KEEPING SECRETS ...

BY JAMES D. NICKEL

One of the pleasant memories of childhood is playing "hide and seek" or making up secret codes so that only you and your closest friend can communicate in complete privacy. Maybe some of you tried something like this with your "secret" pal. You rearranged the alphabet at random, setting each letter of the alphabet to some other letter, let's say, as follows:

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

Only you and your friend have this "key." Using it, you could change any sentence into unintelligible gibberish:

Want to watch cartoons on Saturday morning?

becomes:

Utcy yk utypm ptdkkcr kc Rtyndati okdcqcf?

You might even remove the capital letters, spaces, and punctuation marks to really make it confusing for the uninitiated:

utcyykutypmptdkkcrkcrtyndatiokdcqcf

After decoding this message with your key, you reply:

quqhhrwwiknymwc (I will see you then)

In this childhood example is found all the elements of the science of *cryptography*.[1] A cryptographic system is classified in three ways:

1. Some operation (either randomly as in our example or mathematical) is developed through which important information (text or numbers; also called *plain text*) can be concealed with the use of an *encryption*[2] key.
2. The sender and receiver either use the same key (called a *symmetric*[3] *cryptosystem*) or different keys (called an *asymmetric*[4] [two-key or public-key] *cryptosystem*).
3. Using one or the other key system, a message cipher is produced. The sender transmits a key-encrypted cipher to the receiver. The receiver *decrypts*[5] the cipher according to the given key and, there you have it, the two will watch cartoons on Saturday morning!

Note: This essay is extracted from a Lesson from the forthcoming textbook *Mathematics: Building on Foundations*.

The "uninitiated" who wants to understand the message must break the cipher either by obtaining the key (the easy way) or by determining the key by mathematical analysis. Breaking ciphers by analysis is known as the science of *cryptanalysis*. The simple key devised above is, in fact, easy to break. Anyone skilled in cryptanalysis can do this because they know the nature and structure of language. Given an encrypted message that is lengthy enough, the law of averages set in. For example, in the English language, a *random sample*[6] of prose contains *e* as the most

[1] Cryptography combines two Greek roots, *crypto* meaning "to hide" and *graph* meaning "to write." It literally means "hidden writing." It is the science of codes and ciphers.
[2] Encrypt literally means to "hide in" or to put into a cipher.
[3] Symmetric is Greek for "like measure."
[4] Asymmetric is Greek for "unlike measure."
[5] Decrypt means the same as "decode or decipher." You convert the cipher back to its original plain text or number.

common letter (12 percent; 12 out of every 100 letters), followed by *t* (9 percent), *a* and *o* (8 percent each), *i, n,* and *s* (7 percent each), and *r* (6 percent). The least used letters are *j, k,* and *x* (one half of 1 percent; 1 out of every 200 letters) and *q* and *z* (one-third of 1 percent; 1 out of every 300 letters). Also, combinations of letters are more revealing. You can also tabulate the percentage of occurrence of the 26 × 26 (676) different possible two-letter combinations in the English alphabet and really narrow the field. Certain letters are never doubled in English; e.g., *hh, ii, jj, kk, qq, uu, ww, xx, yy*. The vowels *a, e, i, o,* and *u* appear far more frequently adjacent to other letters than they do to one another. The letter *n* is far more likely to be preceded by a vowel than by a consonant. Certain pairs of letters occur frequently in one order but rarely or never in the reverse; e.g., *ea* versus *ae*, *lm* verses *ml*, *rn* verses *nr*. As you can tell from the above discussion, a cryptanalyst must be skilled in language analysis, logical analysis, and mathematical analysis. It is a challenging vocation.

Civil governments throughout history have recognized the need to keep "state secrets," especially in time of war. During war, the ability of one nation to break the code of another nation produces critical and strategic pieces of intelligence. For example, in World War II the ability of American cryptanalysts to break the Japanese naval code *JN25* was pivotal to the American victory over a superior Japanese fleet at the battle of Midway (June 3-6, 1942). Later in the Pacific Theater of operations (PTO), American cryptanalysts were able to identify the whereabouts of a small group of Japanese planes carrying Admiral Isoroku Yamamoto (1884-1943), the officer who conceived of the surprise attack on the United States naval base at Pearl Harbor on December 7, 1941. A squadron of Lockhead P-38 Lightnings ambushed and shot down Yamamoto's plane over Bouganville Island in the Solomons. After Yamamoto's plane fell in flames to the tropical forest below, a "pop goes the weasel" cipher was sent to American naval Admiral William F. "Bull" Halsey (1882-1959) signifying "mission accomplished." British cryptanalysts were able to break the key to the German *Enigma* ciphering machine allowing German communications to be read virtually "at will." The intelligence unearthed in this manner significantly altered World War II's outcome in the European Theater of operations (ETO).[7]

All cipher systems, except the one we will soon investigate, suffer from two serious defects. First, the recipient of the message must possess a secret key in order to decipher it. The problem with keys is that all potential recipients of your message must possess it (you would need a trusted dispatcher to hand deliver the key). Second, how do we know that the message has not been tampered with in transit? Someone may have obtained the key fraudulently, changed the message, and delivered it to you. We need a guarantee of authenticity.

A unique type of code, called public-key code (asymmetric cryptosystem), resolves both issues. In brief, here is how it works. First, Mr. Receiver makes *public* to all potential senders an enciphering key. Using this key, Mr. Sender enciphers a message and transmits it to Mr. Receiver. Mr. Receiver has a *secret* deciphering key whereby he can decode the message. The uniqueness about this system is that the enciphering key *only works in one direction*; i.e., to encipher a message (also known as the *trapdoor one-way function*). This key is made public to all. No special couriers are needed. Anyone can use it. *Decoding this message is only possible through the use of the secret deciphering key*. The one who sends the message cannot accidentally or deliberating reveal the deciphering key to any would-be interlopers or spies.

How is this done? This amazing technique is accomplished by means of the mathematics of prime numbers and modular arithmetic.[8] Let's first look at how a message is enciphered. Each alphabetic letter is assigned a two-digit number (this is called *substitution*). Next, this two-digit number is shuffled or scrambled according to a mathematical rule (this is called *transposition*). Here is where modular arithmetic enters the picture. Let's set up a five column array of numbers as follows:

---

[6] A random sample is a group or subset of items taken from a given population; whether English prose or English people.
[7] For a history of code breaking in World War II, see Stephen Budiansky, *Battle of Wits* (New York: The Free Press, 2000).
[8] Modular arithmetic is also called the arithmetic of remainders.

KEEPING SECRETS ...

BY JAMES D. NICKEL

Column 1	*Column 2*	*Column 3*	*Column 4*	*Column 5*
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	29	30
31	**32**	33	34	35
36	37	38	39	40

Note that each number in **red** is a power of 2 (i.e., 2, 4, 8, 16, and 32). Note their column placement. 2 (2^1) is in column 2, 4 (2^2) is in column 4, 8 (2^3) is in column 3, 16 (2^4) is in column 1, and 32 (2^5) is in column 2. What column would you think 2^6 (64) is in? Think about it first; then extend the rows of the table to confirm your conjecture. The number 64 (2^6) is in column 4, 128 (2^7) will be in column 3, 256 (2^8) will be in column 1, and 512 (2^9) will return to column 2. An obvious pattern is developing; i.e., 2, 4, 3, 1, 2, 4, 3, 1, etc.

Let's investigate how the number 5 (the number of columns) interfaces with this scheme. Note the following table:

Powers of 2	*Remainder when divided by 5*	*Modular arithmetic*
$2^1 = 2$	2	$2 \equiv 2 \bmod 5$[9]
$2^2 = 4$	4	$4 \equiv 4 \bmod 5$
$2^3 = 8$	3	$8 \equiv 3 \bmod 5$
$2^4 = 16$	1	$16 \equiv 1 \bmod 5$
$2^5 = 32$	2	$32 \equiv 2 \bmod 5$
$2^6 = 64$	4	$64 \equiv 4 \bmod 5$
$2^7 = 128$	3	$128 \equiv 3 \bmod 5$
$2^8 = 256$	1	$256 \equiv 1 \bmod 5$
$2^9 = 512$	2	$512 \equiv 2 \bmod 5$

What we discover from an analysis of this table is this: the remainder of the powers of 2 when divided by 5 *is the column the number resides!* A similar pattern can be discerned by using *any* base (2, 3, 4, 5, etc.) and any number of columns (as long as the number of columns is a *prime number* and the base *does not* have this number as a factor). Let's try base 8 with 5 columns (note: 5 is *not* a factor of 8; the greatest common factor of 5 and 8 is 1 meaning that these two numbers are *relatively prime*). Remember, to find the remainder, all we need to do is look at the last digit of the number (a number is a multiple of 5 if its last digit is 0 or 5). If the digit is greater than 5, then we subtract 5 from the digit to get the remainder. If the digit is less than 5, then we subtract the digit from 5 to get the remainder.

Powers of 8	*Remainder when divided by 5*	*Modular arithmetic*
$8^1 = 8$	3	$8^1 \equiv 3 \bmod 5$

[9] $2 \equiv 2 \bmod 5$ means that "2 divided by 5" results in a remainder of 2. In general, $a \equiv r \bmod n$ means $\frac{a}{n}$ leaves a remainder of *r*. Another example, $32 \equiv 2 \bmod 5$ means that $\frac{32}{5}$ leaves a remainder of 2.

KEEPING SECRETS ...

BY JAMES D. NICKEL

Powers of 8	*Remainder when divided by 5*	*Modular arithmetic*
$8^2 = 64$	4	$8^2 \equiv 4 \bmod 5$
$8^3 = 512$	2	$8^3 \equiv 2 \bmod 5$
$8^4 = 4096$	1	$8^4 \equiv 1 \bmod 5$
$8^5 = 32768$	3	$8^5 \equiv 3 \bmod 5$
$8^6 = 262144$	4	$8^6 \equiv 4 \bmod 5$
$8^7 = 2097152$	2	$8^7 \equiv 2 \bmod 5$
$8^8 = 16777216$	1	$8^8 \equiv 1 \bmod 5$
$8^9 = 134217728$	3	$8^9 \equiv 3 \bmod 5$

Let's try one more, base 10 with 7 columns (note: 7 is *not* a factor of 10; 7 and 10 are relatively prime):

Powers of 10	*Remainder when divided by 7*	*Modular arithmetic*
$10^1 = 10$	3	$10^1 \equiv 3 \bmod 7$
$10^2 = 100$	2	$10^2 \equiv 2 \bmod 7$
$10^3 = 1000$	6	$10^3 \equiv 6 \bmod 7$
$10^4 = 10000$	4	$10^4 \equiv 4 \bmod 7$
$10^5 = 100000$	5	$10^5 \equiv 5 \bmod 7$
$10^6 = 1000000$	1	$10^6 \equiv 1 \bmod 7$
$10^7 = 10000000$	3	$10^7 \equiv 3 \bmod 7$
$10^8 = 100000000$	2	$10^8 \equiv 2 \bmod 7$
$10^9 = 1000000000$	6	$10^9 \equiv 6 \bmod 7$

Note again that the remainder pattern starts to repeat itself based upon the number of columns; i.e., inspecting the last three tables, the remainder sequence has a repeating pattern of 4 digits in mod 5 (3, 4, 2, 1), 6 digits (3, 2, 6, 4, 5, 1) in mod 7. Note also, in the previous three tables, that in mod 5, the fourth sequence gives a remainder of 1 ($2^4 \equiv 1 \bmod 5$ and $8^4 \equiv 1 \bmod 5$). In mod 7, the sixth sequence also gives a remainder of 1 ($10^6 \equiv 1 \bmod 7$). In 1640, the French mathematician Pierre de Fermat (1601-1665) confirmed this pattern in what is today known, in number theory, as *Fermat's Little Theorem*. Here is the formal definition:

Pierre de Fermat
(Public Domain)

> If p is a prime number and n is any integer that does not have p as a factor, then $n^{p-1} \equiv 1 \bmod p$.[10]

Stated in another way, n^{p-1} will always have a remainder of 1 when divided by p. In our examples, $2^{5-1} = 2^4 \equiv 1 \bmod 5$, $8^{5-1} = 8^4 \equiv 1 \bmod 5$, and $10^{7-1} = 10^6 \equiv 1 \bmod 7$.

Stay with me for a few more preliminaries. In 1760, the Swiss mathematician Leonhard Euler (1707-1783) observed another interesting pattern in prime numbers. First, Euler defined a *phi-function* (phi is a Greek letter written as φ) as follows:

[10] Another way of saying the same thing is $n^{p-1}-1 \equiv 0 \bmod p$. This means that p divides into $n^{p-1}-1$ with zero remainder.

KEEPING SECRETS ...

BY JAMES D. NICKEL

Given any natural number *n,* φ(n) represents the number of natural numbers less than *n* that have no factor in common with *n.*


Leonhard Euler (Public Domain)

For example, given the natural number 6, then there are only two numbers, 1 and 5, less than 6 that have no factor in common with 6 (i.e., the ordered pair (1, 6) and (5, 6) are relatively prime; i.e., the GCF of 1 and 6 is 1, the GCF of 5 and 6 is 1). Hence φ(6) = 2. The table below contains the values of φ(n) from *n* = 2 to 15. To augment your familiarity with Euler's definition, verify the results in each instance.

	φ(6) = 2	φ(11) = 10
φ(2) = 1	φ(7) = 6	φ(12) = 4
φ(3) = 2	φ(8) = 4	φ(13) = 12
φ(4) = 2	φ(9) = 6	φ(14) = 6
φ(5) = 4	φ(10) = 4	φ(15) = 8

Look carefully at the phi-function of prime numbers in this table and note the pattern: φ(2) = 1, φ(3) = 2, φ(5) = 4, φ(7) = 6, φ(11) = 10, φ(13) = 12. In general:

If *p* is prime, then φ(p) = p – 1.

Now let's suppose that the numbers *p* and *q* are distinct primes. Let's make this specific. Let p = 7 and q = 17 (both are distinct primes). Then what is φ(pq) = φ(7×17) = φ(7·17)? Consider first the number 7·17 (we will not find its product for reasons that will soon become obvious). To calculate φ(7·17) we start with the numbers 1, 2, 3, 4, 5, 6, 7, 8, 9, …, 7·17 and *eliminate* all the multiples of 7 and 17. Note that among these 7·17 numbers, there are 17 multiples of 7 and 7 multiples of 17. We can then eliminate 7 + 17 = 24 numbers from the total of 7·17. The only *common* multiple of both 7 and 17 is 7·17. So, we subtract 1 from 24 to get 23. What we have left is the number will are looking for; i.e., φ(7·17) = 7·17 – 23. We can write this as follows to note how we got 23:

$$\varphi(7\cdot17) = 7\cdot17 - 7 - 17 + 1$$

Let's apply the distributive rule of multiplication over subtraction to the expression 7·17 – 7. We are essentially factoring 7 from the two terms, 7·17 and –7. Factoring 7 from 7·17 (7·17 divided by 7) gives us 17. Factoring 7 from -7 (-7 divided by 7) gives us -1. We get:

$$7\cdot17 - 7 = 7(17 - 1) = 7(16)$$

We now have 7(16) – 17 + 1. Let's look at the sum of the two terms -17 + 1. What does -17 + 1 equal? You can intuitively determine what happens if I owe someone $17 (-17) and I pay him back $1 (+1). How much will I *owe* that person after I pay back $1? $16. Hence, -17 + 1 = -16. Therefore, 7(16) – 17 + 1 = 7(16) – 16. Again, let's apply the distributive rule of multiplication over subtraction. We factor 16 from the two terms, 7(16) – 16. We get:

$$7(16) - 16 = 16(7 - 1) = 16(6)$$

Hence, φ(7·17) = 6(16) = 16·6 = 96. Euler noted that, in general, if *p* and *q* are distinct primes, then this nifty formula is used to calculate φ(pq):

$$\varphi(pq) = (p - 1)(q - 1)$$

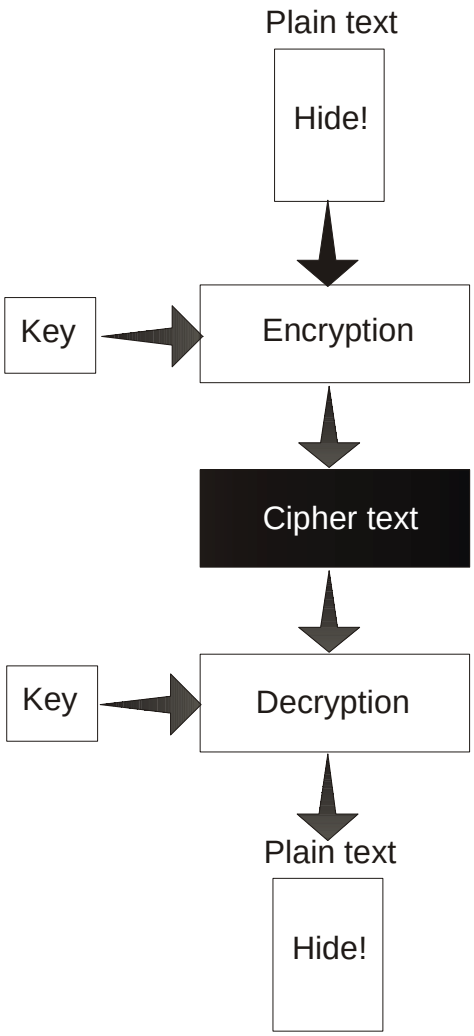
Also in 1760, Euler extended Fermat's Little Theorem using φ notation. If *p* and *q* are *relatively prime* (i.e.; the greatest common factor between *p* and *q* is 1), then:

$$p^{\phi(q)} \equiv 1 \bmod q$$

Some group of symbols, isn't it? Don't get lost in how they look (which will be new to many of you). Instead, understand what the symbols mean. Let's see how this works. If p = 7 and q = 17, then φ(17) = 16. Why? If *p* is prime, then φ(p) = p – 1. Therefore, $7^{16} \equiv 1 \bmod 17$. Let's try one more example. If p = 7 and q = 9 (both relatively prime but 9 is not a prime number), then φ(9) = 6 (from our table above). Therefore, $7^6 = 1 \bmod 9$. To confirm this, note that $7^6 = 117{,}649$. 117,649/9 = 13,072 with remainder 1.

Here is a list, five to be exact, of our theorems, observations, and definitions so far:

1. *Fermat's Little Theorem*: If *p* is a prime number and *n* is any integer that does not have *p* as a factor, then $n^{p-1} \equiv 1 \bmod p$.
2. *phi-function*: Given any natural number *n,* φ(n) represents the number of natural numbers less than *n* that have no factor in common with *n*.
3. If *p* is prime, then φ(p) = p – 1.
4. If *p* and *q* are distinct primes, then φ(pq) = (p – 1)(q – 1).
5. *Euler's extension of Fermat's Little Theorem:* If *p* and *q* are relatively prime, then $p^{\phi(q)} \equiv 1 \bmod q$.



All of these relationships were fixed in the mathematical landscape by the middle of the 18th century. In 1977, three mathematicians, Ronald Rivest (1948-), Adi Shamir (1952-), and Leonard Adleman (1947-), developed a commercial public-key encryption methodology. In 1982, these men founded RSA Data Security, Inc. of Redwood City, California, to market the system. The extraordinary success of the RSA public-key code in the late 20th century business world is owing to the observations of Fermat and Euler; discoveries made over 200 years *before* RSA Data Security, Inc. was founded.

The RSA code exploits item Euler's extension of Fermat's Little Theorem and the fact that, even though modern computers are extremely fast, it still takes them an enormous amount of time to factor numbers that are about 200 digits in length. Here is how the RSA code works. Suppose that *p* and *q* are *two very large prime numbers* (each about 100 digits). The values of these two numbers will be kept concealed; only Mr. Rishad[11] Clandestine knows. These two numbers are the *secret deciphering key*. Their product n = pq, however, will be given to Mr. General Q. Public. *n* is called the modulus of the RSA code; it is the *public enciphering key*. Since Mr. Rishad Clandestine knows the value of *p* and *q*, then he also knows the value of φ(n) = (p – 1)(q – 1).

[11] Mr. Clandestine's first name is a secret code that honors the first two letters of Ronald Rivest, Adi Shamir, and Leonard Adleman's last names.

The security of the code is based on the fact that one has to know *p* and *q* in order to break it. Factorizing *n* to obtain *p* and *q* in any systematic way when *n* is 200 digits takes years of computer time.[12]

Mr. Rishad Clandestine gives Mr. General Q. Public a public encryption key *e*. *e* is a natural number chosen such that it is relatively prime to φ(n); that is, the greatest common factor between *e* and φ(n) is 1.

Mr. General Q. Public now wants to encrypt the message, "Math sure is fun but it takes a lot concentration." He assigns a unique number *x* to each letter of the message such that $x < n$ (no trouble here since *n* is a 200 digit number). Each number *x* is encrypted to another number *c* (also a natural number that is less than *n*) using the following *encryption function*:

$$x^e \equiv c \bmod n$$

Mr. General Q. Public sends his message to Mr. Math Student. Mr. Rishad Clandestine has given Mr. Math Student a private (known only to him) decryption key *d*. *d* is a natural number chosen such that:

$$ed \equiv 1 \bmod \varphi(n)$$

Again, because of the secrecy of φ(n), it would take many years of computer time to calculate *d* from *e*. This is why Mr. Rishad Clandestine must tell Mr. Math Student what *d* is. When Mr. Math Student receives an encoded *c,* he deciphers it to another number *y* (also a natural number that is less than *n*) by using the following *deciphering function*:

$$c^d \equiv y \bmod n$$

I will now show you that $y \equiv x \bmod n$; i.e., *the deciphered number is congruent to Mr. General Q. Public's original number*. Note first that since $ed \equiv 1 \bmod \varphi(n)$, then there exists, by the definition of division, another natural number *k* such that:

$$ed = k[\varphi(n)] + 1$$

Although these symbols may look like nothing but comical hieroglyphics (what with the brackets, parentheses, Greek letter φ, the number 1, +, =, and letters e, d, k, and n), what we are saying, using an example, is this:

$$\text{If } 41 \equiv 1 \bmod 5, \text{ then } 41 = 8 \cdot 5 + 1$$

This should be easy to understand. We've shown how a general formula applies to a specific example. This is the power of algebra, the power of using symbolic notation to reason to a general conclusion. The symbol *ed* represents the product of two numbers. The symbols $k[\varphi(n)] + 1$ also represents the product of two numbers and + 1, well, you should know what that means! In essence, $ed = k[\varphi(n)] + 1$ means "the product of two numbers equals the product of two other numbers plus 1." Or, using different symbols, we can say that if x and y are the first two numbers, and k and z are the next two numbers, then $xy = kz + 1$.

Now, let's continue. Go slow with the following. Symbols are going to start flying all over the place. See if you can understand what is happening. Reread and reread until understanding comes. You will be getting a taste of how mathematicians apply reason with the ordered manipulation of symbols to solve a problem.

Using *mod n* arithmetic (i.e., $c^d \equiv y \bmod n$) we know that:

(1) $y \equiv c^d$

[12] Note, when computers become fast enough to factor 200 digit numbers, all Mr. Rishad Clandestine has to do is select larger prime numbers *p* and *q*. Since the number of prime numbers is infinite in scope, it appears as though Mr. Rishad Clandestine *will always be in business.*

Again, using *mod n* arithmetic (i.e., $x^e \equiv c \bmod n$), we know that $x^e \equiv c$. Substituting x^e for c in (1), we get:

(2) $y \equiv c^d \equiv (x^e)^d$

The product law of exponents states that $a^{mn} = (a^m)^n$. By this law we can conclude that $(x^e)^d = x^{ed}$. Hence, (2) now becomes:

(3) $y \equiv c^d \equiv x^{ed}$

Since, $ed = k[\varphi(n)] + 1$, let's tone down the proliferation of symbols by letting $\varphi(n) = z$. Leonhard Euler used this technique many times to simplify the manipulation of complex algebraic expressions. Hence $ed = kz + 1$. Substituting $kz + 1$ for ed in (3), we get:

(4) $y \equiv c^d \equiv x^{ed} = x^{kz+1}$

The sum law of exponents states that $a^{m+n} = a^m a^n$. By this law, (4) becomes:

(5) $y \equiv c^d \equiv x^{ed} = x^{kz+1} = x^{kz}x^1 = x^{kz}x$ (remember that, by convention, $x^1 = x$)

By the product law of exponents, $a^{mn} = (a^m)^n$, (5) becomes:

(6) $y \equiv c^d \equiv x^{ed} = x^{kz+1} = x^{kz}x^1 = x^{kz}x = \left(x^z\right)^k x$

Now, let's replace z with $\varphi(n)$. What is $\left(x^{\phi(n)}\right)^k x$ congruent to in *mod n arithmetic*? We know, from Euler's extension of Fermat's Little Theorem, that:

$x^{\phi(n)} \equiv 1 \bmod n$

From Euler's extension, we get:

$$\left(x^{\phi(n)}\right)^k x = x\left(x^{\phi(n)}\right)^k \equiv x\left(1 \bmod n\right)^k$$

Note that we applied the commutative law of multiplication (ab = ba) to set $\left(x^{\phi(n)}\right)^k x = x\left(x^{\phi(n)}\right)^k$. Then we substituted $1 \bmod n$ for $x^{\phi(n)}$. The exponent *k* simply "goes along for the ride."

Since $1^k = 1$ (1 raised to any power is 1), then we know that $(1 \bmod n)^k = 1 \bmod n$. Substituting $1 \bmod n$ for $(1 \bmod n)^k$, we now have:

$$\left(x^{\phi(n)}\right)^k x \equiv x\left(1 \bmod n\right)$$

We also know that $x\ (1 \bmod n) \equiv x \bmod n$ (the product of a number and 1 is that number). Hence, $y \equiv x \bmod n$! Stringing all this together and thanks to the methods of algebra, (6) becomes:

(7) $y \equiv c^d \equiv x^{ed} = x^{k[\phi(n)]+1} = \left(x^{\phi(n)}\right)^k x \equiv x \bmod n$, or (7) becomes:

(8) $y \equiv x \bmod n$

QED! We have proved what we set out to prove; i.e., $y \equiv x \bmod n$ or *the deciphered number is congruent to Mr. General Q. Public's original number.*

Now, let's replace the symbols with some numbers to illustrate how the whole process works. Rest assured, I will pick small numbers to work with. High-speed computers can "compute" those 100 and 200

digits numbers faster and more accurately than we could ever do but we need to see how the principle is applied.

Mr. Rishad Clandestine chooses two prime numbers, p = 5 and q = 11. These numbers are the *secret deciphering keys*. Therefore, *n* (the *public enciphering key*) = pq = 5·11 = 55 and φ(n) = (p – 1)(q – 1) = 4·10 = 40. We have all the players now: p = 5, q = 11, n = 55, φ(n) = 40. To keep things simple, let's say that Mr. General Q. Public wants to send the number 2 to Mr. Math Student. So, we let x = 2.

Now Mr. Rishad Clandestine has to give Mr. General Q. Public a public encryption key *e*. Remember, *e* is a natural number such that it is relatively prime to 40. We can choose several; let *e* = 23. Next Mr. Rishad Clandestine has to give Mr. Math Student a secret decryption key *d*. Remember, *d* is a natural number such that 23d ≡ 1 mod 40. Let d = 7 since 23·7 = 161 = 1 mod 40.

We are ready to transmit. Mr. General Q. Public must scramble or encrypt the number 2 to another number *c* according to the *encryption function* $x^e \equiv c \bmod n$. Since x = 2, e = 23 and n = 55, then:

$$2^{23} \equiv c \bmod 55$$

You can use your calculator for this one. 2^{23} = 8,388,608. 8,388,608/55 = 152,520 with remainder of 8. Therefore $2^{23} \equiv 8 \bmod 55$. Mr. General Q. Public transmits c = 8 to Mr. Math Student.

After receiving 8 from Mr. General Q. Public, Mr. Math Student must decrypt 8 to another number *y* according to the *deciphering function* $c^d \equiv y \bmod n$. Since c = 8, d = 7, and n = 55, then:

$$8^7 \equiv y \bmod 55$$

Engage your calculators again. 8^7 = 2,097,152 and 2,097,152/55 = 38,130 with remainder of 2. Therefore $8^7 \equiv 2 \bmod 55$. Mr. Math Student has decoded Mr. General Q. Public's message as y = 2. Message received!

Notice that, with our simple example, we found ourselves working with large numbers (e.g., 2^{23} and 8^7). Imagine starting with two prime numbers that are 100 digits in length! The RSA code provides a safe and secure way to transmit data between companies, people, governments, schools, etc. It is the basis for securing data transmitted across the Internet. Until some ingenious mathematician finds a way to break this coding scheme, it will remain safe (for now). Maybe there is no way to break this scheme. Who knows for sure? Only God does in actuality and it may take man a couple of centuries to catch up with His infinite and comprehensive knowledge.

This was a challenging essay, for sure (from grade school codes to some pretty impressive number theory). Yet, the RSA code was generated from two simple mathematical principles (division and remainders), the law of exponents, basic prime number theorems, and rudimentary algebra. Let this be the lesson learned: *that the innovation of mathematical principles can be very useful to the world in which we live.*