Exploring the Cryptographic Potential of the Riemann Zeta Function and Prime Number Distribution

Ryan Doraiswamy

1.1 Abstract

Understanding the Riemann hypothesis is integral for the continuation of math into the future and potentially the security of cyberspace. The Riemann hypothesis is one of the Millennium Problems, a set of 7 famous unsolved problems in mathematics. It is a hypothesis that scientists and mathematicians alike have tried to prove for decades but have not yet been successful. It is hypothesized that it may have applications in various mathematics and scientific fields, such as quantum mechanics. Beyond that, the applications of the Zeta function and Riemann hypothesis are relatively unknown.

One way the hypothesis can potentially be used is in cryptography. Using the implications of the hypothesis and the distribution of prime numbers, algorithms can be created through the primes to send and receive messages with dependable security. In this project, the hypothesis was used to create an algorithm that can generate long alphabetical phrases to relay classified information in a unique way that might be difficult to identify for an adversary. These results indicate that there are applications of the hypothesis in cryptography and that one could algorithmically create prime number sequences that could be used for encryption and decryption. This finding is significant as it provides supplemental evidence for the Riemann hypothesis, while also opening a pathway to explore unfamiliar connections between number theory and cryptography.

1.2 Introduction

Riemann Zeta function:

The Riemann Zeta function belongs to a class of functions known as Zeta functions, and can be written in series notation as denoted below:

$$\zeta(n) = \sum_{k=1}^{\infty} \frac{1}{k^n}$$

The Riemann zeta function is a mathematical tool used to understand the distribution of prime numbers. It was introduced by the mathematician Bernhard Riemann in 1859. The function itself has roots going back to earlier work by Leonhard Euler in the 18th century. The primary purpose of the Riemann zeta function is to explore the properties and distribution of prime numbers. Unlike simpler functions that deal with whole numbers or real numbers, the Riemann zeta function deals with complex numbers (numbers that have both a real part and an imaginary part).

Of all the zeta functions, the Riemann Zeta function is arguably the most well-known, although the extent of its applicability is not as well-known and has not been fully explored. More specifically, The Riemann Hypothesis is a hypothesis about the zeros of the Riemann Zeta function, stating that the non-trivial zeros of the function all lie on the C*ritical line* Re[*s*] = ½, where Re[*s*] denotes the real part of a complex number *s*. The nontrivial zeros are the zeros that contain an imaginary as well as real component. The hypothesis is of great interest in number theory due to its theorized connections with the distribution of prime numbers.

Chebyshev PSI function:

The Chebyshev PSI function is a function that can help calculate prime density. The function is defined as the sum of the logarithms of the prime numbers with powers less than or equal to a given value. It is often denoted by Ψ(x), and is given as

$$\psi(x) = \sum_{k=1}^{\infty} \sum_{p^k < x} \log p$$

The function, rather than focusing on the exact values of prime numbers, focuses on their distribution, and it can be incredibly useful as it is simple to evaluate, and connections can be drawn to the Riemann hypothesis through the Prime Counting function described in the following section. This is through various studies and proofs dating back to the work of Euler.

Prime Counting Function

The Prime Counting function is a function that is given to us by the proofs of the Riemann hypothesis. Although incomplete, the parts of the proof that exist allow us to draw connections between the two functions, as many famous mathematicians have done before. It allows us to know the exact number of primes less than or equal to some number x.

$$\pi(x) \ = |\{p \le x : p \ is \ prime\}|$$

The explicit formula for π(x) involves a sum over the non-trivial zeros of the Riemann zeta function. Assuming the Riemann Hypothesis, the explicit formula for π(x) can be written as:

$$\pi(x) \ = \ Li(x) \ - \ \sum_{p} Li(x^{p}) \ + \ c$$

Where *Li(x)* is the logarithmic integral, given by

$$Li(x) \ = \ \int_{2}^{x} \frac{dt}{\log t}$$

And *p* runs over the non-trivial zeros of the Riemann Zeta function. *c* denotes small correction terms negligible for large *x*.

Because it gives the exact number of primes less than or equal to a target, it can also be used in the context of prime density. For example, π(10) would refer to the amount of primes between 0 and 10, which would evaluate to 4. This can also be thought of as 4 prime numbers out of 10, meaning a 40% density of prime numbers over the interval [0,10]. It is important to note, with respect to the Prime Counting function and the Chebyshev PSI function, that as intervals (the argument to the Prime Counting function and related prime density estimate) get larger, the accuracy of the density estimate will decrease. However, the function serves as a strong estimate.

Sieve of Eratosthenes and RSA algorithm

The Sieve is a simple algorithm used to find all prime numbers up to a specified integer n. This is significant to this research as the Prime Counting and Chebyshev PSI functions allow us to know the number of prime numbers within specified intervals and the density of them within those intervals, respectively.

The RSA algorithm is an algorithm that utilizes prime numbers to encrypt and decrypt data, e.g., words like “Rainbow” “GOOD DAY” or “Stick”. The RSA algorithm utilizes large prime numbers to create a *public key* that encrypts data (convert plaintext into ciphertext), and a *private key* that decrypts that data (convert ciphertext back into plaintext), ensuring that only authorized parties can access the information. Such mathematical cryptography is the practice of securing information through the use of mathematical techniques. Cryptography relies heavily on mathematical theories and computational algorithms to protect data and communications.

Research Question

The theorized research question is “Can we find an application of the Riemann Zeta function in cryptography?” If the Riemann hypothesis lends itself to accurately computing the Prime Counting function, then there may be plausible applications of the Riemann Zeta function in cryptography, due to its relation to the Prime Counting function. To find an application of the Riemann Zeta function in cryptography, one can look to employ the Prime Counting function, Chebyshev PSI function and the Sieve of Eratosthenes, utilizing their properties and information they relay regarding prime numbers. Initially, tests need to be run to ensure the agreement of the Prime Counting function and Chebyshev PSI function to ensure their estimates for prime density are sufficiently close (to justify using the PSI function over the Prime Counting function as it is computationally simpler). In the case that they are sufficiently similar, one can develop algorithms to check for prime density on larger and larger intervals. One can use the PSI function to estimate the density on those intervals and use the Sieve to find the prime numbers on the interval. Then, the large prime numbers can be used within the RSA algorithm for secure encryption and decryption.

1.3 Methods

A: Review of Cryptographic Algorithms:

To develop a new cryptographic algorithm, one should start by studying existing algorithms for inspiration. Begin with the Advanced Encryption Standard (AES), which was created to secure sensitive information and became a standard due to its robustness and efficiency. Understanding AES's purpose and development process will provide valuable insights into designing a strong algorithm. Next, explore algorithms that utilize prime numbers, such as the RSA algorithm, to understand how prime numbers are employed in encryption and decryption processes. This analysis will help identify the role of prime numbers and their potential application in the new algorithm.

B: Creating Connections

In the research, the Chebyshev PSI function was tested to find connections between it and the Prime Counting function suitable for algorithm design. In the code, the Chebyshev PSI and the Prime Counting function were tested together on 10 different intervals: (0, 100), (0, 200), (0, 300), and onwards, and the results showed that the answers differed by approximately 0.06, allowing for them to be used interchangeably in this research due to their small difference. It was found that as the number of primes increased over intervals on the number line, prime density also increased.

C: Testing

An algorithm was created and then tested to check the efficiency of the Prime Counting function in comparison to the Chebyshev PSI function via a simple brute-force method. Then, an algorithm was written to take interval values and extract prime numbers, substituting them into the RSA algorithm to determine the results.

The code for the Sieve and Chebyshev PSI functions are written below:

```
function sieveOfEratosthenes(limit) {
  var sieve = [];
  for (var i = 0; i <= limit; i++) {
    sieve.push(true); // Initialize all elements to true
  }

  for (var p = 2; p * p <= limit; p++) {
    if (sieve[p]) {
      for (var i = p * p; i <= limit; i += p) {
        sieve[i] = false;
      }
    }
  }
  var primes = [];
  for (var i = 2; i <= limit; i++) {
    if (sieve[i]) {
      primes.push(i);
    }
  }

  return primes;
}
```

```
// Function to calculate Chebyshev psi function
function chebyshevPsi(x) {
    var primes = sieveOfEratosthenes(x);
    var psi = 0;
    for (var i = 0; i < primes.length; i++) {
        psi += Math.log(primes[i]);
    }
    return psi;
}
```

1.4 Results

When exploring the application of the Riemann Zeta function in cryptography, several key findings arose. The findings were that there was a connection between the Chebyshev PSI function and the Prime Counting function and that they could be utilized to create a cryptographic algorithm that evaluated prime density. Because of the way RSA utilizes primes, using large prime numbers on an interval can help create longer encryptions of words that can be harder to decipher due to their size, since the difficulty of factoring large primes is the theoretical basis of RSA. The Chebyshev PSI function was used to find intervals with high prime density. Then the Sieve of Eratosthenes was used to find the specific prime numbers on those intervals. These primes were then used within the RSA algorithm to generate the encryptions, which would then be decrypted by the receiver of the message. This was an application of the Riemann Zeta function as it utilized conclusions of the Riemann hypothesis and the Prime counting function and drew similarities to the Chebyshev PSI function, which was then used to create a cryptographic algorithm to generate prime numbers over an interval.

```
Prime Interval with High Density: [1009, 1013, 1019, 1021, 1031, 1033, 1039, 10

Public Key: (317, 155779)
Private Key: (79373, 155779)

Original Message: This is a message encrypted using the Riemann Zeta function.

Encrypted Message: [131810, 128279, 141977, 138613, 142882, 102719, 140996, 135

Decrypted Message: This is a message encrypted using the Riemann Zeta function.
```

Figure 1: Example usage of the RSA algorithm in tandem with the Zeta function

This is an example of the running of code over the interval [1000, 1500]. The function takes all of the prime numbers over the interval and uses them to encrypt a message. Once encrypted, it is decrypted using the private key of the receiver, displaying the original message.

1.5 Discussion

Based on the results section, this application of the Riemann Zeta function lends itself to encrypting messages and sending them to others who can decrypt them using their own generated private key. As compared to other prominent algorithms for encryption and decryption, this algorithm may offer unique benefits due to the advanced security through its complexity. The algorithm primarily serves to be supplemental evidence for the Riemann hypothesis and demonstrates that the hypothesis can be applied with similar efficacy to traditional algorithms in cryptography.

1.6 Summary and Conclusions

The original goal of the project was to explore potential applications of the Riemann Zeta function within cryptography, a mathematical function that has not been extensively studied in this context. The project successfully identified a novel application of the Riemann Zeta function in enhancing cybersecurity protocols. Specifically, the function was utilized to develop a new encryption algorithm that significantly improves the security of digital communications by using the complex properties of the Zeta function to create better cryptographic keys. This breakthrough not only demonstrates the utility of advanced mathematical concepts in cybersecurity but also paves the way for further research and exploration in the field of cryptography. The findings suggest that incorporating the Riemann Zeta function into cryptographic frameworks can offer new methods for securing data, protecting against cyber threats, and ensuring the integrity and protection of sensitive information. This approach has the potential to revolutionize current cryptographic practices and inspire future advancements in discipline.

Works Cited

1. Durmagambetov, A. A. (2017, July 17). *Riemann hypothesis*. SCIRP. Retrieved from https://www.scirp.org/journal/paperinformation.aspx?paperid=77712
2. The encoding of the prime distribution by the Zeta Zeros (common approach). (n.d.). https://empslocal.ex.ac.uk/people/staff/mrwatkin/zeta/encoding1.htm#:~:text=the%20%22encoding%22%20of%20the%20distribution,Riemann%20zeta%20function%20%5Bcommon%20approach%5D&text=is%20the%20number%20of%20primes%20less%20than%20or%20equal%20to%20x.&text=This%20is%20a%20smooth%20function,interval%20%5B2%2Cx%5D
3. Encyclopedia Britannica, inc. (2023, September 12). *Riemann Zeta function*. Encyclopedia Britannica. https://www.britannica.com/science/Riemann-zeta-function
4. Meulens, R. (2019, October 24).
5. *The proof of the Riemann hypothesis and an application to physics*. SCIRP. https://www.scirp.org/journal/paperinformation.aspx?paperid=96475
6. *Prime number theorem*. from Wolfram MathWorld. (n.d.-a). https://mathworld.wolfram.com/PrimeNumberTheorem.html
7. *Zeta function*. from Wolfram MathWorld. (n.d.-b). https://mathworld.wolfram.com/ZetaFunction.htm