Caesar and Vigenere Substitutions

Given the plaintext

A penny saved is a penny earned

let us use the following substitution

$$\begin{array}{c} \text{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z} \\ \Downarrow \\ \text{D E F G H I J K L M N O P Q R S T U V W X Y Z A B C} \end{array} \tag{1}$$

to encrypt it. First we ignore spaces and write the plaintext as

APENNYSAVEDISAPENNYEARNED

and then substitute each letter with the letter below it in (1). Thus our ciphertext would appear as

DSHQQBVBYHGLVDSHQQBHDUPHG (2)

This substitution is an example of one of the earliest known ciphers, known as *the Caesar cipher* or *Caesar substitution*. This cipher is so named since Julius Caesar is thought to have used it to send a message to Mark Anthony. There are actually twenty-six different forms of Caesar substitutions (one for each letter in the alphabet). For instance, instead of sending every letter to the third letter following it (with wrap around at the end) as we did in (1), we could have sent every letter to the fifteenth letter following it.

$$\begin{array}{c} \text{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z} \\ \Downarrow \\ \text{P Q R S T U V W X Y Z A B C D E F G H I J K L M N O} \end{array} \tag{3}$$

Our message would then appear as

PETCCNHPKTSXHPETCCNTPGCTS.

Ordinary Caesar substitution is *relatively* easy to decrypt using a method called *frequency analysis*. Frequency analysis counts *how often* certain letters appear in our ciphertext. Since every plain language letter is always represented by the same cipher letter, we can use properties of the English language to *guess* which substitutions were made. For example, let us count the number of occurrences of the different cipher letters in line 2.

$$\begin{array}{c} \text{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z} \\ \text{0 3 0 3 0 0 2 5 0 0 0 1 0 0 0 1 4 0 2 0 1 2 0 0 1 0} \end{array}$$

One of the properties of the English language (and we shall deal with more such properties in chapter 4) is that the nine most frequently used letters (in order of most frequently used to less frequently used) are $ETOANIRSH$. Thus we could assume that either the H or the Q would be the E. If we guess that the Q is the cipher letter for E and we replace every letter by the twelth one that follows it (with wrap around) the result is not a distinguishable message. Thus our next attempt would be to guess that the H is the cipher letter for E and once we make the appropriate

substitutions we would get our original plaintext. Note that if neither the H nor the Q worked as the substitution for E we would have next guessed that it was either the B or the D.

Since the ordinary Caesar substitution is *in theory* so easy to decipher, we will now show a modification that will in part *fool* frequency analysis. Namely, *Caesar substitution with keyword* or *Vigenere* makes use of polyalphabetic substitution (in other words, each letter is replaced by a different letter depending on the particular situation) and this creates a more secure system. This system is based on two keys:

1. an n-letter key word $k_1 k_2 \dots k_n$; and
2. the following encipherment square known as the Vigenere square:

	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

We will show how to use this square to encipher the following plain text

A Picture is worth more than a thousand words

Let us assume that our keyword is *BULKY*. Since the length of our keyword is five, we must write the plaintext in 5-grams:

APICT UREIS WORTH MORET HANAT HOUSA NDWOR DS

Now we will encrypt $APICT$ using $BULKY$ in the following manner: The letter A is replaced by the letter in row A and column B (thus $A \Rightarrow B$). The letter P is replaced by the letter in row P and column U (or $P \Rightarrow J$). Similarly, I is replaced by the letter in row I and column L, C is replaced by the letter in row C and column K and finally T is replaced by the letter in row T and column Y. This yields the following substitution:

$$\begin{array}{ccc} \text{A} & \Rightarrow & \text{B} \\ \text{P} & \Rightarrow & \text{J} \\ \text{I} & \Rightarrow & \text{T} \\ \text{C} & \Rightarrow & \text{M} \\ \text{T} & \Rightarrow & \text{R} \end{array}$$

and accordingly, $APICT$ is encrypted by $BJTMR$. Next, we encrypt the 5-gram $UREIS$ in the same manner. In this case, we get that

$$\begin{array}{ccc} \text{U} & \Rightarrow & \text{V} \\ \text{R} & \Rightarrow & \text{L} \\ \text{E} & \Rightarrow & \text{P} \\ \text{I} & \Rightarrow & \text{S} \\ \text{S} & \Rightarrow & \text{Q} \end{array}$$

and thus $UREIS$ is encrypted by $VLPSQ$. Continuing in this fashion we obtain the ciphertext

$$BJTMRVLPSQXICDFNICORIUYKRIIFCYOXHYPEM$$

The number of letters in the keyword is referred to as the period. Thus the above substitution has period five.

Exercises:

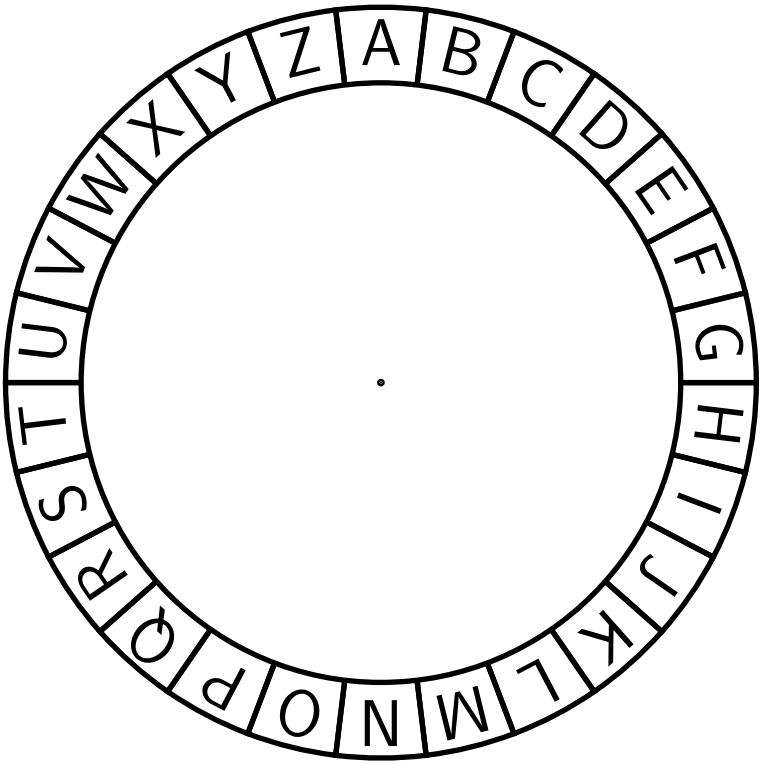
1. Decipher the following Caesar encrypted messages
   (a) **PBZ CHG REF PNA ORN CNV AVA GUR OEN VA**.
   (b) **GZZG IQOT ZNKK BKTO TMUX GZJG CT**.
2. Encrypt the message **Cat got your toungue** with keyword *zip*.
3. Decipher the following messages that were encrypted with the given keyword .
   (a) **LBR UIJ BOZ HYQ GPR JNU WGB GH** Keyword: *sun*
   (b) **CSWNF ZBPJV VWPUW OYFFP JKKKK EHDGS IOJ** Keyword: *crow*
   (c) **RJOZB JWBJO CILHV MEBRG KNDYW E** Keyword: *nokidding*
4. Decipher the following message knowing that it was encrypted with a four letter keyword starting with *se*.

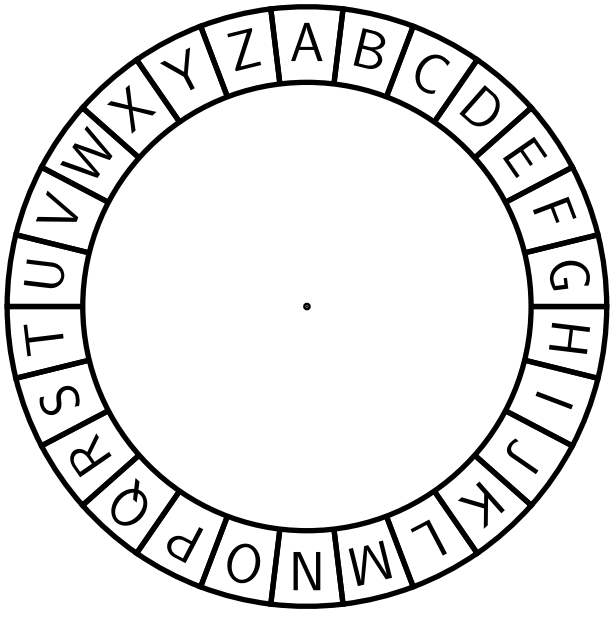
   GTEY TSOV KSPP FROE WWCW GWEO XVIP FHSL FHEY WQIP K

5. Decipher the following messages knowing that they were encrypted with a two letter keyword.

   (a) **CLRMR HGXNS PIZJH NRLFO FYCLR WVMRF LNVGR XPFBW XJHFF YFNBI CYEUG YNNIY ESUCT BFJRY QM**

   (b) **VEVWY XNUZW XLRCJ BVNDK VCKNI CYJEQ VJMHD NKJC**


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


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

Complete Rectangular Transposition with Keyword

This cipher consists of a single key k_1: a word of length n. To give an example of this method we will encode the following plaintext

Challenger lands safely after a five day journey

based on the keyword *CONDOR*.

The letter C is the lexicographically earliest in *CONDOR*, followed by D, N, O and R in that order. We can thus associate the permutation

1 4 3 2 5 6

to *CONDOR* based on that order. The two O's that appear are labelled 4 and 5 from left to right. Now the plaintext is written under this permutation rowwise:

1	4	3	2	5	6
C	H	A	L	L	E
N	G	E	R	L	A
N	D	S	S	A	F
E	L	Y	A	F	T
E	R	A	F	I	V
E	D	A	Y	J	O
U	R	N	E	Y	Q

The last row is completed with dummy letters (in this case Q). The ciphertext is constructed by reading the text vertically in the order of the numbered columns:

CNNEE EULRS AFYEA ESYAA NHGDL RDRLL AFIJY EAFTV OQ

To decipher rectangular transposition, suppose that k is the length of the ciphertext divided by the length of the keyword. Thus, k is the length of the columns. Given this, we divide the ciphertext into $k-grams$ and write the $k-grams$ in the corresponding columns. For example, suppose that we have the following ciphertext

MTRDYHWAOWTYTTANLOAQEAUTREICWNELKNE

based on the keyword *Georgia*. The length of the ciphertext is 40 and the length of our keyword is 8 so our columns must have length 5. Now the permutation corresponding to Georgia is

3 2 6 7 4 5 1

thus the first five letters belong in the seventh column, the second five letters belong in the second column, the third set of five letters belong to the first column, etc. The resulting table would look like

T	H	E	E	N	E	M
Y	W	I	L	L	A	T
T	A	C	K	O	U	R
T	O	W	N	A	T	D
A	W	N	E	Q	R	Y

and yields the message

The enemy will attack our town at dawn

with "eqry" arbitrarily added as extra letters.

Exercises:

1. Decipher the following message knowing that it was encrypted using Rectangular transposition with keyword *forsaken*.

   NTFTN EIPNE OIRLS SLSTS ABAVV ISEII GYOSE ALAOS
   FSEOS ENSHQ TEJEE NIVNN HAORL CTETG IUYII RWRON

2. Decipher the following message knowing it was encrypted using Rectangular Transposition and that the original plaintext contains the word "sundown".

   YNRND TDAIW LLTEU AABUN SDETO IOTLN ULNHS

3. Decipher the following message knowing that it was encrypted using Rectangular Transposition and that the original plaintext contains the words "disease" and "hunger".

   EESS UHWN DENE OEIA GWRM SNEO TSYE DRHT IAHT

Homophonic Substitution

Homophonic substitution is another method that is used to fool frequency analysis. In this cipher, we will replace each letter of the alphabet with a particular number based on a *random process*. This substitution uses the *Latin* alphabet where I and J are considered to be the same letter. We sometimes will denote this letter by I/J or if the context is clear just by I. The alphabet is placed in the first row of an auxiliary rectangle whose successive rows are filled with the numerals $01, 02, \ldots, 24, 25$. The number of rows is determined by the length of the key word. The numerals are placed sequentially with circular wrap-around starting from the position of the corresponding letter of the keyword. An example will suffice to get this across.

From the keyword *GOLF* we construct the four rows of numerals of the auxiliary rectangle as follows:

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

The final rectangle is obtained by adding 25 to all the numbers in the second row, 50 to all the number in the third row, 75 to all the numbers in the fourth row, etc. In this case the final rectangle is

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
20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
38	39	40	41	42	43	44	45	46	47	48	49	50	26	27	28	29	30	31	32	33	34	35	36	37
66	67	68	69	70	71	72	73	74	75	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65
96	97	98	99	100	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95

This done, each letter of plaintext is replaced by any one of the numerals below it in the final rectangle. For example, we could encrypt the phrase

The box will arrive by train

by

59 78 24 97 54 17 34 46 5 81 20 29 87 74 91 42 67 18 31 87 66 3 50

There are many different choices we could make to encrypt this message. If the encryption is done by computer, the selection of the numeral can be carried out by means of a random number generator.

Exercises:

1. Encrypt the message "You take the high road" using Homophonic Substituion with keyword *plan*.
2. Decipher the following message knowing that it was encrypted with Homophonic substituion and keyword *golf*.

31 2 24 8 83 5 94 13 42 57 6 88 20 98 40 24 9 13 70 69 96 57 100
60 53 22 54 7 41 74 13 79 54 53 66 48 58 14 11 29 100 83 69 70 29

3. Decipher the following Homophonic encryted message.

2 58 43 55 63 55 50 37 47 68 69 47 30 13 42 39 79 95 58 86 79 103
67 120 32 58 55 85 55 78 111 13 84 32 59 68 124 22 50 100 63 103

The Playfair Encipherment System

This is an encipherment system devised by the Baron Playfair of St Andrews for the purpose of secret communication. It uses the Latin alphabet and it enciphers based upon a 5×5 square constructed by means of a secret keyword or phrase.

In 25 squares arranged in 5 successive rows of 5 squares each, we insert the letters of the Latin alphabet (J excepted) by the following scheme. Given the key, which usually consists of a single word or short sentence, we start by filling the squares from left to right starting from the top row with the letters of the key, repetitions omitted. This done we fill in the rest of the squares with the unused letters of the alphabet (minus J of course). See the example below which is constructed for the case in which the key is PICKLE.

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

The text to be enciphered, is purged of all punctuation, spaces etc. leaving nothing but letters of the alphabet all capitalized. (Numbers are spelled out in words). Moreover all J's are converted into I's.

The final doctoring of the text consists of spitting it out in 2-grams, separated by spaces. It is of paramount importance for the scheme that there be no 2-grams consisting of two equal letters. Thus doubles are eliminated by inserting a Q whenever a repetition is about to be formed in the splitting process. Note that if the text has an odd number of letters after adding these Q's we add an extra letter at the end of the plaintext. For instance, the sentence

25 Mississippi Ave, Minneapolis

after step 3 is spitted out in the form:

TW OF IV EM IS SI SQ SI PQ PI AV EM IN NE AP OL IS

This done the final encipherment is obtained by converting each 2-gram into a new 2-gram by means of the PLAYFAIR square according to the following rules:

Whenever the two letters are in the same row, replace them by their immediate neighbours to the right, with the convention that the immediate neighbour "to the right" of the letter at the end of a row is the first letter of that same row. Thus the 2-gram SQ is replaced by tr, i.e.

$$\mathbf{SQ} \Rightarrow \mathbf{tr}$$

Whenever the two letters are in the same column, replace them by the letters immediately below them in the square, with the convention that the letter immediately below the bottom letter of a column is the first letter of that same column. For instance,

$$\mathbf{OF} \Rightarrow \mathbf{uo}$$

If the two letters are not in the same row or same column then locate the rectangle which has the two letters as diagonally opposite corners. Replace the two letters by the letters that are in the same row and opposite corners of that rectangle. For instance for the 2-gram TW the corners of the rectangle are (clockwise) T Y W R. Since R is in the same row as T and since Y is in the same row as W we have $\mathbf{T} \Rightarrow \mathbf{R}$ and $W \Rightarrow Y$. So the final replacement is

$$\mathbf{TW} \Rightarrow \mathbf{ry}$$

It is good to adopt the convention that encoded 2-grams are written in lower case letters, to distinguish them from 2-grams to be encoded. Using these rules the final encoding of the sentence

25 Mississippi Ave, Minneapolis

by the Playfair square resulting from the key PICKLE is

ry uo pw bg cr rc tr rc ev ic ew bg kh gd ei uf cr

Deciphering Playfair

In the decipherment process we are given the key and an enciphered message consisting of a sequence of lower case 2 grams and we are to reproduce the original message, all in upper case letters minus punctuation and spaces (i.e. in the form obtained after step 2 of the encipherment process.) Thus decipherment is done in three steps:

First,construct the PLAYFAIR square from the key. (As was indicated above).

Second, convert the sequence of lower case 2-grams into the sequence of upper case 2-grams obtained by reversing the coding operation described in step 4.

Finally, remove the extra Q's and take off the spaces. It should be taken account that in order to remove the extra Q's we must assume that in the original message there were no double Q's and Q was always followed by U. This is no serious restriction for English (or other Romance languages). **Example**: We will decipher the following cryptogram

ungah drudz upgdx klmsm vmhrl mlh

knowing that PLAYFAIR was used with keyword **HUNGARY**.

First, the PLAYFAIR square would be

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

Second, the cyphertext as converted into 2-grams would appear as

un ga hd ru dz up gd rk pq mz mv rm ml gs

Since u and n are in the same row, we replace them by the letters to their immediate left. Thus $u \Rightarrow H$ and $n \Rightarrow U$. Thus

$$un \Rightarrow HU.$$

The reader should check that for the same reason as above, we have

$$ga \Rightarrow NG.$$

Now, H and D are in different rows and columns. The rectangle with H and D as opposite corners would be H A D R. Since A is in the same row as H and since R is in the same row as D, we have that $h \Rightarrow A$ and $d \Rightarrow R$. Thus

$$hd \Rightarrow AR.$$

R and U are in different rows and columns. The rectangle containing R and U is R Y U H. Since Y is in the same row as R and since H is in the same row as U, we have $r \Rightarrow Y$ and $u \Rightarrow H$. Thus,

$$ru \Rightarrow YH.$$

The reader should check the remaining substitutions are correct:

dz	$\Rightarrow$	AS
up	$\Rightarrow$	NO
gd	$\Rightarrow$	AC
rk	$\Rightarrow$	CE
pq	$\Rightarrow$	SQ
mz	$\Rightarrow$	ST
mv	$\Rightarrow$	OT
rm	$\Rightarrow$	HE
ml	$\Rightarrow$	SE
gs	$\Rightarrow$	AQ

This leaves the following message

HU NG AR YH AS NO AC CE SQ ST OT HE SE AQ.

Removing the excess Q's and inserting spaces leaves

HUNGARY HAS NO ACCESS TO THE SEA

Exercises:

1. Decipher the following messages knowing that they were encrypted using Playfair with the given keyword .
   (a) **WQ GB PT BP NR PT FE** Keyword: *guest*
   (b) **MKORA KDKPF LITQR CSUBA HQPKF DTQRC SR** Keyword: *potato*

Hill Encipherment

In the Hill Encipherment, the key consists of the following ingredients:

1. The BLOCK SIZE: An integer k;
2. The HILL MATRIX: A is an $k \times k$ matrix of integers $0, 1, \ldots, 28$ whose determinant is relatively prime to 29.

We assume that the number of letters in the message is a multiple of k. This can be achieved by adding a few random English characters. This given, the encipherment proceeds as follows:

1. The plaintext is divided into blocks of k characters each.
2. The letters A through Z are replaced by the integers $0, 1, \ldots, 25$. Additionally, each period is replaced by 26, each exclamation point is replaced by 27 and each question mark is replaced by 28.

$$\begin{array}{cccccccccccccccccccccccccccc} \text{A} & \text{B} & \text{C} & \text{D} & \text{E} & \text{F} & \text{G} & \text{H} & \text{I} & \text{J} & \text{K} & \text{L} & \text{M} & \text{N} & \text{O} & \text{P} & \text{Q} & \text{R} & \text{S} & \text{T} & \text{U} & \text{V} & \text{W} & \text{X} & \text{Y} & \text{Z} & . & ! & ? \\ \Downarrow & \Downarrow \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 \end{array} \tag{1}$$

   This is done so that each block is replaced by a vector

$$X = (x_1, x_2, \ldots, x_k)$$

   where $0 \leq x_i \leq 28$.

3. Each block vector X is then replaced by its image Y under the transformation

$$Y = AX$$

   obtained by matrix multiplication in Z_{29} arithmetic.

4. This done the resulting vectors are replaced by the k-grams obtained by reversing the replacements given in (1).

Decription is done by reversing the process using the matrix A^{-1}, the inverse of A in (*mod* 29) arithmetic.

Example:
Let

$$A = \begin{pmatrix} 10 & 8 & 19 & 11 \\ 22 & 21 & 8 & 5 \\ 8 & 21 & 11 & 15 \\ 8 & 25 & 11 & 10 \end{pmatrix}$$

Suppose that we wanted to encipher the plaintext

Give peace a chance

We would need to break the plaintext up into 4-grams, namely

GIVE PEAC EACH ANCE

This corresponds to the list of 4-grams (written as column vectors)

$$\begin{pmatrix}6\\8\\21\\4\end{pmatrix},\begin{pmatrix}15\\4\\0\\2\end{pmatrix},\begin{pmatrix}4\\0\\2\\7\end{pmatrix},\begin{pmatrix}0\\13\\2\\4\end{pmatrix} \tag{2}$$

Multiplying each of the above vectors by A yields

$$\begin{pmatrix}16\\24\\14\\26\end{pmatrix},\begin{pmatrix}1\\18\\2\\8\end{pmatrix},\begin{pmatrix}10\\23\\14\\8\end{pmatrix},\begin{pmatrix}12\\19\\7\\10\end{pmatrix}$$

Finally, this is written as

QYO.BSCIKXOIMTHK

You should verify that the matrix

$$A^{-1}=\begin{pmatrix}6&15&27&15\\11&14&17&25\\18&13&3&4\\3&17&8&14\end{pmatrix}$$

is the inverse of A and then decipher the above message to see that we get the original plaintext.

Deciphering Hill

Notice that deciphering a Hill encrypted message requires computating the inverse matrix of A. The inverse matrix can only be computed if the determinant of A has a multiplicative inverse. For example, the general formula for the inverse of a 2×2 matrix is given by

$$A^{-1}=\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1}=\frac{1}{det(A)}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}=\frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}.$$

Ordinarily, this means that $det(A)$ must be nonzero, but when dealing with modular arithmetic modulo m, $1/det(A)$ makes sense only if $det(A)$ does not have any factors in common with m. In other words, $det(A)$ has a multiplicative inverse modulo m if and only if $det(A)$ and m are relatively prime.

This explains why in the previous section we worked modulo 29. As you can see in Table 1, if we had worked modulo 26, the numbers 2,4,6,8,10,12,13,14,16,18,20,22, and 24 do not have

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

Table 1: Multiplication Table mod 26

multiplicative inverses. If the $det(A)$ had been any one of these numbers, we would be unable to obtain the original plaintext meassage. Working modulo 29, we are much less likely to run into this problem because 29 is a prime number and therefore no numbers less than 29 have any factors in common with 29.

Example: Compute the inverse of the following matrix

$$A = \begin{pmatrix} 10 & 7 \\ 10 & 17 \end{pmatrix}.$$

Note that $det(A) \equiv 13 \bmod 29$, which is invertible. Using Table 2, we see that $13 \times 9 \equiv 1 \bmod 29$. This means that the multiplicative inverse of 13 mod 29 is 9 and therefore the matrix A is invertible. Using the above formula and Table 2, we see that

$$A^{-1} = \begin{pmatrix} 8 & 24 \\ 26 & 3 \end{pmatrix}.$$

	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	27	28
1	**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	27	28
2	2	4	6	8	10	12	14	16	18	20	22	24	26	28	**1**	3	5	7	9	11	13	15	17	19	21	23	25	27
3	3	6	9	12	15	18	21	24	27	**1**	4	7	10	13	16	19	22	25	28	2	5	8	11	14	17	20	23	26
4	4	8	12	16	20	24	28	3	7	11	15	19	23	27	2	6	10	14	18	22	26	**1**	5	9	13	17	21	25
5	5	10	15	20	25	**1**	6	11	16	21	26	2	7	12	17	22	27	3	8	13	18	23	28	4	9	14	19	24
6	6	12	18	24	**1**	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23
7	7	14	21	28	6	13	20	27	5	12	19	26	4	11	18	25	3	10	17	24	2	9	16	23	**1**	8	15	22
8	8	16	24	3	11	19	27	6	14	22	**1**	9	17	25	4	12	20	28	7	15	23	2	10	18	26	5	13	21
9	9	18	27	7	16	25	5	14	23	3	12	21	**1**	10	19	28	8	17	26	6	15	24	4	13	22	2	11	20
10	10	20	**1**	11	21	2	12	22	3	13	23	4	14	24	5	15	25	6	16	26	7	17	27	8	18	28	9	19
11	11	22	4	15	26	8	19	**1**	12	23	5	16	27	9	20	2	13	24	6	17	28	10	21	3	14	25	7	18
12	12	24	7	19	2	14	26	9	21	4	16	28	11	23	6	18	**1**	13	25	8	20	3	15	27	10	22	5	17
13	13	26	10	23	7	20	4	17	**1**	14	27	11	24	8	21	5	18	2	15	28	12	25	9	22	6	19	3	16
14	14	28	13	27	12	26	11	25	10	24	9	23	8	22	7	21	6	20	5	19	4	18	3	17	2	16	**1**	15
15	15	**1**	16	2	17	3	18	4	19	5	20	6	21	7	22	8	23	9	24	10	25	11	26	12	27	13	28	14
16	16	3	19	6	22	9	25	12	28	15	2	18	5	21	8	24	11	27	14	**1**	17	4	20	7	23	10	26	13
17	17	5	22	10	27	15	3	20	8	25	13	**1**	18	6	23	11	28	16	4	21	9	26	14	2	19	7	24	12
18	18	7	25	14	3	21	10	28	17	6	24	13	2	20	9	27	16	5	23	12	**1**	19	8	26	15	4	22	11
19	19	9	28	18	8	27	17	7	26	16	6	25	15	5	24	14	4	23	13	3	22	12	2	21	11	**1**	20	10
20	20	11	2	22	13	4	24	15	6	26	17	8	28	19	10	**1**	21	12	3	23	14	5	25	16	7	27	18	9
21	21	13	5	26	18	10	2	23	15	7	28	20	12	4	25	17	9	**1**	22	14	6	27	19	11	3	24	16	8
22	22	15	8	**1**	23	16	9	2	24	17	10	3	25	18	11	4	26	19	12	5	27	20	13	6	28	21	14	7
23	23	17	11	5	28	22	16	10	4	27	21	15	9	3	26	20	14	8	2	25	19	13	7	**1**	24	18	12	6
24	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	**1**	25	20	15	10	5
25	25	21	17	13	9	5	**1**	26	22	18	14	10	6	2	27	23	19	15	11	7	3	28	24	20	16	12	8	4
26	26	23	20	17	14	11	8	5	2	28	25	22	19	16	13	10	7	4	**1**	27	24	21	18	15	12	9	6	3
27	27	25	23	21	19	17	15	13	11	9	7	5	3	**1**	28	26	24	22	20	18	16	14	12	10	8	6	4	2
28	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	**1**

Table 2: Multiplication Table mod 29

We can verify this by checking that the product of A and A^{-1} yields the identity matrix.

$$\begin{aligned}\begin{pmatrix}10 & 7\\ 10 & 17\end{pmatrix}\begin{pmatrix}8 & 24\\ 26 & 3\end{pmatrix} &= \begin{pmatrix}10\cdot 8+7\cdot 26 & 10\cdot 24+7\cdot 3\\ 10\cdot 8+17\cdot 26 & 10\cdot 24+17\cdot 3\end{pmatrix}\\ &\equiv \begin{pmatrix}22+8 & 8+21\\ 22+7 & 8+22\end{pmatrix} \bmod 29\\ &\equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \bmod 29\end{aligned}$$

Exercises:

1. Construct the multiplication tables for $\mathbb{Z}_6$ and $\mathbb{Z}_9$.
2. Solve the following two equations and two unknowns over $\mathbb{Z}_{26}$ if possible

$$\begin{aligned}2x+5y &\equiv 11\\ 4x+3y &\equiv 1\end{aligned}$$

3. Solve the following two equations and two unknowns over $\mathbb{Z}_{26}$ if possible

$$2x + y \equiv 5$$
$$x + 2y \equiv 4$$

4. Solve the following two equations and two unknowns over $\mathbb{Z}_{26}$ if possible

$$2x + 5y \equiv 9$$
$$4x + 3y \equiv 2$$

5. Invert the following matrices over $\mathbb{Z}_{26}$ if possible

(a) $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 11 & 4 \\ 2 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} 3 & 2 \\ 3 & 5 \end{pmatrix}$

6. Verify that if $1 \equiv aei - afh - bdi + bfg + cdh - ceg \ mod\ 29$ then,

$$\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^{-1} = \begin{pmatrix} ie - fh & ch - bi & bf - ce \\ fg - di & ai - cg & cd - af \\ dh - ge & bg - ah & ae - bd \end{pmatrix} \ mod\ 29.$$

7. Decipher the following messages that were encrypted with the given matrix A.

(a) Ciphertext: **IGAW** $A = \begin{pmatrix} 2 & 5 \\ 21 & 9 \end{pmatrix}$ mod 26

(b) Ciphertext: **DGKUKU** $A = \begin{pmatrix} 3 & 12 \\ 6 & 25 \end{pmatrix}$ mod 29

8. Recover the plaintext from the ciphertext **FVGLNPCJSG** given that it was encrypted using the Hill encipherment system with a 2×2 matrix *mod* 29 and the plaintext begins with the letters *tell* .

The ADFGVX System

The *ADFGVX* cipher system consists of two keys:

k_1: A square consisting of 6 rows and 6 columns. The rows and columns are labeled from top to bottom and left to right by A, D, F, G, V and X respectively. Inside the square we randomly fill the cells with the letters from the alphabet $\{A, B, C, \ldots, Z\}$ and the numbers $\{O, 1, 2, \ldots, 9\}$.

k_2: A permutation of n (where n is an even positive integer).

We will show how to use this cipher by encrypting the following message:

HQ requests front line situation by telegram. –HQ 7th Corp

Let us suppose that our key k_1 is

	A	D	F	G	V	X
A	C	O	8	X	F	4
D	M	K	3	A	Z	9
F	N	W	L	0	J	D
G	5	S	I	Y	H	U
V	P	1	V	B	6	R
X	E	Q	7	T	2	G

and that k_2 is a permutation of 20, namely

4 9 5 15 2 8 16 12 13 17 1 18 3 19 10 7 6 11 14 20

Our first step, as in rectangular transposition, is to write the plaintext in a rectangle. The number of columns in general is taken to be $n/2$. If necessary, we fill any empty cells in the bottom row with random letters. In this case, we get the following 5×10 array:

H	Q	R	E	Q	U	E	S	T	S
F	R	O	N	T	L	I	N	E	S
I	T	U	A	T	I	O	N	B	Y
T	E	L	E	G	R	A	M	H	Q
7	T	H	C	O	R	P	S	E	D

Note that we had to add 2 extra letters at the bottom, which we choose randomly to be E and D.

The next step is to place on top of each plaintext letter the pair of letters which give its *coordinates* in the ADFGVX square. For instance, the first letter of plaintext is H, which is in the G-row and V-column of the ADFGVX square. Thus we must place GV on top of H. Let us indicate this by writing

G V
H

The next letter is Q, which is in the X-row and the D-column. This gives

X D
Q

Similarly, we get

V X X A
R ' E ",...

After we carry this out for each plaintext letter, we label the columns occupied by the new letters by the entries permutation k_2. Our final product is then the following array:

4 9	5 15	2 8	16 12	13 17	1 18	3 19	10 7	6 11	14 20
G V H	X D Q	V X R	X A E	X D Q	G X U	X A E	G D S	X G T	G D S
A V F	V X R	A D O	F A N	X G T	F F L	G F I	F A N	X A E	G D S
G F I	X G T	G X U	D G A	X G T	G F I	A D O	F A N	V G B	G G Y
X G T	X A E	F F L	X A E	V V G	V X R	D G A	D A M	G V H	X D Q
X F 7	X G T	G V H	A A C	A D O	V X R	V A P	G D S	X A E	F X D

This given, our ciphertext is obtained by reading the columns in the order given by our permutation k_2. In this case, the column labelled 1 has the letters (reading from top to bottom) *GFGVV*. The column with the 2 has *VAGFG*, etc. We now write the *word* we obtain from the column 1, then the word from column 2, etc. In our example, we would get

GFGVV VAGFG XGADV GAGXX XVXXX XXVGX DAAAD XDXFV VVFGF GFFDG
GAGVA AAGAA XXXVA GGGXF DXGAG XFDXA DGGVD XFFXX AFDGA DDGDX

Exercises:

1. Decipher the following message

GXGDVD AFAAFD DAAAFA AFGAGD GADAAA
DVGVAG GADVVG AXFGDF FFGGFD AVFGGX

knowing that it was encrypted with the following permutation and partially completed square.

5 7 9 8 2 1 4 10 3 6

B	**L**			**S**	
		C			**G**
H	**I**	**J**	**M**	**N**	**O**
		R	**T**	**V**	**W**
X	**Z**		**1**	**2**	**3**

The Vernam Two Tape System

In an early (1926) paper on secret communication by wire and telegraph G. S. Vernam proposed an encryption system based on a pseudo random one time pad. The pad itself was to be constructed from two relatively short random keys.

More precisely, the Vernam system can be described as follows:

1. We have two key sequences
$$U = (u_1, u_2, \ldots, u_p)$$
and
$$V = (v_1, v_2, \ldots, v_q)$$
of 0's and 1's of lengths p and q respectively, where p and q are chosen relatively prime .

2. These sequences are then extended to arbitrary length by setting
$$\begin{aligned} u_{i+p} &= u_i \\ v_{i+q} &= v_i \end{aligned}$$
that is, the extended U and V are made periodic of periods p and q respectively.

3. A long sequence R
$$R = (r_1, r_2, ..., r_n, ...)$$
is then constructed by setting
$$r_i = u_i + v_i \pmod 2 \tag{1}$$
It can be shown that the sequence R will be of period no longer than pq. Moreover, if U and V are randomly selected then with very high probability the period will be exactly pq. For instance for $p = 63$ and $q = 71$ the sequence R can be made to have period 4473. Thus we can see that a long non-repeating sequence can be produced by two quite short sequences. This fact suggested to Vernam that such a sequence as R could replace the random sequences used as one-time pads in a perfect secrecy system.

4. Once R has been constructed, a (0,1)-plaintext message
$$X = (x_1, x_2, \ldots, x_{pq})$$
is encrypted into the cyphertext
$$Y = (y_1, y_2, \ldots, y_{pq})$$
by setting
$$y_i = x_i + r_i \pmod 2 \tag{2}$$

5. The receiver, given the keys U,V calculates the r_i by means of (1) and recovers the original message from the formula
$$\begin{aligned} x_i &= y_i - r_i \\ &\cong y_i + r_i (\text{mod } 2) \end{aligned}$$

Example: Suppose that

$$\begin{aligned} U &= (0,1,0) \\ V &= (1,1,0,1,0) \end{aligned}$$

thus $p = 3$ and $q = 5$. Thus

$$R = (1,0,0,1,1,1,1,1,1,0,0,1,0,0,0).$$

The *message*

$$X = (1,1,0,0,1,1,0,1,1,1,0,0,1,0,1)$$

would be encrytped as

$$Y = (0,1,0,1,0,0,1,0,0,1,0,1,1,0,1).$$

Notice that with no additional effort we can proceed under the assumption that the characters used in U,V,X and Y, are the integers in [0,m-1] and all operations are carried out modulo m.

Example:

The following table summarizes this process applied to the plaintext message

Four score and seven years ago

with keys $\{5,18,3\}$ and $\{7,11,21,2,9\}$. All operations will be performed modulo 26 and the letters A through Z will be replaced by the numbers 0 through 25 in the usual manner.

plaintext	**F**	**O**	**U**	**R**	**S**	**C**	**O**	**R**	**E**	**A**	**N**	**D**	**S**	**E**	**V**	**E**	**N**	**Y**	**E**	**A**	**R**	**S**	**A**	**G**	**O**
	5	14	20	17	18	2	14	17	4	0	13	3	18	4	21	4	13	24	4	0	17	18	0	6	14
U	5	18	3	5	18	3	5	18	3	5	18	3	5	18	3	5	18	3	5	18	3	5	18	3	5
V	7	11	21	2	9	7	11	21	2	9	7	11	21	2	9	7	11	21	2	9	7	11	21	2	9
R	12	3	24	7	1	10	16	13	5	14	25	14	0	20	12	12	3	24	7	1	10	16	13	5	14
	17	17	18	24	19	12	4	4	9	14	12	17	18	24	7	16	16	22	11	1	1	8	13	11	2
ciphertext	**R**	**R**	**S**	**Y**	**T**	**M**	**E**	**E**	**J**	**O**	**M**	**R**	**S**	**Y**	**H**	**Q**	**Q**	**W**	**L**	**B**	**B**	**I**	**N**	**L**	**C**

Exercises:

1. Encrypt the following message using the keys $(11,9,8,17)$ and $(19,2,8,23,1)$

   Help, I've fallen and I can't get up.

2. Decipher the following message knowing that it was encrypted using the keys $(9,5,6)$ and $(11,2,17,21)$

   AVXLU IDMRV ANSKX C