Advances and Applications in Mathematical Sciences
Volume 22, Issue 2, December 2022, Pages 399-405
© 2022 Mili Publications, India

ENCRYPTION TECHNIQUE INVOLVING RAMANUJAN PRIME NUMBERS USING RSA PUBLIC KEY CRYPTOGRAPHY

C. SARANYA

Assistant Professor
PG and Research Department of Mathematics
Cauvery College for Women (Autonomous)
(Affiliated to Bharathidasan University)
Trichy-18, India
E-mail: c.saranyavinoth@gmail.com
saranyac.maths@cauverycollege.ac.in

Abstract

In this communication, an attempt has been made to utilize the possibility of encryption and decryption using RSA public key cryptography in Number theory involving Ramanujan Prime numbers.

Introduction

Number theory is captivating because it has such an enormous number of open problems that appear to be open from an external perspective. Obviously, open problems in number theory are open for a reason. Numbers, in spite of being basic, have an incredibly rich structure which we just comprehend somewhat. During the 20th century, Thue made a significant forward leap in the investigation of Diophantine equations. His proof impacted a great deal of later work in Number theory, including Diophantine equations. Hence, number theory and its different subfields will continue to excite the cerebrums of mathematicians for quite a while.

Number Theory plays a significant part in encryption algorithm.

2020 Mathematics Subject Classification: 11-XX.
Keywords: Prime numbers, Ramanujan prime numbers, Cryptography, RSA public key, Encryption and decryption.
Received July 27, 2021; Accepted January 4, 2022

Cryptography is the act of concealing data, changing some secret information over to not decipherable texts. These outcomes motivated us to examine for encryption in RSA public key cryptography utilizing Ramanujan prime numbers. Many tools in Number Theory like primes, divisors, congruencies and Euler's function are utilized in cryptography for security [1-12]. This paper aims to introduce the reader with uses of Number Theory in cryptography that is the idea of encryption by RSA public key cryptography in Number theory for finding the enciphering exponent and recovery element involving Ramanujan Prime numbers.

Ramanujan Prime Numbers

A Ramanujan prime is a prime number that satisfies a result proved by Srinivasa Ramanujan relating to the prime counting function. The n^{th} Ramanujan prime is the least positive integer R_n for which

$$\pi(x) - \pi(x/2) \geq n, \ \forall \, x \geq R_n, \ n \geq 1$$

where $\pi(x)$ is the prime counting function (number of primes less than or equal to x).

In other words, there are at least n primes between $x/2$ and x whenever $x \geq R_n$.

The first few numbers of this kind are: 11, 17, 29, 41, 47, 59, 67, 71, 97.

RSA Public Key Cryptography

In a public key cryptosystem, the sender and receiver (frequently called Alice and Bob respectively) don't need to concur ahead of time on a secret code. Indeed they each distribute part of their code in public directory. Further an adversary with admittance to the encoded message and the public directory actually can't unravel message. More precisely Alice and Bob will each have two keys a public key and a secret key.

In RSA cryptosystem, Bob pick two prime numbers p and q (which by and by each have at any rate hundred digits) and compute the number $n = p \cdot q$. He likewise picks a number $e \neq 1$ which indeed not have large number of digits but is relative prime to $(p-1)(q-1) = \phi(n)$, so that it has inverse with modulo $((p-1)(q-1) = \phi(n))$ and compute $d = e^{-1}$ with given modulo. Bob publish e and n. The number d is called his public key.

The encryption interaction starts with the change of message to be sent into an integer M by means of digit alphabet in which each letter, number or punctuation mark of the plain text is replaced by two digit integer.

For instance.

A	B	C	D	E	F	G	H	I	J
00	01	02	03	04	05	06	07	08	09

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z	,	.	?	0
20	21	22	23	24	25	26	27	28	29

1	2	3	4	5	6	7	8	9	!
30	31	32	33	34	35	36	37	38	39

Here it is assumed $M > n$; otherwise M is broken up into blocks of digits $M_1, M_2, \ldots, M_s$ of the approximate size. And each block is encrypted separately. The sender disguises the plain text number M as a cipher text number 'r' by raising 'e' power to M and by taking modulus n (i.e.) $M^e \equiv r(\text{mod}\, n)$. At other end the authorized recipient decipher transmitted information by first determining the integer j, the secret recovery exponent for which $e \cdot j \equiv 1(\text{mod}(\phi(n)))$.

Raising the cipher text number to the 'j' power and reducing it modulo n recovers the original plain text number M (i.e.) $r^j \equiv M(\text{mod}\, n)$

Choose the primes p and q in terms of 2-digit Ramanujan Prime numbers for the RSA public key cryptosystem in the process of encryption and decryption where $p \neq q$ and $p < q$.

Method of Analysis. Choosing the primes p and q in terms of 2-digit Ramanujan prime numbers, we can apply the method of RSA public key cryptography.

As an illustration of this concept, select $p = 11$ and $q = 17$.

Then $n = p \cdot q = 187$

$$\phi(n) = \phi(187) = \phi(11) \cdot \phi(17) = 10 * 16 = 160$$

Choose $e = 3$ to be an enciphering exponent where 3 and 160 are co-prime to each other. Then the recovery element j is a unique integer satisfying the congruence $3 \cdot j \equiv (\text{mod}\, 160)$ and $j = 107$ satisfies the given congruence.

Consider the message RAMANUJAN PRIME

The plain text number is 170012001320090013151708 1204

Since $M > n,$ so split M into blocks of two digit numbers

i.e. 17 00 12 00 13 20 09 00 15 17 08 12 04

$17^3 \equiv 051(\text{mod}\, 187)$ $\quad 00^3 \equiv 000(\text{mod}\, 187)$ $\quad 12^3 \equiv 045(\text{mod}\, 187)$

$00^3 \equiv 000(\text{mod}\, 187)$ $\quad 13^3 \equiv 140(\text{mod}\, 187)$ $\quad 20^3 \equiv 146(\text{mod}\, 187)$

$09^3 \equiv 168(\text{mod}\, 187)$ $\quad 00^3 \equiv 000(\text{mod}\, 187)$ $\quad 13^3 \equiv 140(\text{mod}\, 187)$

$15^3 \equiv 009(\text{mod}\, 187)$ $\quad 17^3 \equiv 051(\text{mod}\, 187)$ $\quad 08^3 \equiv 138(\text{mod}\, 187)$

$12^3 \equiv 045(\text{mod}\, 187)$ $\quad 04^3 \equiv 064(\text{mod}\, 187)$

The encryption of the message is

051 000 045 000 140 146 168 000 140 009 051 138 045 064

For all the 2-digit Ramanujan prime numbers the corresponding primes $p, q,$ enciphering exponent e and recovery element j are presented in the table below:

Table 1.

S. No.	Ramanujan Primes		n	$\phi(n)$	e	j
	p	q				
1	11	17	187	160	3	107
2	11	29	319	280	3	187
3	11	41	451	400	3	267
4	11	47	517	460	3	307
5	11	59	649	580	3	387
6	11	67	737	660	7	283
7	11	71	781	700	3	467
8	11	97	1067	960	7	823
9	17	29	493	448	3	299
10	17	41	697	640	3	427
11	17	47	799	736	3	491
12	17	59	1003	928	3	619
13	17	67	1139	1056	5	845
14	17	71	1207	1120	3	747
15	17	97	1649	1536	5	1229
16	29	41	1189	1120	3	747
17	29	47	1363	1288	3	859
18	29	59	1711	1624	3	1083
19	29	67	1943	1848	5	1109
20	29	71	2059	1960	3	1307
21	29	97	2813	2688	5	1613
22	41	47	1927	1840	3	1227

23	41	59	2419	2320	3	1547
24	41	67	2747	2640	7	2263
25	41	71	2911	2800	3	1867
26	41	97	3977	3840	7	2743
27	47	59	2773	2668	5	1779
28	47	67	3149	3036	5	2429
29	47	71	3337	3220	3	2147
30	47	97	4559	4416	5	3533
31	59	67	3953	3828	5	2297
32	59	71	4189	4060	3	2707
33	59	97	5723	5568	5	3341
34	67	71	4757	4620	13	1777
35	67	97	6499	6336	5	5069
36	71	97	6887	6720	11	611

Conclusion

In this paper, we utilize Ramanujan Prime numbers for encryption of messages by the method of RSA public key cryptography. To conclude that, one may search for encryption techniques by different methods with other numbers.

References

[1] R. Cramer and V. Shoup, A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Cipher text Attack, in crypto'98, LNCS1716, Springer-Verlag, Berlin, (1998), 13-25.

[2] M. David, Burton, Elementary Number Theory, 2nd Edition, UBS Publishers.

[3] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Clarendon Press, (1979).

[4] M. D. Hirschhorn, An amazing identity of ramanujan, Math. Mag. 68(3) (1995), 199-201.

[5] J. N. Kapur, Ramanujan's Miracles, Mathematical Sciences Trust Society, (1997).

[6] Melvyn B. Nathanson, Methods in Number Theory, Springer-Verlag, New York, (2006).

[7] T. Nagell, Introduction to number theory, Chelsea publishing company, New York, (1981).

[8] Neal Koblitz, A course in number theory and cryptography, New York: Springer Verlag, (1994).

[9] Niven, Zuckerman and Montgomery, An Introduction to the Theory of Numbers, 5th ed., New York: John Wiley and Sons, (1991).

[10] A. M. S. Ramasamy, Ramanujan's Equation, J. Ramanujan Math Soc. 7(2) (1992), 133-153.

[11] Shailesh Shirali and C. S. Yogananda, Number Theory, University Press, Hyderabad, (2003).

[12] Simon Singh, The codebook, Anchor Books, (1999).