UMAP

Modules in Undergraduate Mathematics and Its Applications

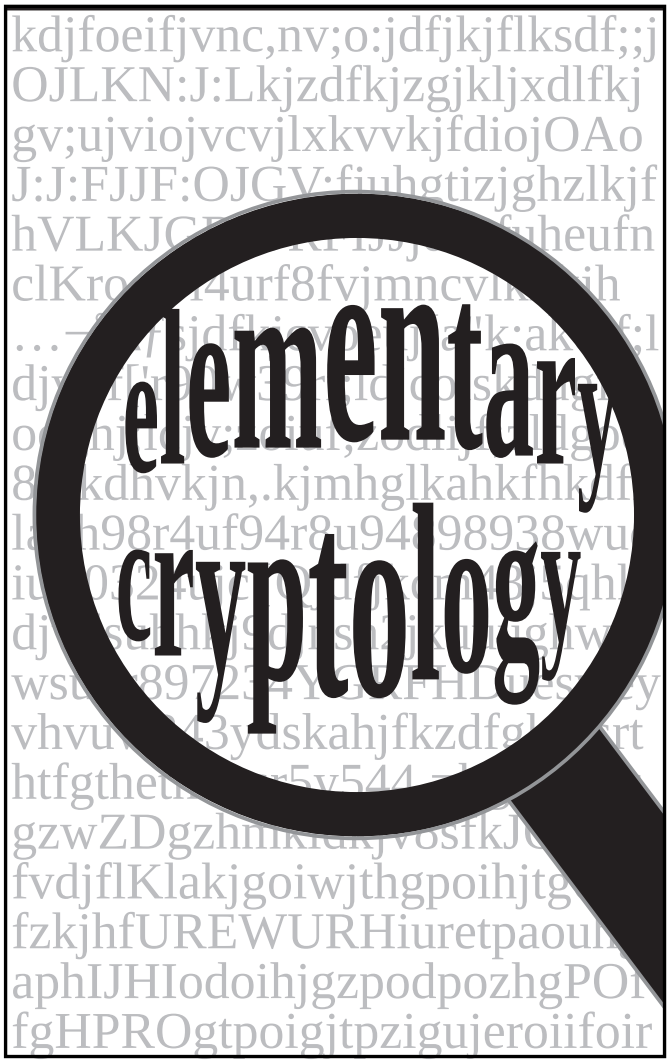
Published in cooperation with the Society for Industrial and Applied Mathematics, the Mathematical Association of America, the National Council of Teachers of Mathematics, the American Mathematical Association of Two-Year Colleges, The Institute of Management Sciences, and the American Statistical Association.

COMAP

Module 733

Elementary Cryptology

Joe F. Wampler



Applications of Matrix Algebra and Probability to Cryptology

COMAP, Inc., Suite 210, 57 Bedford Street, Lexington, MA 02420 (781) 862–7878

INTERMODULAR DESCRIPTION SHEET: UMAP Unit 733

TITLE: Elementary Cryptology

AUTHOR: Joe F. Wampler
Prof. Emeritus of Mathematics
Nebraska Wesleyan University
5000 Saint Paul Ave.
Lincoln, NE 68504–2371

MATHEMATICAL FIELD: Matrix algebra, elementary probability

APPLICATION FIELD: Cryptology

TARGET AUDIENCE: Students in a course in matrix algebra, linear algebra, or finite mathematics.

ABSTRACT: We discuss a few of the methods used in earlier times to illustrate the nature of cryptology, then discuss briefly some of the more current developments in the field. Topics covered include substitution ciphers, affine transformations, polygraphic ciphers, and public-key cryptography.

PREREQUISITES: Familiarity with matrix arithmetic.

This work appeared in *UMAP Modules: Tools for Teaching 1993*, edited by Paul J. Campbell, 111–140. Lexington, MA: COMAP, 1994.

COMAP, Inc., Suite 210, 57 Bedford Street, Lexington, MA 02173
(800) 77-COMAP = (800) 772-6627, or (781) 862-7878; http://www.comap.com

Elementary Cryptology

Joe F. Wampler
Prof. Emeritus of Mathematics
Nebraska Wesleyan University
5000 Saint Paul Ave.
Lincoln, NE 68504–2371

Table of Contents

MODULES AND MONOGRAPHS IN UNDERGRADUATE
MATHEMATICS AND ITS APPLICATIONS (UMAP) PROJECT

The goal of UMAP is to develop, through a community of users and developers, a system of instructional modules in undergraduate mathematics and its applications, to be used to supplement existing courses and from which complete courses may eventually be built.

The Project was guided by a National Advisory Board of mathematicians, scientists, and educators. UMAP was funded by a grant from the National Science Foundation and now is supported by the Consortium for Mathematics and Its Applications (COMAP), Inc., a nonprofit corporation engaged in research and development in mathematics education.

Paul J. Campbell — Editor
Solomon Garfunkel — Executive Director, COMAP

1. Introduction

Cryptology has been defined as the science of making communications unintelligible to all except authorized parties. The study consists of

- *cryptography* (Gr., *kryptos*–hidden, *graphein*–to write), which deals with the design of the secrecy systems, and
- *cryptanalysis*, which deals with the breaking of the secrecy systems.

Cryptology can be traced back to the Egyptians and continues to be used today to a larger extent than most of us realize. We most commonly think of its use in the work of secret agents or for military purposes. However, now that computers are prevalent, it is important to businesses to be able to protect the information stored in their computers, and to be able to communicate information within and between companies without revealing the contents to competitors. The widespread use of electronic funds transfers has made privacy a pressing concern in most financial transactions.

In this Module, we will discuss a few of the methods used in earlier times to illustrate the nature of cryptology, then discuss briefly some of the more current developments in the field.

2. Substitution Ciphers

Before proceeding, we need some terminology for the subject. The *plaintext* is the message that is to be put into secret form. The *cipher* is the method for changing the plaintext, and the *ciphertext* is the secret version of the plaintext. To *encipher* is to change from plaintext to ciphertext. The reverse process of changing from ciphertext to plaintext when one knows the cipher is called *deciphering*. A piece of information called a *key* is used to encipher the plaintext and also to decipher the ciphertext.

One of the easiest and most familiar ciphers is the *substitution cipher*. Here each letter of the alphabet is represented by some other letter. The correspondence may be random or systematic. In fact, 26! substitution ciphers are possible.

The *Caesar cipher*, used by Julius Caesar around 50 B.C., is an example of a systematic substitution cipher. Each letter of the alphabet is associated with the third letter following it; for example, `A` is associated with `D`, `B` with `E`, . . . , `W` with `Z`, `X` with `A`, `Y` with `B`, and `Z` with `C`. If the letters of the alphabet are numbered from 1 to 26, the Caesar cipher may be represented in the following way. If we let p stand for the number assigned to a plaintext letter and c the number assigned to the corresponding ciphertext letter, we have the following relation:

$$c \equiv p + 3 \pmod{26}.$$

If $c \equiv 0 \equiv 26 \pmod{26}$, we will assign to c the letter Z. To decipher a message enciphered in the Caesar cipher, we simply use the key or solve for p in the congruence

$$c \equiv p + 3 \pmod{26},$$

which gives the formula $p \equiv (c - 3) \pmod{26}$.

Nothing is magical about the number 3 as the shift factor in the Caesar cipher. More generally, a cipher can be given by the formula

$$c \equiv p + k \pmod{26},$$

where $1 \leq k \leq 25$. These ciphers are called *shift transformations*, and k is called the *shift factor*.

As an example, suppose we use the formula

$$c \equiv p + 5 \pmod{26};$$

thus, the key is given in **Table 1**.

Table 1.
An example of a shift transformation.

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

If the plaintext message is

MEETING IN MY OFFICE AT NOON,

the ciphertext message will appear as follows (to confuse someone trying to break the cipher, the ciphertext is usually grouped in blocks of 5):

RJJYN SLNSR DTKKN HJFYS TTS.

Consider the following secret message:

WKLVY HULIL HVWKH RUGHU BRXJD YHPHD WWKHP HHWLQ JLQPB RIILF H.

If we know that a shift transformation was used to encipher this message, how can we decipher the message? We need only determine the value of k in the equation

$$c \equiv p + k \pmod{26}.$$

One way, which can become tedious, is to simply try every value of k from 1 to 25 in the equation $p \equiv (c - k) \pmod{26}$ until something intelligible occurs. For example, in the secret message given above, consider the first block:

	W	K	L	V	Y
$k = 1$:	V	J	K	U	X
$k = 2$:	U	I	J	T	W
$k = 3$:	T	H	I	S	V

This last value of k seems to make sense, so we try letting $k = 3$ and $p \equiv (c - 3) \pmod{26}$ and decipher the message.

Another way is to utilize the frequency with which certain letters appear in the English language. Several such counts have been published; one is suggested by Konheim [1981], and one by Sinkov [1966]. The author of this UMAP Module made such a count of 989 letters appearing in a newspaper editorial and arrived at the relative frequency distribution in **Table 2**.

Table 2.

Table of Relative Frequencies in Plaintext.

E	.123	H	.069	L	.039	B	.020	V	.007	Z	.000
T	.099	N	.069	M	.032	U	.020	J	.004		
A	.087	S	.062	C	.028	Y	.013	K	.004		
O	.076	R	.046	W	.028	F	.012	Q	.002		
I	.075	D	.039	G	.021	P	.012	X	.001		

In the secret message given above, the most frequently occurring letter is H. Since in the English language E occurs with the greatest frequency, it seems logical to assume that in the ciphertext H corresponds to E. Since H is the eighth letter of the alphabet and E is the fifth, we might try the relation $8 \equiv 5 + k \pmod{26}$, that is, $k = 3$. Now, if $c \equiv (p + 3) \pmod{26}$, then $p \equiv (c - 3) \pmod{26}$; and if we consider the first block of the ciphertext, we find

W: $p \equiv 23 - 3 \equiv 20 \pmod{26}$, so W corresponds to T;
K: $p \equiv 11 - 3 \equiv 8 \pmod{26}$, so K corresponds to H;
L: $p \equiv 12 - 3 \equiv 9 \pmod{26}$, so L corresponds to I;
V: $p \equiv 22 - 3 \equiv 19 \pmod{26}$, so V corresponds to S.

This correspondence produces a sensible word, so we continue this deciphering and obtain the plaintext message:

THISV ERIFI ESTHE ORDER YOUGA VEMEA TTHEM EETIN GINMY OFFIC E.

3. Affine Transformations

At this point, we can see the need to be trickier to protect messages. A variation of the shift transformation is the *affine (or linear) transformation*, which is defined by the equation

$$c \equiv ap + b \pmod{26}.$$

The natural number a must be relatively prime to 26; otherwise, duplication of letters occurs. Since there are 12 possible values of a (namely, 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, and 25), and 26 possible values of b for each of these values of a, the total number of possible affine transformations is $12 \times 26 = 312$.

The formula to decipher such a transformation is found by solving the equation $c \equiv (ap + b) \pmod{26}$ for p. Thus,

$$ap \equiv c - b \pmod{26},$$

and if we multiply both sides of the congruence by the inverse of a, that is a value a' such that $a'a \equiv 1 \pmod{26}$, we get

$$p \equiv a'(c - b) \pmod{26}.$$

Now the limitation on the value of a is more obvious, since there will exist an a', or inverse of a, only if a and 26 are relatively prime. For example, if $c \equiv 3p + 5 \pmod{26}$, then

$$3p \equiv c - 5 \pmod{26},$$

and since $3(9) \equiv 1 \pmod{26}$, we get

$$p \equiv 9(c - 5) \pmod{26},$$

the deciphering formula.

In shift transformations, successive plaintext letters go to successive ciphertext letters. For the affine transformation, a gap occurs: successive plaintext letters go to ciphertext letters that are a units apart. For example, under the Caesar cipher, the successive plaintext letters `A` and `B` are sent to the successive ciphertext letters `D` and `E`. Under the affine transformation

$$c \equiv 3p + 5 \pmod{26},$$

successive letters `A` and `B` go to `H` and `K`, which are three units apart.

Suppose we are told that the following secret message was enciphered using an affine transformation. Let us attempt to decipher the message:

```
VQHIB  TBUYX  ZDRZE  VBTZG  YQOBB  TBYTZ  GEKHU  TVUYQ
VTPZO  UVULT  PHVKW  ZXZDY  QVUFV  RZDKW  RZDUY  ZUHUB
HOKXO  BTEZU  TBHTY  ZNQVR  QNHXN  BPVLQ  YWBRV  WBYZL  Z
```

If we first make a frequency count of the letters appearing in the ciphertext, we find that `Z` occurs 14 times, `B` 12 times, `V` 11 times, `U` 10 times, `T` 10 times, and `Y` occurs 9 times. All other letters occur fewer times than these. We may use the same procedure as before when deciphering a shift transformation, but with some additional difficulty. For example, if we assume that the most common letters in the ciphertext correspond to the most common letters in the English

alphabet, we could try the correspondence of Z to E and B to T. This would lead us to the two congruences

$$26 \equiv 5a + b \pmod{26}$$

and

$$2 \equiv 20a + b \pmod{26}.$$

Subtracting, we would obtain

$$24 \equiv -15a \pmod{26},$$

which is equivalent to

$$11a \equiv 24 \pmod{26}.$$

Since the inverse of 11 is 19,

$$a \equiv 19(24)14 \pmod{26}.$$

However, we saw that a must be relatively prime to 26, and $a = 14$ does not satisfy this requirement.

If we were to try another assignment, letting B correspond to E and V correspond to T, this would lead to the congruences

$$2 \equiv 5a + b \pmod{26}$$

and

$$22 \equiv 20a + b \pmod{26}.$$

Subtracting yields $20 \equiv 15a \pmod{26}$. Since the inverse of 15 is 7, $a \equiv 7(20) \equiv 10 \pmod{26}$. Again, 10 is not relatively prime to 26. Continuing in this manner, we may try letting B correspond to E and Y correspond to T. This would yield the congruences

$$2 \equiv 5a + b \pmod{26}$$

and

$$25 \equiv 20a + b \pmod{26}.$$

Subtracting, $23 \equiv 15a \pmod{26}$, and since the inverse of 15 is 7, $a \equiv 7(23) \equiv 5 \pmod{26}$. Substituting this value in the first of the congruences, $b \equiv 2 - 5(5) \equiv 3 \pmod{26}$. These values suggest the enciphering formula

$$c \equiv 5p + 3 \pmod{26}.$$

If this formula were used to encipher the message, the deciphering formula would be found by solving this equation for p, that is,

$$5p \equiv c - 3 \pmod{26}.$$

But since the inverse of 5 is 21, $p \equiv 21(c - 3) \pmod{26}$.

If we try this deciphering formula on the first block of the message, we get

V:	$p \equiv 21(22-3)$	$\equiv$	$9 \pmod{26}$,	so V corresponds to I;
Q:	$p \equiv 21(17-3)$	$\equiv$	$8 \pmod{26}$,	so Q corresponds to H;
H:	$p \equiv 21(8-3)$	$\equiv$	$1 \pmod{26}$,	so H corresponds to A;
I:	$p \equiv 21(9-3)$	$\equiv$	$22 \pmod{26}$,	so I corresponds to V;
B:	$p \equiv 21(2-3)$	$\equiv$	$5 \pmod{26}$,	so B corresponds to E.

This method seems to give a meaningful deciphering, so continuing, the entire message will read

```
IHAVE  SENTY  OUCOP  IESOF  THREE  SETSO  FPLAN  SINTH
ISMOR  NINGS  MAILD  OYOUT  HINKI  COULD  COUNT  ONANE
ARLYR  ESPON  SEAST  OWHIC  HWEMI  GHTDE  CIDET  OGO
```

There are other methods of deciphering a message for which an affine transformation was used; these use the fact that the gap between consecutive letters is the constant number a. When relative frequencies are used, it may also be more convenient to use relative frequencies of combinations of letters that occur in the English language.

4. Polygraphic Systems

In the preceding, we have indicated how a substitution cipher can be solved. Even if the original word lengths are concealed and the substitution alphabet is random, it is possible to find a solution by using frequency data, repetition patterns, and information about the ways that letters combine with one another. What makes the solution possible is the fact that a given plain-language letter is always represented by the same cipher letter. As a consequence, all the properties of plain language such as frequencies and combinations are carried over into the cipher and may be used for solution.

Perhaps the way for the cryptographer to prevent the cryptanalyst's successes with letter frequencies might be to make the unit of encipherment a *group* of letters instead of just one. A system of cryptography in which a group of n plaintext letters is replaced as a unit by a group of n cipher letters is called a *polygraphic system*. The use of such a system permits the frequencies to be "scrambled," that is, allowing for numerous representations of the same character within a cipher.

In the simplest case, $n = 2$, the system is called *digraphic*. Each pair of plaintext letters is replaced by a cipher digraph. From a mathematical point of view, a specially interesting type of polygraphic system was described by Hill [1931]. The fundamental notion used is that of linear transformation on n variables. To simplify the exposition, we shall choose $n = 2$, so our system will be digraphic. (Larger values of n will be discussed later.)

As before, we will use a letter-to-number correspondence to permit us to replace each letter by a number corresponding to its position in the normal

alphabet. We will use 29 symbols, rather than the 26 letters of the alphabet, for two reasons:

- it will be convenient to have a symbol for a space, and possibly other punctuation; and
- we will later find it convenient to have a prime number of symbols.

The numerical correspondence will be as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	3	14	15

P	Q	R	S	T	U	V	W	X	Y	Z		?	!
16	17	18	19	20	21	22	23	24	25	26	27	28	29

The encipherment procedure takes two successive plain text letters p_1 and p_2 at a time and substitutes them (their numerical equivalents) into a pair of congruences modulo 29 of the form

$$\begin{aligned} c_1 &\equiv ap_1 + bp_2 \pmod{29} \\ c_2 &\equiv cp_1 + dp_2 \pmod{29}, \end{aligned}$$

thus determining the cipher equivalent c_1c_2 of the plaintext digraph. This process is continued, digraph by digraph, until the entire message has been enciphered.

To illustrate the enciphering procedure, let us choose the values of a, b, c, and d so that the congruences are

$$\begin{aligned} c_1 &\equiv 7p_1 + 9p_2 \pmod{29} \\ c_2 &\equiv 3p_1 + 12p_2 \pmod{29}. \end{aligned}$$

Suppose the message to be enciphered is:

PREPARE TO EVACUATE AT ONCE!

Then the first digraph to be enciphered is PR,

$$p_1 = 16, \qquad p_2 = 18,$$

and we have

$$\begin{aligned} c_1 &\equiv 7(16) + 9(18) \equiv 274 \pmod{29} \\ c_2 &\equiv 3(16) + 12(18) \equiv 264 \pmod{29}. \end{aligned}$$

These numbers cannot be directly converted to letters, so they are reduced to their least residues modulo 29. Since $274 \equiv 13 \pmod{29}$ and $264 \equiv 3 \pmod{29}$, we find that c_1 is the letter M and c_2 is the letter C.

The second digraph to be enciphered is EP, and the encipherment can be accomplished in the same manner; however the process can be carried out in a more convenient manner using matrix multiplication as follows:

$$\begin{bmatrix} 7 & 9 \\ 3 & 12 \end{bmatrix} \cdot \begin{bmatrix} 16 \\ 18 \end{bmatrix} = \begin{bmatrix} 274 \\ 264 \end{bmatrix} = \begin{bmatrix} 13 \\ 3 \end{bmatrix} \longrightarrow \begin{matrix} \texttt{M} \\ \texttt{C} \end{matrix}$$

In the second digraph, E = 5, and P = 16, so

$$\begin{bmatrix} 7 & 9 \\ 3 & 12 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 16 \end{bmatrix} = \begin{bmatrix} 179 \\ 207 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \end{bmatrix} \longrightarrow \begin{matrix} \texttt{E} \\ \texttt{D} \end{matrix}$$

Continuing in this way, the ciphertext becomes:

MCEDXPQTNHBYRTG!MKQTMKE!ITFO

As mentioned earlier, larger values of n may be used, making deciphering by unauthorized persons even more difficult. As an example of $n = 3$ (*trigraphic system*), let the coding matrix be given by

$$M = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 4 & 7 \\ 2 & 3 & 6 \end{bmatrix},$$

and encipher the plaintext word ADD. The numerical equivalents are 1, 4, and 4. We then premultiply the column vector

$$\begin{bmatrix} 1 \\ 4 \\ 4 \end{bmatrix}$$

by the matrix M:

$$\begin{bmatrix} 0 & 2 & 3 \\ 1 & 4 & 7 \\ 2 & 3 & 6 \end{bmatrix} \begin{bmatrix} 1 \\ 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 20 \\ 45 \\ 38 \end{bmatrix}.$$

The last two numbers cannot be directly converted to letters, so they are reduced to their least residues modulo 29. Thus,

$$\begin{bmatrix} 20 \\ 45 \\ 38 \end{bmatrix} \equiv \begin{bmatrix} 20 \\ 16 \\ 9 \end{bmatrix} \pmod{29},$$

and the word ADD is enciphered into TPI. Notice that the D converts to P in one case and into I in the other, disrupting the possibility of frequency analysis.

Using the same enciphering scheme as above, let us illustrate how matrix notation can be used to encipher the plaintext message, UNITED NATIONS. The numerical equivalents are as follows:

U	N	I	T	E	D		N	A	T	I	O	N	S
21	14	9	20	5	4	27	14	1	20	9	15	14	19

Notice that since $n = 3$, the number of characters must be a multiple of 3; therefore, the message may need to be padded with the introduction of extra blanks so that the number of characters is a multiple of 3. For our message, we need to add one extra blank, coded by 27 and underlined below, as we enter the numerical equivalents in columns into a matrix:

$$\begin{bmatrix} 0 & 2 & 3 \\ 1 & 4 & 7 \\ 2 & 3 & 6 \end{bmatrix} \begin{bmatrix} 21 & 20 & 27 & 20 & 14 \\ 14 & 5 & 14 & 9 & 19 \\ 9 & 4 & 1 & 15 & \underline{27} \end{bmatrix} = \begin{bmatrix} 55 & 22 & 31 & 63 & 119 \\ 140 & 68 & 90 & 161 & 279 \\ 138 & 79 & 102 & 157 & 247 \end{bmatrix}.$$

Replacing each of the numbers in the last matrix with their residues modulo 29 gives the matrix

$$\begin{bmatrix} 26 & 22 & 2 & 5 & 3 \\ 24 & 10 & 3 & 16 & 18 \\ 22 & 21 & 15 & 12 & 15 \end{bmatrix} = \begin{bmatrix} \mathtt{Z} & \mathtt{V} & \mathtt{B} & \mathtt{E} & \mathtt{C} \\ \mathtt{X} & \mathtt{J} & \mathtt{C} & \mathtt{P} & \mathtt{R} \\ \mathtt{V} & \mathtt{U} & \mathtt{O} & \mathtt{L} & \mathtt{O} \end{bmatrix}.$$

Thus, the ciphertext for this message is ZXVVJUBCOEPLCRO.

To illustrate the method of deciphering a ciphertext that has used this system, let us consider just the first block of three letters, Z, X, and V. The numerical equivalents are 26, 24, and 22. To decipher this block, we need to find numbers x, y, and z such that

$$M \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 26 \\ 24 \\ 22 \end{bmatrix}.$$

We could solve the resulting system of equations

$$\begin{aligned} p_1 = 0x &+ 2y + 3z \equiv 26 \pmod{29} \\ p_2 = 1x &+ 4y + 7z \equiv 24 \pmod{29} \\ p_3 = 2x &+ 3y + 6z \equiv 22 \pmod{29}; \end{aligned}$$

but since the message will normally be much longer than three characters, it is more economical to first find the inverse of M, the enciphering matrix, and premultiply by this inverse M^{-1}. The inverse of M can be found by using the Gauss-Jordan elimination method, and in this example we have

$$M^{-1} = \begin{bmatrix} 3 & -3 & 2 \\ 8 & -6 & 3 \\ -5 & 4 & -2 \end{bmatrix}.$$

Using the enciphering matrix given above, namely

$$M = \begin{bmatrix} 0 & 2 & 3 \\ 1 & 4 & 7 \\ 2 & 3 & 6 \end{bmatrix},$$

let us decipher the following ciphertext:

```
WUUF!VNSOWVKLMHURLQHKWKI
```

Assigning numerical values to just the first 12 characters

W	U	U	F	!	V	N	S	O	W	V	K
23	21	21	6	29	22	14	19	15	23	22	11

and using the inverse of M found previously, we get

$$\begin{bmatrix} 3 & -3 & 2 \\ 8 & -6 & 3 \\ -5 & 4 & -2 \end{bmatrix} \begin{bmatrix} 23 & 6 & 14 & 23 \\ 21 & 29 & 19 & 22 \\ 21 & 22 & 15 & 11 \end{bmatrix} = \begin{bmatrix} 48 & -25 & 15 & 25 \\ 121 & -60 & 43 & 85 \\ -73 & 42 & -24 & -49 \end{bmatrix}.$$

Reducing the entries modulo 29 in the product yields

$$\begin{bmatrix} 19 & 4 & 15 & 25 \\ 5 & 27 & 14 & 27 \\ 14 & 13 & 5 & 9 \end{bmatrix}.$$

Continuing in this manner, the complete message is deciphered as

```
SEND MONEY IMMEDIATELY!
```

If the reader would like to try deciphering a secret message, suppose the secret encoding matrix is

$$\begin{bmatrix} 5 & 4 & 10 \\ 2 & 2 & 5 \\ 6 & 1 & 3 \end{bmatrix}.$$

Decipher the ciphertext:

```
HW FDIYYWDFB !GUIVOGKOTTZFCJYYKJ SILQ?U
```

While we have used examples where $n = 2$ and $n = 3$, there is no reason why larger values of n cannot be used. In fact, to ensure the security of the system, there could be periodic changes not only in the elements of the enciphering matrix but also in the dimensions of the enciphering matrix. The elements of the enciphering matrix and its inverse must be integers; such matrices are not always easy to find, and the following discussion shows how they may be constructed.

5. Integer Matrices

Theorem. *If A is an $n \times n$ matrix such that $\det(A) = 1$ and all of its elements are integers, then too all of the elements of A^{-1} are integers.* [Anton 1994, 104–107]

One way to generate such a matrix is to place all 1s down the diagonal, all 0s in the upper triangle, and random integers in the lower triangle. Then using the rules for matrices, transform this matrix into one that still has the same value for the determinant (1) but has numbers other than 0 in the upper triangle. For example, start with

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & -1 & 1 \end{bmatrix}.$$

Note that $\det(A) = 1$.

Change this matrix, perhaps by multiplying the first column by -2 and adding to the second column; then multiply the first column by 3 and add to the third column:

$$\begin{bmatrix} 1 & -2 & 3 \\ 2 & -3 & 5 \\ 3 & -7 & 10 \end{bmatrix}.$$

Note that the determinant is still 1.

The inverse of this matrix is

$$\begin{bmatrix} 12 & -1 & -3 \\ -2 & -3 & 6 \\ -5 & 1 & 1 \end{bmatrix}.$$

For a slight variation, instead of all 1s down the diagonal, use any 2×2 in the lower right corner that has a determinant of 1, 1s along the rest of the diagonal, 0s for the other elements of the upper triangle, and random integers in the lower triangle. Example:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 2 & 3 & 2 & 5 \\ 6 & -1 & 1 & 3 \end{bmatrix}.$$

Note that the determinant is 1. Multiply row 3 by -2, add to row 2. Then in turn multiply column 1 by 3, 2, and -1, adding to columns 2, 3, and 4, respectively. The matrix has been transformed into the matrix

$$\begin{bmatrix} 1 & 3 & 2 & -1 \\ -4 & -17 & -12 & -6 \\ 2 & 9 & 6 & 3 \\ 6 & 17 & 13 & -3 \end{bmatrix}.$$

Note that the determinant is still 1. The inverse of this matrix with determinant 1 is

$$\begin{bmatrix} -57 & 30 & 53 & 12 \\ 0 & 1 & 2 & 0 \\ 24 & -14 & -25 & -5 \\ -10 & 5 & 9 & 2 \end{bmatrix}.$$

6. Public-Key Cryptography

In the systems discussed so far, the sender and receiver jointly have a secret key. The sender uses the key to encipher the plaintext to be sent, while the receiver uses the same key in order to decipher the ciphertext obtained. These systems are called *one-key systems*. Therefore, the key had to be kept secret and yet be available to both sender and recipient. The problem with these one-key systems is that before communication can take place, the secret key must be distributed in a separate transaction.

In 1976, Whitfield Diffie and Martin Hellman, two electrical engineers at Stanford University, proposed a two-key system. Although they had no workable method for carrying out their scheme, its properties were as follows. The two keys are an enciphering key and a deciphering key. Although the two keys effect inverse operations and are therefore related, there is no easily computed method of deriving the deciphering key from the enciphering key. Thus, the enciphering key can be made public without compromising the deciphering key; each user can encipher messages, but only the intended recipient (whose deciphering key is kept secret) can decipher them. A major advantage of such a *public-key cryptography system* is that it is unnecessary for each sender and receiver to exchange a key in advance of their decision to communicate with each other.

Any two people with entries in the public-key directory could communicate privately without any prior exchange of keys. For example, suppose Art wants to send a message M to Beth. Art looks up Beth's enciphering key E_B in the public directory. He enciphers M using E_B to get ciphertext C, where $C = E_B(M)$, and sends C to Beth. The function notation $E_B(M)$ means apply Beth's enciphering key to M. Beth then uses her secret deciphering key D_B to convert the ciphertext C back into its original plaintext form M, where $M = D_B(C)$. Only Beth can decipher C, because she is the only person who knows her deciphering key D_B.

Using this system, messages can be authenticated and thus protect against forgeries. For example, suppose that Beth is expecting a message from Art and wants to be sure that the message really is from Art and not from anyone else. Beth and Art follow this procedure to protect against forgery: Art first "deciphers" M with his secret deciphering key D_A and then enciphers the result with Beth's public enciphering key E_B, sending Beth the ciphertext $C = E_B(D_A(M))$.

When Beth receives C, she first deciphers it with her private deciphering key D_B, which gives $D_B(C) = D_A(M)$, because D_B and E_B are inverse functions. She then "enciphers" the result using Art's public enciphering key E_A, which recovers M because $E_A(D_A(M)) = M$. This last step ensures that the message came from Art, because only Art would have known D_A.

In 1977, Ronald L. Rivest, Adi Shamir, and Leonard Adleman at the Massachusetts Institute of Technology developed a practical way of implementing Diffie and Hellman's concept, by using elementary number theory. Their

method is now called the *RSA public-key cryptography system*, after the initials of the inventors. Its security depends on the assumption that in the current state of computer technology, the factorization of composite numbers with large prime factors is prohibitively time-consuming.

Before a message can be enciphered, it must be put into numerical form, M. Convert each letter, number, or punctuation mark of the plaintext into some numerical equivalent, such as the ASCII code, or, as in **Table 3**, the two-digit numbers 00–40, with 00 indicating a space between words.

Table 3.
A numerical coding for plaintext.

A = 01	K = 11	U = 21	1 = 31
B = 02	L = 12	V = 22	2 = 32
C = 03	M = 13	W = 23	3 = 33
D = 04	N = 14	X = 24	4 = 34
E = 05	O = 15	Y = 25	5 = 35
F = 06	P = 16	Z = 26	6 = 36
G = 07	Q = 17	, = 27	7 = 37
H = 08	R = 18	. = 28	8 = 38
I = 09	S = 19	? = 29	9 = 39
J = 10	T = 20	0 = 30	! = 40

For each user, enciphering requires two positive integers: a number n, which is equal to the product of two primes, and another number e, which is computed from the two primes by a method that will be described later. The RSA system enciphers by raising the message M (or each block of M, if M is too long) to the power e and finding its remainder modulo n. That is, the ciphertext C is the remainder when M^e is divided by n:

$$E(M) = M^e \equiv C \pmod{n}.$$

The message M is restored by the same operation but using a different exponent, integer d, also described later, which acts as a kind of inverse to e:

$$D(C) = C^d \equiv M \pmod{n}.$$

Here is a simple example using small primes. Suppose that the plaintext message is PHONE. Let $p = 13$ and $q = 19$; then $n = pq = 247$. Suppose we take $e = 31$ and $d = 7$. In numerical form, the message is $M = 1608151405$. It is assumed that $M < n$, but M is too large in this case; so we break M into blocks so that each block is less than n. Thus, $M_1 = 16$, $M_2 = 08$, $M_3 = 15$, $M_4 = 14$, and $M_5 = 05$. We then encipher each M_i separately, yielding

$$\begin{aligned}
C_1 = M_1^{31} &= 16^{31} \equiv 081 \pmod{247}\\
C_2 = M_2^{31} &= 8^{31} \equiv 122 \pmod{247}\\
C_3 = M_3^{31} &= 15^{31} \equiv 219 \pmod{247}\\
C_4 = M_4^{31} &= 14^{31} \equiv 040 \pmod{247}\\
C_5 = M_5^{31} &= 5^{31} \equiv 112 \pmod{247}.
\end{aligned}$$

The enciphered message would be $C = 081\ 122\ 219\ 040\ 112$. A simple computer program can be written to find residues modulo 247 (see **Appendix A** for a BASIC program to find modular residues).

To *de*cipher the ciphertext, we use a similar method:

$$\begin{aligned} M_1 = C_1^7 = \quad & 81^7 \quad \equiv 16 \pmod{247} \\ M_2 = C_2^7 = \quad & 122^7 \quad \equiv 08 \pmod{247} \\ & \vdots \\ M_5 = C_5^7 = \quad & 112^7 \quad \equiv 05 \pmod{247}. \end{aligned}$$

In practice, the integers n, e, and d must be much larger to ensure security. Rivest et al. described how to choose the integers so that the properties of a public-key system suggested by Diffie and Hellman are satisfied. Computers are necessary to implement the system. To compute n, the person designing the system finds two large (100 digits or more) primes p and q and sets $n = pq$. Several very fast primality-testing algorithms exist and can test in about 40 seconds whether an arbitrary 100-digit integer is prime.

The designer selects the enciphering exponent as a large integer e such that $\gcd(e, r) = 1$, where $r = (p-1)(q-1)$. The number e should also satisfy $2^e > n$, so that some reduction modulo n actually takes place, and so that the plaintext block M cannot be recovered by just taking eth roots. Finally, the designer computes the deciphering key d such that $ed \equiv 1 \pmod{r}$. Such a value of d will always exist, since $\gcd(e, r) = 1$.

To illustrate the procedure, suppose that the designer selects two primes $p = 73$ and $q = 97$ (we have chosen small primes for illustration). Then $n = (73)(97) = 7081$ and $r = (72)(96) = 6912$. Since e must be chosen so that $\gcd(e, r) = 1$, e may be taken as any prime larger than both p and q. For the chosen value of e, d can be computed by knowing that d is an integer less than or equal to r satisfying the congruence $ed \equiv 1 \pmod{r}$. A few of the possibilities for e and d are shown in **Table 4** (see **Appendix B** for a BASIC program in for finding solutions to this congruence).

Table 4.
Some of the values that satisfy $ed \equiv 1 \pmod{r}$.

e	d
101	2669
211	3931
307	1531
31	223

The last choice of e in the table was made by factoring $(r + 1)$ and choosing as e one of the prime factors. This procedure will always give a choice for e; but if $(r + 1)$ is prime, one should choose a different value for e, since either e or d would be 1.

For the given values of n and r, suppose that the designer decides to use $e = 101$ and $d = 2669$. The public key would be published in a directory for

this sender in the form (e, n): in this case, $(101, 7081)$. Suppose the message to be sent is the plaintext POUNDS. The numerical equivalent is $M = 161521140419$. Since this number is larger than n, we will break M into blocks of four digits each. Using $e = 101$ and $n = 7081$, we obtain

$$\begin{aligned} 1615^{101} &\equiv 4226 \pmod{7081} \\ 2114^{101} &\equiv 1582 \pmod{7081} \\ 0419^{101} &\equiv 765 \pmod{7081}. \end{aligned}$$

Thus, the ciphertext is $C = 4226\ 1582\ 0765$. The receiver, whose deciphering key is $d = 2669$, then deciphers the ciphertext as follows:

$$\begin{aligned} 4226^{2669} &\equiv 1615 \pmod{7081} \\ 1582^{2669} &\equiv 2114 \pmod{7081} \\ 0765^{2669} &\equiv 0419 \pmod{7081}. \end{aligned}$$

Let us consider a second example, again using small values of p and q to illustrate. Suppose we choose the primes $p = 47$ and $q = 73$. Then we have $n = (47)(73) = 3431$ and $r = (46)(72) = 3312$. Since in this case $(r + 1)$ is a prime, we will select e (and the resulting d) by considering prime numbers that are larger than both p and q. A few of the possible values of e and d are listed in **Table 5**.

Table 5.
Some of the values that satisfy $ed \equiv 1 \pmod{r}$.

e	d
79	2767
181	2269
269	197
353	2993

Suppose that for a particular sender, the public key is $(269, 3431)$. If we consider the same plaintext as before, that is, POUNDS, for which the numerical value is $M = 161521140419$, the sender computes the following:

$$\begin{aligned} 1615^{269} &\equiv 1379 \pmod{3431} \\ 2114^{269} &\equiv 2020 \pmod{3431} \\ 419^{269} &\equiv 2167 \pmod{3431}. \end{aligned}$$

Thus, the ciphertext is $C = 1379\ 2020\ 2167$. To decipher this message, the receiver uses his value of $d = 197$ and computes as follows:

$$\begin{aligned} 1379^{197} &\equiv 1615 \pmod{3431} \\ 2020^{197} &\equiv 2114 \pmod{3431} \\ 2167^{197} &\equiv 0419 \pmod{3431}. \end{aligned}$$

To summarize, using the RSA enciphering system, users can encipher and decipher messages easily (with the aid of a computer). If the prime numbers p and q are chosen to be very large (100 digits or more for each), the security of the system is assured. The integer pairs (e, n) make up the "public key" of the system and are put in a public-key directory. The pair (d, n), as well as the primes p and q, are kept secret, known only to the user. Someone who does not know d but who wants to find it (e.g., a spy who wants to crack the system) needs to know p and q. The direct method of attack would be to attempt to factor n, an integer of huge magnitude (at least 200 digits in length). Once the factors are determined, the recovery of the deciphering key d can be calculated from $r = (p-1)(q-1)$ and the value of e.

Confidence in the RSA system in based on the expected amount of computer time needed to factor the product of two large primes. Factoring is computationally more difficult than distinguishing between primes and composites. On today's fastest computers, a 200-digit number can routinely be tested for primality in less than 10 minutes, whereas the running time required to factor a composite number of the same size is prohibitive. It has been estimated that the quickest factoring algorithm known can use approximately 1.2×10^{23} computer operations to resolve an integer with 200 digits into its prime factors. Assuming that each operation takes one microsecond (10^{-6} seconds), then the factorization time would be about 3.8×10^{9} years. Given unlimited computing time and some unimaginably efficient factoring algorithm, the RSA enciphering system could be broken; but, for the present, it appears to be quite safe.

7. What's in Use Today?

Despite the opposition of the U.S. government, many computer companies have licensed the RSA public-key cryptosystem from its developers. The list includes Apple, AT&T, Digital, Lotus, Microsoft, Motorola, Northern Telecom, Novell, Sun, and IBM. Microsoft licensed the technology for use its Windows NT operating system, and Apple plans to include RSA encryption in its Open Collaboration Environment operating system. Even U.S. governmental agencies have licensed RSA, including the National Science Foundation, NASA, the Central Intelligence Agency, the Pentagon, and the State Department. Other licensees include Chase Manhattan Bank, Chemical Bank, Boeing, Du Pont, Exxon, Hughes Aircraft, Raytheon, Rockwell International, Texas Instruments, and Whirlpool [Uehling 1993].

8. Exercises

1. Encipher the plaintext message using Caesar's cipher:

WHAT WOULD LIFE BE WITHOUT ARITHMETIC BUT A SCENE OF HORRORS

2. Knowing that a shift transformation was used, decipher the ciphertext:

YUBRO TMKWA GZOUT YOYTU ZYURB OTMVX UHRKS Y

3. Knowing that an affine (linear) transformation was used, decipher the ciphertext:

VUVNU GBUOI TGDFT GURVE UORUP OTEVU VNELU VELBG SLPTG ULMTU

TGXVE TPORU VNUGB TPTLB HOUUL ALQQL PPORU VNXLN USGLY RYQT

Use the table of relative frequencies of letters occurring in the English language given in **Table 6**.

Table 6.
Frequency of letters in English text, from Sinkov [1966].

A	.073	J	.002	S	.063
B	.009	K	.003	T	.093
C	.030	L	.035	U	.027
D	.044	M	.025	V	.013
E	.130	N	.078	W	.016
F	.028	O	.074	X	.005
G	.016	P	.027	Y	.019
H	.016	Q	.003	Z	.001
I	.035	R	.077		

4. Use a polygraphic transformation using the enciphering matrix

$$\begin{bmatrix} 5 & 6 & 10 \\ 6 & 4 & 7 \\ 4 & 1 & 2 \end{bmatrix}$$

to encipher the plaintext message GONE WITH THE WIND. Assign numbers to letters of the alphabet in the usual manner but include the assignment of a space to the number 27, ? to the number 28, and ! to the number 29.

5. If the enciphering matrix is

$$\begin{bmatrix} 8 & 1 & 1 \\ 15 & 2 & 2 \\ 2 & 0 & 1 \end{bmatrix},$$

decipher the ciphertext:

?GPKXRXJPX?LZCXWLHP?FKJQ?VHEIV TH?GPOQX

6. Suppose we select the two primes $p = 43$ and $q = 31$.

a) Determine one of the many possible enciphering keys, e and encipher the plaintext message SCHOOL. (Assign numerical values to alphabetical letters as in **Exercises 4–5**.)

b) Determine the corresponding deciphering key, d, for your choice of e in part **(a)**.

7. The ciphertext $C = 08036\ 10402\ 02173\ 10396\ 06686\ 13132$ is received from Mary. If you know that $p = 97$, $q = 157$, and that your public key is $(881, 15229)$, decipher her message. (Of course, you must first determine your own decipher key, d.)

9. Solutions to the Exercises

1. The enciphering formula is $c \equiv (p + 3) \pmod{26}$.

Plaintext:	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher:	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
Cipher:	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Answer:
ZKDWZ RXOGO LIHEH ZLWKR XWDUL WKPHW LFEXW DVFHQ HRIKR UURUV

2. Since $c \equiv (p + k) \pmod{26}$, we have $p \equiv (c - k) \pmod{26}$. One solution is to consider the first block and try several values of k. Of course, there are only 25 possibilities for k, so the method may take a considerable amount of time.

	Y	U	R	B	O
$k = 1$	X	T	Q	A	N
$k = 2$	W	S	P	Z	M
$k = 3$	V	R	O	Y	L
$k = 4$	U	Q	N	X	K
$k = 5$	T	P	M	W	J
$k = 6$	S	O	L	V	I

The value $k = 6$ seems to make sense, so try $p \equiv (c - 6) \pmod{26}$.
Answer: SOLVING EQUATIONS IS NOT SOLVING PROBLEMS

3. First, count the frequency of occurrence of each letter in the ciphertext:

Letter:	U	T	L	V	G	O	P	N	R	E	B
Frequency:	16	10	10	9	8	6	6	5	5	5	4
Letter:	Q	S	Y	X	I	F	H	A	D	M	
Frequency:	3	2	2	2	1	1	1	1	1	1	

We need to determine a and b for $c \equiv (ap + b) \pmod{26}$; and if we let U correspond to E and T correspond to T, the congruences that must be solved are

$$\begin{aligned} 21 &\equiv 5a + b \pmod{26} \\ 20 &\equiv 20a + b \pmod{26}. \end{aligned}$$

Subtracting, we obtain $1 \equiv -15a \equiv 11a \pmod{26}$. Since the inverse of 11 is $19 \pmod{26}$, we have

$$19(11a) \equiv a \equiv 19(1) \equiv 19 \pmod{26}.$$

Substituting this value of a into the first congruence, we get

$$b \equiv 21 - 5(19) \equiv 4 \pmod{26}.$$

Thus, $c \equiv (19p + 4) \pmod{26}$, or $19p \equiv (c - 4) \pmod{26}$. Multiplying by the inverse of 19 yields the formula

$$11(19p) \equiv 11(c - 4) \pmod{26},$$

or $p \equiv 11(c-4)$. Using this formula and the first block of the ciphertext, we obtain

$$\begin{aligned} \texttt{V}:\ p &\equiv 11(22 - 4) \equiv 11(18) \equiv 16 \Longrightarrow \texttt{P} \\ \texttt{U}:\ p &\equiv 11(21 - 4) \equiv 11(17) \equiv 5 \Longrightarrow \texttt{E} \\ \texttt{V}:\ p &\equiv 11(22 - 4) \equiv 11(18) \equiv 16 \Longrightarrow \texttt{P} \\ \texttt{N}:\ p &\equiv 11(14 - 4) \equiv 11(10) \equiv 6 \Longrightarrow \texttt{F} \\ \texttt{U}:\ p &\equiv 11(21 - 4) \equiv 11(17) \equiv 5 \Longrightarrow \texttt{E} \end{aligned}$$

This correspondence doesn't seem to make sense, so we will try another correspondence taking into consideration the frequencies. Suppose we try T corresponding to E and U corresponding to T. Then the appropriate congruences are

$$\begin{aligned} 20 &\equiv 5a + b \pmod{26} \\ 21 &\equiv 20a + b \pmod{26}. \end{aligned}$$

Again subtracting, we obtain $-1 \equiv 25 \equiv -15a \equiv 11a \pmod{26}$.

$$19(11a) \equiv a \equiv 19(25) \equiv 7 \pmod{26}.$$

Substituting in the first congruence,

$$b \equiv 20 - 5(7) \equiv 11 \pmod{26}.$$

Thus, the formula will be $c \equiv 7p + 11$, or

$$7p \equiv c - 11 \pmod{26}.$$

Now the inverse of $7 \pmod{26}$ is 15, so

$$15(7p) \equiv p \equiv 15(c - 11) \pmod{26}.$$

Trying this formula on the first block results in

$$\begin{array}{rrrr}
\texttt{V}: & p \equiv 15(22 - 11) & \equiv & 9 \Longrightarrow \texttt{I} \\
\texttt{U}: & p \equiv 15(21 - 11) & \equiv & 20 \Longrightarrow \texttt{T} \\
\texttt{V}: & p \equiv 15(22 - 11) & \equiv & 9 \Longrightarrow \texttt{I} \\
\texttt{N}: & p \equiv 15(14 - 11) & \equiv & 19 \Longrightarrow \texttt{S} \\
\texttt{U}: & p \equiv 15(21 - 11) & \equiv & 20 \Longrightarrow \texttt{T}
\end{array}$$

This formula seems to be making some sense, so continue deciphering other blocks.
Answer:
IT IS TRUTH VERY CERTAIN THAT WHEN IT IS NOT IN OUR POWER TO DETERMINE WHAT IS TRUE WE OUGHT TO FOLLOW WHAT IS PROBABLE

4. Assigning numbers to the letters of the plaintext, we obtain

G	O	N	E		W	I	T	H		T	H	E		W	I	N	D
07	15	14	05	27	23	09	20	08	27	20	08	05	27	23	09	14	04

$$\begin{bmatrix} 5 & 6 & 10 \\ 6 & 4 & 7 \\ 4 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 7 & 5 & 9 & 5 & 9 \\ 15 & 27 & 20 & 27 & 14 \\ 14 & 23 & 8 & 23 & 4 \end{bmatrix} = \begin{bmatrix} 265 & 417 & 245 & 417 & 169 \\ 200 & 299 & 190 & 299 & 138 \\ 71 & 93 & 72 & 93 & 58 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 4 & 11 & 13 & 11 & 24 \\ 26 & 9 & 16 & 9 & 22 \\ 13 & 6 & 14 & 6 & 29 \end{bmatrix} \pmod{29}.$$

Answer: DZMKIFMPNPH?KIFXV!

5. First, find the inverse of the encoding matrix. Using the Gauss-Jordan elimination method,

$$\begin{bmatrix} 8 & 1 & 1 & 1 & 0 & 0 \\ 15 & 2 & 2 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0.125 & 0.125 & 0.125 & 0 & 0 \\ 15 & 2 & 2 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0.125 & 0.125 & 0.125 & 0 & 0 \\ 0 & 1 & 1 & -15 & 8 & 0 \\ 0 & -0.250 & 0.750 & -0.250 & 0 & 1 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 1 & 1 & -15 & 8 & 0 \\ 0 & 0 & 1 & -4 & 2 & 1 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 1 & 0 & -11 & 6 & -1 \\ 0 & 0 & 1 & -4 & 2 & 1 \end{bmatrix}.$$

Thus, the inverse of the encoding matrix is

$$\begin{bmatrix} 2 & -1 & 0 \\ -11 & 6 & -1 \\ -4 & 2 & 1 \end{bmatrix}.$$

We translate the message:

$$\begin{bmatrix} 2 & -1 & 0 \\ -11 & 6 & -1 \\ -4 & 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 28 & 11 & 24 & 24 & 26 & 23 & 16 & 11 & 28 & 5 & 27 & 28 & 15 \\ 7 & 24 & 10 & 28 & 3 & 12 & 28 & 10 & 22 & 9 & 20 & 7 & 17 \\ 16 & 18 & 16 & 12 & 24 & 8 & 6 & 17 & 8 & 22 & 8 & 16 & 24 \end{bmatrix} \equiv$$

$$\begin{bmatrix} 49 & -2 & 38 & 20 & 49 & 34 & 4 & 12 & 34 & 1 & 34 & 49 & 13 \\ -282 & 5 & -220 & -108 & -292 & -189 & -14 & -78 & -184 & -23 & -185 & -282 & -87 \\ -82 & 22 & -60 & -28 & -74 & -60 & -2 & -7 & -60 & 20 & -60 & -82 & -2 \end{bmatrix}$$

$$\equiv \begin{bmatrix} 20 & 27 & 9 & 20 & 20 & 5 & 4 & 12 & 5 & 1 & 5 & 20 & 13 \\ 8 & 5 & 12 & 8 & 27 & 14 & 15 & 9 & 19 & 6 & 18 & 8 & 29 \\ 5 & 22 & 27 & 1 & 13 & 27 & 27 & 22 & 27 & 20 & 27 & 5 & 27 \end{bmatrix} \pmod{29}$$

Answer: `THE EVIL THAT MEN DO LIVES AFTER THEM!`

6. a) For $p = 43$, $q = 31$, $n = pq = 1333$, we have $r = (p-1)(q-1) = (42)(30) = 1260$, so $(r+1) = 1261 = (13)(97)$. Therefore, e can be taken to be 13, 97, or any prime number greater than both p and q. Thus, a few possible values of e are 13, 47, 53, 59, 61, etc. Suppose we take $e = 13$.

S	C	H	O	O	L
19	03	08	15	15	12

The plaintext message is therefore $P = 190\,308\,151\,512$. (Remember that each block must have a value less than n.)

$$\begin{aligned} 190^{13} &\equiv 932 \pmod{1333} \\ 308^{13} &\equiv 953 \pmod{1333} \\ 151^{13} &\equiv 432 \pmod{1333} \\ 512^{13} &\equiv 376 \pmod{1333}. \end{aligned}$$

(See **Appendix A** for a computer program to do modular reduction.)
Answer: $C = 932\,953\,432\,376$.

b) To find a suitable value of d, we must solve $13d \equiv 1 \pmod{1260}$. One way is to use a suitable computer program (see **Appendix B**). Another is to use the Euclidean algorithm, which gives $\gcd(13, 1260)$:

$$1260 = 13(96) + 12$$

$$13 = 12(1) + 1.$$

Thus, $1 = 13 - (1)(12) = 13 - [1260 - 13(96)]$, or $1 = 13(97) - 1260$, that is, $13(97) \equiv 1 \pmod{1260}$. A suitable value of d then is 97.

Had we chosen $e = 47$, then to find d we would need to solve $47d \equiv 1 \pmod{1260}$. Using the Euclidean algorithm, we have

$$\begin{aligned} 1260 &= 47(26) + 38 \\ 47 &= 38(1) + 9 \\ 38 &= 9(4) + 2 \\ 9 &= 2(4) + 1. \end{aligned}$$

Thus,

$$\begin{aligned} 1 &= 9 - 4(2) = 9 - 4[38 - 9(4)] \\ 1 &= 17(9) - 4(38) = 17[47 - 38] - 4(38) \\ 1 &= 17(47) - 21(38) = 17(47) - 21[1260 - 47(26)] \\ 1 &= 47(563) - 21(1260), \end{aligned}$$

that is, $47(563) \equiv 1 \pmod{1260}$. A suitable value of d corresponding to $e = 47$ is 563.

7. For $p = 97$, $q = 157$, and $n = pq = 15229$, we have $r = (96)(156) = 14976$. Now, e is given to be 881; thus, to find the value of d, we must solve $881d \equiv 1 \pmod{14976}$. Using either the computer program or the Euclidean algorithm, we obtain $d = 17$:

$$\begin{aligned} 14976 &= 881(16) + 880 \\ 881 &= 880(1) + 1, \qquad \text{thus} \\ 1 &= 881 - 880 = 881 - [14976 - 881(16)] \\ 1 &= 881(17) - 14976, \end{aligned}$$

that is, $881(17) \equiv 1 \pmod{14976}$ and d can be 17.

$$\begin{aligned} 08036^{17} &\equiv 1301 \pmod{15229} \\ 10402^{17} &\equiv 2008 \pmod{15229} \\ 02173^{17} &\equiv 2709 \pmod{15229} \\ 10396^{17} &\equiv 1927 \pmod{15229} \\ 06686^{17} &\equiv 0621 \pmod{15229} \\ 13132^{17} &\equiv 1429 \pmod{15229}. \end{aligned}$$

Therefore, the plaintext value is $P = 130120082709192706211429$, or using the alphabet assignments, we arrive at:
Answer: `MATH IS FUN!`

10. Appendix A: BASIC Program for Modular Reduction

```
100 HOME
110 PRINT "FIND THE RESIDUE OF X^A (MOD M)"
120 PRINT
130 DIM K(500)
140 INPUT "A = "; A
150 LET A1 = A
160 LET I = 0
170 LET C = INT (A/2)
180 LET B = A - C*2
190 IF B = 1 THEN K(I) = 1:  GOTO 210
200 LET K(I) = 0
210 LET I = I + 1
220 LET A = C
230 IF A = 1 THEN K(I) = 1:  GOTO 250
240 GOTO 170
250 INPUT "M = "; M
260 INPUT "X = (ENTER 0 TO END)"; X
265 IF X = 0 THEN END
270 LET Z = 1
280 LET Y = X
290 FOR J = 1 TO I
300 LET Y = Y*Y
310 LET Y = Y - M * INT(Y/M)
320 IF K(J) = 1 THEN Z = Z*Y
330 LET Z = Z - M * INT(Z/M)
340 NEXT J
350 IF K(0) = 1 THEN Z = X*Z
360 LET Z = Z - M * INT(Z/M)
365 PRINT
370 PRINT X;"^";A1;" IS CONGRUENT TO ";Z;" (MOD ";M:")"
380 PRINT : GOTO 260
390 END
```

11. Appendix B: BASIC Program to Solve $ed \equiv 1$

```
100 HOME
110 PRINT "FOR THE RSA PUBLIC-KEY CRYPTOGRAPHY"
120 PRINT "SYSTEM, THIS PROGRAM FINDS THE DECIPHERING"
130 PRINT "EXPONENT D, GIVEN PRIMES P AND Q AND"
140 PRINT "THE ENCIPHERING EXPONENT E. MORE GENERALLY,"
150 PRINT "THFOR A=(P-1)(Q-1) AND B = E, THE PROGRAM"
160 PRINT "IMPLEMENTS THE ALGORITHM FOR FINDING"
170 PRINT "G = GCD (A,B) AND SOLVING AX + BY = G."
180 PRINT "IF G = 1, THEN Y IS THE DECIPHERING"
190 PRINT "EXPONENT D."
200 REM
210 REM INITIALIZES SEQUENCES
220 REM
230 LET A0 = 1
240 LET A1 = 0
250 LET B0 = 0
260 LET B1 = 1
270 PRINT
280 REM ENTER P, Q, AND E AND SET UP A AND B
290 REM
300 INPUT "ENTER PRIMES P AND Q ";P,Q
310 INPUT "ENTER ENCRYPT EXPONENT E ";E
320 LET A = (P - 1) * (Q - 1)
330 LET B = E
340 REM
350 REM EUCLIDEAN ALGORITHM TO FIND GCD (A,B)
360 REM
370 LET M1 = A
380 LET N1 = B
390 LET T = M1
400 LET M1 = N1
410 LET Q = INT (T / N1)
420 LET N1 = T - N1 * Q
430 REM
440 REM WHEN N1 = 0, END EUCLIDEAN ALGORITHM WITH M1 = GCD (A,B)
450 REM
460 IF N1 = 0 THEN 610
470 REM
480 REM COMPUTATION OF SEQUENCES
490 REM
500 LET A2 = A0 - A1 * Q
```

```
510 LET B2 = B0 - B1 * Q
520 LET A0 = A1
530 LET B0 = B1
540 LET A1 = A2
550 LET B1 = B2
560 GOTO 390
570 REM
580 REM TO ENSURE POSITIVE SOLUTION X = A2 AND Y = B2
590 REM TO A*X = G MOD B AND TO B*Y = G MOD A
600 REM
610 IF B2 < 0 THEN B2 = A / M1 + B2
620 IF A2 < 0 THEN A2 = B / M1 + A2
630 REM
640 REM PRINT RESULTS
650 REM
660 IF M1 <> 1 THEN PRINT "GCD <> 1" :  GOTO 680
670 PRINT "DECRYPT EXPONENT IS ";B2
680 END
```

References

Anton, Howard. 1994. *Elementary Linear Algebra.* 7th ed. New York: Wiley.

Burton, David M. 1989. *Elementary Number Theory.* Dubuque, IA: William C. Brown.

Camp, Dave R. 1985. Secret code with matrices. *Mathematics Teacher* 78 (December 1985).

Diffe, Whitfield, and Martin E. Hellman. 1976. New dimensions in cryptography. *IEEE Transactions on Information Theory* IT–22 (November 1976): 644–654.

Hill, Lester S. Concerning certain linear transformation apparatus of cryptography. *American Mathematical Monthly* 38 (March 1931).

Kahn, David. 1967. *The Codebreakers.* New York: Macmillan.

Konheim, Alan. 1981. *Cryptography: A Primer.* New York: Wiley.

Lefton, Phyllis. 1991. Number theory and public-key cryptography. *Mathematics Teacher* 84 (January 1991).

Rivest, Ronald L., Adi Shamir, and Leonard Adelman. 1978. A method of obtaining digital structures and public-key cryptosystems. *Communications of the Association for Computing Machinery* 21: 120-26.

Sinkov, Abraham. 1966. *Elementary Cryptanalysis: A Mathematical Approach.* Washington, DC: Mathematical Association of America.

Snow, Joanne R. 1989. An application of number theory to cryptology. *Mathematics Teacher* 82 (January 1989).

Uehling, Mark D. 1993. Cracking the code. *Popular Science* 242 (January 1993).

About the Author

Prof. Wampler earned his A.B. and M.A. degrees from the University of Kansas, and the Ph.D. degree from the University of Nebraska—Lincoln. He taught mathematics at Nebraska Wesleyan University in Lincoln from 1954 until his retirement in 1992. His special interests have been in number theory and statistics.