A Modern Day Application of Euler's Theorem: The RSA Cryptosystem

Megan Maxey

December 7, 2012

Abstract

The RSA Cryptosystem is an assymetric key cipher in which the the encryption keys are made completely public. The security of the RSA lies in an algorithm based on Euler's Theorem and Fermat's Little Theorem. This cryptosystem has proven to be unbreakable, as long as it is implemented correctly, for over 30 years. This system is a classic example of how the theorems of ancient mathematicians used to advance mathematical thought in history are being used to advance technology today.

1 Introduction

In the 1970's, three researchers at MIT, Ron Rivest, Adi Shamir, and Len Adleman, introduced to the world the first type of public key cipher, creatively named RSA. The idea was published in a paper, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, in 1978. The researchers began the paper with a very accurate prediction, "The era of 'electronic mail' may soon be upon us" [3]. In 1978, the primary means of communication was paper mail, in which the mail is supposedly private and signed. But, even paper mail has its disadvantages. Today, as predicted by the creators of RSA, email is a primary source of communication, and these three researchers invented a cipher that preserves the two important characteristics of the paper mail system. In 1982, Rivest, Shamir, and Adleman created the RSA Data Security Corporation to market and promote their cipher. Fourteen years later, the RSA cipher sold for $400 million. The RSA cipher is used worldwide today. The RSA algorithm is built into operating systems such as Microsoft, Apple, Sun, and Novell, found in secure telephones, and incorporated into secure internet communications. RSA ciphers are also used in the exchange of money over the internet and ATM machines.

2 Symmetric Key

In 1976, Stanford University graduate student Whitfield Diffie and his mentor, Martin Hellman introduced the idea of the public key cipher. This idea was published in a paper, *New Directions in Cryptography*. Until the idea of a public key cipher, the ciphers that existed were those in which the sender and receiver were required to secretly agree on an encryption key. These ciphers are called symmetric or private key ciphers. Before 1970, all cryptosystems were symmetric. The affine cipher and the shift cipher are two examples of symmetric key ciphers which were used to achieve secure communication. The following table is used for the shift and affine ciphers, and it contains each letter of the alphabet along with the corresponding numeric value:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

p	q	r	s	t	u	v	w	x	y	z
15	16	17	18	19	20	21	22	23	24	25

The shift cipher is the simplest monoalphabetic substitution cipher. Julius Caesar used a shift cipher for military campaigns, and this is why it is known as the Caesar Cipher. The user decides on a key, and shifts the alphabet to the right the appropriate amount of units. For example, a shift cipher with a key of 3 would assign plaintext a to D, b to E, c to F, and so on. In modular arithmetic, the encryption function is $c \equiv (p+3) \pmod{26}$, where c and p are the numeric values corresponding to the ciphertext and plaintext, respectively. The receiver of the ciphertext will know the chosen key and shift accordingly to determine the plaintext. The decryption function, with a key of 3, is $p \equiv (c-3) \pmod{26}$. This cipher is not secure, since the chosen cipher is one of 25 choices and can be determined through trial and error with ease and little computational effort.

The affine cipher is a symmetric key cipher in which each letter in the alphabet is mapped to its numeric equivalent according to a simple mathematical function using modular arithmetic. The affine cipher uses two keys: a multiplicative key and an additive key. The encryption key is given by $c \equiv \alpha p + \beta \pmod{26}$, where α is the multiplicative key, with $gcd(\alpha, 26) = 1$, and β is the additive key. The variable p represents the numerical position of the plaintext letter, and the variable c represents the numerical position of the ciphertext letter. The decryption function is determined by the manipulation of the encryption function as explained in the following example.

Example 1. *Let 9 be the multiplicative key, and let 2 be the additive key. The encryption process is given by the encryption function* $9p + 2 \pmod{26}$. *The plaintext to be encrypted is "april."*

Plaintext:	*a*	*p*	*r*	*i*	*l*
Numerical Value:	*0*	*15*	*17*	*8*	*11*
$(9p+2) \pmod{26}$*:*	*2*	*7*	*25*	*22*	*23*
Ciphertext:	*C*	*H*	*Z*	*W*	*X*

In order to determine the decryption process, the recipient must manipulate the encryption function as follows:

$$c \equiv 9p + 2 \pmod{26} \implies 9p + 2 \equiv c \pmod{26}$$
$$\implies 9p \equiv c - 2 \pmod{26}$$
$$\implies 9^{-1}9x \equiv 9^{-1}(c-2) \pmod{26}.$$

By the definition of modular inverse, in order to find $9^{-1} \pmod{26}$, *we must solve* $9(t) \equiv 1 \pmod{26}$. *Since* $9(3) \equiv 1 \pmod{26}, t = 9^{-1} \pmod{26} = 3$. *Thus, the decryption function becomes:*

$$9^{-1}9x \equiv 9^{-1}(c-2) \pmod{26} \implies p \equiv 3(c-2) \pmod{26}$$
$$\implies p \equiv 3c - 6 \pmod{26}$$
$$\implies p \equiv 3c + 20 \pmod{26}$$

Ciphertext:	*C*	*H*	*Z*	*W*	*X*
Numerical Value:	*2*	*7*	*25*	*22*	*23*
$(3c+20) \pmod{26}$*:*	*0*	*15*	*17*	*8*	*11*
Plaintext:	*a*	*p*	*r*	*i*	*l*

The security of these two ciphers and all symmetric key ciphers lies in keeping the encryption and decryption keys a secret. Both of these types of symmetric cryptosystems are insecure and are vulnerable to numerous attacks. The fact that the key must be agreed upon by two separate parties is itself a disadvantage. The security of the system is always in question. Is the messenger trustworthy? Is the author of this message who we believe it is? How can we agree on something when we are miles apart? Also, the longer the message, the more susceptible it is to attacks by frequency analysis. This is because, in this type of cryptosystem, each plaintext letter is assigned to one numerical value which corresponds to its ciphertext letter. For example, the letter e is the most frequently used letter in the English alphabet. If a ciphertext is considerably long, and the most recurring letter is h, then it is useful to assume the ciphertext h corresponds to the plaintext e. Because of the insecurities of the symmetric cryptosystem, it became increasingly important to invent another form of cryptosystem not dependent on secret keys.

3 Assymetric Key

A public key cipher is a cipher in which it is not necessary to keep the encryption key a secret because the security of the cipher does not depend on it. It is also known as an assymetric cryptosystem. An assymetric cryptosystem is one in which the sender and receiver possess his or her own enciphering public key and deciphering private key. The keys of one person are in no way related to the keys of another. The advantages of assymetric cryptosystems over symmetric cryptosystems are numerous, while the disadvantages are few. The disadvantage of this system is that it is more complex; therefore, it requires more time to perform along with more computer resources. The advantages include message authentication, detection of tampering, and better security. It is no suprise that the invention of the public key has become such a breakthrough in the future of cryptosystems.

The RSA cipher's security rests in the fact that the process of factoring composite numbers with large prime factors is extremely laborous and virtually impossible, even with today's cutting-edge technology. On today's most advanced computers, it is estimated that "the fastest 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 1 nanosecond, the factorization time would be about $(3.8)10^{6}$ years" [2]. That is 3.8 million years, and this fact is the reason why the RSA cryptosystem is virtually unbreakable if implemented correctly. The RSA cryptosystem relies heavily on "several very famous, old, and relatively simple mathematical facts" [4]. These include Fermat's Little Theorem and Euler's Theorem. In Rivest, Shamir, and Adleman's original paper, they combine these two theorems to explain how the RSA cipher works.

4 Useful Theorems

Theorem 1 (Fermat's Little Theorem)**.** *If p is prime and $a \in \mathbb{Z}$ with gcd(a,p)=1, then* $a^{p-1} \equiv 1 \pmod{p}$.

For example, let $p = 11$. Then for each integer with $\gcd(a, 11) = 1$, we have $a^{10} \equiv 1 \pmod{11}$. Thus, $11|(a^{10} - 1)$.

Definition 1 (Euler's Phi Function). *Let n be a positive integer. Euler's Phi Function, denoted $\phi(n)$, is the number of positive integers $\leq n$ which are relatively prime to n.*

For example, let $n = 9$. Then $\phi(9) = 6$, since the positive integers ≤ 9 which are relatively prime to 9 are 1, 2, 4, 5, 7, and 8.

Theorem 2 (Euler's Theorem). *If n and a are integers with $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

For example, let $n = 4$ and $a = 15$. Here, $\phi(n) = \phi(4) = 2$ since 1 and 2 are the positive integers which are relatively prime to 4 and are ≤ 4. Observe:

$$a^{\phi(n)} = 15^2 = 225.$$
$$\text{Thus, } 225 \equiv 1 \pmod{4} \implies 224 \equiv \pmod{4} \implies 4|224 \implies 224 = (56)4.$$

Following from the definition of Euler's Phi Function, we have two Lemmas.

Lemma 1. *If n is prime, then $\phi(n) = n - 1$.*

Proof: Let n be a prime number. Since n is prime, $1, 2, 3, 4, ..., n - 1$ are relatively prime to n. Therefore, $\phi(n) = n - 1$.

For example, let $n = 13$. The positive integers which are relatively prime to 13 and are ≤ 13 are 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12. Thus, $\phi(13) = 12 = 13 - 1$

Lemma 2. *If p and q are prime, then $\phi(pq) = \phi(p)\phi(q)$.*

Proof: Let p and q be prime. The product of two primes is composite. Since p and q are prime and coprime, the integers less than pq and not relatively prime to p are $\{p, 2p, 3p, 4p, ..., (q - 1)p\}$. The integers less than pq and not relatively prime to q are $\{q, 2q, 3q, 4q, ..., (p-1)q\}$. Thus, in order to get $\phi(pq)$, we take the $pq - 1$ positive integers less than pq. We subtract subtract the number of integers less than pq and not relatively prime to p, and we subtract the number of integers less than pq and not relatively prime to q. Thus, we have:

$$\phi(pq) = pq - 1 - (p - 1) - (q - 1) = pq - p - q + 1 = (p - 1)(q - 1) = \phi(p)\phi(q).$$

Lemma 2 can be generalized as follows: If $\gcd(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$; that is, ϕ is multiplicative. For the purposes of this paper, we only need a and b to be prime.

5 RSA Process

The process of the RSA cryptosystem begins with the intended recipient sending the orignator two integers. These integers are chosen as follows. First, he decides on two prime integers p and q. Then, he calculates $n = pq$, and $\phi(n) = \phi(pq) = \phi(p)\phi(q) = (p - 1)(q - 1)$. Lastly, he chooses an integer e such that $1 < e < \phi(n)$ with $\gcd(e, \phi(n)) = 1$. The reason the $\gcd(e, \phi(n))$ must be 1 is to ensure $d = e^{-1} \pmod{\phi(n)}$ exists. If $\gcd(e, \phi(n)) \neq 1$, the inverse of $e \pmod{\phi(n)}$ does not exist. The intended recipient then sends only the values for e and n to the originator. Thus, these values are made public while p and q are kept secret. Only the intended recipient knows p and q.

When the originator receives the two values for e and n, he then has all the information he needs to encrypt the message he plans to send over insecure channels to the intended recipient. The public encryption key is e, and the encryption function is $y \equiv x^e(\mod n)$, where y is the integer value equivalent to the ciphertext, and x is the interger value equivalent to the plaintext. The originator can then send the encrypted text to the intended recipient.

When the intended recipient receives the encrypted ciphertext, he first finds an integer d such that $d = e^{-1}(\mod \phi(n))$. This d is the private decryption key. He knows such a $d \in \mathbb{Z}$ exists since $gcd(e, \phi(n)) = 1$. He can find d by using the Euclidean Algorithm. The decryption function is given by $x \equiv y^d(\mod n)$.

The American Standard Code for Information Interchange, or ASCII, is a list of numbers and their corresponding characters. These characters include all 95 printable keyboard characters, denoted by integers 32 through 126 [4]. The following table is a version of the ASCII and will be used thoughout this paper.

Char	Num	Char	Num	Char	Num	Char	Num
(space)	32	8	56	P	80	h	104
!	33	9	57	Q	81	i	105
”	34	:	58	R	82	j	106
#	35	;	59	S	83	k	107
$	36	<	60	T	84	l	108
%	37	=	61	U	85	m	109
&	38	>	62	V	86	n	110
apostrophe	39	?	63	W	87	o	111
L Paren.	40	@	64	X	88	p	112
R Paren.	41	A	65	Y	89	q	113
∗	42	B	66	Z	90	r	114
+	43	C	67	R Brack.	91	s	115
,	44	D	68	\	92	t	116
−	45	E	69	L Brack.	93	u	117
.	46	F	70	caret	94	v	118
/	47	G	71	underscore	95	w	119
0	48	H	72	grave	96	x	120
1	49	I	73	a	97	y	121
2	50	J	74	b	98	z	122
3	51	K	75	c	99	{	123
4	52	L	76	d	100	‖	124
5	53	M	77	e	101	}	125
6	54	N	78	f	102	tilda	126
7	55	O	79	g	103		

The following examples of the RSA cipher will use small primes. However, this is not realistic because in order for the system to work effectively, the primes must be more than 100 digits in length.

Example 2. *Let Sarah be the intended recipient and Sidney be the originator. Sarah is an American working for the CIA, and Sidney is an American spy stationed in another country. Sidney hears of a possible attack against America and needs to relay a top secret message to Sarah.*

Sarah starts the process by deciding on two primes, $p = 13$ *and* $q = 29$. *Sarah finds* $n = 377$ *and* $\phi(n) = (p-1)(q-1) = (13-1)(29-1) = 336$. *She then decides on an* $e \in \mathbb{Z}$, *such that* $1 < e < 336$ *and* $gcd(e, 336) = 1$. *She picks* $e = 11$. *She sends the two integer values,* 11 *and* 377, *to Sidney across an insecure communication network; therefore, these values are made public.*

Sidney receives Sarah's public key, $(11, 377)$, *and can now begin the encryption process using the encryption key* 11 *and the encryption function* $y \equiv x^{11} \pmod{377}$. *Sidney wants to encrypt the message,"now". She first converts the plaintext characters into their integer counterparts using the ASCII table. The plaintext becomes* 110, 111, 119. *She can now begin the encryption process.*

$$\begin{aligned} y &\equiv 110^{11} \equiv 310 \pmod{377} \\ y &\equiv 111^{11} \equiv 132 \pmod{377} \\ y &\equiv 119^{11} \equiv 189 \pmod{377} \end{aligned}$$

Sidney now sends the encryption ciphertext, 310, 132, 189, to Sarah. In order to decrypt this message, Sarah first finds d *such that* $11d \equiv 1 \pmod{336}$, *that is,* $d = 11^{-1} \pmod{336}$. *Since* $11(275) \equiv 1 \pmod{336}$, *Sarah deduces that the decryption key* d *is 275; thus, the decryption function becomes* $x \equiv y^{275} \pmod{377}$. *Sarah can now begin the decryption process.*

$$\begin{aligned} x &\equiv 310^{275} \pmod{377} \equiv 110 \pmod{377} \\ x &\equiv 132^{275} \pmod{377} \equiv 111 \pmod{377} \\ x &\equiv 189^{275} \pmod{377} \equiv 119 \pmod{377} \end{aligned}$$

Sarah can now convert these values into the corresponding values according to the ASCII table. She uncovers the plaintext message: "now".

Example 3. *Let* $p = 3181$, $q = 227$, *and* $e = 953$. *Encrypt the following plaintext: "161 MAIN STREET". Then, determine the decryption key, d, and decrypt the ciphertext.*

$$\begin{gathered} n = pq = (3181)(227) = 722087 \\ \phi(n) = (p-1)(q-1) = (3180)(226) = 718680 \end{gathered}$$

Using the ASCII Table, the numeric plaintext becomes "4954493277657378328384696984". We will encrypt in the following blocks: 495449, 327765, 73783, 283846, 96984. Let y_1, y_2, y_3, y_4, *and* y_5 *represent the ciphertext corresponding to each plaintext block.*

$$\begin{aligned} y_1 &\equiv 495449^{953} \pmod{722087} \equiv 199229 \pmod{722087} \\ y_2 &\equiv 327765^{953} \pmod{722087} \equiv 251774 \pmod{722087} \\ y_3 &\equiv 73783^{953} \pmod{722087} \equiv 33119 \pmod{722087} \\ y_4 &\equiv 283846^{953} \pmod{722087} \equiv 578189 \pmod{722087} \\ y_5 &\equiv 96984^{953} \pmod{722087} \equiv 24334 \pmod{722087} \end{aligned}$$

Thus, the ciphertext is 199229, 251774, 33119, 578189, 24334.
In order to determine the decryption key, d, we must find $d \equiv e^{-1} \pmod{\phi(n)}$.

$$d \equiv 953^{-1} \pmod{718680} \implies 953d \equiv 1 \pmod{718680}$$
$$953(639497) \equiv 1 \pmod{718680}$$
$$d = 639497$$

We can now begin to decrypt the ciphertext. Let x_1, x_2, x_3, x_4, and x_5 represent the plaintext blocks corresponding to the ciphertext blocks.

$$x_1 \equiv 199229^{639497} \pmod{722087} \equiv 495449 \pmod{722087}$$
$$x_2 \equiv 251774^{639497} \pmod{722087} \equiv 327765 \pmod{722087}$$
$$x_3 \equiv 33119^{639497} \pmod{722087} \equiv 73783 \pmod{722087}$$
$$x_4 \equiv 578189^{639497} \pmod{722087} \equiv 283846 \pmod{722087}$$
$$x_5 \equiv 24334^{639497} \pmod{722087} \equiv 96984 \pmod{722087}$$

Thus, the plaintext is ”4954493277657378328384696984”. Using the ASCII Table, the plaintext becomes ”161 MAIN STREET”.

6 Why Does it Work?

In this section, we will show how the intended recipient can decrypt the ciphertext, e, using the private key, d, to obtain the original message, M.

Claim: Let M be the plaintext message that the originator will encrypt and send to the intended recipient. And, let e be the public encryption key, d the private decryption key, c the ciphertext, n the public value $n = pq$, and $\phi(n) = (p-1)(q-1)$. The originator encrypts M by by computing $c \equiv M^e(\mod n)$ and sends c to the intended recipient. Now, the intended recipient converts c back into plaintext by calculating, $c^d \equiv \pmod{n}$. We will show that $c^d \equiv M \pmod{n}$. That is, $c^d \pmod{n}$ gives the original value M.

Proof: Note that $c^d \equiv (M^e)^d \pmod{n} \equiv M^{ed} \pmod{n}$. The intended recipient knows that $ed \equiv 1 \pmod{\phi(n)}$. Observe the following:

$$ed \equiv 1(\mod \phi(n)) \implies \phi(n)|(ed-1)$$
$$\implies (ed-1) = \phi(n)k, \text{for some } k \in \mathbb{Z}$$
$$\implies ed = 1 + \phi(n)k, \text{for some } k \in \mathbb{Z}$$

Thus, $c^d \equiv M^{ed} \equiv M^{1+\phi(n)k} \equiv M^1(M^{\phi(n)})^k \pmod{n}$. Now by Euler’s Theorem, $M^{\phi(n)} \equiv 1 \pmod{n}$ since gcd $(M, n) = 1$. Hence $M^1(M^{\phi(n)})^k \equiv M(1)^k \equiv M \pmod{n}$. Therefore, we deduce that $c^d \equiv M \pmod{n}$.

Let us do an example to illustrate the implementation of the RSA cipher. Imagine a directory in which a community of coworkers share their values for e and n as follows:

Mary	Rob	Chris
(11,35)	(23,247)	(31,187)

If Rob wishes to send Mary an encrypted message, he must use Mary's values; therefore, he would send Mary $M^{11} \pmod{35}$, where M is the intended plaintext. She can then decrypt the message from Rob using her private value $\phi(n)$ and calculated d. On the other hand, if Chris tries to decrypt that message from Rob, he will be unable to since he does not know Mary's value of $\phi(n)$. In other words, he does not know how her value for n factors into two primes. This fact applies to large prime numbers and a large value n. Additionally, if Chris encrypts a message for Rob using Mary's encryption keys, Rob will not be able to decrypt the message. Essentially, while the values used for the encryption process are completely public, the determination of someone's decryption keys from his or her encryption keys is not possible under the correct circumstances of the cryptosystem.

7 Attacks

While the RSA cipher is relatively unbreakable because of the extensive means necessary to break the cipher, it is still possible. In fact, in order to help market the cryptosystem, the three researchers encouraged readers of *Scientific American* to decrypt messages and offered monetary rewards. The difficulty of this challenge is perhaps the cause of RSA's popularity. Of course, the algorithm would not be used in such important systems if it were not proven effective. The possibility of successfully decrypting an RSA cipher lies in whether or not the cipher was implemented correctly. When implementing the RSA cryptosystem, the two parties must assume e and n are known to an attacker.

Naturally, the first method of attack would be to determine the two prime numbers, whose product gives the public value n. If the value p and q are compromised, the attacker can calculate $\phi(n)$. The attacker would then have the values e, n, and $\phi(n)$, and once the attacker knows $\phi(n)$, he can determine the private decryption key, d. He could then encrypt and decrypt messages inside of this RSA network. If the intended recipient's chosen prime numbers are too small, factoring n would be relatively simple; therefore, the size of the prime numbers is of great importance. It is necessary that p and q be very large prime integers, approximately 100 digits in length, so that the value m is impossible to solve for. This would require the factoring of an extremely large composite number, whose prime factorization consists of only two large prime factors. The security of this system is based on the fact that this is computationally impossible, since the value for n will have approximately 200 or more digits. "On today's fastest computers, the running time to factor a composite number of $200+$ digits is prohibitive" [2]. Therefore, the intended recipient of the encryption must choose p and q in such a way that factoring them from n is computationally infeasible.

While it is of great importance to choose p and q to be large, it is also of great importance to choose e and d to be somewhat large. The intended recipient may wish to save time by choosing e and d to be lower and computationally simpler numbers; however, this makes the system more vulnerable to attacks. For example, in order to expedite the encryption process, RSA systems choose $e = 3$. However, if the same message is encrypted three times with $e = 3$ and different moduli, then the message can be retrieved using the Chinese Remainder Theorem.

Theorem 3 (Chinese Remainder Theorem)**.** *Suppose $gcd(m, n) = 1$. Given integers a and b, there exist exactly one solution x modulo mn to the simultaneous congruences*

$$x \equiv a \pmod{m},\ x \equiv b \pmod{n}.$$

Proof: There exist integers s and t such that $ms + nt = 1$. Then $ms \equiv 1 \pmod{n}$ and $nt \equiv 1 \pmod{m}$. Let $x = bms + ant$. Then $x \equiv ant \equiv a \pmod{m}$, and $x \equiv bms \equiv b \pmod{n}$, so a solution x exists. Suppose x_1 is another solution. Then $x \equiv x_1 \pmod{m}$ and $x \equiv x_1 \pmod{n}$, so $x - x_1$ is a multiple of both m and n. [5]

There are more possible attacks on the cryptosystem. For the most part, the success of these attacks generally have one factor in common. That common factor is the incorrect implementation of the cryptosystem.

8 Applications

The RSA cryptosystem is used in many systems today. If the security of digital data is of importance, then RSA is more than likely implemented into the software or system. It is used to guarantee secrecy and authenticity in email, electronic credit card payments, and website login sessions. The secrecy of the RSA cryptosystem and its secureness has been demonstrated. Similar to a signed letter in the mail, email can also be signed by using digital signatures. In order for Sidney to ensure a message received is genuinely from an appropriate sender, the sender, Sarah, can digitially sign the message. Sarah must ecrypt a signature with her private decryption process, $x \equiv y^d \pmod{m}$. When the message is received, Sidney can decrypt the signature with the encryption process. If Sarah's signature emerges, Sidney knows Sarah sent her the message. This is feasible because Sarah is the only person who knows the decryption process. Therefore, no one else could have encrypted his or her own signature in such a way that, when decrypted using the encryption process, the signature is recognizable.

9 Conclusion

The RSA cryptosystem is over 30 years old, and its vulnerability continues to reside beyond the bounds of possibility. It is likely that sometime in the future, technology will become advanced enough to factor extremely large composite numbers. However, when that time comes, it is conceivable that a more precocious cryptosystem beyond the means of extremely advanced technology will also be created. Rivest, Shamir, and Adleman invented an amazingly powerful cryptosystem capable of overcoming attacks from all sides, and they accomplished this using very old theorems. Euler's Theorem was an accomplishment of Swiss mathematician Leonhard Euler in the early 1700's. When dreaming of this theorem, Euler was advancing mathematical thought and encouraging more in depth ideas. He probably never dreamed that his theorem would be used to secure communication, increase internet security, and further the advancement of technology 300 years later. Now, modern mathematicians take the astonishing thoughts, theorems, proofs, lemmas, and corollaries of ancient mathematicians and transform and manipulate them into a basis of computer technology, modern industry, and higher education. Only time will tell whether or not the RSA cipher can avoid the rapid advancement of technology. Until then, the RSA cipher will remain an incredibly valuable, unquestionably useful, and easily comprehensible cryptosystem.

References

[1] Dan Boneh, Twenty Years of Attacks on the RSA Cryptosystem. *Notices of the AMS, Volume 2*, (1999), 203-213.

[2] David Burton, Elementary Number Theory, Fifth Edidtion, McGraw-Hill, 2002, (147-155).

[3] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, Volume 21*, (1978), 120-126.

[4] Richard Klima, Neil Sigmon, Cryptology: Classical and Modern with Maplets, First Edition, CRC Press, 2012, 275-327.

[5] Wade Trappe, Lawrence Washington, Introduction to Cryptography with Coding Theory, Second Edition, Pearson Education, Inc., 2006, 76-78, 164-192.

[6] W. Diffie, M. Hellman, New Directions in Cryptography. *IEEE Transactions on Information Theory, Volume 6*, (1976), 644-654.