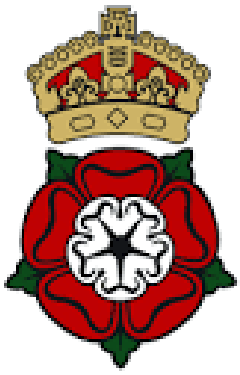
The implications of Prime numbers and the Riemann hypothesis on Asymmetric Cryptography



Royal Grammar School, Guildford

5th form Transitional Research Project
June 30, 2020
Ishan Nathan

Abstract

The academic study of prime numbers has been of mathematical interest for centuries and over time remarkable progress has been made in understanding the unique properties and patterns of these numbers. Over the last fifty years, the discovery of mathematical models has aided the progression of computer science. Whilst encryption, previously used for communication in the wars, has now been adopted into quotidian life. Mathematicians have discovered new methods for the secure transmission of information and have augmented them by introducing new messaging platforms using encryption algorithms based on prime numbers. In this dissertation, the importance of prime numbers and their application to asymmetric cryptographic systems will be outlined. Furthermore, it will be shown how effective modern-day public-key cryptographic systems are, based on a coded model of the RSA algorithm. Moreover, it will be evident why the Riemann Hypothesis could encode the best possible prediction of the distribution of primes to a high degree of accuracy and how it can have significant implications on modern-day cryptographic systems.

I Introduction

It is widely accepted that Prime numbers are important in the field of number theory as they act as the "atoms of arithmetic" [11]. Mathematicians first studied primes explicitly in 300BC in Ancient Greek Mathematics, where Euclid proved that there was an infinitude of primes [20]. Since then the understanding of primes has developed and the characteristics of primes enable it to have profound applications in security codes, blockchain analysis, cicada's cycles, and Cryptography. Nevertheless, mathematicians do not understand the primes fully, due to their enigmatic behaviour whereby they appear to act randomly despite having some aspects of their behaviour which are predictable.

In this dissertation, the pathway to understanding the profound impact of prime numbers on the modern world will journey through why the properties of primes make these numbers so special. Then to see how prime numbers are implemented into modern-day cryptographic systems, in a model code of the RSA algorithm. The Riemann zeta function will then develop from a simple Dirichlet series to a complex function encoding deep connections to the distribution of prime numbers [14]. Once it is clear why the million-pound conjecture of the Riemann Hypothesis could conceal the best possible estimation of the distribution of primes up to a given value, it is necessary to consider why some mathematicians and computer scientists believe that proof or disproof of this supposition could have significant implications on public-key cryptosystems.

II Prime numbers and why mathematicians are so interested in them

In the realm of natural numbers in number theory there are Prime numbers which are natural numbers greater than one, that are only divisible by exactly two numbers, one and itself. There are also composite numbers which are integers that are greater than one but are not prime. 1 is neither prime nor composite. According to the *Fundamental Theorem of Arithmetic* [16], any whole natural number greater than one can be written as a product of prime numbers. Hence, Prime numbers make up all composite numbers and they can be factorised into their constituent primes.

Example 1. *24 can be broken down into $2\times2\times2\times3$*

Prime numbers have been known to mathematicians since 1550BC, although the first documented evidence of them was in Euclid's Elements (300BC). Here Euclid proved the infinitude of prime numbers and the fundamental theorem of arithmetic [1].

Euclid's Proof for the infinitude of Prime numbers:

Lemma: *The number of primes is infinite*

To demonstrate Euclid's proof one must present an argument so that for any finite list of prime numbers, there is always at least one more prime number after it that is not included in the previous list [20].

Proof:

Proof by contradiction by acknowledging the fact that "every integer N>1 can be written uniquely as a product of finitely many prime numbers." [16]

> *Example 2.* $N = (2\times3\times5\times7\times11\times13)+1 = 30031$ *(where N is the product of the primes we know up to 15 plus one)*

If every natural number can be written as a product of prime numbers it means that N can be written as a product of prime numbers too. Yet if N is divided by any of the above primes (2,3,5,7,11,13) a remainder of one will occur. This means that there must be at least one new prime greater than thirteen that is not on our finite list. The prime factors of N (30031) are (59 and 509). Hence, there are two new primes that are not on the original list. A similar argument would also work for a larger or different set of finite primes to find at least one more prime - thus proving that there are infinitely many primes [20].

III Prime numbers application in Cryptography

Cryptography is the analysis of methods that will ensure the secure transmission of information. There are two main types of Cryptography, the first is a modern method using a public key whereby it allows secure communication despite the number of users being high. [21] The second is a classical method using a private key, whereby the number of users is on a small scale and it relies upon the users exchanging secret keys with everyone before the use of the communication system [10].

The emergence of the internet has led to a rapid increase in the number of online transactions taking place all over the internet on sites like eBay and Amazon. Due to this increase in demand for e-commerce, traditional passwords do not work because having a separate password for each purchase is unfeasible for the people involved and it is laborious to create these different passwords. Instead, modern-day cryptographic methods establish a mechanism for secure communication with a one-way form of communication.

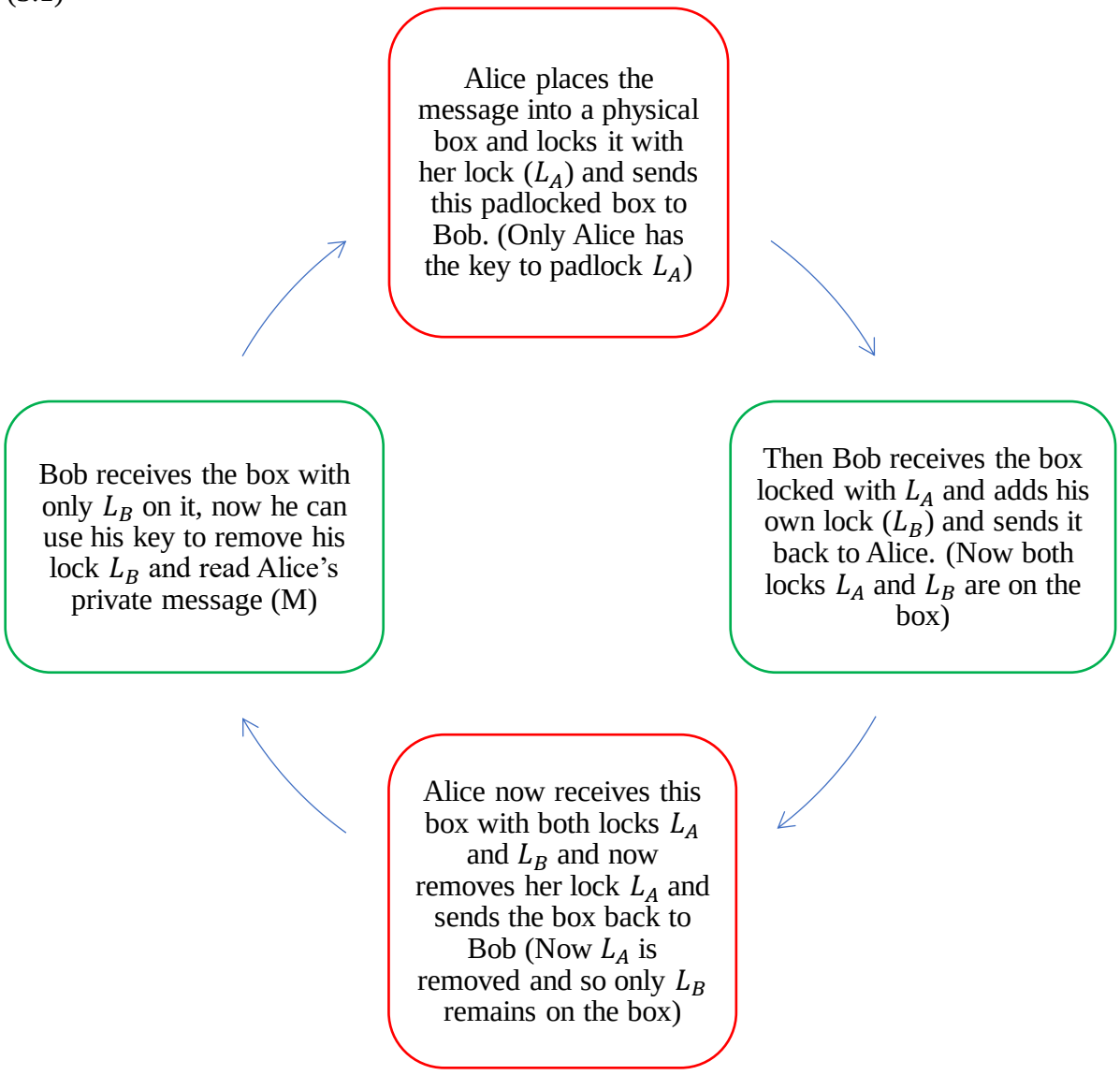
Modern-day cryptography relies upon prime numbers sporadic arrangement in the order of natural numbers. It is built upon the assumption that predicting the next prime number is near impossible due to primes sparsity and unpredictability. One of the most widely used applications of prime numbers in computing is the RSA encryption system developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 [9]. The algorithm enables the secure transmission of messages on online platforms whilst paving the way for e-commerce, protecting our sensitive information such as credit cards when shopping and in the global market place.

Modern public-key cryptography uses mathematical functions which are easy to compute in one direction, but hard to reverse. The process that is synonymous with public-key encryption is prime factorisation. The difficulty of this process is epitomised by Gauss' quote in 1801, "The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic" [7].

The asymmetric cryptosystem in RSA relies upon the difficulty of the prime factorisation because multiplying two primes (x, y) is a simple task and does not require a great deal of computational power to find that result (N). However, given that (N) is a large natural number it is arduous to find the two prime factors (x, y) as it requires much more processing power and could take many years to decrypt depending on the size of the integer [8].

To demonstrate the asymmetric cryptosystem used in the RSA algorithm analogically, here are two fictional characters Alice and Bob [9].

(3.1)



The analogy in (3.1) is implemented mathematically into the RSA algorithm where Alice can send a secret message to Bob using this form of cryptography. See Appendix A for the code in Python script replicating the RSA model.

Python Code results from Appendix A:

(3.2)

```
Alice, type in your message number = 23

Bob's random Prime number x = 9949
Bob's random Prime number y = 71879

Bob's number (N) by mulptiplying two random primes (x,y) = 715124171

ϕ(N) = 715042344

Public key = 257

Bob's Private key = 278226593

Bob sends N and the Public key to Alice

Encrypted message = 678444613

Alice sends the Encrypted message to Bob

Bob decrypts the message by using his Private key

Alice's Decrypted Message = 23
```

IV Riemann Hypothesis

The Riemann Hypothesis is widely accepted as one of the biggest mathematical unproven conjectures of our millennium. It is argued that the Riemann Hypothesis predicts the distribution of the primes and their enigmatic behaviour better than any other theorem and is as good as it gets, provided the truth of it [2].

The Riemann Hypothesis is defined as "The nontrivial zeros of $\zeta(s)$ have real part equal to $\frac{1}{2}$"[18].

The theory concerns itself with the zero values of the Riemann zeta function. It states that the Riemann zeta function has its trivial zeros at only negative even integers (-2, -4, -6, -8…) and its non-trivial zeros only on the critical line in the critical strip between the imaginary axis and the real part of one [15]. Mathematicians are concerned with the zeros of the Riemann zeta function because a zero of a function is a value that you can input into the function and get a zero to output.

The Zeta function was introduced by Leonhard Euler as a function of natural numbers where $s>1$, defined by the equation:

(4.1)

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

Hence Zeta (2) would be:

(4.2)

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots$$

From (4.2) one can see that $\zeta(2)$ is the infinite sum of the squares of the reciprocal of the counting numbers. However, Bernhard Riemann considered using *s* as a complex variable

instead of a natural integer greater than one [4]. The Riemann zeta function uses the complex variable s where $s=x+iy$ (s is, a complex variable satisfied by the values of x along the x-axis, $i=\sqrt{-1}$ and y-values along the y-axis) [14].

(4.3)

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

From (4.3) it is evident that the zeta function can be written as a sum of the integers [12]. However, Riemann realised that the Riemann zeta function is intrinsically connected to prime numbers because the Riemann zeta function for the complex variable s can be rewritten as a product over the prime numbers in the Euler Pi Prime product formula (4.4).

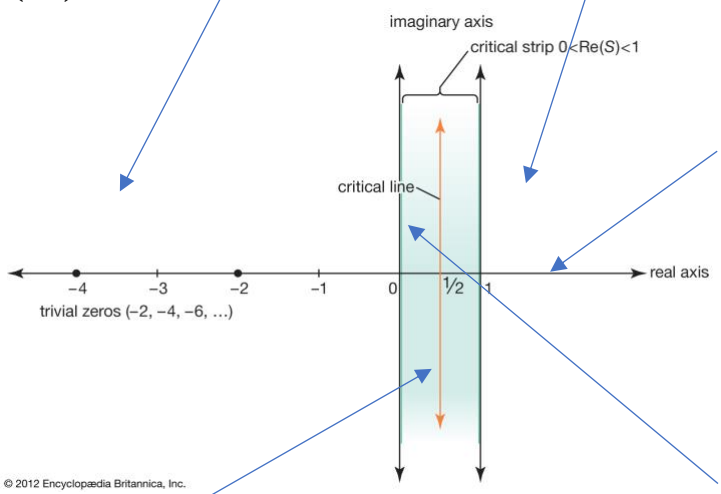
(4.4)

$$\zeta(s) = \left(\frac{1}{1-\frac{1}{2^s}}\right) \times \left(\frac{1}{1-\frac{1}{3^s}}\right) \times \left(\frac{1}{1-\frac{1}{5^s}}\right) \times \left(\frac{1}{1-\frac{1}{7^s}}\right) \times \left(\frac{1}{1-\frac{1}{11^s}}\right) \times \ldots$$

As the Riemann zeta function can be rewritten as a product over the primes (4.4) it means that the Riemann zeta function encodes information about the primes, as it contains all the primes in its denominator. Thus, if you work out how the information in the Riemann zeta function is encoded you can work out the patterns of the primes.

The formula in (4.4) works for all values where (x>1) in the region to the right of the critical strip and when (x<1) for all values to the left of the critical strip.

(4.5)



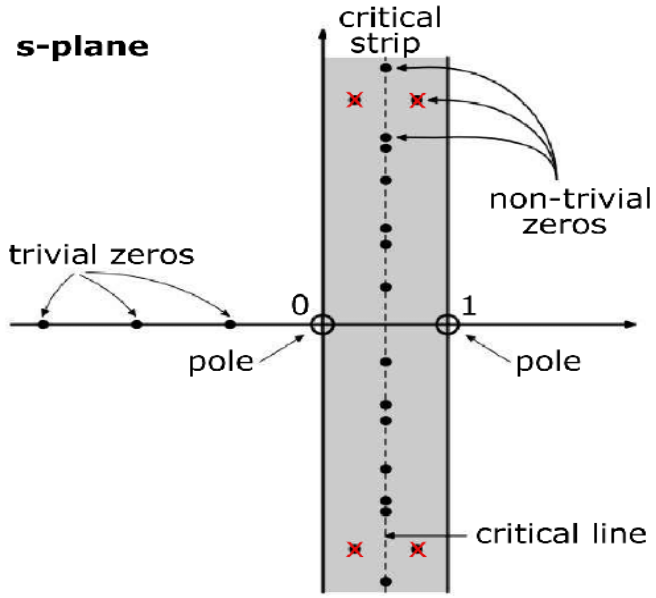
The complex plane in (4.5) is a two-dimensional number plane.

Real part (2,3,4…) where for all complex values for real part greater than one it converges. It can be asserted that from Euler's pi product formula of zeta, zeta cannot be zero in the real part area where s>1 because this area is convergent and so it can only be zero if one of its factors is zero too [13].

Imaginary axis (20i, 30i…)

The orange line is the line of symmetry of the Riemann zeta function. This means that if there is known point in the region of (x>1), then that point can be reflected across the symmetry line to find its corresponding value in the region where (x<1) [13]. It is this symmetry line where the Riemann hypothesis states that all zero values other than the trivial ones are believed to lie.

(4.6)



There are trivial zero values at all negative even integers e.g.($\zeta(-4) = 0$)

There are infinitely many zero values within the critical strip where these nontrivial zero values satisfy the complex variable $s=x + iy$. Although, the Riemann Hypothesis states that they all lie upon this critical line in the critical strip at the x-value $\frac{1}{2}$. Calculations have yielded that the hypothesis has stood true for all values of y less than ten trillion and that there is not a misbehaving zero-value found outside the critical line.

V The implications of the Riemann Hypothesis on Cryptography

One could assert that an abstract proof of the Riemann Hypothesis could threaten modern-day cryptographic systems. This is because proof of this theory would improve mathematicians' understanding of prime factorisation, providing the insight and proficiency required to crack these RSA codes [17]. A proof of the Riemann Hypothesis would not necessarily explicitly inform mathematicians' how to construct a prime factorisation method that could threaten the security of the RSA algorithm, albeit it could provide a theoretical insight into how efficient an algorithm could run. Thus, if the Riemann hypothesis is proven to be true then it would most probably be due to the proof of a certain algebraic or symmetrical construct that is connected to prime numbers, but is not fully comprehended yet by modern mathematicians'.

Conversely, it has been argued that if the Riemann Hypothesis is deemed to be false, presuming that, there is a zero value that lies outside of the critical line of the Riemann zeta function. It could denote that the distribution of primes as is comprehended currently, could either have a different type of structure or rather, have more structure than first anticipated. By disproving the conjecture in this way, a result could be leveraged for cryptographical analysis of the RSA algorithm. In contempt of this, a disproof of the supposition would not have a first-hand impact on the asymmetric cryptosystem in RSA. Alternatively, by analysing the reasons for the failure of the Riemann hypothesis, mathematicians could be provided with the valuable information needed to expose vulnerabilities in the RSA security system.

Therefore, it is not that by proving or disproving the Riemann Hypothesis mathematicians could lead to a breakthrough against the RSA algorithm. Instead, it is that the methodology leading to a proof or disproof of this conjecture may lead to a discovery about the prime numbers that could make prime factorisation less computer-intensive, posing a potential breach to the RSA security method [17]. If mathematicians ever do prove or disprove the Riemann Hypothesis, it would lead to reconsiderations in many theoretical algorithms in number theory and computer science, especially those concerned with cryptography.

VI Conclusions

In conclusion, prime numbers application to modern-day life is not always apparent, as is their properties and patterns. Yet prime numbers play a fundamental part in our lives and act as a cornerstone for both: day to day messaging on encrypted platforms such as WhatsApp, and for consumers' online e-commerce activities. Modern-day cryptographic systems rely upon the quick speed for performing operations to determine large primes, and the computer-intensive reverse process in factorising large integers, in turn assuring the security of public-key cryptography. It is this high level of encryption that ensures the world of e-commerce to function. Yet what if there was a way to overcome this? An abstract proof of the Riemann Hypothesis will undoubtedly enhance our understanding of primes and thus could lead to vulnerabilities within asymmetric cryptography. However, primes are special and they are like no other group of numbers. "317 is a prime, not because we think so, or because our minds are shaped in one way rather than another, but because it is so, because mathematical reality is built that way" [5]. Therefore, despite mathematicians limited understanding of these numbers, a secure online communication network across the world has been created; just imagine the possibilities that could unravel when understanding the true enigmatic behaviour of prime numbers.

Word Count (excluding Appendix A, references and bibliography): **2493**

Appendix A:

Below is the Python code which was written by the author, replicating the RSA encryption model. It takes a message from Alice and uses the steps of the RSA algorithm to create an encrypted message sent to Bob, for him to decrypt using his 'private key'. RSA-2048 and RSA-4096, normally used for encryption in the public domain uses two 1024-bit or two 2048-bit prime numbers respectively [3]. However, this model replicates an RSA-32 model using two 16-bit prime numbers, the size of the primes had to be scaled down due to the vast computer processing power required to generate a prime of size 2^{2048} in RSA-4096.

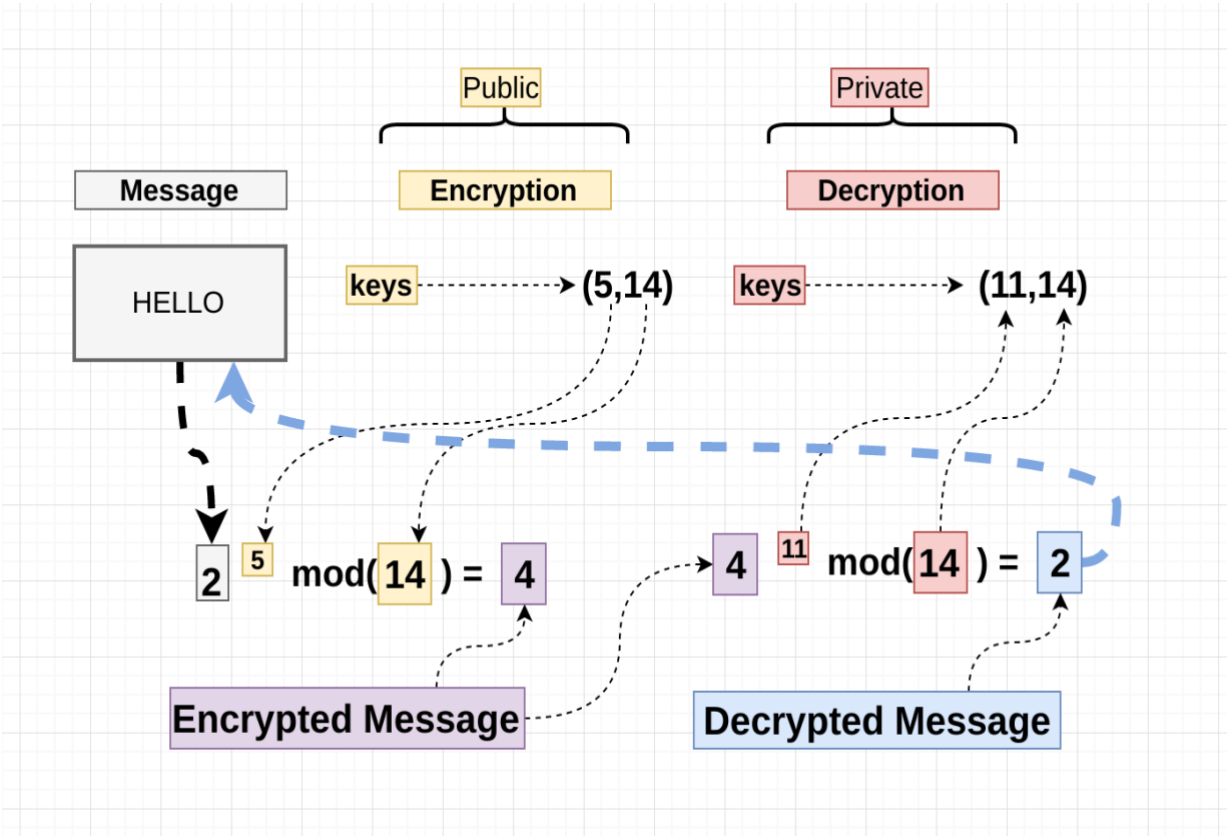
(A.1)

In [3]:

```
#RSA 1
#Ishan Nathan
#################################################################################################################################
#Alice
#Shecreates a message which is converted to a number using a padding system

message = int (input("Alice, type in your message number = "))

#Bob
#He generates 2 random prime numbers x and y

import random
lowerbound = 1    #lowerbound can be any integer
upperbound = 100000 #upperbound can be any integer

prime_numbers=0
listOfprime=[]

for num in range(lowerbound, upperbound + 1):
    if num > 1:
        for i in range(2, num):
            if (num % i) == 0:
                break
        else:
            prime_numbers += 1
            listOfprime.append(num)

#Choosing 2 random prime numbers between lowebound and upperbound to use as x and y for Bob

randomX = random.choice(listOfprime)
randomY = random.choice(listOfprime)

print ("\n" + "Bob's random Prime number x = " + str(randomX))
print ("Bob's random Prime number y = " + str(randomY)+ "\n")

#Calculate large natural composite number N by multiplying Bob's two primes x and y
#This is because multiplication is easy
#But finding the prime factors of a large Natural commposite number is very difficult

N = randomX * randomY
print("Bob's number (N) by mulptiplying two random primes (x,y) = " + str(N)+"\n")

#Euler totient function (Phi (ϕ) function)- measures the factorisation of a certain number
#Fiding the Phi function of a prime number is simple because primes have factors of only 1 and itself
#Phi(ϕ) function of a prime number = Prime number - 1
#Phi function is multiplicative
#If we know that N is a large natural composite number and the primes x and y multiply to form it
#PhiN = (x-1) * (y-1)

PhiN=(randomX-1)*(randomY-1)
print("ϕ(N) = "+ str(PhiN)+"\n")

#Generate e - the public key - an integer that is relatively prime or coprime to PhiN
#Relatively prime or coprime means does not share a common factor - e must not share a common factor with PhiN

publicKeyList=[3,5,17,257,65537]
e = random.choice(publicKeyList)
print("Public key = " + str(e)+"\n")

#private key - d
#Calculate the modular inverse of e - the inverse will be called d

d = 0
while d < PhiN:
    if (e * d)% PhiN == 1:
        break
    d = d+1
print("Bob's Private key = " + str(d) + "\n")

#Bob send N and e to Alice
print("Bob sends N and the Public key to Alice" + "\n")

#Alice

#Using discrete logarithms Alice can generate an encrypted message r
#Alice uses the formula m^e mod N = r
#pow function takes 'message' as the base, 'e' as the exponent to the 'modulus of N' to give the 'r' the remainder

r= pow (message, e, N)
print("Encrypted message = "+ str(r) + "\n")

#Alice sends the encrypted message r(remainder) back to Bob
print("Alice sends the Encrypted message to Bob" + "\n")

#Bob
#Using discrete logarithms Bob can now decipher Alice's encrypted message
#Bob decrypts the message by using his "Private key" d using the formula
#r^d mod N = m
print("Bob decrypts the message by using his Private key" + "\n")
#pow function takes 'r' as the base, 'd' as the exponent to the 'modulus of N' to give the 'm' the decrypted message

decryptedMessage = pow(r, d, N)
print ("Alice's Decrypted Message = "+ str(decryptedMessage))

#################################################################################################################################
#If anyone had encrypted message, N or public Key. They would be unable to work out the message without private key
#They can only calculate the private key (d) if they work out PhiN which require great computational power
#This is because they do not know the prime factorisation of N
#Therefore, the message is encrypted unless they found the prime fatorisation of a large 300 digit integer
#This could require hundreds of years of computational power using current technology and understanding
```

```
Alice, type in your message number = 23

Bob's random Prime number x = 9949
Bob's random Prime number y = 71879

Bob's number (N) by mulptiplying two random primes (x,y) = 715124171

ϕ(N) = 715042344

Public key = 257

Bob's Private key = 278226593

Bob sends N and the Public key to Alice

Encrypted message = 678444613

Alice sends the Encrypted message to Bob

Bob decrypts the message by using his Private key

Alice's Decrypted Message = 23
```

(A.2)



In the Python code and in (A.2), the RSA system works by converting the message from Alice to the number 2 using a padding system [9]. Bob then generates two large random prime numbers 2,7 and multiplies them to get a result 14 (in the figure above). The number 14 is the modulus used for the RSA algorithm. Using the Euler totient function Bob works out Phi (ϕ) of this result where the Phi function measures the factorisation of a certain number, by calculating the number of numbers below 14 that are coprime to 14 [19]. After this, Bob generates two keys, the first is a public key. This is a number that does not share a factor with Phi (14), it can either be (2,5,17,257,65537) [6]; in (A.2) the public key is (5mod14). The second key is the private key which is concerned with the multiplicative inverse of the public key modulo ϕ(N). Bob sends 14 and the public key 5 to Alice. Using the equation in (A.2) she creates an encrypted message number 4. Following this process, Alice sends the encrypted message back to Bob, where Bob can now decrypt her encrypted message, using his private key, to get the original message number 2.

References

[1] Ash, J. M., & Peterson, T. K. (n.d.). Many proofs that the primes are infinite. Retrieved 20-5-18, from https://math.depaul.edu/tpeter21/ManyPrimeProofs.pdf

[2] Borwein, P., Choi, S., Rooney, B., & Weirathmueller, A. (2006, August 18). The Riemann Hypothesis for the aficionado and virtuoso alike. *Springer* . Retrieved May 27, 2020, from https://bbs.pku.edu.cn/attach/8d/89/8d895d221266d1cd/book.pdf

[3] Buchanan, B. (2019, May 8). So How Many Bits Does The Prime Number Have? *Medium*. Retrieved May 30, 2020, from https://medium.com/asecuritysite-when-bob-met-alice/so-how-many-bits-does-the-prime-number-have-e5dbbdf568ea

[4] Erickson, C. (n.d.). Prime numbers and the Riemann Hypothesis. Retrieved May 30, 2020, from http://www.math.pitt.edu/~caw203/pdfs/primes_and_riemann.pdf

[5] Hardy, G. H. (1992). *A Mathematician's Apology* (pp. 38–39). New York: Cambridge University Press.

[6] Ireland, D. (n.d.). RSA Algorithm. *DI Management Services Pty Limited*. Retrieved May 30, 2020, from https://www.di-mgt.com.au/rsa_alg.html#note2

[7] Ribenboim, P. (2012). *The Book of Prime Number Records* (p. 13). Springer Science & Business Media.

[8] Riesel, H. (1994). Prime Numbers and Cryptography, 226–238. Retrieved May 30, 2020, from 10.1007/978-1-4612-0251-6_7

[9] Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Retrieved May 30, 2020, from https://people.csail.mit.edu/rivest/Rsapaper.pdf

[10] Rouse, M., Brush, K., Rosencrance, L., & Cobb, M. (2020, March 20). What Is Asymmetric Cryptography And How Does It Work? *SearchSecurity*. Retrieved May 30, 2020, from https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

[11] Sautoy, M. du. (2012). *The Music of the Primes: Why an unsolved problem in mathematics matters (Text Only)* (p. 19,23). HarperCollins UK.

[12] Sondow, J. (1994). Analytic continuation of Riemann's Zeta function and values at negative integers via Euler's transformation of series. *American Mathematical Society* . Retrieved 20-5-27, from https://www.ams.org/journals/proc/1994-120-02/S0002-9939-1994-1172954-7/S0002-9939-1994-1172954-7.pdf

[13] Spira, R. (1965). Zero-Free Regions of ζ(k)(s). *Journal of the London Mathematical Society*, *40*(1), 677–682. Retrieved May 30, 2020, from 10.1112/jlms/s1-40.1.677

[14] Veisdal, J. (2020, April 14). The Riemann Hypothesis, Explained. *Medium* . Retrieved May 27, 2020, from https://medium.com/cantors-paradise/the-riemann-hypothesis-explained-fa01c1f75d3f

[15] Weisstein, E. (n.d.). Riemann Zeta Function Zeros -- From Wolfram MathWorld. *Wolfram Research* . Retrieved 20-5-28, from https://mathworld.wolfram.com/RiemannZetaFunctionZeros.html

[16] Weisstein, E. (n.d.). Fundamental Theorem Of Arithmetic -- From Wolfram MathWorld Resource. *Wolfram Research* . Retrieved 20-5-18, from https://mathworld.wolfram.com/FundamentalTheoremofArithmetic.html

[17] (2012, November 28). Reimann Hypothesis And Its Connection To Cryptography. *PERPETUAL ENIGMA* . Retrieved May 22, 2020, from https://prateekvjoshi.com/2012/11/28/reimann-hypothesis-and-its-connection-to-cryptography/

[18] (n.d.). Riemann Hypothesis | Clay Mathematics Institute. Retrieved 20-5-20, from https://www.claymath.org/millennium-problems/riemann-hypothesis

[19] (n.d.). 3.8 The Euler Phi Function. Retrieved May 30, 2020b, from https://www.whitman.edu/mathematics/higher_math_online/section03.08.html

[20] (n.d.). Euclid's Proof Of The Infinitude Of Primes (c. 300 BC). Retrieved May 7, 2020e, from https://primes.utm.edu/notes/proofs/infinite/euclids.html

[21] (n.d.). Modern Cryptography - Tutorialspoint. Retrieved May 31, 2020g, from https://www.tutorialspoint.com/cryptography/modern_cryptography.htm

Bibliography

Ash, J. M., & Peterson, T. K. (n.d.). Many proofs that the primes are infinite. Retrieved 20-5-18, from https://math.depaul.edu/tpeter21/ManyPrimeProofs.pdf

Borwein, P., Choi, S., Rooney, B., & Weirathmueller, A. (2006, August 18). The Riemann Hypothesis for the aficionado and virtuoso alike. *Springer* . Retrieved May 27, 2020, from https://bbs.pku.edu.cn/attach/8d/89/8d895d221266d1cd/book.pdf

Britannica, E. (n.d.). Riemann Zeta Function. *Encyclopedia Britannica*. Retrieved 20-5-28, from https://www.britannica.com/science/Riemann-zeta-function

Buchanan, B. (2019, May 8). So How Many Bits Does The Prime Number Have? *Medium*. Retrieved May 30, 2020, from https://medium.com/asecuritysite-when-bob-met-alice/so-how-many-bits-does-the-prime-number-have-e5dbbdf568ea

Davenport, H. (2008). *The Higher Arithmetic* (8th ed., pp. 1-25,165-200). Cambridge University Press. Retrieved from https://www.academia.edu/9891358/THE_HIGHER_ARITHMETIC_AN_INTRODUCTION_TO_THE_THEORY_OF_NUMBERS_Eighth_edition

Erickson, C. (n.d.). Prime numbers and the Riemann Hypothesis. Retrieved May 30, 2020, from http://www.math.pitt.edu/~caw203/pdfs/primes_and_riemann.pdf

Hardy, G. H. (1992). *A Mathematician's Apology* (pp. 38–39). New York: Cambridge University Press.

Hartnett, K. (2020, May 14). Big Question About Primes Proved In Small Number Systems | Quanta Magazine. *Quanta Magazine* . Retrieved May 25, 2020, from https://www.quantamagazine.org/big-question-about-primes-proved-in-small-number-systems-20190926/

Ireland, D. (n.d.). RSA Algorithm. *DI Management Services Pty Limited*. Retrieved May 30, 2020, from https://www.di-mgt.com.au/rsa_alg.html#note2

Jarvis, F. (2014). *Algebraic Number Theory* (p. 207). Springer.

Parker, M. (2014). *Things to Make and Do in the Fourth Dimension* (pp. 130–154). Penguin UK.

Rabah, K. (2006). Review of Methods for Integer Factorization Applied to Cryptography. *Journal of Applied Sciences* . Retrieved from https://scialert.net/abstract/?doi=jas.2006.458.481

Ribenboim, P. (2012). *The Book of Prime Number Records* (p. 13). Springer Science & Business Media.

Riesel, H. (1994). Prime Numbers and Cryptography, 226–238. Retrieved May 30, 2020, from 10.1007/978-1-4612-0251-6_7

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Retrieved May 30, 2020, from https://people.csail.mit.edu/rivest/Rsapaper.pdf

Rouse, M., Brush, K., Rosencrance, L., & Cobb, M. (2020, March 20). What Is Asymmetric Cryptography And How Does It Work? *SearchSecurity*. Retrieved May 30, 2020, from https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

Sautoy, M. du. (2012). *The Music of the Primes: Why an unsolved problem in mathematics matters (Text Only)* (p. 19,23). HarperCollins UK.

Sondow, J. (1994). Analytic continuation of Riemann's Zeta function and values at negative integers via Euler's transformation of series. *American Mathematical Society* . Retrieved 20-5-27, from https://www.ams.org/journals/proc/1994-120-02/S0002-9939-1994-1172954-7/S0002-9939-1994-1172954-7.pdf

Spira, R. (1965). Zero-Free Regions of ζ(k)(s). *Journal of the London Mathematical Society*, *40*(1), 677–682. Retrieved May 30, 2020, from 10.1112/jlms/s1-40.1.677

Spira, R. (1970). Another zero-free region for $\zeta \sp{(k)}\,(s)$. *Proc. Amer. Math. Soc.*, *26*(2), 246–246. Retrieved May 30, 2020, from 10.1090/s0002-9939-1970-0263754-4

Spira, R. (1973). Zeros of $\zeta^{\prime} (s)$ and the Riemann hypothesis. *Illinois J. Math.*, *17*(1), 147–152. Retrieved May 30, 2020, from 10.1215/ijm/1256052045

Veisdal, J. (2020, April 14). The Riemann Hypothesis, Explained. *Medium* . Retrieved May 27, 2020, from https://medium.com/cantors-paradise/the-riemann-hypothesis-explained-fa01c1f75d3f

Weisstein, E. (n.d.). Riemann Zeta Function Zeros -- From Wolfram MathWorld. *Wolfram Research* . Retrieved 20-5-28, from https://mathworld.wolfram.com/RiemannZetaFunctionZeros.html

Weisstein, E. (n.d.). Fundamental Theorem Of Arithmetic -- From Wolfram MathWorld Resource. *Wolfram Research* . Retrieved 20-5-18, from https://mathworld.wolfram.com/FundamentalTheoremofArithmetic.html

Zudilin, W. (n.d.). Millennium Prize: The Riemann Hypothesis. *The Conversation* . Retrieved 20-5-18, from https://theconversation.com/millennium-prize-the-riemann-hypothesis-3847

(2012, November 28). Reimann Hypothesis And Its Connection To Cryptography. *PERPETUAL ENIGMA* . Retrieved May 22, 2020, from https://prateekvjoshi.com/2012/11/28/reimann-hypothesis-and-its-connection-to-cryptography/

(n.d.). Riemann Hypothesis | Clay Mathematics Institute. Retrieved 20-5-20, from https://www.claymath.org/millennium-problems/riemann-hypothesis

(n.d.). 3.8 The Euler Phi Function. Retrieved May 30, 2020b, from https://www.whitman.edu/mathematics/higher_math_online/section03.08.html

(n.d.). How Many Primes Are There? Retrieved 20-5-18, from https://primes.utm.edu/howmany.html

(n.d.). Goldbach's Proof Of The Infinitude Of Primes (1730). Retrieved 20-5-23, from https://primes.utm.edu/notes/proofs/infinite/goldbach.html

(n.d.). Euclid's Proof Of The Infinitude Of Primes (c. 300 BC). Retrieved May 7, 2020e, from https://primes.utm.edu/notes/proofs/infinite/euclids.html

(n.d.). RSA Encrypt / Decrypt - Examples. Retrieved May 30, 2020f, from https://cryptobook.nakov.com/asymmetric-key-ciphers/rsa-encrypt-decrypt-examples

(n.d.). Modern Cryptography - Tutorialspoint. Retrieved May 31, 2020g, from https://www.tutorialspoint.com/cryptography/modern_cryptography.htm