Design and Implement on The Optimized Algorithm for Generating Prime Numbers Suitable for Cryptographic Applications

Poonam Kumari, Research Scholar, Department of Mathematics, Singhania University, Pacheri Bari, Jhunjhunu (Raj.), India
Dr. Vijesh Kumar, Research Supervisor, Department of Mathematics, Singhania University, Pacheri Bari, Jhunjhunu (Raj.), India

Abstract

Number theory, a branch of pure mathematics, has significantly influenced modern cryptography's development of safe data security and communication techniques. This study examines how number theory is used to contemporary cryptography algorithms and protocols, highlighting recent advancements and their useful applications. The mathematical foundations of numerous cryptographic primitives based on number-theoretic concepts, such as public-key cryptography, digital signatures, and secure communication protocols, are examined in this study. The reader will learn about the applications of number theory in chemistry, statics, and cryptography in this chapter. We will specifically cover the use of RSA public key cryptography to encrypt data and determine the enciphering exponent and recovery element, the linear Diophantine equation for balancing chemical equations using matrices, and the Pythagorean triangles involving Jarasandha numbers for solving ladder problems in statics.

Keywords: Number theory, cryptanalysis, public key cryptography, quantum number.

1. INTRODUCTION

Mathematicians have been studying prime numbers since ancient times. Prime numbers are natural numbers greater than one that only have one and themselves as positive divisors. They are arithmetic's fundamental building blocks. Every natural number greater than one can be expressed as a distinct product of prime numbers, according to the Fundamental Theorem of Arithmetic. This demonstrates their significance in number theory. Mathematicians are still researching the distribution and characteristics of prime numbers, despite their apparent simplicity. Despite being more than just numbers, prime numbers are crucial to modern computer science, particularly in the field of encryption. The availability of large prime integers is essential to the security of several cryptographic techniques, including the well-known public-key systems RSA, Diffie-Hellman, and Elliptic Curve Cryptography. These systems make use of factors such as the difficulty of factoring the product of two large prime numbers. This enables private data interchange, e-commerce, online banking, and secure digital communication. To keep digital information safe and secure in today's world, it is crucial to be able to generate large prime numbers fast and consistently. Finding the ideal mix between speed and accuracy is the challenge when producing prime numbers. Early methods such as trial division and the Sieve of Eratosthenes are simple to comprehend and effective for small integers, but they are ineffective for cryptographic applications that require handling very large numbers.

Consequently, several more sophisticated algorithms have been developed. These include deterministic tests like the AKS primality test, which ensure correctness but are frequently more expensive to conduct, and probabilistic tests like the Miller-Rabin and Fermat tests, which can rapidly identify plausible primes with a very small error margin.

Cryptography is one branch of mathematics that has influenced our day-to-day lives. It is the science of creating secure and efficient codes that use various algorithms, or cryptosystems, to send and receive encrypted communications. Ancient societies laid the foundation for cryptography, which is still widely used today. Every time a computer is used or a credit card is swiped, a cryptosystem-based security mechanism is employed. It is particularly crucial in relation to cyber and national security matters. Cryptography is strongly related to number theory, which is a separate branch of mathematics.

This study will primarily concentrate on the particular applications of number theory that are relevant to cryptography. Secure communication, or cryptography, has always been a crucial part of safeguarding private information. With the exponential growth of the internet and digital

communication, robust cryptographic systems are now crucial. Number theory, a fundamental branch of mathematics, has developed into a powerful tool in modern cryptography that offers complex solutions to a variety of security issues. The use of number theory to cryptography gained significant attention in the 1970s with the advent of public-key cryptography.

The concept of using a public key and a private key for encryption and decryption, respectively, was developed by asymmetric cryptography, also known as public-key cryptography. This innovative method makes it computationally hard for attackers to decrypt the data due to the mathematical intricacy of a number of number theory problems. Numerous unresolved problems that seem understandable from the outside are what make number theory so fascinating. Naturally, there is a reason why certain problems in number theory remain unresolved. Even though they are simple, numbers have a tremendously intricate structure that is only partially understood by humans. Number theory and its many subfields will continue to engage mathematicians' attention for a very long time. The Jarasandha, Nasty, and Dhuruva numbers are three more fascinating number patterns besides polygonal numbers. In our Indian epic, the Mahabharata, we encounter 'JARASANDHA,' a demoniac being. One of his blessings was that if he were split into two parts and thrown apart, the parts would reassemble and come back to life. In fact, he was given life by the two parts of his body. In mathematics, there are numbers that share Jarasandha's trait. Look at a few instances of the form XC. A combination of these integers may result in the separation of X and C.

Squared, we get the same number XC. (i.e.) 2 XC = (X+C)

Also, if C is an n-digit number, then X C X C n (+) = (10^n) (X)+C

Number theory is a fundamental part of encryption techniques. Cryptography can be used to conceal information by converting some secret data into incomprehensible text. These results motivated our study of encryption in RSA public key cryptography. Diophantine equations have many real-world applications. In statics, they are used to solve mathematical, age-related, network flow, and ladder problems. Business word problems can be solved using Diophantine equations. Another field that makes use of the Diophantine equation is chemistry. Chemical equations are easy to balance thanks to Diophantine equations. The Pythagorean triangle can be used with Jarasandha numbers to solve statics ladder problems. For the discussion, three sections of this chapter should be taken into account. The first portion uses the encryption method for RSA public key cryptography. In Section 2, chemical equations are balanced using the linear Diophantine equation, and the static ladder problem is analyzed in Section 3 using Pythagorean triangles with Jarasandha numbers.

2. LITERATURE REVIEW

Abdulqader et al. (2024) conducted a recent study on atypical relaxation models in the prime number distribution and examined their potential applications in sustainable development education. Their research examined prime numbers as concepts that can help us comprehend how complex and unpredictable life can be, in addition to numbers. According to the authors, the peculiar prime distribution resembles some dynamic systems seen in society and nature. They are therefore appropriate for demonstrating nonlinear thinking in educational contexts. This study demonstrated the potential of prime number theory as a teaching tool for a variety of courses, particularly in assisting students with system thinking and problem-solving through arithmetic.

Carbó-Dorca (2023) focused on how to produce and couple prime numbers, which aided in the computational analysis of primes. He developed novel methods for locating and classifying prime pairs, which are crucial for numerous algorithmic operations and cryptographic applications. In order to simplify and speed up related computational activities, the study examined the speed at which primes can be formed as well as their logical pairing. By enhancing the techniques for locating prime pairs, this study contributed to the development of encryption systems and mathematical software that must swiftly examine large prime values.

Curtis and Tularam (2011) emphasized the significance of comprehending prime numbers in

and of themselves by taking a more philosophical and fundamental approach to the topic. They investigated several mathematical and historical issues about the origins of primes, their frequency, and their enigmatic nature. Their results demonstrated that despite hundreds of years of study, many aspects of the distribution of prime numbers remain unclear. The authors stated that more investigation into the fundamental characteristics of primes is necessary. They recommended that this study blend abstract theoretical investigation with practical analysis. The notion that primes are not only practical but may also pique genuine mathematical interest and inquiry was reinforced by their discussion.

Ezz-Eldien et al. (2024) resolved the major issues with prime number generation, particularly in the area of cybersecurity. Their study provided a comprehensive understanding of the use of prime numbers in public-key cryptosystems, such as RSA, and encryption methods where large primes are required to create keys. The authors identified several issues with typical generating methods' performance and proposed algorithmic solutions to speed up and improve the process's dependability. Their findings demonstrated the significance of prime number theory for contemporary information security systems and the need to continuously develop new methods for performing cryptographic computations.

Gunasekara et al. (2015) spoke extensively about prime numbers' theory, history, and applications. Important developments in the study of prime numbers were examined in their work, including the development of techniques for testing primes, the demonstration that the number of primes is infinite, and advancements in determining the distribution of primes using the Riemann Hypothesis and other tools. The paper also discussed the practical applications of these concepts in fields like signal processing and blockchain technologies. Decades of research were compiled by the authors to provide a comprehensive picture that not only contextualized recent findings but also identified intriguing directions for further investigation.

Knežević (2021) looked into using evolutionary algorithms to find prime numbers and came up with a new heuristic-based way to evolve possible prime candidates over time. This method was different from standard deterministic algorithms since it used ideas from biological evolution, like mutation, selection, and crossover, to find prime numbers in a set range of numbers. The study showed that genetic algorithms could be useful for generating huge numbers of prime numbers, especially in limited or specialized settings, even if they might not always be as fast as sieve-based approaches.

Kwame, Owa, and Tawfik (2024) discussed the practical issue of generating prime integers for RSA encryption in particular. They proposed a quick method that would maintain the high security requirements of public-key infrastructures while reducing the cost of creating large prime numbers. Their approach focused on reducing the number of pointless steps in the creation process and optimizing the primality testing phase. The findings demonstrated that their approach significantly reduced processing time and energy consumption, which makes it suitable for real-time cryptography applications, particularly in resource-constrained environments.

Lee and Kim (2024) employed sparse encoding techniques for classification problems to provide a fresh perspective on prime number research. Finding primes from a large set of natural numbers with a high recall rate and rapid convergence was the main goal of their study. They demonstrated how machine learning techniques, particularly sparse representation, may be used to learn and sort prime numbers with great accuracy due to their unique features. According to the study, data-driven techniques may expedite the process of determining prime numbers, which may result in hybrid models that combine statistical learning and mathematical principles.

Loconsole and Regolin (2022) investigated if prime numbers differ from other numbers due to biological or cognitive "special" characteristics. The authors examined how humans and animals perceive number patterns, with a special focus on prime numbers, utilizing insights from cognitive neuroscience and the life sciences. Their findings suggested that primes may

have cognitive significance due to their irregular distribution and inability to be separated. In jobs involving pattern identification, this could make them more engaging or challenging to comprehend. This study took a novel approach to prime numbers, suggesting that their perceived uniqueness may have biological and psychological implications in addition to mathematical ones.

3. OBJECTIVES OF THE STUDY

- **To design and implement an optimized algorithm** for generating prime numbers suitable for cryptographic applications.
- **To evaluate the performance of the proposed algorithm** against existing methods in terms of speed, accuracy, and resource usage.

4. NEED OF THE STUDY

The need for designing and implementing an optimized algorithm for generating prime numbers suitable for cryptographic applications arises from several critical requirements in modern security systems:

- Cryptographic algorithms, particularly public-key systems like RSA, rely on the use of large prime numbers. Generating these primes efficiently is crucial, as the process can be computationally intensive, especially for very large numbers required for strong security. Optimized algorithms reduce the time and resources needed for key generation and other cryptographic operations.
- The security of many cryptographic systems directly depends on the size and randomness of the prime numbers used. Generating primes that are truly random and sufficiently large makes it computationally infeasible for attackers to factor the numbers and compromise the system. Optimized algorithms can ensure the generation of primes meeting these stringent security requirements.
- As computational power increases and cryptographic threats evolve, the need for larger and more secure primes grows. Optimized algorithms must be scalable to handle increasing bit lengths and adaptable to new security standards and requirements.
- In some advanced security schemes, like dynamic key updates, the ability to rapidly generate and synchronize new prime numbers is essential for maintaining robust security against evolving threats. Optimized algorithms facilitate such dynamic key management strategies.

In essence, the optimization of prime number generation algorithms is a continuous effort to balance the demands of strong cryptographic security with the practical realities of computational resources and performance requirements.

5. SCOPE OF THE STUDY

Only the creation of prime integers large enough to be practical for current cryptographic standards particularly for public-key encryption systems is examined in this work. The study does not examine how to optimize hardware or leverage specialized computing platforms like quantum computers; instead, it concentrates on how effective and scalable algorithms are. Additionally, the study solely examines benchmarking and the deployment of software-based methods in conventional computer systems. The findings are intended to aid in the development of more efficient methods for producing prime numbers that can be applied to data encryption, secure communication, and other fields requiring large prime numbers.

6. SIGNIFICANCE OF THE STUDY

This study holds significant value in advancing the understanding and practical application of prime number generation, a fundamental component of modern cryptographic systems and computational mathematics. Improved algorithms can lead to faster processing times and reduced computational costs, benefiting industries reliant on secure transactions, such as banking, e-commerce, and cybersecurity. Additionally, the study provides a valuable reference for researchers and practitioners in computer science and mathematics, offering insights that could guide future innovations in algorithm design and cryptographic standards.

7. RESEARCH METHODOLOGY AND DATA ANALYSIS

7.1 Applications of number theory in cryptography:

The purpose of this section is to provide an introduction to the applications of number theory in cryptography, specifically the concept of using Jarasandha numbers to encode data in number theory including RSA public key encryption. When using a cryptosystem that uses public keys, the source and the beneficiary—who are typically referred to as Alice and Sway separately do not need to agree in advance on a mystery code. Undoubtedly, each of them contributes a portion of their code to a publicly accessible catalog. Furthermore, the message cannot be translated by an adversary who accesses both the public index and the encoded message. More specifically, Alice and Weave will each have two keys, one of which will be public and the other will be covered up. To determine a mystery key in the RSA cryptosystem, Bounce selects two prime whole numbers, p and q, which also happen to contain at least 100 digits each. Then, it registers the number n p q. In a similar manner, he chooses the number e 1, which has a relatively small number of digits but is relative prime to (p 1) (q 1) (n), suggesting that it has an opposite with the modulo (p 1) (q 1) (n). He then uses the given modulo to get d = e - 1. Both e and n are distributed by Bounce. The letter "d" in this line refers to his public key. The encryption cycle's most crucial step involves converting the message to be delivered into a whole number, M, using a sequence of digit letters. Any letter, number, or accentuation mark in the unrefined text is converted to a two-digit number during this cycle.

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	U
10	11	12	13	14	15	16	17	18	19	20

V	W	X	Y	Z	,	.	?	0
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

It is anticipated that M will be more noticeable than n in this case; if not, M is divided into digit-wide regions, M1 M2 Ms, of approximate size. What's more, the encryption cycle is rehashed for every individual block. By taking modulus n (i.e., M r (mod n) e) and increasing the force of 'e' to M, the source transforms the plain text number M into the scrambled text number 'r'. At the opposite end, the approved beneficiary unravels the data that was supplied by first differentiating the number j, which is the mystery recuperation type for which e j 1mod(n). The first plain text number M can be recuperated by raising the encoded text number to the force of j and afterward diminishing it modulo n; this is signified by the documentation r M (mod n).

7.2 Numerical Example:

If we choose two distinct primes p = 43and q = 47 then n = p·q = 2021 (Current Year)

$\phi(n) = \phi(2021) = \phi(43)\cdot\phi(47) = 42*46 = 1932$

Select the exponent e less than 5 as your enciphering exponent if both 5 and 1932 are prime values. The recovery element j will be a unique number that fulfils the congruence if this is the case.

$e \cdot j \equiv 1(\mathrm{mod}(\phi(n)))$

So that $5\cdot j \equiv 1(\mathrm{mod}1932)$

The modus operandi of trial-and-error reveals that j > 773 is well-suited through the congruence that has be provided.

Take a appear at the memo. THEORY OF NUMBERS

The number uttered in basic text is 132012010417190704141724.

In view of the fact that M is superior to n, divide M into group of information by three digits.

i.e., 132 012 010 417 190 704 141 724

Since M r (mod n) e ≡ , n = 2021 and e = 5

M^e- r /n = 2021 integer say k+ r
In favour of the first wedge of the plain set book number 132
132^5= 2021k + r
When k =19829115 we get r =1017
132 1017 (mod2021)
5 ≡ 012 0249(mod2021)
5 ≡ 010 0971(mod2021)
5 ≡ 417 0872(mod2021)
5 ≡ 190 1395(mod2021)
5 ≡ 704 1267(mod2021)
5 ≡ 141 1410(mod2021)
5 ≡ 724 0000(mod2021)
The encrypted version of the message is 1017 0249 0971 0872 1395 1267 1410 0000. In this instance, the decoding exponent is 773, whereas the enciphering exponent is 5. The cipher text number can be raised to the power of 'j=773' and then lowered modulo 2021 to obtain the original plain text number M. The outcome is identical to that of r773 (mod2021).

7.3 APPLICATIONS OF NUMBER THEORY FOR LADDER PROBLEMS IN STATICS

To paint a wall, we will require a vertical wall, a horizontal floor, and a ladder. For the x variable, the height of the wall to be painted is chosen; for the y variable, the distance between the vertical wall and the floor where the ladder will be fixed to paint is chosen; and for the z variable, the ladder's length is chosen. The following formula applies to Pythagorean triangles: Y 2mn, 2 2 z m n, and 2 2 x m n). The following situations arise when Jarasandha numerals are used to represent each variable:

Case 1: When x equals 83, which is a two-digit Jarasandha number, the Pythagorean triangles that are obtained are shown in the table that follows:

Table 1: When x equals 83, which is a two-digit Jarasandha number, the Pythagorean triangles that are obtained are shown in the table

m	n	x	y	z
17	14	83	365	364
43	42	83	3286	3280

Case 2: The Pythagorean triangles that are produced when x equals 2021, which is the four-digit Jarasandha number, are detailed in the table that follows:

Table 2: Pythagorean triangles that are produced when x equals 2021, which is the four-digit Jarasandha number, are detailed in the table

m	n	x	y	z
53	26	2021	2450	3000
51	30	2021	2976	3500
71	70	2021	8996	9000
120	120	2021	25676	25003
200	225	2021	82311	82031
340	354	2021	227610	23000
1020	1112	2021	2050300	2057612

Case 3: When x equals 3000, which is the four-digit Jarasandha number, the Pythagorean triangles that are obtained are shown in table 3 as follows:

Table 3: When x equals 3000, which is the four-digit Jarasandha number, the Pythagorean triangles that are obtained are shown in table

m	n	x	y	z
75	50	3000	6995	7500
147	140	3000	37741	37473

309	350	3000	182414	187070
1527	1572	3000	4674300	4076270

8. CONCLUSION

In this chapter, the encryption process is covered in detail and the plain text is recovered using RSA public key cryptography. Pythagorean triangles utilizing Jarasandha numbers can be utilized to solve statics problems that need ladders, and linear Diophantine equations can be used to balance ladder problems in both statics and chemical equations. The goal is to gain a deep understanding of and compare several algorithms for generating prime numbers, pointing out their pros and cons in terms of how fast and scalable they are. The goal of the research is to create a new or improved algorithm that works better than current ones by generating prime numbers faster and using fewer resources, making it ideal for cryptographic applications. The study will also provide real-world proof through benchmarking and performance evaluation, showing that the proposed solution is better than traditional methods. This will add useful knowledge and tools for generating prime numbers safely and quickly in both the computing and security fields.

9. LIMITATIONS OF THE STUDY

This study only looks at and rates software-based prime number generation methods; it doesn't look at or optimize hardware-level implementations. Also, the study only looks at prime numbers that are within ranges that are important to existing cryptography standards. It doesn't look at really large primes that are outside of these ranges because of limitations in computing power. The performance evaluation uses certain programming languages and test environments, which could make it impossible to apply the results to other platforms or hardware setups.

10. REFERENCES

1. Abdulqader, S. A., Al_Barazanchi, I. I., Jaaz, Z. A., Sekhar, R., Shah, P., &Malge, S. (2024). Exploring Anomalous Relaxation Models in Prime Number Distribution and Their Relevance to Sustainable Development Education. Mathematical Modelling of Engineering Problems, 11(5).
2. Carbó-Dorca, R. (2023). On prime numbers generation and pairing. International Journal of Innovative Research in Sciences and Engineering Studies, 3, 12-17.
3. Curtis, M., & Tularam, G. A. (2011). The importance of numbers and the need to study primes: The prime questions. Journal of Mathematics and Statistics, 7(4), 262-269.
4. Ezz-Eldien, A., Ezz, M., Alsirhani, A., Mostafa, A. M., Alomari, A., Alserhani, F., & Alshahrani, M. M. (2024). Computational challenges and solutions: Prime number generation for enhanced data security. PloS one, 19(11), e0311782.
5. Gunasekara, A. D. V., Jayathilake, A. A. C. A., & Perera, A. A. I. (2015). Survey on prime numbers. Elixir Appl. Math, 88, 36296-36301.
6. Knežević, K. (2021, September). Generating Prime Numbers Using Genetic Algorithms. In 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO) (pp. 1224-1229). IEEE.
7. Kwame, A. A., Owa, K., & Tawfik, A. H. (2024, July). An Efficient Generation of Prime Numbers for RSA Encryption Scheme. In World Congress in Computer Science, Computer Engineering & Applied Computing (pp. 409-420). Cham: Springer Nature Switzerland.
8. Lee, S., & Kim, S. (2024). Exploring Prime Number Classification: Achieving High Recall Rate and Rapid Convergence with Sparse Encoding. arXiv preprint arXiv:2402.03363.
9. Loconsole, M., & Regolin, L. (2022). Are prime numbers special? Insights from the life sciences. Biology Direct, 17(1), 11.
10. Mabrouk, E., Hernández-Castro, J. C., & Fukushima, M. (2011). Prime number generation using memetic programming. Artificial Life and Robotics, 16, 53-56.
11. Machado, J. T., & Lopes, A. M. (2020). Multidimensional scaling and visualization of patterns in prime numbers. Communications in Nonlinear Science and Numerical Simulation, 83, 105128.
12. Singh, S. (2024). Prime Generation via Polynomials: Analysis and Applications.
13. Sipilä, J. (2018). On Generating Prime Numbers Efficiently.
14. Wells, D. (2011). Prime numbers: the most mysterious figures in math. Turner Publishing Company.
15. Zaman, B. U. (2023). Prime discovery a formula generating primes and their composites. Authorea Preprints.