ISSN – 2277-7911
Impact Factor – 5.519

YOUNG RESEARCHER
A Multidisciplinary Peer-Reviewed Refereed Research Journal

July-Aug-Sept 2024
Vol. 13 No. 3

A Comprehensive Study On The Evolution Of Cryptographic Algorithms Using Principles Of Number Theory

Dixit[1] & Dr. Bhawana[2]

[1]*Research Scholar, Department of Mathematics,*
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India
[2]*Assistant Professor and Research Guide, Department of Mathematics,*
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India

Corresponding Author: Dixit

DOI - 10.5281/zenodo.15811326

ABSTRACT:

Cryptography, which comes from the Greek word for "hidden writing," is a method of protecting information by rendering it unreadable through the application of mathematical procedures. The scientific study of cryptography began approximately one hundred years ago, but its development accelerated with the birth of the information age in the early 1900s. Therefore, cryptography is considered to be a relatively modern field of study. The field of cryptography has progressed from simple methods of information protection to sophisticated systems that make use of number theory to protect data for billions of people all over the world. Cryptography is built on mathematical principles such as modular arithmetic, the Euclidean algorithm, and Euler's totient function. These are the fundamental building blocks of cryptography. This article examines the development of cryptography, beginning with the first methods of information concealment, such as simple letter shifts, and on to the most recent algorithms, which are founded on advanced number theory. The study demonstrates how early cryptographic approaches paved the way for present encryption techniques by analyzing historical practices as well as practices that are now in use. Throughout the course of its development, cryptography has demonstrated its indispensable function in the protection of data in the modern digital age.

Keywords: Modular Arithmetic, Cryptography, Number Theory, Encryption, Decryption

INTRODUCTION:

The word "cryptography" comes from the Greek language and in a general sense may be translated as "hidden writing." A procedure that involves concealing information via the use of a variety of mathematical methods in order to display the information in a manner that cannot be read is known as cryptography. As some of the oldest examples of the secret code writing known as cryptography, many historians refer to the usage of encrypted clay tablets and hieroglyphics in Mesopotamia around the year 1500 B.C. and in Egypt around the year 1900 B.C.E. (Kessler & Phillips, 2020). The current study of cryptography has developed into a subfield of computer science that use mathematical functions, more especially number theory, to encrypt information in such a way that it cannot be recognized by anyone who are not allowed to access it. The encryption and decryption processes are typically the two stages that make up this procedure. This process takes text that can be read, sometimes known as plain text, and converts it into a string of letters that cannot be comprehended by the human tongue. Encryption is the procedure that is used to construct this string of characters that cannot be recognized, and the ciphertext is the name given to this string of characters. The purpose of this is to ensure that the information is sent in a manner that only the person who is supposed to receive it can read it. Decryption is the process of converting the information that has been encrypted back into the format that it was originally stored in. This technique of encryption and decryption has been used as a means of protecting all of our data; it offers assistance in encrypting financial information, as well as online transactions, purchases made with credit card electronic chips, and other financial transactions.

The fact that private information is being sent across a public network, which is referred to as the internet, in order to reach the intended recipient, such as the bank, is one of the most significant risks associated with the business transactions and data exchanges that take place online. The need of ensuring the safety of this information resulted in the development of secure methods to conceal essential information via the use of number theory. According to Ghosal (2021), "Number theory is probably one of the most important areas of mathematics used in Computer Science and the basics behind all of modern Cryptography" (p.35). This statement was made by Ghosal about the importance of number theory. Both the Caesar cipher and the Vigenere cipher are examples of some of the oldest and most well-known systems of encryption that made use of simple number theory. of order to encrypt a message, these ciphers required the letters of the alphabet to be used in a certain order. These techniques were first developed as a means of concealing information; as a result of the development of number theory, these methods shifted from being straightforward shift ciphers to becoming block ciphers, in which data is encrypted in blocks by using a key similar to the Rivest–Shamir–Adleman (RSA) cipher. This article analyzes the link between the first forms of information concealment, which occurred before cryptography was founded as an official subject of study, and the RSA cryptographic technique, which employs sophisticated number theory to protect information. Specifically, the work focuses on the correlation between the two. One of the most significant distinctions between the early types of information concealing and its contemporary successors is the quantity of data that is being encrypted between the two. The Caesar and Vigenere ciphers had a use rate that was far lower than the RSA technique, which was established in the late 1900s and has since become a method for encrypting the data of millions of individuals. These three ways of information concealment have similarities in the ideas of encryption and decryption, and they all have weaknesses in the encryption methods owing to flaws in the number theory that was used to build them. Although the quantity of data that is being protected by each of these methods varies, they all share similarities in the concepts of encryption and decryption.

UNDERSTANDING CRYPTOGRAPHY: ENCRYPTION AND DECRYPTION:

The field of mathematics known as number theory is dedicated to the study of positive integers. These numbers may be expressed as the set of natural numbers denoted by the symbol ℕ, where ℕ is a set consisting of the numbers 0 through 3. There are two sets of numbers that are combined to form integers. These sets contain the values of prime and composite numbers, which are employed to establish the basis for cryptography in the RSA method. Integers are a mixture of these two sets of numbers. One way to define prime numbers is as a number that is bigger than one and has two factors: the number itself and the number itself. A number is considered to be composite if it is a multiple of at least two numbers other than one and itself. This definition applies to composite numbers. Number theory is a branch of mathematics that investigates discrete sets of numbers, such as integers ℕ, which contains the sets of numbers that are being studied in this article. Some of the most fundamental applications of number theory are associated with fundamental mathematical concepts like divisibility and modular arithmetic. These concepts are employed to provide the groundwork for some of the oldest kinds of encryption. One example of an early kind of cryptography that made use of these fundamental mathematical concepts is the Caesar cipher. According to Samaila and Pur (2013), "An example of such a cipher is the Caesar cipher; named after Julius Caesar, who reportedly used it to encrypt information during the Gallic Wars by shifting each letter in the message three positions to the right" (p.27). This cipher is named after Julius Caesar. In the case of the Caesar cipher, which is an example of a shift or substitution cipher, the data is encrypted by replacing the letters that were originally included in the message with a predetermined amount of characters that are located farther forward in the alphabet. In the case of the Caesar cipher, the shift that was selected was three characters forward in the alphabet. This cipher is an excellent illustration of how mathematics may be used in an effort to achieve the goal of protecting sensitive information. For the sake of this example, let us assume that the plaintext that has to be encrypted the phrase "CIPHER." The cipher was designed to function properly. A representation of the transformation or replacement may be made using the two different sets of alphabets. One of them is the English alphabet, which is referred to as "Plaintext," and the other is the encrypted alphabet, which is referred to as "Encrypted." In the encrypted alphabet, the English alphabet is moved forward three places. The beginning word "CIPHER" would be encrypted to become "FLSKHU" in this particular particular situation. This mathematical concept, which was based upon modular arithmetic, is followed by these processes for encryption and decoding in the Caesar cipher. The mathematical model for the Caesar cipher is described by the equation for encryption (Amanie, 2020, as mentioned in Ryabko & Fionov, 2004 and Victor, 2014). This model may be seen in (1).

$$c = (m + k) \bmod n \qquad (1)$$

In equation (1), the letter c represents the ciphertext, the letter m represents the location of a letter in the alphabet according to its numerical equivalent, the letter k represents the encryption key or the number of letters that have been pushed forward, and the letter n represents the size of the alphabet respectively. Using this information, we are able to describe the modular equation for the Caesar cipher, which can be found in (2). After that, we will proceed to provide an illustration of how the cipher is configured to function.

$$c = (m + k) \bmod 26 \quad (2)$$

where $m \in Z_{26}$

In this context, the value of m is equal to the numerical value of any of the 26 letters that make up the alphabet, and mod 26 is a representation of the 26 letters. As an example, the letter C appears in the word "CIPHER," which has a value of three since it is the third letter in the alphabet. The method of encryption that is used for the word "CIPHER." The modular equation for the Caesar cipher is c = m + 3 (mod 26), where the 3 represents the number of letters that have been moved to the right during the course of the encryption process. As a result, this demonstrates yet another illustration of how the cipher computes the encrypted word to produce 'FLSKHU'. The decryption equation (Amanie, 2020, as mentioned in Ryabko & Fionov, 2004 and Victor, 2014) defines the mathematical model for the Caesar cipher, which can be seen in (3). This definition is identical to the one used in the previous explanation.

$$m = (c - k) \bmod 26 \quad (3)$$

where $k \in Z_{26}$

For the purpose of shifting, encrypting, and decrypting a message, the Caesar cipher makes use of fundamental modular arithmetic and takes just a little amount of CPU resources. As a continuation, Caesar saw the alphabet to be a cycle, and the letter that comes after Z is the letter A (Samaila & Pur, 2013). Because of this, if the value of (c - k) is more than 26, modular arithmetic would cause the letters to return to the beginning of the alphabet. This is because there would be a remainder that is equal to the letter. This would cause the letters to return to their original position. Because there are only 26 letters in the English alphabet, the Caesar cipher became outdated over the course of time. This was due in part to their limited number of letters. Despite the fact that the shift number might be increased in order to make the process of decoding the message more difficult, the decryption procedure could be accomplished by using modular arithmetic concepts. However, after some time had passed, the technique that could be used to break the Caesar cipher was discovered. The Caesar cipher was used as a way of concealing information. In most cases, the term "cracking" the cipher refers to the process of decrypting any particular cipher with the help of a person who does not possess the information that is required to decrypt it. A technique that was used in the process of deciphering the encryption was referred to as frequency analysis. It has been stated by Kartha, R. S., and Paul, V. (2018) that the approach known as frequency analysis is the most advanced method for the cryptanalysis of monoalphabetic ciphers It is based on the language that we utilized for encryption, which is characterized by the occurrence of certain letters and combinations of letters with widely varied frequencies" (p.125). In order to be able to forecast the ciphertext, frequency analysis is one method that is used to make predictions about the frequency of a certain letter inside the alphabet. As an example, the letter E is the most often used letter in the English language. Therefore, a hacker may utilize frequency analysis to establish a connection between the letter E and the text that they are attempting to interpret. The letters that appear the most often in the English language. By use frequency analysis to determine the letters that are shown the most often in an encoded message, it is possible to break the shift cipher. This is accomplished by studying the letters that are shown the most frequently. It was discovered that this was the most significant flaw in the encryption, and as a result, the cipher was deemed ineffective as a means of concealing information. The passage of time would result in the development of novel and sophisticated methods of concealing information. The flaws that were present in earlier techniques of information concealment served as a source of inspiration for these new approaches, which were designed to avoid the same errors that were present in the earlier systems.

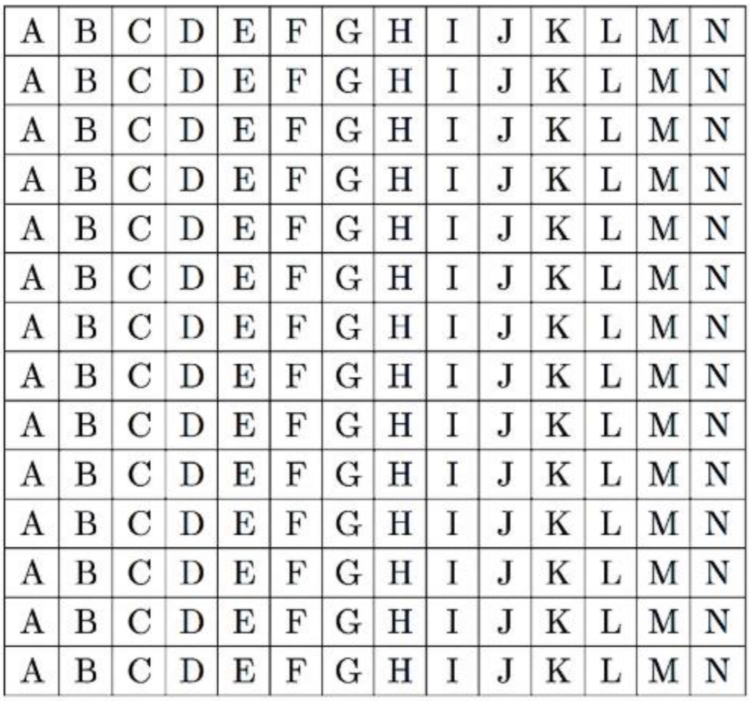
EARLY FORMS OF CRYPTOGRAPHY: CAESAR AND VIGENÈRE CIPHERS:

Information was concealed by the use of the Vigenere cipher, which is a technique that is comparable to the Caesar cipher and makes use of simple number theory. According to Hamilton and Yankosky (2004), the Vigenere cipher is an example of a polyalphabetic cipher, which is a kind of cipher that is based on substitution and makes use of several replacements of the alphabet. For the purpose of encrypting the information included inside the message, this approach makes use of a secret'shift' word and employs numerous shift strategies throughout the message. Furthermore, the Vigenere cipher provides an illustration of how number theory has contributed to the development of cryptography throughout the course of its history. The Caesar cipher ultimately proved to be an insufficient method of concealing information over the course of time, as was previously established. The Vigenere Cipher, on the other hand, makes use of the same number theory concepts as the Caesar Cipher, but it helps prevent frequency analysis from being used as a method of decrypting the information. The Vigenere encryption employs a number of Caesar ciphers that are distinct from one another, each of which is applied to a specific keyword. The Vigenere cipher is considered to be one of the most well-known private-key cryptosystems, as stated by Hamilton and Yankosky (2004).The Vigenere cipher was first explained in terms of a table called the Vigenere Square and a secret keyword (p.19). This was the initial description of how encryption and decryption were being performed. During the course of the development of number theory, the cryptosystem of the Vigenere cipher evolved into a method of concealing information that rectified the flaws that were discovered in the Caesar cipher. According to Hamilton (2004), the Vigenere cipher, which was first introduced in the late 1500s and takes its name from the Frenchman Blaise de Vigenere, may be explained by referring to the characteristics of modular arithmetic. Consider the following scenario: the plaintext that has to be encrypted for this cipher is the phrase "MATHISREALLYCOOL," and the keyword that needs to be encrypted is "DISCRETE." The cipher was designed to function properly. This illustration illustrates the encrypted phrase that corresponds to the word "MATHISREALLYCOOL." In most cases, these ciphers include quite lengthy keywords; nonetheless, this is a simplification that is intended to facilitate the development of an understanding of the Vigenere cipher. Using a concept that is comparable to that of the Caesar cipher, Hamilton and Yankosky (2004) provide an explanation of the encryption equation for the Vigenere cipher, which may be obtained from (4).

$$c = (p + k) \bmod 26 \tag{4}$$

where $k \in \mathbb{Z}_{26}$

p represents the plaintext letters, c represents the ciphertext letters, k represents the number of letters in the alphabet or the letters of the key, and 26 represents the letters of the alphabet. This equation includes all of the letters in the alphabet. A significant distinction between the Vigenere and Caesar ciphers is that the letter 'A' is equivalent to the number 0. This is one of the most important discrepancies. The Caesar cipher involves the values A=1, B=2, and Z=26. The Vigenere cipher has the values A=0, B=1, and Z=25 at the moment. For this particular instance, the key is 'DISCRETE,' but it will be extended to 'DISCRETEDISCRETE' in order to ensure that the key is repeated to the same length as the plaintext. In this particular instance, the plaintext "MATHISREALLYCOOL" will be encrypted for the purpose of becoming "PILJZWKIDTDATSHP." For both encrypting and decrypting the Vigenere encryption, this technique makes use of the Vigenere Square, which is seen in Figure 1. A number that corresponds to each letter in the alphabet, up to a maximum of 26 letters, is based on the letter's position in the alphabet. In the Vigenere cipher, the alphabet is spelled out 26 times in a series of rows and columns that are collectively referred to as the Vigenere square. This composition is seen in Figure 1. As can be seen in the first column of Figure 1, each row of the cipher is moved to the right by one letter in comparison to the row that is directly above it. This may be thought of as a total of twenty-six distinct Caesar ciphers with increasing shift capabilities. Regarding this particular case, the plaintext may be encrypted manually by hand due to the fact that it is quite brief. We are able to determine which rows to check for in the mapping by using the letters that are included in the key. If we were to begin with the first letter of the word "MATHISREALLYCOOL," for instance, we would begin at row M on the Vigenere square. In the next step, we would go to the initial letter of the word "DISCRETE," which would be located in column D. A return of the ciphered value of 'P' would be obtained from this. In its most basic form, the Vigenere cipher is a method of increasing the complexity of the encryption by using modular arithmetic and the concepts of the Caesar cipher. Hamilton and Yankosky (2004) provide an explanation of the decryption equation for the Vigenere cipher, which can be seen in (5). This explanation is based on a description of the Vigenere encryption cipher that is comparable.



A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	B	C	D	E	F	G	H	I	J	K	L	M	N

Figure 1: Composition

$$p = (c + (26 - k)) \bmod 26 \text{ where } k \in Z_{26} \qquad (5)$$

In continuation of their explanation, Hamilton and Yankosky (2004) state that "the primary entries of the table correspond to ciphertext letters and...Prior to using the Vigenere Cipher, it is necessary for two correspondents to reach a consensus on a secret keyword or key phrase. (page 21) In the context of cryptography, the process of encrypting and decrypting the Vigenere cipher is illustrative of the development of number theory throughout time. As a result of the Caesar cipher's limited scope, which consisted of just 26 characters, it was possible to decrypt the information via the use of frequency analysis of the English language. This was the one weakness of the Caesar cipher. The Vigenere cipher makes use of modular arithmetic to transform the alphabet into a collection of twenty-six Caesar ciphers. This makes the cipher more difficult to decipher and increases its level of security. The Vigenere cipher was a more advanced method of encrypting data, and it used a secret key of arbitrary length. It was used for both encryption and decryption purposes. There is a representation of each of the 26 Caesar ciphers that are conceivable in the Vigenere Square (one in each row). Because the same plaintext letter will not always be encrypted to the same ciphertext letter, the benefit of the cipher is that it is not susceptible to frequency analysis as a method for breaking the cipher. This is because the encryption is not susceptible to being cracked. A further application of probability is used by this cipher to demonstrate that there are 26 thousand potential values for each given letter. K represents the length of the keyword in this particular occurrence. If a keyword is seven letters long, then there are eight billion possible ways that the phrase might be constructed in the Vigenere square. The repeating key is the source of this cipher's vulnerability, which is as follows. It is possible to break the encryption using modular arithmetic if the individual is able to make an educated estimate about the length of the key. This is due to the fact that once the length of the key word has been determined, the ciphertext may be cracked using a Caesar cipher. In order to get the key to match the phrase, we had to repeat our key, which was 'DISCRETE,' twice. This was necessary since the phrase we used in our example consisted of sixteen letters. In the event that the phrase is sufficiently lengthy and is accompanied by a short key, it is unavoidable that the key and the ciphertext will include repeated letters or patterns. This is due to the fact that the key must be repeated in order to correspond with the length of the phrase. On the other hand, if a phrase that is 150 words long is used in conjunction with a random key that is also 150 words long and does not repeat itself, then it will be very difficult to decrypt this message since there are no inherent defects or repeated keys in the message. The Vigenere encryption is an example of how the Caesar cipher was enhanced to make the process of information concealment more safe. Despite the fact that it had certain drawbacks connected to the number theory that was utilized to develop the cipher, the Vigenere cipher was able to do this.

TRANSITION TO MODERN CRYPTOGRAPHY: RSA ALGORITHM:

(Tan, C. M. S., Arada, G. P, 2021) In today's digital world, when practically everything is available over the internet, including education, shopping, banking, and social media, cryptography has developed into a need. This is because cryptography has evolved to become required. Because all of this information is stored on the internet, the challenge now is to develop a means to protect all of this information in a way that is both effective and efficient. This is an issue that neither Julius Caesar nor Blaise de Vigenere encountered or had to find a solution to when they launched their respective ciphers on the market. Advanced mathematical theorems were required to be added in order to offer data protection and privacy for all of this data. These theorems differ greatly from the basic number theory that is used in the Caesar and Vigenere Ciphers. The RSA algorithm was first developed as a means of encrypting and decrypting information during the information era. This is the next algorithm that will be introduced. In ciphers such as the Vigenere cipher, it was usual practice to discuss and record a public key in advance. This was one of the characteristics that made for a secure encryption. The public key was used to determine the number of letter shifts in the Caesar cipher, but in the Vigenere cipher, it was used to determine the significance of the keyword. Currently, the RSA technique consists of two sets of keys: one for encryption and another for decryption. The following is an explanation provided by Kulkarni (2017): "RSA was invented by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978...A block cipher system is an example of an asymmetric cryptosystem that is based on number theory. This cryptosystem is a public key cryptosystem. According to Kulkarni (2017), the RSA method is able to produce a public key, which is used for the purpose of key encryption, and a private key, which is utilized for authentication purposes. This is accomplished by using two prime integers. In order to ensure the safety of the RSA scheme, the amount of complexity associated with the factoring of very big numbers is taken into consideration (Lagarias, 2017). In order to encrypt and decrypt data, the RSA method makes use of a wide variety of subfields within number theory. These subfields include modular exponentiation and congruences, general divisors and greatest common divisor (GCD), the Euclidean algorithm, and Euler's Totient theorem (Karunankitha et al, 2021). The mathematical theorems that are used to encrypt and secure data have gone a long way from the basic shifting of the letters of the alphabet that was employed in the Caesar cipher. This is clear at first look, since the progress of cryptography via number theory is evident. First things first, before we get started with the discussion on RSA algorithms, we need to go over some of the fundamental ideas of number theory that are essential for comprehending how the algorithm works. I will begin by describing the process of the RSA algorithm that is involved in the process of key generation. After that, I will explain the mathematics that is behind the process, and finally, I will provide an example. In accordance with the explanation provided by Kulkrani (2017), the process of RSA key creation is comprised of five steps:

- Choose two large prime numbers (p and q)
- Compute n = p * q
- Calculate φ(n) = (p-1)*(q-1)
- Choose an integer e such that 1 < e < φ(n)
- Ensure that gcd(e, φ(n)) = 1
- Ensure that e and φ(n) are coprime
- Compute an integer d, such that d = e^{-1} mod φ(n)

As was previously described, prime numbers, in addition to a great number of other theorems from solid number theory, play a significant part in the manner in which the RSA algorithm encrypts data and ensures that the data integrity is preserved. To begin, primes are numbers that can only have factors of one and themselves. Primes are also known as prime numbers. RSA is a cryptographic procedure that uses primes expressly for the purpose of key creation. Primes have become an integral component of the majority of current cryptography systems. The concept of coprime numbers, sometimes known as comparatively prime numbers, is an additional mathematical notion that is essential to the RSA algorithm. The term "coprime" is used to describe numbers that only have the number 1 as their shared common point. The number 18 contains the elements 1, 2, 3, 6, 9, and 18; similarly, the number 35 has the factors 1, 5, 7, and 35. These numbers are regarded to be co-prime numbers since the sole factor that they have in common is 1. A further explanation of the concept of coprime may be provided by introducing the concept of the greatest common divisor, sometimes known as the GCD. When there are two or more numbers, the greatest common divisor of those integers is the biggest integer that divides each of the integers independently. Additionally, it is possible to demonstrate that two integers are coprime if the greatest common divisor of each of them is 1. (Karunankitha et al, 2021). As a continuation of the preceding illustration, we can demonstrate that the GCD of 18 and 35 is equal to 1. We are able to claim that 18 is coprime to 35 and that 35 is coprime to 18 if the gcd of 18 and 35 is equal to 1. Prime numbers that are hundreds of digits long are often used by algorithms such as the RSA method in order to encrypt the information that they are responsible for. Using the Euclidean procedure, one is able to determine the greatest common divisor for prime integers that are very big. (Karunankitha et al, 2021) The Euclidean Algorithm is a method that was devised by the Greek mathematician Euclid as a method for rapidly determining the GCD of two numbers. As an illustration, let us take the numbers 270 and 192 as an example to demonstrate how the Euclidean method may assist in determining the greatest common divisor of two integers. In equation (6), the equation for the Euclidean method that was developed by Karanankitha et al. in 2021 can be observed.

$$a = bq + r \qquad \text{where} \quad 0 \le r \le b$$
$$b = rq_1 + r_1 \qquad \text{where} \quad 0 \le r_1 \le r \quad (6)$$

In this example,

$$270 = 1 * 192 + 78$$
$$192 = 2 * 78 + 36$$
$$78 = 2 * 36 + 6$$
$$36 = 6 * 6 + 0$$

It has been shown that the greatest common divisor of 270 and 192 is the number 6, given that the number 6 is the biggest divisor that exists prior to the equation having a remainder of 0. As a result of the fact that the last positive residual is 6, this may alternatively be expressed as gcd(270,192) = 6. The following theorem, which is a fundamental component of the RSA method, is Euler's elaboration of Pierre de Fermat's theorem, which eventually became known as the Euler totient function. The RSA algorithm contains this equation, which is used in the process of encrypting data. "Euler's totient function was first proposed by Leonhard Euler; as a function that counts the numbers that are both less than n and had no other frequent divisor with n other than 1 (that is, they are co-prime with n)," Karunankitha et al (2021) said. "Euler's totient function" This is page 3215. In order to count positive integers up to a specific number n that are substantially prime to n, Euler's totient theorem is used while counting positive integers. This equation for Euler's Totient Function (Karunankitha et al, 2021) is written as shown in (7), where Φ is the symbol for phi. If n is the product of two primes p and q, then the equation for n is n = pq.

$$\Phi\,(n) = \Phi\,(p)\,\Phi\,(q) = (p-1)\,(q-1) \quad (7)$$

According to Karanankitha et al. (2021), the Euler's totient function, which is sometimes referred to as the Euler's phi function, is a function in which the equation is either $1 < e < \varphi(n)$ or for which the greatest common divisor exists as gcd(en, e) = 1. In order to fulfill the requirements of the Euler function, the greatest common divisor is applied once again, just as it was utilized and presented for the first time. By using the extended Euclidean method and the equation (Karunankitha et al, 2021) presented in (8), the last phase of the key generation process in the RSA algorithm is to determine the value of d, which is a member of the private key. This is accomplished by utilizing the RSA algorithm.

$$d \equiv e^{-1} \bmod (p\text{-}1)(q\text{-}1) \qquad (8)$$

In his 2017 research, Kulkarni came to

the following conclusions:

The observation that it is possible to obtain three very big positive numbers e, d, and n in such a way that modular exponentiation may be used for any m, and that even if one knows e and n or even m, it can be exceedingly challenging to get d (p.100) is the fundamental idea that provides the foundation for the Secure Random Numbers (RSA) algorithm.

It is now possible to provide the encryption equation (Karunankitha et al, 2021), which can be seen in (9). This is because the processes for generating a key have successfully been covered.

$$C = M^e \bmod n \qquad (9)$$

In the equation that has been supplied, the letter c represents the ciphertext, while the letter m represents the message text. Both of these letters are symbolized by the letter m. Kulkarni continues his explanation by stating that the activities of RSA may be split down into three steps, which are as follows: The procedures of key creation, encryption, and decryption are discussed in Kulkarni's (2017) article. For the purpose of providing an example of the RSA encryption and decryption process, the following is taken into account. The challenge of factorizing a large number serves as the basis upon which the RSA technique for generating RSA keys is constructed.

Despite the fact that the approach in issue often makes use of prime numbers that are hundreds of digits in length, this example will include prime numbers that are very small for the benefit of comprehension. In order to determine whether or not the technique is trustworthy, let us pretend that the sender plans to encrypt and transmit a message to the recipient that includes the letter "B." This will allow us to determine whether or not the method is dependable. Set p equal to two and q equal to seven so that we may compare them to the two prime numbers that are the smallest. It is possible to extract the first component of the public key by multiplying the two prime integers, which will result in the equation n = pq. This will allow one to derive the public key. We would get the value of n equal to 14 if we were to use the formula N = pq. In order to get the value of Φ(n) = (p-1)(q-1) as shown in equation (10), we would like to continue with the presentation of Euler's totient function, which was recently published by Karanankitha et al. in the year 2021.

$$\Phi(n) = (p\text{-}1)(q\text{-}1) = (2\text{-}1)(7\text{-}1) = (1)(6) = 6 \qquad (10)$$

At this point, it is necessary for us to determine the values of e, which represents the encryption value, and d, which represents the decryption value. The next step is to choose an integer (e) according to the equation 1 < e < phi(n), where e is an integer that is not a factor of n and meets the condition that phi(n) not equals e. For this particular issue, the value of e may be determined by using the equation gcd(e, phi(n)) = 1. This particular equation indicates that e must be more than 1 but less than phi(n), which is 1. The remainder of gcd(5,6) equals one when it is entered into the function, which is the correct answer. The potential values of e are 5, and the possible values of d are 5, 11, and 17. One may determine these numbers using computation. As of right now, the public key is made up of the pair (5,14). For the purpose of decrypting information, which includes the value of e and the value of n, the private key is inaccessible to anybody other than the person who created the data. The public key is responsible for encrypting the information. On account of the fact that the letter B in the alphabet has a numerical value of 2, the term "B" is now comparable to the number 2. When considering the Caesar and Vigenere ciphers, it is important to note that the position of a letter inside the alphabet is a significant factor in determining its value within the algorithm. The encryption equation is now defined by the equation C = Me mod n, which is represented by (9), where C is the modular congruence of Me mod n. This equation defines the encryption equation. Therefore, the value of the encryption is 25 multiplied by 14, where 2 is the mathematical value of the letter 'B'. Furthermore, it is said that the value of the encryption value is 5, and the value of n is 14. At this point, the issue is solved by using the equation that was presented in the previous section (9).

$$C = M^e \bmod n$$

$$C = 2^5 \bmod 14$$

$$C = 32 \bmod 14 = 4$$

At this point, the message that has been encrypted is the number 4, which corresponds to the value of the letter D in the alphabet. Following the "shifting" of all of the letters in a cipher, an encrypted message would be produced as the final byproduct. In order to decode the message, we will now make use of the private key (11,14) and the decryption equation (Karunankitha et al, 2021), which can be found in (11).

$$M = C^d \text{ (mod n)} \qquad (11)$$

$$M = 4^{11} \text{ (mod 14)}$$

$$M = 4{,}194{,}304 \bmod 14 = 2$$

It is now clear that the number 4,194,304 divided by 14 is equivalent to a number that has a residual of 2. The result of this analysis would indicate that the message that has been encrypted is the number 2, and the value of 2 corresponds to the letter B in the alphabet. This particular example uses the public key, which is (5,14), and the private key, which is (11,14). The substantial number theory that underpins the RSA algorithms is a significant contributor to the demonstration of the development of cryptography on the basis of number theory. The RSA cipher makes use of modular arithmetic in addition to a significant number of new theorems that are based on the creation and factorization of very big prime numbers. This is in contrast to the shift ciphers that are present in the Caesar and Vigenere ciphers. There are still certain drawbacks associated with the RSA method, despite the fact that it makes use of a far greater number of number theory components than the other ciphers that were reviewed before. The RSA encryption has a number of drawbacks, including a sluggish data transmission rate and a lengthy computation time because of the high prime numbers needed to do the calculation. included in Even with this information, there is still no established method to break the encryption, even if a key that is sufficiently big is employed. SSL, which stands for Secure Sockets Layer, is one of the methods that may be used to ensure the safety of an internet connection. RSA has been modified to produce SSL. The RSA algorithm may be used to encrypt data for illegal reasons, despite the fact that it currently offers a relatively safe method of data transit. This implies that the technique can also be used for other purposes. In addition, there is no discernible gain in security seen in relation to the processing power that is used in the process of generating the key as the prime numbers continue to grow in length. since of this, the RSA method requires a significant amount of resources since it takes a remarkable amount of time to perform operations on such very huge prime numbers. As a result of the very lengthy processing time that is induced by the use of prime factorization to generate the keys in RSA, other ways of encrypting data have been introduced in order to safeguard stored information.

Table 1: Comparing Classical and Modern Cryptographic Techniques

Feature	Caesar Cipher	Vigenère Cipher	RSA Algorithm
Type	Substitution (Mono)	Substitution (Poly)	Asymmetric Key Encryption
Mathematical Basis	Modular Arithmetic	Modular + Key Repetition	Number Theory, Modular Arithmetic
Key Type	Single Integer Shift	Repeating Key	Public & Private Key Pair
Vulnerability	Frequency Analysis	Frequency Analysis	Factoring Large Numbers
Scalability	Low	Medium	High (Used for millions of users)

According to the findings presented in this article, the huge growth of the area of number theory has been used to assist in the development of the field of cryptography and to assist in the protection of information. As early as the year 1900 BCE, there were indications that cryptography was being employed for the first time. In the vicinity of 300 B.C. and in the 1700s, respectively, further theorems such as the Euclidean algorithm and Euler's Totient Function were presented to the scientific community. During the latter part of the 20th century, the RSA algorithm made use of a number of theorems, including these and others. A wide variety of theorems have been used in the development of cryptography. These theorems vary from the earliest forms of basic number theory to the more contemporary improvements to number theory. The article explains that the primary objective of the development of cryptography has been to ensure the security of our information, and that the advancement of number theory has made it possible for cryptography to develop throughout time. The need for cryptography has significantly increased as a result of the technical advancements that our civilization has recently made. According to Kessler and Phillips (2020), "With the commercialization of the Internet and the dawning of the World Wide Web in the early 1990s, the government realized that there were legitimate needs for public use of strong cryptography" (p.2-3). This is supported by the fact that the government recognized the necessity for strong cryptography. The developments in number theory that have made it possible to construct safe cryptosystems are the reason why cryptography plays a part in our daily lives, as was said before. This is because cryptography involves the use of numbers. The usage of cryptography may be seen in a variety of everyday activities, including using our phones, making phone calls, opening our email accounts, placing online food orders, using our credit cards, watching television, and even driving our automobiles. Because of the number theory that underpins the systems, all of this information is safeguarded properly. It is impossible to imagine the level of progress that has been made in the area of cryptography if it were not for the developments that have taken place in the subject of number theory. There is significant information that is generated and used on a daily basis, and in order to protect our privacy, this information has to be encrypted. Because to the strength of number theory and cryptography, we are able to utilize our mobile devices to engage in activities such as video chatting, browsing the internet, and playing games. Encryption and decryption are the procedures that have led to the development of contemporary cryptography. These processes have been developed via the progression of cryptography, beginning with basic shift ciphers and progressing to the RSA cipher. In comparison to the cryptographic systems that are used today, these procedures do contain flaws that are both observable and susceptible to being exploited. As was said before, the Caesar and Vigenere ciphers were made useless once the system was discovered due to frequency analysis, which rendered the ciphers useless. When contrasted with the RSA encryption, which does not exhibit any discernible vulnerabilities when a prime integer of sufficient magnitude is used, the progression of cryptography is readily apparent.

CONCLUSION:

There were a number of mathematicians, including Euler and Euclid, who made significant contributions to number theory and were essential in the presentation of these theorems. These mathematicians laid the groundwork for the development of cryptography through their efforts. Despite the fact that the historical periods that are discussed in this article range from the beginning of civilization in the B.C. with the Caesar cipher to the late 1900s with the RSA method, the necessity of cryptography and its effectiveness have been evident even in the earliest forms of civilization that we have ever come across. Two examples of encryption methods that were initially developed in the 1970s and 2001, respectively, are the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). Both of these encryption methods are considered to be more secure than the RSA algorithm. For the purpose of continuing to make these cryptographic systems more secure through the use of number theory, it is still important to be conducting additional research.

REFERENCES:

1. Amanie, H. A. (2020). Comparison between integer splitting cipher and traditional substitution ciphers, based on modular arithmetic. *IOP Conference Series.Materials Science and Engineering, 919*(5). http://dx.doi.org/10.1088/1757-899X/919/5/052004
2. Ghosal, G. (2021). A study on the development and application of number theory in engineering field. *International Journal of Applied Science and Engineering, 9*(1), 35-40. http://dx.doi.org/10.30954/2322-0465.1.2021.4

3. Hamilton, M., & Yankosky, B. (2004). The vigenere cipher with the TI-83. *Mathematics and Computer Education, 38*(1), 19-31. https://libprox.northampton.edu/login?url
4. =https://www.proquest.com/scholarly-journals/vigenere-cipher-with-ti-83/docview/23586 0079/se-2?accountid=39096
5. Karunankitha, L., Sravya, P., Aparna, G., Navya, S., Abhigna, P., & Suneela, B. (2021). An Efficient and high performance architecture design and implementation approach of cryptographic algorithm computation for authentication in modern wireless communication applications. *Turkish Journal of Computer and Mathematics Education, 12*(11), 3206-3228. https://libprox.northampton.edu/login?url=https://www.proquest.com/scholarly-journals/efficient-high-performance-architecture-design/docview/2623918350/s e-2
6. Kartha, R. S., & Paul, V. (2018). An efficient algorithm for polyalphabetic substitution using random tables. *International Journal of Advanced Technology and Engineering Exploration, 5*(43), 124-133. http://dx.doi.org.libprox.northampton.edu/10.19101/ IJATEE.2018.543001
7. Kessler, G. C., & Phillips, A. M. (2020). Cryptography, Passwords, Privacy, and the Fifth Amendment. *The Journal of Digital Forensics, Security and Law : JDFSL, 15*(2), 0_1,1-23. http://dx.doi.org/10.15394/jdfsl.2020.1678
8. Kulkarni, S. (2017). Study of modern cryptographic algorithms. *International Journal of Advanced Research in Computer Science, 8*(3) https://libprox.northampton.edu/login? url=https://www.proquest.com/scholarly-journals/study-modern-cryptographic-algorithm s/docview/1901457990/se-2
9. Lagarias, J. C. (1989). A course in number theory and cryptography (Neil Koblitz). *SIAM Review, 31*(3), 508-3. http://dx.doi.org/10.1137/1031111
10. Samaila, D., & Pur, M. P. (2013). Secret sharing scheme using transpositions in symmetric group. *International Journal of Pure and Applied Sciences and Technology, 14*(1), 27-32. https://libprox.northampton.edu/login?url=https://www.proquest.com/scholarly-journals/s ecret-sharing-scheme-using-transpositions/docview/1349963697/se-2
11. Shores, Dawson. (2020). *The Evolution of Cryptography through Number Theory - Gcsu.edu*, https://www.gcsu.edu/sites/default/files/documents/2021-06/shores.pdf
12. Tan, C. M. S., Arada, G. P., Abad, A. C., & Magsino, E. R. (2021). A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher. *Journal of Physics: Conference Series, 1997*(1) http://dx.doi.org.libprox.northampton.edu/10.1088/1742-6596/1997/1/012021