24					12			
	24	12								24					12								24				
	25					12								24					12								24

There are 50 combinations of *a* and *b* that give 12. There are 50 combinations of *c* and *d* that give 24. So in all there are (50)(50) = 2,500 possibilities of *a*, *b, c,* and *d.* Since there were originally $26^4 = 459,976$ possibilities of *a*, *b, c,* and *d,* that is a dramatic decrease.

We can even make it slightly easier. We know that *a* and *b* (or *c* and *d*) cannot both be even numbers because the determinant *ad* - *bc* would also be even and that cannot create a valid key. So here is the chart with those possibilities eliminated.

													b	or	d												
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	0				24																		12				
	1								24					12								24					12
	2				12								24														
	3			24					12								24					12					
	4												12								24						
	5			12								24					12								24		
	6		24																		12						
	7						24					12								24					12		
	8		12								24																
	9	24					12								24					12							
	10										12								24								
a	11	12								24					12								24				
or	12																		12								24
c	13				24					12								24					12				
	14								24																		12
	15				12								24					12								24	
	16								12								24										
	17							24					12								24					12	
	18																12								24		
	19		24					12								24					12						
	20						24																		12		
	21		12								24					12								24			
	22						12								24												
	23					24					12								24					12			
	24									24					12												
	25					12								24					12								24

There are now 39 combinations of *a* and *b* that give 12. There are 39 combinations of *c* and *d* that give 24. So all there are (39)(39) = 1,521 possibilities of *a, b, c,* and *d.* We have saved almost another 1,000 trials. One combination works. So which one is it? Try one - *a* = 12, *b* = 17, *c* = 19, and *d* = 1. That doesn't work. How about - *a* = 1, *b* = 25, *c* = 3, and *d* = 2. Still no good.

At this point, unless you have another pair of letters which appear a fair number of times, you are down to trial and error. Still, using the stipulation that *ad* – *bc* must be odd and not divisible by 13, you can bring your trial choices down to roughly (19)(19) = 361 choices. Not bad considering that we started from almost half a million possibilities.

By the way, the answer is *a* = 9, *b* = 5, *c* = 2, and *d* = 11. Plug them into the Hill digraph spreadsheet – cells B10, C10, B11, C11 with the ciphertext in cell N27.

Our previous statement that there were 26^4 possibilities for *a*, *b, c,* and *d* is in error. Many of these create duplicate enciphering. The reason is that any permutation of two letters has only 26^2 = 676 different digraphs beginning with AA, AB, AC , …, BA, BB, …, YA, YB, …, ZX, ZY, and ZZ. So this message, which was seemingly impossible to decipher, can be done so rather easily by computer, even if there is no clue. The clue simply helps nail it in an easier fashion.

Remember though that all of this work was based on the assumption that the two letter combination "LX" represents "th." That is a big assumption. If the message is a long one, that assumption is certainly a good place to begin. It should be apparent that the longer the ciphertext , the greater change that you can get a clue from it. So don't get intimidated by the length of the message. Longer messages are better!

Exercises: Both of the following were created by the Hill Digraph Method. You can find these in the "data" worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell itself, and then paste in the decoding section of the Digraph worksheet to save yourself a lot of typing.

3. The only piece of information about this message is that its subject is Bob.

```
LIRYS KLWVO IBVOU UAHRM RBAUT ADCVO UDDPE LJUXC
OPYEB TQWJQ LGSSS SJQEE KOGXZ IYTSS SSJQO VAFWF
AUZDI SWBKZ AAVCZ KRDKG NLKTI EHIVS
```

4. No clues:

```
VTFWK UMESJ JYXUZ ANYWE VTJYV TCSLI CSTKE MKCZK
WKKUK TYSQQ FIFTZ CNTMX IYSJE GSJKX QXSAA ZHQUJ
YVFIU NOCML WLPUJ YUJAV AAVTT S
```

C. The Hill Trigraph Cipher

We have seen that the Hill Digraph system is not as impressive as it initially seemed. There are only $26^2 = 676$ possible permutations of a two-letter permutation. A computer could easily check each out in seconds. So something harder is needed.

The Hill Trigraph method uses blocks of three letters in plaintext to create a ciphertext. So there are a possible $26^3 = 17{,}576$ ways of enciphering three consecutive letters. While this is not a huge number for a computer, decoding a message by hand will take a long time.

In order to encipher a message in the Hill Trigraph system, you need to input a 3 by 3 key matrix in the form: $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$. If the plaintext begins with the word "new", you would convert each letter in "new" to its position: "n" = 14, "e" = 5, and "w" = 23. If the key matrix were: $\begin{pmatrix} 4 & 3 & 5 \\ 2 & 1 & 6 \\ 7 & 11 & 2 \end{pmatrix}$, to find the ciphertext, you would multiply the matrices: $\begin{pmatrix} 4 & 3 & 5 \\ 2 & 1 & 6 \\ 7 & 11 & 2 \end{pmatrix}\begin{pmatrix} 14 \\ 5 \\ 23 \end{pmatrix}$. This multiplication would result in:

$$\begin{pmatrix} 4 & 3 & 5 \\ 2 & 1 & 6 \\ 7 & 11 & 2 \end{pmatrix}\begin{pmatrix} 14 \\ 5 \\ 23 \end{pmatrix} = \begin{pmatrix} 4\cdot 14 + 3\cdot 5 + 5\cdot 23 \\ 2\cdot 14 + 1\cdot 5 + 6\cdot 23 \\ 7\cdot 14 + 11\cdot 5 + 2\cdot 23 \end{pmatrix} = \begin{pmatrix} 186 \\ 171 \\ 199 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 15 \\ 17 \end{pmatrix}$$

So “new” is converted to “DOQ” under this system.

Of course, the spreadsheet will do all of this grunt work for you. Got to the Hill Trigraph Method sheet and, as always, input your plaintext in cell F2. The key matrix will be placed in cells B10, C10, D10, B11, C11, D11, D10, D11, and D12.

The caveat is that the determinant of the key 3 by 3 matrix may not be even or divisible by 13. This determinant is work to calculate. The determinant of $\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$ is $aei - afh - dbi + dch + gbf - gce$.

However, there is an easier method to use which we will find is helpful to know when we decode:

$$\det\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = a\begin{pmatrix} e & f \\ h & i \end{pmatrix} - b\begin{pmatrix} d & f \\ g & i \end{pmatrix} + c\begin{pmatrix} d & e \\ g & h \end{pmatrix}$$

Deciphering a message under this system is similar to the method used with the digraph method. It is necessary to find the inverse of the key matrix. If you are interested in the mechanics of this process, it is explained below but is not necessary to understand to decipher.

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^{-1} \bmod 26 = \left(aei - afh - dbi + dch + gbf - gce\right)^{-1} \bmod 26 \cdot \begin{pmatrix} ei - fh & ch - bi & bf - ce \\ fg - di & ai - cg & cd - af \\ dh - eg & bg - ah & ae - bd \end{pmatrix}$$

Let’s try to decipher a message using the Hill trigraph system. Suppose you received the following message created using a trigraph. The only thing you know is that the plaintext begins with “Calculators.”

LYGTS EKBQG GVJSD WIVGF OKOBK BJROV PYUMP QAKWM WCGLC ASBTA KMQLQ KIUUD FCZXK GKDMB LSXBQ XBJBA AAMIW ITLYI IWCEU NNGMY WRMTK UXKIM TUAQ

We will concentrate on the first three letters. “LYG” which were converted from “cal.” So:

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}\begin{pmatrix} 3 \\ 1 \\ 12 \end{pmatrix} = \begin{pmatrix} 12 \\ 25 \\ 7 \end{pmatrix} \quad \text{or} \quad \begin{aligned} 3a + b + 12c &= 12 \bmod 26 \\ 3d + e + 12f &= 25 \bmod 26 \\ 3g + h + 12i &= 7 \bmod 26 \end{aligned}$$

We know that there are many solutions to these. Since we do not have a spreadsheet to check them out, we will try to find one by trial and error. The problem is that the determinant of your matrix key must be odd. Here is a way to insure this: Have your matrix key in the form of:

$$\begin{pmatrix} odd & odd & even \\ even & odd & even \\ even & odd & odd \end{pmatrix} \text{ or } \begin{pmatrix} even & odd & odd \\ even & odd & odd \\ odd & odd & odd \end{pmatrix}$$

Let's use the first model: Choose small numbers. It's easy at first.

In $3a + b + 12c = 12 \bmod 26$, let c = 0 (even). If a = 3 and b = 3, we have a solution.
In $3d + e + 12f = 25 \bmod 26$, again let c = 0. If d = 8 and e = 1, we have a solution. Is it that easy?

The last equation is a bit harder: In $3g + h + 12i = 7 \bmod 26$, we can't let I = 0 as we need an odd number. S let I =1. That gives us $3g + h$ + 12 = 7 mod 26. We subtract 12 and get $3g + h$ = 21. We need g to be even and h to be odd to solve it. One solution is g = 4 and h = 9.

So a solution is: $\begin{pmatrix} 3 & 3 & 0 \\ 8 & 1 & 0 \\ 4 & 9 & 1 \end{pmatrix}$. Test it in your trigraph spreadsheet and you will see that you have a solution. Obviously, this is not the only solution. There are hundreds more. And, as you saw, it was surprisingly easy to find. If you want a more difficult enciphering method, you can extend your enciphering matrix to a 4 by 4, 5 by 5, etc. using blocks of 4 letters, 5 letters or more. While the number of possible encoding permutations increases dramatically, so do the number of possible solutions. So it is clear that for important messages or information, a much more secure enciphering method is needed.

Exercises: Both of the following were created by the Hill Trigraph Method. You can find these in the "data" worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell itself, and then paste in the decoding section of the Trigraph worksheet to save yourself a lot of typing.

1. The only piece of information you have is the first word is "Red."

```
GKQBG IQMZW FERBC VHQEX WVDAZ ITIIY TCZHC PZQJW
JYQYM IPQKJ UROGX EXYTW SASAJ COVGQ XVCVS EXWAK
KKKBM HDKJU ROGFG HYHCM EIZYS NYP
```

2. No clues other than the most common trigraphs that appear in the English language.

```
YRFGT RGCOU TYLUK YRFQC UGNGN MTCIA UKHCO WSQTR
ESSPJ YRFEJ QXOCZ QDQSK QCMIL SNJMT VGANQ CGWYR
FKLKS GPCMC YRFDI AEVDI LEIFV LBOMD YOBC
```

C. The Vigenère Square

As good as the Hill systems are, you can see that with some work, they can be decrypted. What we would like is a system that is polyalphabetic which does not lend itself to easy decryption either by analysis or exhaustion (examining all the possibilities). Such a method was devised in 1856 by a French diplomat by the name of Blaise de Vigenère.

The Vigenère Square method starts with deciding a keyword of any length. It can be a common word or just a string of letters. You write the plaintext across the page and then the keyword, character for character under the plaintext. You repeat the keyword as many times as is necessary. For instance, suppose the keyword is “humor” and the plaintext is “The Pepsi is in the refrigerator.” You then write:

```
t h e p e p s i i s i n t h e r e f r i g e r a t o r
h u m o r h u m o r h u m o r h u m o r h u m o r h u
```

You then replace the plaintext letter with the letter that lies in the Vigenère Square below at the intersection of the column headed by the plaintext letter and the row corresponding keyword letter. The Vigenère Square is very easy to remember with no formulas as occurred in the affine or Hill methods.

	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

```
  t h e p e p s i i s i n t h e r e f r i g e r a t o r
 h u m o r h u m o r h u m o r h u m o r h u m o r h u
  A B Q D V W M U W J P H F V V Y Y R F Z N Y D O K V L
```

So the Vigenère cipher gives the result above. Notice that since the Vigenère Square is symmetric, it does not matter whether you use to top or side for the keyword.
The spreadsheet program, of course, handles all of this heavy duty work. As usual, you type your plaintext in cell F2 (all lower case, no spaces, 120 characters maximum). You type your keyword in cell B8. The result is shown below.

Note that the spreadsheet does not actually use a Vigenère Square. It merely takes a letter of plaintext, converts into a position number, and does the same with a letter of the keyword. Those two numbers are added (mod 26) and one is subtracted from that number. That will be the position number of the ciphertext. That will simulate the use of the Vigenère Square.

Using the example on the previous page, “t” = 20, “h” = 8, 20 + 8 – 1 = 27 mod 26 = 1 = “A.”

Of course, the question now comes up: how does one actually decipher a message using the Vigenère Square? If one has the keyword, it is easy: just reverse the process. To decipher, the spreadsheet will convert the ciphertext and letter from the keyword to position numbers, subtract them (mod 26) and add one. That number is reconverted to a letter.

Using the example on the previous page, “A” = 1, “h” = 8, 1 – 8 + 1 = -6 mod 26 = 20 = “T.”

So obviously, the keyword controls everything. Do you think it is possible to decode a message using the Vigenère Square if the keyword is unknown? Hard to believe, but there are ways to come up with the keyword involving a lot of analysis and trial and error.

Suppose you had a message that was encoded by a Vigenère Square but you had no idea what the keyword was. Here is such a message:

```
EZSRL IVSUW PABBO VBTVH PKDSS ACXBB OABBO VJADL FJOWU
LBMOS YJBTV HSQXO BBVIB ADRJV OGVXC SGEKX FZKHB GGLFV
ISVIB IUPSV TBIAB BOVRC ORDPO WJB
```

Where do we begin? First, look at the ciphertext closely. Do you see any repeating pattern?

The pattern **ABBO** occurs three times. Underline them. Can we assume that since **ABBO** occurs three times, that its plaintext counterpart occurs three times as well? Not really. It is possible that the first **ABBO** comes from a certain plaintext combined with a part of the keyword, and the second **ABBO** comes from a completely different plaintext with perhaps another part of the keyword. But not very likely! After all, in this relatively short message, how likely that **ABBO** will occur three times just by chance?

A cryptologist by the name of Kasiski came up with a method in 1863 to determine a possible length of the keyword. It is called the Kasiski Test. It says:

If a string of characters appears repeatedly in a polyalphabetic ciphertext message, it is possible (but not certain) that the distance between the occurrences is a multiple of the length of the keyword.
Let’s apply the Kasiski Test to **ABBO.**

Position of first letter of **ABBO** in the ciphertext	Distance between pairs of occurrence of **ABBO**	Prime factorization between pairs of occurrences of **ABBO**
12		
32	20	$2^2 \cdot 5$
104	72	$2^3 \cdot 3^2$

If you examine the prime factorization of these distances, you see that the number which divides evenly into these distances is 2^2 or 4. So a good bet is that the keyword has length four. In the Cipher System spreadsheet, there is a worksheet called "Analysis." If you type or paste your message in cell B3, then type your search string of letters in cell AC1, you will see a blue stripe down the left side of the screen with the position of the first letter of your search string in white.

There are other ways to determine the best possibility for the length of the keyword. We are basing our analysis on only 3 uses of **ABBO** which is not a lot of evidence. Obviously, the longer the ciphertext, the better shot for this analysis to work.

Now comes the fun part. Since we believe that the length of the keyword is 4, we will now do two procedures: 1) We will write the ciphertext in 4 columns, moving across and then down. 2) We will then put each of these columns in alphabetical order.

1	**2**	**3**	**4**
E	Z	S	R
L	I	V	S
U	W	P	A
B	B	O	V
B	T	V	H
P	K	D	S
S	A	C	X
B	B	O	A
B	B	O	V
J	A	D	L
F	J	O	W
U	L	B	M
O	S	Y	J
B	T	V	H
S	Q	X	O
B	B	V	I
B	A	D	R
J	V	O	G
V	X	C	S
G	E	K	X
F	Z	K	H
B	G	G	L
F	V	I	S
V	I	B	I
U	P	S	V
T	B	I	A
B	B	O	V
R	C	O	R
D	P	O	W
J	B		

1	**2**	**3**	**4**
B	A	B	A
B	A	B	A
B	A	C	A
B	B	C	G
B	B	D	H
B	B	D	H
B	B	D	H
B	B	G	I
B	B	I	I
D	B	I	J
E	C	K	L
F	E	K	L
F	G	O	M
F	I	O	O
G	I	O	R
J	J	O	R
J	K	O	R
J	L	O	S
L	P	O	S
O	P	O	S
P	Q	P	S
R	S	S	V
S	T	S	V
S	T	V	V
T	V	V	V
U	V	V	W
U	W	V	W
U	X	X	X
V	Z	Y	X
V	Z		

This is a great deal of work. Fortunately, you have been provided a way to generate this chart: To accomplish this, go to the worksheet called “Analysis.” Type or paste (from the ”Data” worksheet) the ciphertext and place it in cell A3. If you paste it in, be sure that you highlight the data from the cell and not the entire cell. Your ciphertext can be up to 240 characters in length.

In cell N4, type in your guess for your keyword length. Your ciphertext will now be placed in the correct number of columns. To sort the data, simply press the button called “Sort Columns.” You will see your data now sorted on the right side of the screen. It will be in reverse alphabetical order but a quick perusal will tell you which letters appear the most times.

Examine the alphabetical order columns. There are letters which appear quite a few times, especially in the first three columns. In the first column, notice that there are a large number of B’s. We know that there are letters in the alphabet that occur more often than others. One of these letters is “e.” It may be a good assumption that the letter “B” of the ciphertext corresponds to the letter “e” of the plaintext.

To make the conversion, go to row “e” of the Vigenère Square. Read over to the letter “B” than up to the column header. This letter would correspond to the first letter of the keyword. Unfortunately, it is the letter ”x.” Not very promising.

Another one of these common letters is “t.” It may be a good assumption that the letter “B” of the ciphertext corresponds to the letter “t” of the plaintext. To make the conversion, go to row “t” of the Vigenère Square. Read over to the letter “B” than up to the column header. This letter would correspond to the first letter of the keyword. This time, it is the letter ”i.”

Let’s do one more, the letter “a.” It may be a good assumption that the letter “B” of the ciphertext corresponds to the letter “a” of the plaintext. To make the conversion, go to row “a” of the Vigenère Square. Read over to the letter “B” than up to the column header. This letter would correspond to the first letter of the keyword. This time, it is the letter ”b.”

Now let’s do that with the all three columns. Column 2 is the same as column 1. We will refrain from analyzing the last column because there is no obvious letter occurring more than any other. The result:

English common letter	Column 1 (B)	Column 2 (B)	Column 3 (O)
e	**x**	**x**	**k**
t	**i**	**i**	**v**
a	**b**	**b**	**o**

Now your knowledge of the English language comes into play. You need a 4 letter keyword. Assuming that it is a real English word, it is unlikely that the word starts or contains the letter “x.” Eliminating those possibilities, here are what is left:

`iik   iiv   iio   ibk   ibv   ibo   bik   biv   bio   bbk   bbv   bbo`

Again, assuming the keyword is a normal English word, the only strong possibility is “bik.” Since the keyword is believed to have 4 letters, there only is one word starting with “bik.” and that word is __________. Try it by entering the ciphertext in cell O19 and the keyword in cell B8.

BINGO!

Lucky? Maybe. We have made a lot of assumptions. However, if your ciphertext is long (much longer than this example), these methods are tried and true and with some work, you can actually solve these ciphers by seemingly pull the answer out of the air. However it takes a lot of time and patience, and again, it makes sense to tackle these problems in teams.

Exercises: Both of the following were created with a Vigenère Square. You can find these in the "data" worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell itself, and then paste in the decoding section of the Vigenère worksheet to save yourself a lot of typing

1. The only clue you have is that the first word of the plaintext is also the keyword.

```
EOYYW IKACJ DSYED LGZGI MCCUD CWSAU OOPED PHCJY
SOCIA NFRVP LHDDG MANTQ LPWSO BZEMG CUKNC SLWYQ
VTWWE YNOWI GUUKK LKWHU QDLXL GUBSP HLDJT YKPWH
```

2. The only clue you have is that the first word of the plaintext is the word "Titanic."

```
OQVTV UXQUM PQOPK KLYJA VPQPZ TAKMO JOPBH QYEQK
LUIBJ XEAMT FYWXG WYBVS BWFTV PXWET KAGI
```

3. No clues. Good luck!

```
MOMEO BZICY IBTNB MOMBB RAPND TUMYO IOIAD VHVOO
EBKXI MOMEO TYMCO HWTRG AVPNF XFWHN KHENX XSMCR
TUBJR XUMAD XYQAQ MOMVB AVCFO MOMLK KLVHD L
```

E. The Playfair Cipher

The Playfair cipher was developed for telegraph secrecy and was the first digraph substitution cipher. It was used by the British forces in the Boer War and World War I and also by the Australians in World War II. It was invented by Sir Charles Wheatstone in 1854, but he named it after his friend Lyon Playfair. Playfair was a scientist and a public figure of Victorian England.

The Playfair system in its easiest form uses a 5 by 5 alphabet matrix. It also assumes that the letters "i" and "j" are the same. Since "j" does not appear that much in typical English use, all "j"s will be converted to the letter "i." So the plaintext message:

"it seems that John won't join us" is converted to "itseemsthatiohnwontioinus."

Here is the typical matrix used:

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**

Suppose the message is: "the end of the summer is really only three weeks away."

First, this is written as plaintext without any spaces: theendofthesummerisreallyonlythreeweeksaway

Next: if there are any double letters, an "x" is inserted in between the letters:

thexendofthesumxmerisrealxlyonlythrxeewexeksaway

Next, the plaintext above is written in groups of two letters: If the last group only has one letter, attach an "x" onto it. We get:

th ex en do ft he su mx me ri sr ea lx ly on ly th rx ee we xe ks aw ay

Each of the two letter combinations will have three possible relationships with each other in the matrix; they can be in the same column, same row, or neither. The following rules for replacement are used:

a) if the two letters are in the same column of the matrix, use the letter below it as the ciphertext. If you are on the last column, go back to the first.
b) if the two letters are in the same row of the matrix, use the letter to the right of it as the ciphertext. If you are on the last column, go back to the first.
c) if the two letters are in neither the same row or column, then each are exchanged with the letter at the intersection of its own row and the other column.

So, in the above, "th" is replaced by "IS." "ex" is replaced by "ZC." Both of these are examples of c) above. "do" is replaced by "IT" – an example of a). "sr" is replaced by "TS" – an example of b). the entire translation is:

IS ZC PC IT QI CK TQ WN BP GT TS AB VO PO VO IS BW CZ BW CZ BZ CZ UH VB VD

Deciphering reverses the rules but will take time. Unfortunately, you are not guaranteed to get the original message because of the double letter problem. Your plaintext will possibly be littered with the letter "x." Still, it should be readable. Here is the deciphering of the ciphertext above.

thexendofthesumxmerisrealyonlythwrxewexeksaway

On the spreadsheet, you have been given a worksheet called “Playfair” which will do the enciphering and deciphering. It works just like the other worksheets: Put your plaintext in E2 in lowercase and no spaces. It will automatically dceipher for you as well. If you are given a Playfair cipher and you wish to decipher it, you can enter your ciphertext in cell E40 (all caps, no spaces).

Still, this is a very easy ciphering routine as was abandoned early as a secure method. However, it can be made more difficult by not placing the letters in the Playfair matrix in alphabetical order. You can choose a keyword and eliminate all repeating letters. For instance, if the keyword is ”mathematical,” you would write it as “matheicl.” You would then fill the Playfair matrix starting at the top left with these letters and then fill in the rest of the alphabet. You would get:

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

The rules stay the same. So the message “see you at the mall” becomes: “sexeyouatxthemalxl”

se xe yo ua tx th em al xl

So the enciphering will be:

UH ZT ZN QU LT MA CT TK

Obviously, to decipher such a message would be difficult without the keyword. But once you have it, deciphering will take time but is routine. Obviously, we need a method that does not depend on a keyword. We will cover that in the last section on public key cryptography.

Exercises: Both of the following were created with a Playfair system. You can find these in the ”data” worksheet of the Cipher spreadsheet. Highlight the data from the cell (not the cell itself, and then paste in the decoding section of the Playfair worksheet to save yourself a lot of typing

1. IS UD UC YR QC CF BT RE YO VI TP UQ ID YZ TP GY VN AO YM PA NV

2. Ray decided to cipher his message twice using the Playfair system. This is the result of his second enciphering. Can you decipher it? Was this smart on his part?

   OY NT FO BR ET XT HE PR ET KP LS

3. A message was intercept using this Playfair matrix with the keyword “average”. Can you decipher it?

```
MB US YO DE RV QI OP SH GV YD MB DF TI PH SI DE
```

F. The Permutation Cipher

The Permutation Cipher (also known as the Transposition Cipher) has been in use for hundreds of years. It was invented in 1563 by Giovanni Porta. This is a system where it is more convenient to actually use alphabetic characters rather than a modulo 26 system because there are no algebraic operations being performed in encryption or decryption.

A permutation for any number *b* is simply the integers from 1 through *b* arrange in some random order. For instance, if *b* = 5, then a possible permutation would be 4, 3, 5, 2, 1 or 5, 4, 3, 1, 2.

To use this system, first you decide on a block length *b*. It can be any number greater than one. You then block off your plaintext in blocks of *b*. For instance, suppose *b* = 6 and the message is: “it was the best of times, it was the worst of times.” So your blocking is:

```
itwast hebest oftime sitwas thewor stofti mes
```

Now you devise a permutation of your block length *b*. For instance, my permutation might be:

Letter	1	2	3	4	5	6
Permutation	4	6	2	1	5	3

What this says is for each block, we create a new block interchanging the original letter of the block with the permutation letter of the block. For the first block, the following chart explains the procedure:

#	1	2	3	4	5	6
Permutation #	4	6	2	1	5	3
Permutation letter	a	t	t	i	s	w

So for this block, the ciphertext will be “attisw.” The entire message will thus be:

```
attisw etehsb iemotf iefomt wsiaat wrhtoe fitsto ems
```

To decode, we simply need to find the inverse permutation. All we need do is to interchange the two rows of the permutation table and rearrange the columns so that the first row is in increasing order:

Letter	1	2	3	4	5	6
Inverse Permutation	4	3	6	1	5	2

What this says is for each block of the ciphertext, we create a new block interchanging the original letter of the block with the permutation letter of the block. This would be the result for the first block.

#	1	2	3	4	5	6
Inverse Permutation	4	3	6	1	5	2
Letter	i	t	w	a	s	t

Obviously, if you are told that an encrypted message was the result of a permutation cipher, deciphering is not that difficult. It certainly helps to have the block length. If the block length is 4, for instance there are 4 factorial (4!) = 24 possibilities for the plaintext. If the block length is 5, there are 5! = 120 possibilities for the plaintext. In general, there are b! possibilities for the plaintext for block length *b*. Once *b* gets above 6, it will take a lot of trial and error to come up with the right one. Not knowing *b* makes it all the more difficult.

Using the Permutation worksheet of the Cipher spreadsheet takes some care. You input your plaintext in cell E2 (120 characters maximum no spaces). In cell G4, you input your block *b*. The block must me a whole number greater than one and less than or equal to eight. In cells A9 through B16, you are given a table. In black will be the whole numbers from 1 through block *b*. You then input in column B in blue, the permutations. Obviously every number from 1 through *b* must be present with no repetitions. If you have a repetition, you will be given notice. It is also important that there are blanks in the cells below and to the right of *b*.

If you have an approved permutation, your ciphertext will appear in red in the middle of the screen. If the cells are filled with #####, that is your notice that your permutation is not allowable or that you have extra information in column B below your block *b*.

Your last few letters of the ciphertext may have spaces embedded in them. Ignore these spaces.

Different from the other cipher worksheets, this permutation spreadsheet will only decipher the original plaintext as you can see in green below. To accomplish this, you must tell the spreadsheet to calculate the inverse permutation. Simply press the button "Get Inverse" to make this occur. You must do this whenever you change the block or the permutation.

This worksheet will not let you input your own ciphertext as the others do. To decipher, you will have to use your ingenuity. However, you can input your possible plaintext answer, block, and permutation, and see if you get the given ciphertext.

Interestingly enough, the Permutation Cipher is really a special case of the Hill Cipher. To show this fact, let's try a simple message in the Permutation cipher: "That book can be founding the library." Use a block of 3 with permutation 1-3, 2-1, 3-2. You should get this ciphertext:

`athotbcokbanoefduntinlheribyar`

Now go to the Hill Trigraph worksheet, and use the same plaintext: "That book can be founding the library." Since in the permutation, one translates to three, place a 1 in the third column of the first row. Since two translates to one, place a 1 in the first column of row 2. Since three translates to two, place a 1 in the second column of row 3. Your matrix should look like this:

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

You will see that the ciphertext is exactly the same. So when you are using a block of 5 for example, you are really using a special case of a Hill system with a 5 by 5 matrix.

Exercises: The following ciphertexts were created with permutation ciphers. You will be given the block length and for convenience, the ciphertexts will be given to you in those blocks. See if you can decipher them.

1. `epsr eind utsb phpa leea odct gorn sefs qour kiac dned scii avce otni ftio tgch poor trea afur d` (block is 4)

2. `aerhht nsfior odvrmo etwehi moadwi srbeik oensda ciinna anbetd arrado asnsiu ecauln muasbr nier` (block is 6)

3. `oiuyftwanacsteplaauccraavnttoiaaceksreiunagolitn ehespdiaagssaelniaaks` (no block given – good luck)

5. Deciding between Monoalphabetic and Polyalphabetic

You have been given a message but have no idea whether or not it was created by monoalphabetic (every unique letter of the plaintext is always replaced by the same letter) and polyalphabetic (there is no guarantee that unique letters are always replaced by the same letters).

If you are given an encrypted message, it is probably easier to check out the monoalphabetic possibilities first. The additive and multiplicative ciphers are simply individual cased of the affine cipher, ap + b. In the additive cipher, $a = 0$. In the multiplicative cipher, $b = 0$. With “only” 392 possibilities in the affine cipher, it is a probably a good place to start.

Still, if it isn’t affine, you have wasted a great deal of time and effort. Also, there are other monoalphabetic ciphers that are not affine. There has to be a better way.

William F. Friedman is said to be the dean of modern American cryptologists. He did most of his work from 1920 through 1955. he is responsible for the Friedman test, a test which will help determine whether an enciphered message is monoalphabetic or polyalphabetic.

The Friedman test determines what is known as the **Index of Coincidence (IC)**, the probability of two letters randomly selected from a text being equal, suggesting whether the underlying enciphering scheme is monoalphabetic or polyalphabetic.

To compute the IC, let

$$\begin{aligned} &n = \text{number of letters in the text;} \\ &n_1 = \text{number of a's in the text;} \\ &n_2 = \text{number of b's in the text;} \\ &\vdots \\ &n_{26} = \text{number of z's in the text;} \end{aligned}$$

Friedman determined that the Index of Coincidence is:

$$\text{I.C} = \frac{n_1(n_1-1)}{n(n-1)} + \frac{n_2(n_2-1)}{n(n-1)} + \frac{n_3(n_3-1)}{n(n-1)} + \ldots + \frac{n_{26}(n_{26}-1)}{n(n-1)} = \sum_{i=1}^{26} \frac{n_i(n_i-1)}{n(n-1)}$$

If a message is from a monoalphabetic cipher, certain letters will appear more than others. The IC for the English language is approximately .065.

If a message is from a polyalphabetic cipher, letters will have the same chance of being chosen; no one letter should appear more than others. If all letters have the same chance of being chosen, the IC is approximately .038, about half of the IC for the English language.

For instance, suppose you were given this ciphertext with no other clues.

```
QKCQG NXSNY CKSTG MSLLG JCFEX GFYCK XSHGF CNJCF GNXGX CIGEC
TOJCF KNTYS FJDSO GCKNN XGNGS MXGTU NUQPG QNNCS JIUNY CKTDS
ULKTG NCJCU N
```

An analysis of the frequency of letters gives:

A	**0**	**J**	**6**	**S**	**9**
B	**0**	**K**	**7**	**T**	**6**
C	**14**	**L**	**3**	**U**	**5**
D	**2**	**M**	**2**	**V**	**0**
E	**2**	**N**	**14**	**W**	**0**
F	**6**	**O**	**2**	**X**	**7**
G	**14**	**P**	**1**	**Y**	**4**
H	**1**	**Q**	**4**	**Z**	**2**
I	**2**	**R**	**0**		

From this, the IC (there were 111 letters in the message) comes out to be .06978. This is very strong evidence that the message came from a monoalphabetic ciphering scheme. It did, it was from an affine scheme. The message was:

> Suppose that you are called on when you have not done the homework. Don't try and fake out the teacher It is best to admit your failure to do it ($a = 23$, $b = 22$)

Suppose you received this ciphertext with no clue as to the method.

```
GTFHG VEMNC HGOZE OORGC VEZKL YDKTC OZNCB CFIBD MYEMD KREGJ
ABHUZ KDUFF SJNZR SKZOZ NJDKF SWXDK ZQVAI UAXNJ MLRGW GWLQK
RSQQQ KEMYE SBDR
```

An analysis of the frequency of letters gives:

A	**3**	**J**	**4**	**S**	**5**
B	**4**	**K**	**9**	**T**	**2**
C	**5**	**L**	**3**	**U**	**3**
D	**7**	**M**	**5**	**V**	**3**
E	**7**	**N**	**5**	**W**	**3**
F	**5**	**O**	**5**	**X**	**2**
G	**7**	**P**	**0**	**Y**	**3**
H	**3**	**Q**	**5**	**Z**	**8**
I	**2**	**R**	**6**	**S**	**5**

From this, the IC (there were 114 letters in the message) comes out to be .038508. This is very strong evidence that the message came from a polyalphabetic ciphering scheme. It did, it was from a Hill Digraph scheme with $a = 11$ $b = 4$, $c = 5$, $d = 15$). The message is exactly the same.
The worksheet called "Analysis" of the general Cipher spreadsheet will do the analysis for you. All you need to do is to type (or paste) your text into cell B3 (up to 240) characters. The frequency of letter chart will be on the left of the screen and the IC on the right along with the general recommendation of monoalphabetic or polyalphabetic. Please keep in mind that this type of analysis is best used when you have long messages. A short message simply does not have enough data to make a good judgment.

In the Vigenère Square ciphering system, we needed a keyword. To decipher, we need to find that keyword. We have seen that finding a string of letters that seems to occur more often than others will help us to find the possible length of the keyword. The Analysis sheet will help you find the position of any keyword you believe to repeat. But there is another way to help you come up with a possible length of the keyword instead of having to carefully examine the possibly long message in search for a repeated set of characters. Without proof we state:

If a message of length n and Index of Coincidence IC is coded using a Vigenère Square, then r, the length of the keyword is given by the approximation formula:

$$\boxed{r \approx \left| \frac{0.027n}{(n-1)\text{IC} - 0.038n + .065} \right|}$$

The Analysis spreadsheet will calculate this automatically for you. However, unless you have a lot of data (a long message), the value it gives you could be well off. It is wise to use this formula in conjunction with the Kasiski test. Exercise 4 below will put you to the test.

Exercises: Determine if the following ciphers are most likely based on a monoalphabetic or polyalphabetic scheme. You can find these in the ”data” worksheet of the Cipher spreadsheet. Copy and paste it into cell B3 of the analysis spreadsheet. Can you actually solve them?

```
1.  YGLLC EQNCF GFSNU CFSLZ STOLC MSNGJ UFNXG FCTNX
    EGQNM CTFGT CDEYC IUFAS FJSJR SMGFN ZSTNQ CDICF
    NSFNS SFJUJ SXCMC FNSUF QCHGT XSLDC DSLLO FCEFA
    GYQGT QZIGS TNXDG ECDNX GQGXY JTCNX GTISL QZGMN
    SMLGQ STGTG AKLST GFCKA XNCPG SFNUM UZSNG JSMMK
    TSNGL YCLJD SUNXD KLUQC FGQKM XAGYQ GT
```

```
2.  WLSOR IHMCQ OEKUF DONBA QQWIT QWMSZ HYDJG VSXFG
    GKUDK FUWNF PMMWR YOULQ GOODN OUREB MYDZU NUVSX
    FYQLP MHBKI KKYOM AKDGS UWHYD JKUWG RVKRS IYWGE
    YOKVH INALR MNMLD TJMMC LXGWT IJSGX YMWNM OWSCA
    YOOLU XGSED MRINL FSTOD COQYM WVZUP MHRQK UYIER
    EKNYH CSHBE VDWYH IGULS XEDCY BKLLG WOURB YMDL
```

```
3.  TCOQU TKRGM HIDUC XKIPW TEYUZ HITUY OVRVR XGAUD
    VVNVE KPSJY PJTJK MYUOK GJCQX MZNWO MFRWX YRSVO
    KAUOZ AZGJO KRNFD AIOYP TITJO KKHCX XMETF XWOTO
    PYAVS LRLNY PZNID AZSVY HTCWB MNOQP MYEHK VKOTC
    PYIER TIEEK NJIPQ MYIUZ AVNQW XEOPK KVTTK BETGM
    AEISE XJAPN BDPTY OVMGX MZNGA NZPOO GK
```

4. This comes from a Vigenère Square cipher. Good luck!

```
    EPWFW IBQTA BGCWQ XJJIG DIBQJ BVRDI BQTAG BQBWS
    JWICF AVNSI BQTVW GTBTR PTGYT SSFFO OEEPS BNMOA
    LVRGS MGNYL ANVMV NHIWV LADRN QOYWI BQ
```

6. Public Key Cryptography

Several of the assignment problems have started by telling you the actual enciphering scheme, be it additive, multiplicative, affine, or Hill. (there are many, many others). The question is: why would you know this? If secrecy and privacy is so important, why help someone out by telling them the actual scheme? Granted, a lot of work is still need to decipher the message, but why give someone a head start?

Here is the answer: Suppose Bob owns a business and he wishes to communicate with one of his employees, Alice, in privacy. First, they must meet in secret to decide on one of the classical systems of enciphering. Then they will have to decide on a key. If they cannot meet, they will need a trusted associate to act as a go-between. Still, that is not too much work.

But suppose Bob's business involves 100 employees, each wanting to talk with each other in privacy. That would involve 4,950 enciphering schemes with 4,950 keys.

If the business was huge (like America On-line), and there were a million people all wishing to communicate with each other, it would involve about 500,000,000 (about half a trillion) enciphering schemes and keys.

Public Key cryptography systems is based on publishing, for the entire world to see, the means by which messages are enciphered. This is done with the full assurance and confidence that this knowledge alone does not lead to the deciphering process being discovered, at least in a reasonable amount of time.

Before public key cryptography was invented, cryptographic systems, now referred to as private key or classical systems, depended for their security on the knowledge that both keys (encryption and decryption) were kept private.

In these systems, if the encryption key is known, the decryption key is known as well. In the cases of an additive or multiplicative system, the decryption key is known immediately. In the case of an affine method, some work is needed to find the decryption key. In the case of the Hill digraph system, having a crib can help us find the key. But even without a crib, computers, even home computers, can find the key by trial and error (called the method of exhaustion) in a short period of time. In short, these methods are insecure.

With public key cryptography, knowing the key for the enciphering process does not give you the key for the deciphering process. These systems use keys with such large numbers (often over 100 digits in length) that using trial and error to decipher would take 3.8 billion years, even with a state-of-the-art computer.

Any two people with entries in the public-key directory could communicate with each other without any prior exchange of keys. If Alice wants to send a message to Bob, Alice looks up Bob's enciphering key in the public directory. She writes her message, then uses Bob's enciphering key to get a ciphertext which she send to Bob. Bob then uses his secret deciphering key (not public) to convert the ciphertext back to the original message. Only Bob can decipher the message because he is the only person who knows the deciphering key.

Using this system, messages can be authenticated and protected from forgeries. For instance, suppose Alice is expecting an important message from Alice and wants to be sure that the message is really from Bob and not a forgery. This is the procedure.

- Bob composes a message (”send money”) and uses Alice's public enciphering key to get a ciphertext (”ABCDEFGHI”)

- Alice deciphers the ciphertext with her private deciphering key. She gets “send money”. Did it come from Bob?

- Alice then uses Bob's public enciphering key to get a ciphertext ”ZYXWVUTSR”

- When Bob receives the ciphertext message, he deciphers it with his private key and gets “send money.”

- Bob then enciphers that message with Alice's public key to get a ciphertext (“ABCDEFGHI”)

- Alice then deciphers the message with her private deciphering key. She gets “send money”. She knows it came from Bob because only Bob would have been able to decrypt ”ZYXWVUTSR”.

Unfortunately, the technical aspect of public key cryptography is well beyond the scope of this manual. It involves knowledge of abstract algebra and number theory, courses you will take in college if you go into a mathematics related field.

References:

Flannery, Sarah. 2001. *In Code*. Thomas Allen & Son Limited.

Lewand, Robert. 2000. *Cryptological Mathematics*. Mathematical Association of America.

Stinson, Douglas. 2002. *Cryptography, Theory and Practice*. Chapman and Hall.

Wampler, Joe. 1999. *Elementary Cryptology*. COMAP, Inc.

Wrixon, Fred B. *Codes and Ciphers*

Answers to Exercises:

Additive exercise answers:

1. The car I would most like to have is a Porsche. (encipher key = 6, decipher key = 20).
2. When you get the answer to problem nine please call me. (encipher key = 14, decipher key = 12)
3. Don't forget to buy tickets to the concert (encipher key = 18, decipher key = 8)
4. When the defense blitzes, we will throw a screen pass. (encipher key = 24, decipher key = 2)
5. We plan to vacation in Bermuda instead of Florida this year (encipher key = 13, decipher key = 13)

Multiplicative exercises answers:

1. I am sure the Eagles will win by more than 6 points this year (mult key is 9)
2. The internet site is www.milkshake.com (additive decipher key is 9)
3. There is a great show on TV tonight - channel six at ten (mult key is 21)
4. If the appliances go out, be sure to turn off all appliances (additive decipher key is 1)
5. Circuit City is having a big sale on DVD's today - half off (mult key is 25)

Affine exercises answers:

1. Don't forget to see the elephants when you take your trip to the zoo. (Key: *a* = 7, *b* = 15)
2. I went to see the new Star Wars movie but I didn't enjoy it as much as the earlier ones. (Key: *a* = 17, *b* = 4)
3. The latest version of the school newspaper contained a large error that caused it to be recalled and reprinted, costing the club a lot of money (Key: *a* = 3, *b* = 24)
4. Try to take the test at a time when the teacher is present so he can take questions that come up. (Key: *a* = 23, *b* = 22)

Matrices exercises answers:

1. $\begin{pmatrix} 19 & 20 \\ 15 & 12 \end{pmatrix}$ 2. $\begin{pmatrix} 5 & 18 \\ 18 & 17 \end{pmatrix}$ 3. $\begin{pmatrix} 13 & 19 \\ 10 & 24 \end{pmatrix}$

4. $\begin{pmatrix} 7 \\ 2 \end{pmatrix}$ 5. $\begin{pmatrix} 1 \\ 17 \end{pmatrix}$ 6. $\begin{pmatrix} 10 & 6 \\ 2 & 18 \end{pmatrix}$ 7. $\begin{pmatrix} 14 \\ 24 \end{pmatrix}$

Inverse Matrix Answers:

1. $\begin{pmatrix} 10 & 19 \\ 19 & 5 \end{pmatrix}$ 2. $\begin{pmatrix} 2 & 25 \\ 9 & 7 \end{pmatrix}$ 3. $\begin{pmatrix} 6 & 23 \\ 25 & 17 \end{pmatrix}$ 4. $\begin{pmatrix} 24 & 21 \\ 23 & 6 \end{pmatrix}$

Hill Digraph Method Answers:

1. If Mr. Schwartz is absent, let’s cut class. (Key matrix is: $\begin{pmatrix} 7 & 3 \\ 3 & 2 \end{pmatrix}$)
2. Meet you at the mall at nine. (Key matrix is: $\begin{pmatrix} 5 & 3 \\ 9 & 6 \end{pmatrix}$)
3. Bob wants to go to Great Adventure tomorrow but I would rather go to the shore. If we go to the amusement park we will spend all day in line. (one possible key matrix: $\begin{pmatrix} 15 & 4 \\ 9 & 15 \end{pmatrix}$)
4. There is great evidence that the more money you receive as a windfall the more careful you need to be in deciding what to do with it. (one possible key matrix: $\begin{pmatrix} 24 & 11 \\ 9 & 6 \end{pmatrix}$)

Hill Trigraph Method Answers:

1. Red is the important color to wear. If I see you wearing red I know it is safe to talk. Any other color and I will know its quite dangerous. (one possible key matrix: $\begin{pmatrix} 1 & 5 & 4 \\ 6 & 5 & 2 \\ 2 & 3 & 11 \end{pmatrix}$)
2. The Brady Bunch is the television show that confounds the critics more than any other but when the show ended the people still wanted more. (one possible key matrix: $\begin{pmatrix} 8 & 3 & 15 \\ 0 & 1 & 2 \\ 3 & 9 & 6 \end{pmatrix}$)

Vigenère Square Method Answers:

1. Puzzles like humor have universal appeal and know no boundaries, cultural, educational, or otherwise.
People of all ages are attracted to puzzles. (keyword is puzzles)

2. Titanic is the third most widely recognized word in the world following god and coca cola. (keyword is victim)

3. There is a popular theory that an elephant can be lucky there are people who have you draw an elephant when entering their house They are nuts. (keyword is think).

Playfair Answers:

1. The test was hard but if you study you will do well.

2. Don’t forget the pretzels. (not smart, part of the original message is shown in the ciphertext)

3. If you see a lot of traffic, don’t come.

Permutation Answers:

1. President Bush appealed to Congress for quick and decisive action to fight corporate fraud.
   Permutation: 1-3, 2-1, 3-4, 4-2

2. The Harrison Ford movie the Widowmaker is based on an incident aboard a Russian nuclear submarine. Permutation: : 1-5, 2-3, 3-6, 4-2, 5-4, 6-1

3. If you want a spectacular vacation take a cruise along the Inside Passage in Alaska.
   Block is 5. Permutation:1-4, 2-1, 3-5, 4-3, 5-2

Analysis Answers:

1. This came from a monoalphabetic affine cipher. The CI was .06340. The message is: Yellowstone National Park, located in the northwest corner of Wyoming and adjacent to parts of Montana and Idaho, contains over half of all known geysers on earth. Few of these hydrothermal spectacles are regular enough to be anticipated accurately. Old Faithful is one such geyser ($a = 23$, $b = 22$)

2. This came from a polyalphabetic Hill Trigraph system. The CI was .04237. One characteristic of modern science is gathering data and the describing the data with a mathematical model. For instance if you examine the data from a sample of people you see that Leonardo Da Vinci’s famous drawing that indicates a person’s height and arms span are equal is correct. ($a = 0,$ $b =5$, $c = 1$, $d = 6$, $e = 3$, $f = 2,$ $g = 3,$ $h = 9$, $i = 6$)

3. This came from a polyalphabetic Vigenère system The CI was .044428. A look at records set in many sports over the past century shows that humans continue to run faster jump higher and throw farther than ever before. What is allowing this to occur? Two of the factors which are causing this phenomenon are train techniques and improvement in equipment. (keyword is track

4. This land isn’t rocky but sandy. The sand is soft. If you push a hand in it it feels like sugar . The ocean and the sand make Hawaii a special land. (keyword is lion).