International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02462
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Securing Messages with RSA Cryptography Using Wagstaff Primes.

S. Shanmuga Priya[1], G. Janaki [2]

[1]PG and Research Department of Mathematics, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Trichy-18
[2]PG and Research Department of Mathematics, Cauvery College for Women (Autonomous), Affiliated to Bharathidasan University, Trichy-18

Abstract - This study delves into the intriguing synthesis of number theory and cryptographic applications, presenting an innovative perspective on RSA public key encryption. It explores the practical implementation of Wagstaff Prime number—a distinctive class of numerical patterns—within the framework of RSA cryptography. By leveraging the mathematical richness of Wagstaff Prime numbers, the paper seeks to enhance the conventional encryption paradigm.

***Key Words*:** Wagstaff Prime, Encryption, Decryption, RSA algorithm

1. INTRODUCTION

Number theory stands as a cornerstone of mathematical intrigue, offering a wealth of open problems that appear deceptively approachable. Yet, these challenges persist due to the profound complexity underlying seemingly simple numerical structures, which remain only partially understood. The mid-twentieth century witnessed a monumental advance in Diophantine equation studies, thanks to Thue's innovative proof—a pioneer of the polynomial method. This groundbreaking work reverberated through subsequent developments in number theory, profoundly shaping the exploration of Diophantine equations. With its diverse subfields and endless mysteries, number theory will continue captivating mathematicians for generations [1-6].

Beyond polygonal numbers, the study of unique number patterns such as Jarasandha numbers, Nasty numbers, and Dhuruva numbers adds further layers of fascination. These intriguing patterns have been extensively documented and studied [7-17].

Number theory also plays a pivotal role in the realm of cryptography, the science of safeguarding information by transforming it into unreadable formats. Fundamental tools of number theory, including primes, divisors, congruences, and Euler's φ function, form the backbone of cryptographic security mechanisms. This paper introduces readers to the application of number theory in cryptography, specifically showcasing encryption through RSA public key cryptography integrated with Wagstaff prime number with 2 digits.

.

2. WAGSTAFF PRIME NUMBER

In number theory, a Wagstaff prime is defined as a prime number that takes the form $\frac{2^q+1}{3}$, where q itself is an odd prime.

Some of the illustrations are 3, 11, 43, 683, 2731, 43691, 174763, 2796203, 715827883, 2932031007403, ...

3. RSA PUBLIC KEY CRYPTOGRAPHY

In 1977, R. Rivest, A. Shamir, and L. Adleman introduced a revolutionary public key cryptosystem rooted in fundamental concepts of number theory, known as RSA. This cryptographic system addresses the challenges posed by traditional codebook-based encryption methods. In a public key framework, two parties—commonly referred to as Alice (the sender) and Bob (the receiver)—are not required to pre-arrange a shared secret code. Instead, both individuals make a portion of their encryption details publicly available in a directory. Remarkably, even with access to this public information and the encrypted message, a potential eavesdropper cannot decrypt the information. Each participant in this system possesses two keys: a public key and a private (or secret) key.

In the RSA cryptosystem, Bob begins by selecting two large prime numbers, r and s, each typically comprising at least 100 digits. He calculates $w = r.s$ and chooses a number $g \neq 1$, which satisfies the fact $\gcd(g, \phi(w)) = 1$, where $\phi(w) = (r-1)(s-1)$. The number g, though not excessively large, has an inverse modulo $\phi(w)$, denoted as $f = g^{-1} \bmod \phi(w)$. Bob then publishes g and w, forming his public key, while retaining f as his private key.

The encryption process involves converting the plaintext message into an integer B using a digit-based alphabet where each letter, number, or punctuation mark is substituted with a two-digit numeric representation. This encoded message is then encrypted using Bob's public key for secure transmission.

Consider the following table values for alphabets and special character.

A	B	C	D	E	F	G	H	I	J	K	L
00	01	02	03	04	05	06	07	08	09	10	11

M	N	O	P	Q	R	S	T	U	V	W	X
12	13	14	15	16	17	18	19	20	21	22	23

Y	Z	,	.	?	0	1	2	3	4	5	6
24	25	26	27	28	29	30	31	32	33	34	35

7	8	9	!
36	37	38	39

When B is smaller than w, the plaintext message B may be split into smaller blocks, labelled $B_1, B_2, \dots, B_s$ if required. Each block undergoes individual encryption. The sender encrypts B by computing:

$$B^g \equiv H(\, mod\, w)$$

where g is the encryption exponent, ensuring the plaintext is securely encoded as H.

On the recipient's side, decryption is performed using the private key j, determined such that $g.j \equiv 1\ (mod\ (\phi(w))$. The ciphertext H is decrypted by evaluating:

$$H^j \equiv B(mod\, w),$$

recovering the original plaintext B. This encryption-decryption mechanism relies on modular arithmetic and the properties of $\phi(w)$, offering robust security for transmitted data.

4. METHOD OF ANALYSIS

Here, the value of r, s are considered as Wagstaff prime number with 2 digits.

Encryption:

Let $r = 11,\ s = 43$ be the two wagstaff prime numbers with 2 digits, then $w = 11 \times 43 = 473$

$$\phi(w) = \phi(473) = 10 \times 42 = 420$$

Choose $g = 11$, which is relatively prime to 420. It is found that $j = 191$ that satisfies $11\ .j \equiv 1(mod\ 420)$.

Consider the message “CONFIDENTIAL”. The corresponding Plain text number is 02141305080304131908001 1, which is higher than w. Hence, B is split up into blocks of two digit numbers.

i.e. 02 14 13 05 08 03 04 13 19 08 00 11

$$02^{11} \equiv 156\ (mod\ 473)$$

$$14^{11} \equiv 311\ (mod\ 473)$$

$$13^{11} \equiv 453\ (mod\ 473)$$

$$05^{11} \equiv 335\ (mod\ 473)$$

$$08^{11} \equiv 118\ (mod\ 473)$$

$$03^{11} \equiv 245\ (mod\ 473)$$

$$04^{11} \equiv 213\ (mod\ 473)$$

$$13^{11} \equiv 453\ (mod\ 473)$$

$$19^{11} \equiv 459\ (mod\ 473)$$

$$08^{11} \equiv 118\ (mod\ 473)$$

$$00^{11} \equiv 000(mod\ 473)$$

$$11^{11} \equiv 451\ (mod\ 473)$$

The encrypted message H is

156 311 453 335 118 245 213 453 459 118 000 451

Decryption:

Consider $g\ .j \equiv 1\ mod(420)$

Since $g = 11$, from the above congruence, it is found that $j = 191$. With the help of j, the plain text B is obtained from the cipher text H using the following constraint

$$H^j = B(mod\, w)$$

3. CONCLUSION

This paper employs Wagstaff prime numbers to encrypt messages using the RSA public key cryptography method. In conclusion, exploring encryption techniques through alternative approaches and different number systems could be a promising area for further investigation.

REFERENCES

[1] David, M. Burton, Elementary Number Theory, 2nd Edition, UBS Publishers.
[2] G. H. Hardy, and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Clarendon Press, 1979
[3] Niven, Zuckerman and Montgomery, An Introduction to the Theory of Numbers, 5th ed., New York: John Wiley and Sons,1991
[4] Neal Koblitz, A course in Number Theory and Cryptography, New York: Springer Verlag,1994
[5] R. Cramer and V. shoup, A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Cipher text Attack. In crypto’98, LNCS1716, pages13-25, SpringerVerlag, Berlin,1998
[6] Simon Singh, The codebook, Anchor Books, 1999.
[7] G.Janaki & C.Saranya, “Special Pairs Of Pythagorean Triangles & Jarasandha Numbers”, American International Journal Of Research In Science, Technology, Engineering & Mathematics, Issue-13, 118-120, Dec 2015-Feb 2016.
[8] G.Janaki & C.Saranya, “Connection Between Special Pythagorean Triangles & Jarasandha Numbers”, International Journal Of Multidisciplinary Research & Development, Vol-3, Issue-3, 236-239, March 2016.
[9] G.Janaki & C.Saranya, “Special Rectangles & Jarasandha Numbers”, Bulletin Of Mathematics & Statistics Research, Vol-4, Issue-2, 63-67, Apr-June 2016.
[10] G.Janaki & C.Saranya, “Special Pairs Of Rectangles & Jarasandha Numbers”, Asian Journal Of Science &Technology, Vol-7, Issue-5, 3015-3017, May 2016.
[11] G.Janaki & C.Saranya, “Pythagorean Triangle With Area/Perimeter As A Jarasandha Number Of Orders 2 & 4”,

International Research Journal Of Engineering & Technology, Vol 3, Issue 7, 1259-1264, July 2016.

[12] G.Janaki & C.Saranya, "Connection Between Frustum Of The Cone With Jarasandha Numbers & Some Special Numbers", International Journal Of Research In Engineering & Applied Sciences, Vol 7, Issue 3, 45-50, March 2017.

[13] C.Saranya & G.Janaki, "Integer Triples Comprising Of Jarasandha Numbers In Arithmetic Progression & Geometric Progression", International Journal Of Research & Analytical Reviews, Vol 6, Issue 1, 751-752, Jan 2019.

[14] C.Saranya & G.Janaki, "Solutions Of Pell's Equation Involving Jarasandha Numbers", International Journal Of Scientific Research In Mathematical & Statistical Sciences, Vol 6, Issue 1, 234-236, Feb 2019.

[15] C.Saranya & G.Janaki, "On Generalized Fermat Equations Involving Jarasandha Numbers", Parishodh Journal, Vol IX, Issue II, 712-716, Feb 2019.

[16] C.Saranya & G.Janaki, "Solution Of Exponential Diophantine Equation Involving Jarasandha Numbers", Advances and Applications in Mathematical Sciences, Volume 18, Issue 12, 1625-1629, Oct 2019.

[17] C.Saranya & G.Janaki, "Ramanujan-Type Diophantine Equation Involving Jarasandha Numbers", Aryabhatta Journal of Mathematics & Informatics, Vol 12, Issue 1, 7-10, Jan-June 2020.

