# RSA Encryption 1

## Table of Contents



## I. Introduction

In this day and age, the amount of information that traverses the internet increases every day. Much of this information is sensitive and must be kept private, especially where e-commerce is concerned. The primary manner in which this is accomplished is so-called asymmetric key encryption. The prototype for this type of encryption is RSA encryption, named after its founders, Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman. The practical implementation of this algorithm is complex and tedious. While the

theory behind this method is not exactly simple, especially for laymen like myself, I find it both interesting and ingenious. It is this theory of RSA that is the subject of this article.

An analogy that may help to elucidate the basic paradigm is as follows:

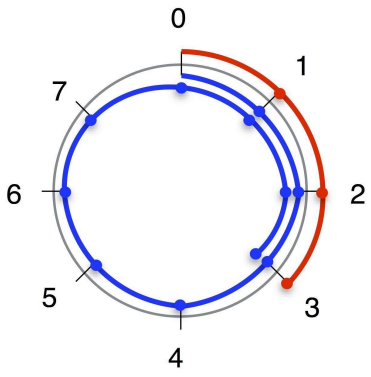
Say Alice wants to send a confidential message to Bob and keep it from Eve, who's always trying to intercept it. Bob sends an open padlock to Alice, a padlock a copy of which Eve or anyone else who wants one can have. Alice puts her message in a box and locks it with the padlock. The nature of the box and lock are such that no one can cut off the lock, cut a hole in the box or otherwise access the message except by using the key to open it, a key that only Bob has. Alice sends the locked message back to Bob, in plain view of Eve, who, without the key, can't open it. When Bob receives the box, he easily opens the box and reads the message. This is an example of a one-way function. The padlock is easy to lock but hard to unlock. Unless, of course, you have the key.

In RSA encryption, the functions of the physical lock and key are accomplished with mathematics. The padlock function is performed by a thing called the public key while the function of the key that Bob uses to unlock the padlock is referred to as the private key.

## II. Necessary Mathematics

### II.A Modular arithmetic[1]

The basis of this algorithm is modular arithmetic, therefore, an introduction to this subject is in order. Modular arithmetic is clock arithmetic. Consider a clock with 8 numbers on its face as follows:




Traveling in the clockwise direction is considered positive; traveling in the counterclockwise direction is considered negative. If you start at 0, there are an infinite number of ways that you could get to the the number 3. Two of these are illustrated in the diagram. The red arc indicates that you could start at 0 and travel three units in the positive direction (i.e, clockwise). A second way is to start at 0 and travel 11 units clockwise. Another way (not illustrated) would be to start at 0 and travel 19 units clockwise. Notice that if you take the number of units traveled and divide it by the number of units

around the face of the clock (in this case 8) you get a remainder of 3 (which is the number at which you end up in each case. These states can be summarized by the following 3 equations:

3 = 3 mod 8
3 = 11 mod 8
3 = 19 mod 8

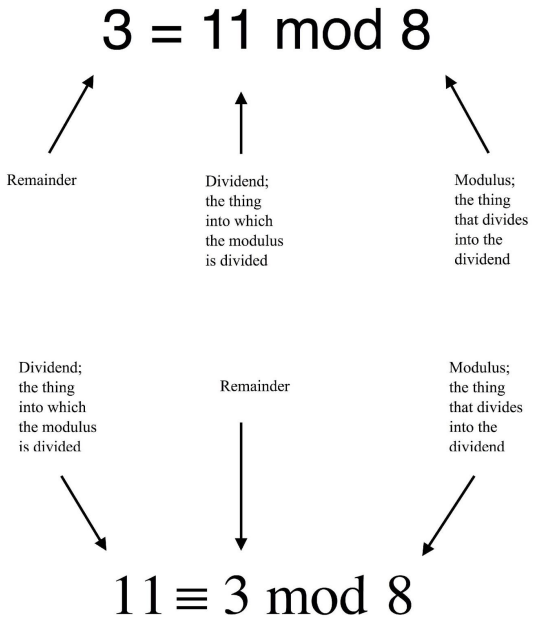
In these equations, "mod" stands for modulus. It corresponds to the number of units around the face of the clock. The number to the left of "mod" is the dividend - the thing into which the modulus is divided. In each case, this operation results in the a remainder, the number on the left side of the equation, in these cases, 3.

Another way of saying all this is the following:

$$3 \equiv 3 \bmod 8$$
$$11 \equiv 3 \bmod 8$$
$$19 \equiv 3 \bmod 8$$

Take the second equation above. In words, this equation says: 11 is congruent to 3 mod 8. In this equation, 8, again is the divisor (the thing that does the dividing); 11 is the dividend (the thing that gets divided by the divisor); and 3 is the remainder.

All of the above is summarized in the following diagram:



The last issue to be discussed in this section is one of nomenclature. The expression $m \mid a_1 - a_2$ means $m$ goes into $a_1 - a_2$ evenly, without a remainder. For example, $8 \mid 18-2$ (i.e., 8 divides 18-2—which equals 16—two times, without a remainder). There's a lot more to modular arithmetic than is presented here but this will do for sake of this discussion.

## II.B Exponents and roots[2]

$a^n$ means multiply $a$ together $n$ times. $a$ is referred to as a base. $n$ is referred to as an exponent. For example, $2^3 = 2 \times 2 \times 2 = 8$. In words, we would say that 2 raised to the 3rd power equals 8, or 2 to the third power equals 8.

$\sqrt[n]{b}$ means find a number, , that when multiplied together  times, will equal b. For example, $\sqrt[3]{8}$ means find a number that, when multiplied together 3 times will equal 8. In this case, $a = 2$, $b = 8$ and $n = 3$. $2 \times 2 \times 2 = 8 = 2^3$, thus $\sqrt[3]{8} = 2$. In words, we would say that the cube root (or third root) of 8 is 2. Or alternatively, 2 is the cube root (or third root) of 8. If $n = 2$ (i.e., $a = \sqrt[2]{b}$) we would say that $a$ is the square root of $b$. If $n = 7$, (i.e., $a = \sqrt[7]{b}$), we would say that $a$ is the 7th root of $b$, and so forth. Note that if no $n$ is specified, then $n$ is assumed to be 2. For example, $\sqrt{25} = \sqrt[2]{25} = 5$.

$\sqrt[n]{b}$ can also be expressed as an exponent. Specifically, $\sqrt[n]{b} = b^{1/n}$. For example, $\sqrt[3]{8} = 8^{1/3} = 2$ and $\sqrt{25} = 25^{1/2} = 5$.

When two exponential expressions have the same bases (i.e., the same $a$), if you multiply the two expressions together, to get the answer, you add the two exponents together and raise the base number to that sum. For example, $2^2 \cdot 2^3 = 2^{(2+3)} = 2^5 = 2 \times 2 \times 2 \times 2 \times 2 = 32$, or more generally, $\left(a^n\right) \cdot \left(a^m\right) = a^{(n+m)}$. The following might be helpful in showing why this is true: $2^2 = 2 \times 2$. $2^3 = 2 \times 2 \times 2$. $2^2 \cdot 2^3$ means multiply $2^2$ times $2^3$ which equals $(2 \times 2) \times (2 \times 2 \times 2)$ which equals $2 \times 2 \times 2 \times 2 \times 2$ which is another way of saying $2^5$. Notice that if you simply add the exponents of the exponential expressions to be multiplied, this will tell you how many times to multiply the base number together with itself. And the number of times you multiply the base number together with itself is, by definition, the exponent to which you raise the base number to get the answer.

If you have two exponential expressions have the same bases (i.e., the same $a$), if you divide one of the expressions into the other, to get the answer, you subtract the exponent of the divisor (the expression thats doing the dividing) from the exponent of the dividend (the expression thats being divided by the divisor) and raise the base number to that difference. For example,

$$\frac{2^5}{2^3} = \frac{32}{8} = 4 = 2^2 = 2^{(5-3)}$$

In general,

$$\frac{a^m}{a^n} = a^{(m-n)}$$

If you have an expression with an exponent, and you raise that expression to an exponent, you multiply the exponents together and raise the base number to that new exponent. For example,

$$\left(2^3\right)^2 = 8^2 = 64 = \left(2\times 2\times 2\right)^2 = \left(2\times 2\times 2\right)\cdot\left(2\times 2\times 2\right) = 2^{3\cdot 2} = 2^6$$

Or more generally,

$$\left(a^m\right)^n = a^{(m\cdot n)}$$

**II.C Logarithms**[3]

Definition: if $a^x = y$ then $log_a\, y = x$. In words, the logarithm ($log$) of some number, $y$, is the exponent, $x$, that you need to raise the base number, $a$, to to get the number $y$.

Properties:

(1) Product rule

a. Statement: $log_x\, a \cdot b = log_x\, a \;+\; log_x\, b$

b. Proof

Let $log_x\, a = n \Rightarrow x^n = a \Rightarrow x^{log_x a} = a$
Let $x^l = a \Rightarrow log_x\, a = l$
$x^m = b \Rightarrow log_x\, b = m$
$x^n = a \cdot b \Rightarrow log_x\, a \cdot b = n$
$x^n = x^l \cdot x^m$
$x^n = x^{(l+m)}$; therefore
$n = l + m$; substituting
$log_x\, a \cdot b = log_x\, a + log_x\, b$

(2) Quotient rule

a. Statement: $log_x \frac{a}{b} = log_x\, a - log_x\, b$

b. Proof

Let $log_x\, a = n \Rightarrow x^n = a \Rightarrow x^{log_x a} = a$
Let $x^l = a \Rightarrow log_x\, a = l$
$x^m = b \Rightarrow log_x\, b = m$
$x^n = a \cdot b \Rightarrow log_x\, a \cdot b = n$
$x^n = \frac{x^l}{x^m}$
$x^n = x^{(l-m)}$; therefore
$n = l - m$; substituting
$log_x \frac{a}{b} = log_x\, a - log_x\, b$

(3) Power rule

a. Statement: $log_x\, a^c = c\, log_x\, a$

b. Proof

| | |
|---|---|
| Let $log_x\, a = b \Rightarrow x^b = a$; | multiply by $c$ |
| $c\, log_x\, a = b \cdot c$ | |
| $(x^b)^c = x^{bc} = a^c$; | this means that |
| $log_x\, a^c = bc$ ; | substituting |
| $log_x\, a^c = c\, log_x\, a$ | |

(4) Change of base rule

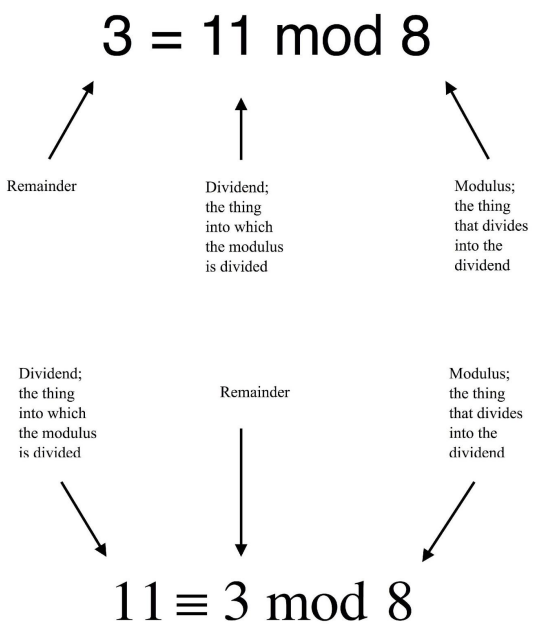
a. Statement: $log_a\, x = \frac{log_b x}{log_b a}$

b. Proof

| | |
|---|---|
| Let $log_a\, x = y$; | then |
| $a^y =$ x; | take log to the base b of both sides |
| $log_b\, a^y = log_b\, x$; | apply power rule |
| $y\ log_b\, a = log_b\ x$; | divide both sides by $log_b\, a$ |
| $y = \frac{log_b x}{log_b a}$; | substitute for $y$ |
| $log_a\, x = \frac{log_b x}{log_b a}$ | |

## II.D Summary of mathematics

1. Modular arithmetic




2. Exponents and roots

   a. Exponent

$$a_i{}^n = a_1 \cdot a_2 \cdot a_3 \cdot \ \ldots \ a_n$$

$$a^n \cdot a^m = a^{(n+m)}$$

$$\frac{a^m}{a^n} = a^{(m-n)}$$

$$(a^m)^n = a^{m \cdot n}$$

   b. Root

$$\text{if } y = a^n \Rightarrow \sqrt[n]{y} = a$$

$$\sqrt[n]{y} = y^{\frac{1}{n}} = a$$

3. Logarithms

if $a^x = y$ then $log_a\, y = x$

$log_x\, a \cdot b = log_x\, a \; + \; log_x\, b$

$log_x\, \frac{a}{b} = log_x\, a \; - \; log_x\, b$

$log_x\, a^c = c\, log_x\, a$

$log_a\, x = \frac{log_b x}{log_b a}$

## III. Proof

### III.A Proof of Euler's Totipotent Theorem[4]

The mathematical function that's used to serve as the lock and key described in the introduction to this article is called a trapdoor function. The equation, itself, is easy to solve but it has an inverse that's difficult to solve. Hopefully, how such a function can be used for encryption will become more clear by the end of this discussion. The theorem on which RSA encryption is based is Euler's Totipotent theorem. This is the equation that describes that theorem:

$$m^{\Phi(n)} \equiv 1 \bmod n$$

where,

$n$ tells us how many numbers are on "the face of the clock" that we're going to use to do modular arithmetic; said differently, $n$ is the number we're going to divide into $m^{\Phi(n)}$ to get a remainder of 1.

$\Phi(n)$, **Euler's totient function**,[5] is a function that counts the number of relatively prime positive integers less than or equal to $n$. By positive integers, I mean whole numbers like 1, 2, 3, 4, etc. Relatively prime means that the integer and $n$ share no common factors other than 1.

$\Phi(n)$ is a number. In this case we're using it as an exponent. In the equation above, it means to multiply $m$ together with itself $\Phi(n)$ times.

Here are some examples that demonstrate the concept of relatively prime.

$\Phi(1)=1$

$\Phi(2)=1$

$\Phi(3)=2$ (i.e. 1,2)

$\Phi(4)=2$ (i.e. 1,3)

$\Phi(5)=4$ (i.e. 1,2,3,4)

$\Phi(6)=2$ (i.e. 1,5)

$\Phi(7)=6$ (i.e. 1,2,3,4,5,6)

$\Phi(8)=4$ (i.e. 1,3,5,7)

$\Phi(9)=6$ (i.e. 1,2,4,5,7,8)

$\Phi(10)=4$ (i.e. 1,3,7,9)

Let's examine $\Phi(9)$ in more detail to clarify its meaning. In order to do this, we have to start by making a list of numbers less than 9 that are relatively prime to 9 (i.e, that share no factor with 9 other than 1):

1 is relatively prime to everything because 1 is the only factor of 1, so include 1.

No number other than 1 divides both 2 and 9 evenly, so include 2 in our list.

3 divides evenly into 3 and 9; that is, 3 and 9 share a factor of 3 so exclude 3.

No number other than 1 divides both 4 and 9 evenly so include 4 in our list.

No number other than 1 divides both 5 and 9 evenly so include 5 in our list.

3 goes into 6 twice and 9 three times; 6 and 9 share a factor of 3 so exclude 6.

No number other than 1 divides 7 and 9 evenly so include 7 in our list.

No number other than 1 divides 8 and 9 evenly so include 8 in our list.

So here's our list: 1, 2, 4, 5, 7, 8. Count the numbers in our list: 6 - that's the value of $\Phi(9)$.

Notice something. For any prime number $n$, $\Phi(n)$ is $n-1$. This makes sense since the definition of a prime number is that the only factors it has are 1 and itself. You can't include the number itself in $\Phi(n)$ because any number goes into itself once. For example, for $n = 7$, 7 goes into 7 once, so when calculating $\Phi(n)$, you have to exclude 7. But you would include all the other numbers from 1 to 6 in enumerating $\Phi(n)$.

Now back to Euler's totient theorem. That's the equation we started with: $m^{\Phi(n)} \equiv 1 \bmod n$. First of all, it only works if $m$ and $n$ are relatively prime to each other. Now let me prove it to you. We'll be abstract and use letters to start, then put in some numbers to make it clearer.

Let's find a set of numbers that consists of all the positive integers that are relatively prime to $n$, like we would do if we were trying to figure out Euler's totient function for that number. Notice that when

you do this, all of the members of the set, called the set's elements, have to be different from each other (i.e. each number is unique.) Call that set $A$. $A$ would consist of $r_1$, $r_2$, $r_3$, $r_4$ $\ldots r_{\Phi(n)}$, where $r$ are numbers relatively prime to $n$. (In the example of $n=9$, the first element of the set, $r_1$ is 1 because, as we've already said, 1 is relatively prime to all numbers. The other elements are $r_2=2$, $r_3=3$, $r_4=5$, $r_5=7$, $r_6=8$. $\Phi(n)$ is 6, so $r_{\Phi(n)}=r_6$ — or the $\Phi(n)^{\text{th}}$ (the 6th) relatively prime number in the series—in this case, that relatively prime number is 8.) When you define a set in math, you put the elements of the set in curly brackets. So $A=\{r_1, r_2, r_3, r_4 \ldots r_{\Phi(n)}\}$. Now we'll define a second set, $B$, by multiplying each element in $A$ by the number, $m$. So $B=\{m\cdot r_1, m\cdot r_2, m\cdot r_3, m\cdot r_4 \ldots m\cdot r_{\Phi(n)}\}$. We're just multiplying each element of $A$ by the same number, so like $A$, all the elements of $B$ have to be unique. Now let's take the $\bmod n$ of sets $A$ and $B$. That means take $\bmod n$ of each element in $A$ to make a new set, $A'$, and take $\bmod n$ of each element in $B$ to make a new set, $B'$. It turns out, if we do this, $A'$ and $B'$ will be the same. To see this, let's put in some numbers.

Let $m=5$, $n=8$. Notice that 5 and 8 are relatively prime. (As stated at the outset, they have to be or this thing won't work.) A different way of putting it is that the greatest common divisor of 5 and 8 is 1. Or, said yet another way, the greatest number that divides both 5 and 8 evenly is 1. Anyway,

$$\begin{aligned} A &= \{1, 3, 5, 7\} \\ B &= \{5\cdot 1, 5\cdot 3, 5\cdot 5, 5\cdot 7\} \\ &= \{5, 15, 25, 35\} \end{aligned}$$

So for each element, we're going to take $\bmod n$. Mathematically speaking, we can write this as $r_i \bmod n$; $i$, in this case, being 1, 2, 3 or 4.

| For $A'$ | For $B'$ |
|---|---|
| $1 \bmod 8 = 1$ | $5 \bmod 8 = 5$ |
| $3 \bmod 8 = 3$ | $15 \bmod 8 = 7$ |
| $5 \bmod 8 = 5$ | $25 \bmod 8 = 1$ |
| $7 \bmod 8 = 7$ | $35 \bmod 8 = 3$ |

So $A = A' = \{1, 3, 5, 7, \}$ and $B' = \{5, 7, 1, 3, \}$; From this, you can see that $A'$ and $B'$ have the same elements.

Since the elements of the sets are the same, if the elements of each set are multiplied together with each other, the resulting products should be equal:

$$(1 \cdot 3 \cdot 5 \cdot 7) = (5 \cdot 7 \cdot 1 \cdot 3)$$

But remember where these numbers came from:

$$[(1 \bmod 8) \cdot (3 \bmod 8) \cdot (5 \bmod 8) \cdot (7 \bmod 8)] = [(5 \bmod 8) \cdot (15 \bmod 8) \cdot (25 \bmod 8) \cdot (35 \bmod 8)]$$

It's easy to prove that $[(a \bmod n) \cdot (b \bmod n)] \bmod n = (a \cdot b) \bmod n$ [6]

Let $a$, $b$, $q_1$, $q_2$, $q_3$, $r_1$, $r_2$ and $r_3$ be integers

By definition

$r_1 = a \bmod n$ means $a = q_1 n + r_1$

$r_2 = b \bmod n$ means $b = q_2 n + r_2$

$r_3 = r_1 \cdot r_2 \bmod n$ means $r_1 \cdot r_2 = q_3 n + r_3$

with $0 \le r_1, r_2, r_3 < n$

We've seen that

$r_1 = a \bmod n$ and $r_2 = b \bmod n$

Therefore,

$r_1 \cdot r_2 = \left(a \bmod n\right) \cdot \left(b \bmod n\right)$

And since

$r_3 = r_1 \cdot r_2 \bmod n$

then

$r_3 = \left[\left(a \bmod n\right) \cdot \left(b \bmod n\right)\right] \bmod n$

From what I've already told you

$$a \cdot b = \left(q_1 n + r_1\right)(q_2 n + r_2)$$

$$= q_1 q_2 n^2 + (q_1 r_2 + q_2 r_1) n + r_1 r_2$$

$$= q_1 q_2 n^2 + (q_1 r_2 + q_2 r_1) n + q_3 n + r_3$$

$$= (q_1 q_2 n + q_1 r_2 + q_2 r_1 + q_3) n + r_3$$

The equation $a \cdot b = \left(q_1 q_2 n + q_1 r_2 + q_2 r_1 + q_3\right) n + r_3$ should look familiar

It means that if you divide $a \cdot b$ by $n$ you get a remainder of $r_3$

Which means $r_3 = \left(a \cdot b\right) \bmod n$

But $r_3 = \left[\left(a \bmod n\right) \cdot \left(b \bmod n\right)\right] \bmod n$

Therefore, $\left[\left(a \bmod n\right) \cdot \left(b \bmod n\right)\right] \bmod n = \left(a \cdot b\right) \bmod n$

Which is what we were trying to prove. Let's check it out by trying some numbers:

$$\left[(10 \bmod 8)\cdot(15 \bmod 8) \bmod 8\right] = (10\cdot 15) \bmod 8$$

$$(2\cdot 7) \bmod 8 = 150 \bmod 8$$

$$14 \bmod 8 = 6 = 150 \bmod 8 \ .$$

That is, 14/8 = 1 with remainder 6; 150/8 = 18 with the same remainder: 6.
By similar arguments to those just employed, you can generalize this result and show that any number of terms can be multiplied together on each side. Like this:

$$\left[(a \bmod n)\cdot(b \bmod n)\cdot(c \bmod n)\cdot(d \bmod n)\ldots\right] \bmod n = (a\cdot b\cdot c\cdot d\cdot\ldots) \bmod n$$

Now take mod 8 of the following equation:

$$\left[(1 \bmod 8)\cdot(3 \bmod 8)\cdot(5 \bmod 8)\cdot(7 \bmod 8)\right] = \left[(5 \bmod 8)\cdot(15 \bmod 8)\cdot(25 \bmod 8)\cdot(35 \bmod 8)\right]$$

You get:

$$\left[(1 \bmod 8)\cdot(3 \bmod 8)\cdot(5 \bmod 8)\cdot(7 \bmod 8)\right] \bmod 8 = \left[(5 \bmod 8)\cdot(15 \bmod 8)\cdot(25 \bmod 8)\cdot(35 \bmod 8)\right] \bmod 8$$

$$\left[(1 \bmod 8)\cdot(3 \bmod 8)\cdot(5 \bmod 8)\cdot(7 \bmod 8)\right] \bmod 8 = \left[(5\cdot 1 \bmod 8)\cdot(5\cdot 3 \bmod 8)\cdot(5\cdot 5 \bmod 8)\cdot(5\cdot 7 \bmod 8)\right] \bmod 8$$

$$(1 \bmod 8\cdot 3 \bmod 8\cdot 5 \bmod 8\cdot 7 \bmod 8) = \left[(5\cdot 1)\cdot(5\cdot 3)\cdot(5\cdot 5)\cdot(5\cdot 7)\right] \bmod 8$$

This gives

$$(1\cdot 3\cdot 5\cdot 7) = (5\cdot 1\cdot 5\cdot 3\cdot 5\cdot 5\cdot 5\cdot 7) \bmod 8$$

$$(1\cdot 3\cdot 5\cdot 7) = (5\cdot 5\cdot 5\cdot 5\cdot 1\cdot 3\cdot 5\cdot 7) \bmod 8$$

$$(1\cdot3\cdot5\cdot7)=(5\cdot5\cdot5\cdot5)(1\cdot3\cdot5\cdot7)\bmod 8$$

$$(1\cdot3\cdot5\cdot7)=5^4(1\cdot3\cdot5\cdot7)\bmod 8$$

$105=105(5^4)\bmod 8$ ; Divide both sides by $105$

$$1=5^4 \bmod 8$$

This means, if you divide $5^4$ by 8, you get a remainder of 1. Hmm, that looks a lot like the Euler's Totipotent theorem equation. Recall that $m = 5$ and $n = 8$. Making these substitutions, the above equation becomes:

$$1=m^4 \bmod n$$

But notice that the exponent 4 is the same as $\Phi(n)$. It has to be because we multiplied $m$ times each element in the set $A$ to get set $B$ and the number of elements in set $A$ *is* $\Phi(n)$. So,

$$1=m^{\Phi(n)} \bmod n$$

That's the Euler's Totipotent theorem expressed as a standard equation with an equal sign instead of as a congruence relationship, as it was first presented above. We could put in variables and make the above demonstration more rigorous, but I think you get the idea.

There are a few other things that need to be discussed before it can be shown how the above equation is used for encryption.

**III.B Deriving** $m=m^{k\cdot\Phi(n)+1} \bmod n$

$1^k=1$ You can put in any number you want for $k$. $1^3=1\cdot1\cdot1$. $1^5=1\cdot1\cdot1\cdot1\cdot1$. No matter how many times you multiply one with itself, you still get 1. Let's go back to this equation for a minute: $1=m^{\Phi(n)} \bmod n$. Both sides of this equation are equal to 1, so if we raise both sides of this equation to

the $k^{\text{th}}$ power, we don't change the value of either side. Recall from the Exponent section you raise a number that is already raised to an exponent, by another exponent, you multiply the exponents together. For example, $\left(2^2\right)^3 = 4^3 = 4 \cdot 4 \cdot 4 = 64$. Equivalently, $\left(2^2\right)^3 = 2^{2 \cdot 3} = 2^6 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64$. So $1 = 1^k = \left(m^{\Phi(n)}\right)^k \bmod n$; therefore, $1 = m^{k \cdot \Phi(n)} \bmod n$.

Next multiply both sides of this equation by $m$. We get $m \cdot 1 = m \cdot m^{k \cdot \Phi(n)} \bmod n$ which means $m = m \cdot m^{k \cdot \Phi(n)} \bmod n$. Any number (or variable) raised to the 1rst power is just that number or variable. So $m = m^1$. Again, recall from the Exponents review section that when you multiply a number raised to one exponent by the same number raised to another exponent, you get the number raised to the two exponents added together. Example: $2^2 \cdot 2^3 = 4 \cdot 8 = 32 = 2^{(2+3)} = 2^5$. Therefore, $m = m^1 \cdot m^{k \cdot \Phi(n)} \bmod n$ is equivalent to $m = m^{k \cdot \Phi(n)+1} \bmod n$.

### III.C Product of 2 primes

The number $n$ can be broken down into the product of two prime numbers, $P_1$ and $P_2$:

$$n = P_1 \cdot P_2$$

### III.D Proof of $\Phi(n) = \Phi(P_1) \cdot \Phi(P_2)$ [7]

### III.D.1 Example

$\Phi(n) = \Phi(P_1) \cdot \Phi(P_2)$. To see this, the best thing to do is start with an example. Note before starting that for this to work, $P_1$ and $P_2$ need to be relatively prime (that is, their greatest common denominator is 1, or equivalently—as has been stated previously—the only common factor they share is 1).

Consider $n = P_1 \cdot P_2 = 21, P_1 = 3, P_2 = 7$ . List the relatively prime numbers that you need to calculate $\Phi(P_1 \cdot P_2)$ and put them into, set $S_1$ :

$$S_1 = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$$

Call the elements in $S_1$ , $a_i$ where $i = 1,2 \ldots \Phi(P_1 \cdot P_2)$ .

Next, list the relatively prime numbers that you need to calculate

$$\Phi(P_1) = \Phi(3) \Rightarrow 1, 2$$

$$\Phi(P_1) = \Phi(7) \Rightarrow 1, 2, 3, 4, 5, 6$$

Put those numbers into a set in which you pair numbers from $\Phi(P_1)$ and $\Phi(P_2)$ . Call it $S_2$ :

$$S_2 = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6), (2,1), (2,2), (2,3), (2,4), (2,5), (2,6)\}$$

Call the first pair of the elements of $S_2$ , $b_j$ where $j = 1 \ldots \Phi(P_1)$ . Call the second pair of the elements of $S_2$ , $c_k$ where $k = 1 \ldots \Phi(P_2)$ .

Now we need to count elements in each set. By definition, the number of elements in $S_1$ is $\Phi(P_1 \cdot P_2)$ , in this case, 12. To find the number of elements in $S_2$ , we have to consider how we made the set. Namely, we took each element from $\Phi(P_1)$ and paired it with each element of $\Phi(P_2)$ :

| | | | From $\Phi(P_2)$ | | | |
|---|---|---|---|---|---|---|
| From $\Phi(P_1)$ | **1** | **2** | **3** | **4** | **5** | **6** |
| **1** | 1,1 | 1,2 | 1,3 | 1,4 | 1,5 | 1,6 |
| **2** | 2,1 | 2,2 | 2,3 | 2,4 | 2,5 | 2,6 |

You can see from this table that the number of elements in the set is just the number of rows times the number of columns: 2 x 6. If the table were a 3 by 5 table, then the number of elements would be 3 x 5 = 15. In every case, the number of rows is $\Phi(P_1)$ and the number of columns is $\Phi(P_2)$. Therefore, in general, the number of elements in such a set is $\Phi(P_1)\cdot\Phi(P_2)$.

### III.D.2 Introduction to proof of one-to-one correspondences between elements of sets $S_1$ and $S_2$

The next thing to do is to prove that there is a one-to-one correspondence between elements of sets $S_1$ and $S_2$. To do this, we need to associate elements $a_1 \mathrm{mod} P_1 P_2$ from $S_1$ with paired elements $a_1 \mathrm{mod} P_1, a_1 \mathrm{mod} P_2$ from $S_2$. It looks like this:

$$
\begin{aligned}
1 &\rightarrow 1mod3,\ 1mod7 \rightarrow 1,1\\
2 &\rightarrow 2mod3,\ 2mod7 \rightarrow 2,2\\
4 &\rightarrow 4mod3,\ 4mod7 \rightarrow 1,4\\
5 &\rightarrow 5mod3,\ 5mod7 \rightarrow 2,5\\
8 &\rightarrow 8mod3,\ 8mod7 \rightarrow 2,1\\
10 &\rightarrow 10mod3, 10mod7 \rightarrow 1,3\\
11 &\rightarrow 11mod3, 11mod7 \rightarrow 2,4\\
13 &\rightarrow 13mod3, 13mod7 \rightarrow 1,6\\
16 &\rightarrow 16mod3, 16mod7 \rightarrow 1,2\\
17 &\rightarrow 17mod3, 17mod7 \rightarrow 2,3\\
19 &\rightarrow 19mod3, 19mod7 \rightarrow 1,5\\
20 &\rightarrow 20mod3, 20mod7 \rightarrow 2,6
\end{aligned}
$$

You can see from the table that, in this case, there is, in fact, a one-to-one correspondence between elements of sets $S_1$ and $S_2$. However, to generalize this result, we have to show:

1. Different elements in $S_1$ are associated with different pairs in $S_2$

2. Each pair in $S_2$ is associated with a unique element in $S_1$

### III.D.3 Different elements in $S_1$ are associated with different pairs in $S_2$

To accomplish #1, suppose $a_1$ and $a_2$ are different elements of $S_1$ but are both mapped to the same element in $S_2$. If this were the case, then, for example:

$$a_1 \Rightarrow a_2 \bmod P_1,\ a_2 \bmod P_2$$
and
$$a_2 \Rightarrow a_2 \bmod P,\ a_2 \bmod P_2$$

Let's take the case of $a_1 \Rightarrow a_2 \bmod P_1,\ a_2 \bmod P_2$. This means

$$a_1 \equiv a_2 \bmod P_1 \text{ and } a_1 \equiv a_2 \bmod P_2$$

Remember,

$a_1 \equiv a_2 mod P_1$ means $a_1 = P_1 \cdot y + a_2$
and
$a_1 \equiv a_2 mod P_2$ means $a_1 = P_2 \cdot y + a_2$
where
$x$ and $y$ are integers (i.e., not fractions)

Rearranging the right-sided equations:

$a_1 - a_2 = P_1 x$ and $a_1 - a_2 = P_2 y$

so

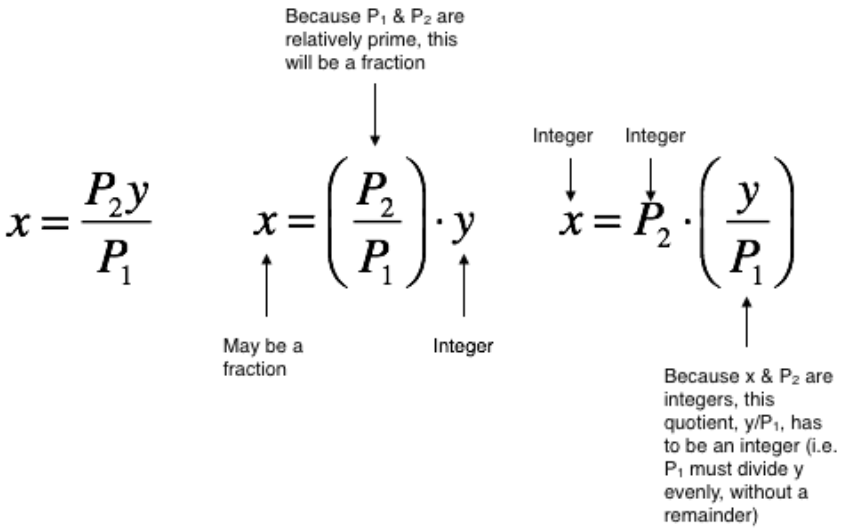
$P_1 x = P_2 y$

and

$$x = \frac{P_2 y}{P_1}$$

That means that $P_1$ divides $y$ evenly (i.e., without a remainder). Mathematically, this is expressed as follows: $P_1 | y$. Why is this true? Well, $P_1$, $P_2$, $x$ and $y$ are all integers. $P_1$ and $P_2$ are relatively prime. That means that they share no common factors except 1. Therefore, if you divide $P_1$ into $P_2$, you get a fraction. If you multiply a fraction by an integer, like $y$, you may make their product, $x$, an integer but it's also possible that their product may be a fraction. But that won't do because we've already said that $x$ *is definitely* an integer. In order to make $x$ an integer, $P_1$ would have to divide evenly into y to get an integer. Then when you multiply that integer, y/ $P_1$, with another integer, $P_2$, their product, $x$, is sure to be an integer.

This diagram may help you visualize it better:



So if $P_1$ divides $y$ evenly, that means that $y = P_1 \cdot q$ where $q$ is a positive integer. We've seen previously that $a_1 = P_2 \cdot y + a_2$. Substituting $y = P_1 \cdot q$, we get $a_1 = (P_1 \cdot P_2)q + a_2$. But $a_1 = (P_1 \cdot P_2)q + a_2$ is another way of saying $a_1 \equiv a_2 \bmod P_1 \cdot P_2$, just as $a_1 \equiv a_2 \bmod P_1$ means $a_1 = P_1 \cdot x + a_2$ and $a_1 \equiv a_2 \bmod P_2$ means $a_1 = P_2 \cdot y + a_2$.

So after all this, we end up with $a_1 \equiv a_2 \bmod P_1 \cdot P_2$. For this equation to be true, $a_1$ must equal $a_2$. But this contradicts our original premise that $a_1$ and $a_2$ are different. Why must $a_1 = a_2$ in the equation $a_1 \equiv a_2 \bmod P_1 \cdot P_2$? Because all of the elements of set $S_1$ are relatively prime to, and less than, $P_1 \cdot P_2$. When you take $\bmod P_1 \cdot P_2$ of $a_1$, you divide $P_1 \cdot P_2$ into $a_1$. Since every element of set $S_1$ is less than $P_1 \cdot P_2$, $P_1 \cdot P_2$ goes into every element, $a_i$, zero times. The only way to make the equation $a_1 \equiv a_2 mod P_1 P_2$ true is if the remainder, $a_2$, equals $a_1$. Another way of saying it is $a_1 = P_1 \cdot P_2 \cdot q + a_2$; $q = 0$ so $a_1 = P_1 \cdot P_2 \cdot 0 + a_2 \Rightarrow a_1 = 0 + a_2 \Rightarrow a_1 = a_2$.

The above argument shows that it's not possible for any two elements of $S_1$ to map to the same element in $S_2$. Therefore, it must be that only one element from $S_1$ can map to a given element of $S_2$. So that proves #1.

### III.D.4 Each pair in $S_2$ is associated with a unique element in $S_1$ (proof of existence)

### III.D.4.a Chinese Remainder Theorem

To prove #2, we need to show that each paired element of $S_2$, $(b,c)$, maps to a unique element of $S_1$, $a$. Mathematically, this can be expressed as follows:

$$a = b \bmod P_1 \text{ and } a = c \bmod P_2$$

This is essentially the Chinese Remainder Theorem so we need to prove that theorem.

The equation $a = b \bmod P_1$ means that if you multiply $P_1$ by some integer (call that integer $y$) then add a remainder of $b$ to it, you get $a$: $a = P_1 y + b$. Likewise, $a = c \bmod P_2$ means $a = P_2 z + c$ where $z$ is any integer. Since the right side of both of these equations are equal to $a$:

$$P_1 y + b = P_2 z + c \text{ and}$$

$$P_1 y = P_2 z = c - b \text{ where } c \text{ and } b \text{ are just integers}$$

The last equation above is called **Bezout's identity**[8].

### III.D.4.b Bezout's identity I

The proof of Bezout's identity is as follows:

$y$ and $z$ are positive integers, both of which are not zero. By definition, let $c - b$ in the above equation equal $g$. Let $m = P_1 y + P_2 z > 0$. We'll call $m$ a linear combination of $P_1$ and $P_2$. Let $S_{lc}$ be the set of all linear combinations that satisfy the conditions of $m$. Because both $y$ and $z$ are not both zero, there must be at least one value for $m$. Therefore, $S_{lc}$ has at least one element and so is not an empty set. There's a thing called the **well-ordered principle**[9] that states that, given a nonempty set of

natural numbers (i.e., positive integers), such a set must have a least element. This is so intuitive that we won't prove it in this article but a proof of this principle can be found here. At any rate, applying the well-ordered principle, $S_{lc}$ must have a least element.

Now choose $y$ and $z$ so that $m$ *is* that least element. Furthermore, choose $g$ such that it is the greatest common divisor of $P_1$ and $P_2$.

Since $g$ is a common divisor of $P_1$ and $P_2$, it must also be a divisor of $m$. This can be seen as follows:

If $g$ is a divisor of $P_1$, that means that $P_1 = kg$ and $P_2 = lg$ where $k$ and $l$ are integers.

Thus,

$$m = P_1 y + P_2 z = kyg + lzg = (ky + lz)\, g$$

$$m/g = ky + lz$$

$k$, $l$, $y$ and $z$ are all integers.

Therefore $ky + lz$ is an integer.

Therefore $\frac{m}{g}$ yields an integer which means that $g$ is a divisor of $m$.

In particular, $g$ must be $\leq m$ or else $\frac{m}{g}$ would be a fraction (which it can't be because we just showed it was an integer).

### III.D.4.c Bezout's identity II

Next, $m$ is also a common divisor of $P_1$ and $P_2$ (i.e. $m$ divides both $P_1$ and $P_2$ evenly). The proof of this is as follows:

Let $m = P_1 y + P_2 z > 0$; $P_1$, $P_2$, $y$ and $z$ are all integers; $y$ and $z$ are not both 0

Furthermore, choose $y$ and $z$ such that $m$ is the least positive linear combination of $P_1$ and $P_2$.

We're trying to divide $m$ into $P_1$ and $P_2$. Let's consider the case of dividing $m$ into $P_1$ since the case of dividing $m$ into $P_2$ is similar.

When you divide $m$ into $P_1$, you get an answer, $q$, and a remainder, $r$. You can get back $P_1$ by multiplying $q$ by $m$ and adding the remainder, $r$. That is,

$$P_1 = qm + r \text{ where } 0 \le r < m$$

This is called the **quotient-remainder theorem**[10]. It's so intuitive that we won't prove it here although a proof can be found at the link listed below.

Substituting in from our original definition of $m$ above, we get

$$r = P_1 - qm = P_1 - q(P_1 y + P_2 z) = P_1 - qP_1 y - qP_2 z$$

rearranging:

$$r = (1 - qy)P_1 + (-qz)P_2$$

Look at the form of this last equation. It means that $r$ is a non-negative linear combination of $P_1$ and $P_2$, non-negative because we already said that $r$ is greater than or equal to zero (i.e., $0 \leq r < m$).

But we also said that $m$ is the *least* positive linear combination of $P_1$ and $P_2$. This can't be true if $r$ is greater than 0 since $r$ is also less than $m$. If that were true then $r$ would be the least positive linear combination of $P_1$ and $P_2$. The only way that $m$ could be the least positive linear combination and $r$ could be $\geq 0$ and $< m$ is if $r = 0$.

But if $r = 0$, that means that $m$ divides $P_1$ evenly, which is what we were trying to prove.

As stated above, the proof that $m$ divides $P_2$ evenly is similar.

**III.D.4.d Bezout's identity III**

In the previous section, we showed that $g$, the greatest common divisor of $P_1$ and $P_2$, is $\leq m$. In this last section, we showed that $m$ is also a divisor of $P_1$ and $P_2$. But it can't be true that $g < m$ because $g$ is the *greatest* common divisor. Therefore, it must be true that $g$ *equals* $m$. Now do some algebraic manipulation:

$g = m$; rearrange this
$m = g$; recall that $m = P_1y + P_2z$ and $g = c - b$; substitute for $m$ and $g$
$P_1y + P_2z = c - b$

$P_1y + P_2z = c - b$; That's what we were trying to prove.

$P_1y + P_2z = c - b$ was derived from $a = bmodP_1$ and $a = cmodP_2$. We showed that $P_1y + P_2z = c - b$ is true. Therefore, $a = bmodP_1$ and $a = cmodP_2$ must be true. $a = bmodP_1$ and $a = cmodP_2$ is a mathematical expression of the statement that each pair $bc$ from set $S_2$ maps to an element, $a$, from set $S_1$. Since $a = bmodP_1$ and $a = cmodP_2$ is true, then the statement that it mathematically represents must be true. This proves that such a correspondence between $S_2$ to $S_1$ *exists*. What remains to be proven is that each of those '$a$' element to which each '$bc$' pair maps are *unique* (i.e., there's only one '$bc$' pair for each 'a').

**III.D.4.e Bezout's identity IV**

That proof is similar to one we've already seen. It goes like this: if $a = n$ and $a = n'$ both satisfy

$$a = bmodP_1 \text{ and } a = cmodP_2$$

then $n \equiv n'modP_1$ and $n \equiv n'modP_2$. If that's true, then $P_1|(n - n')$ and $P_1|(n - n')$. And because $P_1$ and $P_2$ are relatively prime, $P_1 \cdot P_2|(n - n')$. That means $n \equiv n'modP_1P_2$, which means that $n$ and $n'$ are the same modulo $P_1 \cdot P_2$ (i.e., $n$ and $n'$ correspond to the same element of $S_1$ which means that each pair '$bc$' in set $S_2$ maps to only one element of $S_1$).

**III.E Completion of the Main Proof**

So we've finally seen why $\Phi(n) = \Phi(P_1) \cdot \Phi(P_2)$. Now what we need to do is show how this fact can be used in RSA encryption.

Recall that $\phi(P)$ of any prime number is $P - 1$ (i.e., one less than the number). So,

$\phi(P_1) = P_1 - 1$ and $\phi(P_2) = P_2 - 1$; then,

$$\phi(n) = \phi(P_1) \cdot \phi(P_2) = (P_1 - 1)(P_2 - 1)$$

Next, define the product $e \cdot d$ such that $e \cdot d = k \cdot \phi(n) + 1$

Remember the equation $m = m^{k \cdot \Phi(n)+1} \bmod n$ ? Substitute $e \cdot d$ for $k \cdot \phi(n) + 1$ . We get

$$m = m^{e \cdot d} \bmod n$$

From $e \cdot d = k \cdot \phi(n) + 1$ , we find that $d = \frac{k \cdot \phi(n)+1}{e} = \frac{k \cdot (P_1 - 1)(P_2 - 1)+1}{e}$

We picked $P_1$ and $P_2$ . That's how we came up with $n$ . We also choose $k$ . So we have all the information needed to determine $d$ . $d$ , it turns out, is the secret key needed to decode a message sent to us. Let me show you how it all works.

**IV. Application of the formula**[11]

If Bob wants to receive a message from Alice, he sends his public key, which consists of the numbers $e$ and $n$ , to her. Eve—and anyone else who wants it—has access to that key. Since computers only understand numbers, Alice's message consists of a string of numbers. Each number stands for a character like you can type on a keyboard. There is a standardized system of translation from characters to numbers that computers use, called ASCII, which stands for American Standard Code for Information Interchange. Let's say Alice's message is just the letter J. The ASCII code for J is 74. 74 would be the value of $m$ . Alice uses the values of $c$ , $e$ and $n$ to generate an encrypted message—let's call it $c$ —according to the following equation:

$$c = m^e \bmod n$$

Alice sends the encrypted message, $c$ , to Bob. We said that Alice's message is just the letter J. In reality, most messages are long train of characters which translate into a number with a long string of digits. In actuality, additional digits are interjected into the encrypted message to make it more secure (called padding). However, the details regarding padding are far too practical for this discussion. The bottom line for this article is that Eve can see the encrypted message but can't decrypt it."

But why can't Eve decrypt it? After all, she knows $c$, $e$ and $n$. She should be able to figure out $m$. The reason that she can't is because RSA encryption makes use of modular arithmetic. Remember,

$$c = m^e \bmod n \text{ means } m^e = nq + c \text{ where q is some integer}$$

therefore,

$$m = \sqrt[e]{n \cdot q + c}$$

As we've said, Eve knows $c$, $e$ and $n$—they're just numbers that anyone can see. However, she has no idea what $m$ and $q$ are. What you have, then, is one equation with two unknowns. There is no unique solution to such an equation; $m$ and $q$, literally, could be anything. Presumably, Eve could try putting in values for $m$ and $q$ by trial and error, then check to see if the message encoded by the string of numbers that is $m$, makes sense. However, because $P_1$ and $P_2$ are so large, the range of values that $q$ could be would be astronomical. The time it would take to test values of $q$ and find the correct answer would be so long as to make this method impractical, on a par with trying to factor $n$ and guess the private key. (How long would it take? See below.)

Bob, however, has the secret key, $d$, which he can use to recover the message, $m$, by using the equation

$$c = m^e \bmod n$$

Eve knows $e$ and could decrypt the message if she could factor $n$ since the factors of $n$ are $P_1$ and $P_2$, and $P_1$ and $P_2$ determine $d$. Why can't she do it? Because we make are $P_1$ and $P_2$ very large; so large that it would be impractical to factor $n$.

How large do we make $n$? Typical values of $n$ are 1024 or 2048 bits. How long would it take to factor such a number (and what is a bit)? These are questions that will be discussed in the second installment of this subject.

## V. References


**1.** **Modular arithmetic**
https://en.wikipedia.org/wiki/Modular_arithmetic

**2.** **Exponents and roots**
https://www.mathplanet.com/education/pre-algebra/discover-fractions-and-factors/powers-and-exponents

**3.** **Logarithms**
https://www.khanacademy.org/math/algebra2/exponential-and-logarithmic-functions

**4.** **Euler's Totipotent Theorem**
http://artofproblemsolving.com/wiki/index.php?title=Euler%27s_Totient_Theorem
https://www.chegg.com/homework-help/definitions/eulers-theorem-33
http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/fermatlittletheorem.pdf

**5.** **Euler's Totipotent Function**
http://mathworld.wolfram.com/TotientFunction.html

**6.** **Proof of** $\left[\left(a \bmod n\right)\cdot\left(b \bmod n\right)\right]\bmod n=\left(a\cdot b\right)\bmod n$
https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/modular-multiplication

**7.** **Proof of** $\Phi\left(n\right)=\Phi\left(P_1\right)\cdot\Phi\left(P_2\right)$
http://www.oxfordmathcenter.com/drupal7/node/172

**8.** **Bezout's Identity**
https://public.csusm.edu/aitken_html/m422/Handout1.pdf
http://people.sju.edu/~pklingsb/gcd.lincomb.pdf

**9.** **Well-ordered principle**
https://web.stanford.edu/class/cs103x/2007/solutions3.pdf

**10.** **Quotient-remainder theorem proof**
https://public.csusm.edu/aitken_html/m372/divremain.pdf

**11. RSA encryption overview**

https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/the-fundamental-theorem-of-arithmetic-1

https://en.wikipedia.org/wiki/RSA_(cryptosystem)