ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 21, August 2017

Application of Euler's Theorem: The RSA Cryptosystem

Dr.S.V.B. Subrahmanyeswara Rao
Dept.of Mathematics
Ramachandra College of Engineering
Eluru,A.P.India.
manyam4463@gmail.com

Yalamanchili.Anjani
Dept.of Computer Science,
VKR,VNB& AGK College of
EngineeringGudivada,A.P.India
anjaniyalamanchili@gmail.com

Abstract

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

Keywords: RSA,asymmetric,encryption,ciphertext,cryptosystem

I. INTRODUCTION

In the 1970's, three researchers at MIT, Ron Rivest, Adi Shamir, and Len Adleman, introducedto the world the first type of public key cipher, creatively named RSA. The idea was publishedin 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' maysoon be upon us". In 1978, the primary means of communication was paper mail, in whichthe mail is supposedly private and signed. But, even paper mail has its disadvantages. Today, aspredicted by the creators of RSA, email is a primary source of communication, and these threeresearchers invented a cipher that preserves the two important characteristics of the paper mailsystem. In 1982, Rivest, Shamir, and Adleman created the RSA Data Security Corporation tomarket and promote their cipher. Fourteen years later, the RSA cipher sold for $400 million. TheRSA cipher is used worldwide today. The RSA algorithm is built into operating systems suchas Microsoft, Apple, Sun, and Novell, found in secure telephones, and incorporated into secureinternet communications. RSA ciphers are also used in the exchange of money over the internetand ATM machines.

The RSA cryptosystemrelies heavily on "several very famous, old, and relatively simple mathematical facts" [4]. Theseinclude Fermat's Little Theorem and Euler's Theorem. In Rivest, Shamir, and Adleman's originalpaper, they combine these two theorems to explain how the RSA cipher works.

II. SYMMETRIC & ASYMMETRIC KEYS

In 1976, Stanford University graduate student Whitfield Diffie and his mentor, Martin Hellman introduced the idea of the public key cipher. 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 or Single-key or Secret key ciphers. Before 1970, all cryptosystems were symmetric. Examples of Symmetric key ciphers are affine cipher and the shift cipher which were used to achieve secure communication.

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. [3] proposed a system which is an innovative congestion control algorithm named FAQ-MAST TCP (Fast Active Queue Management Stability Transmission Control Protocol) is aimed for high-speed long-latency networks. Four major difficulties in FAQ-MAST TCP are highlighted at both packet and flow levels. The architecture and characterization of equilibrium and stability properties of FAQ-MAST TCP are discussed. Experimental results are presented comparing the first Linux prototype with TCP Reno, HSTCP, and STCP in terms of throughput, fairness, stability, and responsiveness. FAQ-MAST TCP aims to rapidly stabilize high-speed long-latency networks into steady, efficient and fair operating points, in dynamic sharing environments, and the preliminary results are produced as output of our project. The Proposed architecture is explained with the help of an existing real-time example as to explain why FAQ-MAST TCP download is chosen rather than FTP download.

A. USEFUL THEOREMS

Theorem 1 (Fermat's Little Theorem)

Statement: If p is prime and a is a positive integer not divisible by p, then$a^{p-1} \equiv 1\ (\,modp\,)$

*Proof:*Consider the set of positive integers less than $p{:}\,\{1{,}2 - - -\ (p-1)\}$ and multiply each element by a, modulo p, to get$X = \{\,amodp, 2amodp - - - -(p-1)amodp\,\}$

Here, none of the elements of X is equal to zero because P does not divide a

No two of the integers in are equal.

To see this, assume that, $ja \equiv kamodp, where\ 1 \le j < k \le (p-1)$.

Because a is relatively prime to p, we can eliminate a from both sides of the equation resulting in $j \equiv k\ (\,modp\,)$

Note: Two numbers are Relatively prime, if they have no prime factors in common; that is, their only common divisor is 1 [or] Two numbers are Relatively prime, if their Greatest Common Divisor is 1

This last equality is impossible, because j and k are both positive integers less than p.

Therefore, we know that the *(p-1)* elements of X are all positive integers with no two elements are equal.

We can conclude the X consists of set of integers $\{\,1{,}2, - - -(p-1)\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result *modp* yields

$$a \times 2a \times - - - - \times (p-1)a \equiv [(1 \times 2 \times - - - \times (p-1)](modp)$$

$$a^{p-1}(p-1)!\ \equiv (p-1)!\,modp$$

We can cancel the $(p-1)!$ term because it is relatively prime to p $\ a^{p-1} \equiv 1\ (modp\ )$

Ex: a = 7 p = 19

$7^2 = 49\ \equiv 11\ (mod\ 19\ )$

$7^4 = 121\ \equiv 7\ (mod\ 19\ )$

$7^8 = 49\ \equiv 11\ (mod\ 19\ )$

$7^{16} = 121\ \equiv 7\ (mod\ 19\ )$

$a^{p-1} = 7^{18} = 7^{16} \times 7^2 = 7\ \times 11 \equiv 1\ (mod\ 19\ )$

Note: If $p$is prime and a is a positive integer, then $a^p \equiv a\ (\,modp\,)$

This alternative form does not requires that a be relatively prime to p as given in statement of Fermat's theorem

Ex: If p = 5, a = 3

$then, a^p = 3^5 = 243 = 3\ (mod\ 5) = a\ (modp)$

If p = 5, a = 10

$$then, a^p = 10^5 = 100000 = 10\ (mod\ 5)$$

$$\equiv 0\ (mod\ 5) = a\ (modp)$$

Definition 1 (Euler's Phi Function): It is defined as the number of positive integers less than n and relatively prime to n and is written as $\emptyset(n)$

By convention, $\emptyset(1) = 1$

1. Determine $\emptyset(37)$.

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to37.

Thus $\emptyset(37) = 36$.

2. Determine $\emptyset(35)$.

List all of the positive integers less than 35 that are relatively prime to it:

There are 24 numbers on the list, so $\emptyset(35) = 24$

They are 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

Table lists the first 30 values of $\emptyset(n)$.

Value $\emptyset(1)$is without meaning but is defined to have the value 1.

n	$\emptyset(\boldsymbol{n})$	***n***	$\emptyset(\boldsymbol{n})$	***n***	$\emptyset(\boldsymbol{n})$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	3	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

For a prime number p, $\emptyset(p) = (p-1)$.

Now suppose that we have two prime numbers p and q with $\neq q$. Then we can show that,

for $n = pq, \emptyset(n) = \emptyset(pq) = \emptyset(p) \times \emptyset(q) = (p-1)(q-1)$

Ex: $\emptyset(21) = \emptyset(7 \times 3) = \emptyset(7) \times \emptyset(3) = (7-1)(3-1) = 2 \times 6 = 12$

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

To see that $\emptyset(n) = \emptyset(p) \times \emptyset(q)$, consider that the set of positive integers less that n is the set $[1, ---(pq-1)]$.Integers in this set that are not relatively prime to n are the set $\{p, 2p, ---(q-1)p\}$and the set $\{q, 2q, ---(p-1)q\}$. Accordingly,$\emptyset(n) = (pq-1) - [(q-1) + (p-1)] = (p-1)(q-1) = \emptyset(p) \times \emptyset(q)$

Theorem 2 (Euler's Theorem).

Statement: For every a and n that are relatively prime $a^{\emptyset(n)} \equiv 1(modn)$

Proof: Above Equation is true if n is prime, because in that case $\emptyset(n) = (n-1)$ and Fermat's theorem holds good.

However, it also holds for any integer *n*.

Recall that $\emptyset(n)$is the number of positive integers less than *n* that are relatively prime to *n*.

Consider the set of such integers, labeled as $R = \{x_1, x_2 --- x_{\emptyset(n)}\}$

That is, each element $x_i$of R is a unique positive integer less than *n* with $GCD(x_i, n) = 1$

. Now multiply each element by *a*, *modulo n :*

$$S = \{(ax_1 modn, ax_2 modn --- (ax_{\emptyset(n)} modn)\}$$

Set *S* is a permutation of *R*, by the following line of reasoning:

1. Because a is relatively prime to n and $x_i$is relatively prime to n, ax_imust also be relatively prime to *n*. Thus, all the members of *S*are integers that are less than *n* and that are relatively prime to n.

2. There are no duplicates in *S*.

If $ax_i modn = ax_j modnthenx_i = x_j$

Therefore

$$\prod_{i=1}^{\emptyset(n)} (ax_i modn) = \prod_{i=1}^{\emptyset(n)} x_i$$

$$\prod_{i=1}^{\emptyset(n)} (ax_i) \equiv \prod_{i=1}^{\emptyset(n)} x_i\ (modn)$$

$$a^{\emptyset(n)} \prod_{i=1}^{\emptyset(n)} (x_i) = \prod_{i=1}^{\emptyset(n)} x_i\ (modn)$$

$$a^{\emptyset(n)} \equiv 1(modn)$$

Ex: *If* $a = 3$; $n = 10$; $\emptyset(10) = 4\{1,2,5,10\}$

$a^{\emptyset(n)} \equiv 1(mod n)$

$a^{\emptyset(n)} = 3^4 = 81 = 1 \text{ (mod 10)} = 1 \text{ (mod } n)$

If $a = 2$; $n = 11$; $\emptyset(11) = 10$

$a^{\emptyset(n)} = 2^{10}$

$= 1024$

$= 1 \text{ (mod 11)} = 1 \text{ (mod } n)$

B. RSA ALGORITHM:

A new approach to cryptography by Diffie and Hellman, in effect, challenged cryptologists to come up with a cryptographic algorithm that met requirements for public-key systems. One of the first successful responses to the challenge was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978. Most widely accepted and implemented general-purpose approach to public-key encryption.

The RSAscheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.

A typical size for n is 1024 bits, or 309 decimal digits. That is, n <1024.

Description of the Algorithm

RSA makes use of an expression with exponentials.

Plaintext is encrypted in blocks, with each block having a binary value less than some number n.

That is, the block size must be less than or equal to $\log_2(n) + 1$; in practice, the block size is i bits, where $2^i < n \leq 2^{i+1}$.

Encryption and decryption for some plaintext block M and cipher text block C.

$$C = M^e mod n$$

$M = C^d mod n$

$= (M)^{ed} mod n$

$= M^{ed} mod n$

Both sender and receiver must know the value of n.

Sender knows the value of e, and only the receiver knows the value of d.

Thus, this is a public-key encryption algorithm with a public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$.

For this algorithm to be satisfactory for public-key encryption, the following requirementsmust be met.

1. It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.

2. It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$.

3. It is infeasible to determine d given e and n.

We need to find a relationship of the form

$M^{ed} \bmod n = M$

The preceding relationship holds if e and d are multiplicative inverses modulo φ(n), where φ(n) is the Euler totient function.

Forp, qprime, $\varphi(pq) = (p-1)(q-1)$

Relationship between e and d can be expressed as

$$ed mod \varphi(n) = 1$$

$$ed mod n \equiv 1 \, mod \varphi(n)$$

$$d \equiv e^{-1} mod \varphi(n)$$

$e$and d are multiplicative inverses $mod \varphi(n)$.

Note: According to the rules of Modular arithmetic, this is true only if d (and therefore e) is relatively prime to $\varphi(n)$. Equivalently, gcd($\varphi(n)$, d) = 1.

RSA Scheme:

The ingredients are the following:

p, q, two prime numbers (Private, Chosen)

$n = pq$ (Public, Calculated)

e, with gcd($\varphi(n)$, e) = 1; 1 <e <$\varphi(n)$, (Public, Chosen)

d ≡ e^{-1} mod $\varphi(n)$(Private, Calculated)

Private key consists of {d, n} and Public key consists of {e, n}.

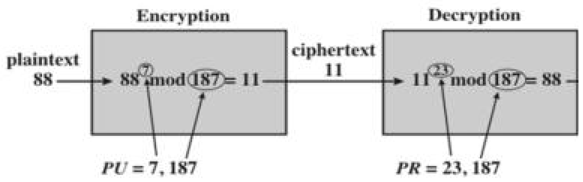
Suppose that user A has published its public key and that user B wishes to send the message$M$ to

On receipt of this ciphertext,user A decrypts by calculating $M = C^d mod n$.

Figure summarizes the RSA algorithm.

Alice generates a public/private key pair; Bob encrypts using Alice's public key; and Alicedecrypts using her private key.

An example is shown below:



For this example, the keys were generated as follows.

1. Select two prime numbers, $p = 17$ and $q = 11$.

2. Calculate $n = pq= 17 \times 11 = 187$.

3. Calculate $\varphi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.

4. Select e such that e is relatively prime to $\varphi(n) = 160$ and less than $\varphi(n)$

Possible values for e are 3,7etc

We choose $e = 7$.

5. Determine d such that $de = 1\ mod\varphi(n)$ and $d < \varphi(n)$

$de = 1\ (mod\ 160)$and

$d = e^{-1} mod\ 160$

$d< 160$

$e = 7$

$d = 7^{-1} mod\ 160$

Correct value is $d = 23$,because $23 \times 7 = 161 = (1 \times 160) + 1$;

$d$can be calculated using the extended Euclid's algorithm.

Resulting keys are public key $PU = \{7, 187\}$ and private key $PR = \{23, 187\}$.

Example shows the use of these keys for a plaintext input of $M = 88$.

For encryption, we need to calculate

$C = 88^7$ mod 187.

Exploiting the properties of modular arithmetic, we can do this as follows.

88^7 mod 187 = [(88^4 mod 187) × (88^2 mod 187) × (88^1 mod 187)] mod 187

88^1 mod 187 = 88

88^2 mod 187 = 7744 mod 187 = 77

88^4 mod 187 = 59,969,536 mod 187 = 132

88^7 mod 187 = (88 × 77 × 132) mod 187

= 894,432 mod 187 = 11

For decryption, we calculate $M = 11^{23}$ mod 187:

11^{23} mod 187

= [(11^1 mod 187) × (11^2 mod 187) × (11^4 mod 187) × (11^8 mod 187) × (11^8 mod 187)] mod 187

11^1 mod 187 = 11

11^2 mod 187 = 121

11^4 mod 187 = 14,641 mod 187 = 55

11^8 mod 187 = 214,358,881 mod 187 = 33

11^{23} mod 187 = (11 × 121 × 55 × 33 × 33) mod 187

= 79,720,245 mod 187 = 88

III. 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 toguarantee secrecy and authenticity in email, electronic credit card payments, and website loginsessions. The secrecy of the RSA cryptosystem and its secureness has been demonstrated. Similarto a signed letter in the mail, email can also be signed by using digital signatures.

IV. CONCLUSION

The RSA cryptosystem is over 30 years old, and its vulnerability continues to reside beyond thebounds of possibility. It is likely that sometime in the future, technology will become advancedenough to factor extremely large composite numbers. However, when that time comes, it is conceivablethat a more precocious cryptosystem beyond the means of extremely advanced technologywill also be created.

Rivest, Shamir, and Adleman invented an amazingly powerful cryptosystemcapable 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 early1700's. He probably never dreamed that his theorem would be used to securecommunication, increase internet security, and further the advancement of technology 300 yearslater. Now, modern mathematicians take the astonishing thoughts, theorems, proofs, lemmas, andcorollaries of ancient mathematicians and transform and manipulate them into a basis of computertechnology, modern industry, and higher education. Only time will tell whether or not the RSAcipher can avoid the rapid advancement of technology. Until then, the RSA cipher will remain anincredibly valuable, unquestionably useful, and easily comprehensible cryptosystem.

V. ACKNOWLEDGMENTS

Dr.SVBSubrahmanyeswara Rao has 16 years of teaching experience. He is presently working in RamaChandra College of Engineering, Eluru in the Department of Mathematics. His areas of interest are Commutative Algebra and Cryptography.The author thanks the Management of RCE for the support.

Mrs.Y.Anjani has 10 years of teaching experience. She is presently working in VKR,VNB& AGK College of Engineering, Gudivada in the Department of Computer Science & Engineering. Her areas of interest are Cryptography and Network Security, Mobile Computing

V. REFERENCES

[1]Dan Boneh, Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS, Volume2, (1999), 203-213.

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

[3] Christo Ananth, S.Esakki Rajavel, I.AnnaDurai, A.Mydeen@SyedAli, C.Sudalai@UtchiMahali, M.Ruban Kingston, "FAQ-MAST TCP for Secure Download", International Journal of Communication and Computer Technologies (IJCCTS), Volume 02 – No.13 Issue: 01 , Mar 2014, pp 78-85

[4]Richard Klima, Neil Sigmon, Cryptology: Classical and Modern with Maplets, FirstEdition,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 InformationTheory, Volume 6, (1976), 644-654.