International Journal of Mathematics And Its Applications
Vol.2 No.4 (2014), pp.71-82
ISSN: 2347-1557(Online)

Number Theory and Applications in Cryptography

Mukesh Punia[†,1]

[†]Department of Mathematics, S D (PG) College, Panipat, Haryana, India

Abstract : Number theory, a branch of pure mathematics, has found an indispensable role in the realm of modern cryptography. This article provides a comprehensive overview of the fundamental principles of number theory and their applications in cryptographic systems. Number theory serves as the bedrock for encryption and decryption techniques that safeguard sensitive information in an increasingly interconnected world. Cryptographic algorithms, designed to secure digital communication and protect data integrity, rely on number-theoretic properties for their robustness. This article explores the profound significance of number theory in cryptography, elucidating key concepts and their practical implications. One of the cornerstones of number theory in cryptography is prime numbers. Prime factorization serves as the basis for public key cryptography, where the difficulty of factoring large semiprime numbers ensures the security of data transmission. Additionally, modular arithmetic, a central component of number theory, is used to implement cryptographic operations like encryption and digital signatures. The article delves into elliptic curve cryptography (ECC), which leverages the algebraic structure

[1] Corresponding author email: sapraeducation9@gmail.com (Mukesh Punia)

of elliptic curves over finite fields. ECC provides strong security with smaller key sizes, making it particularly well-suited for resource-constrained devices and applications. We also explore the discrete logarithm problem, a formidable challenge in number theory, and its implications in cryptography. Understanding the intricacies of number theory empowers cryptographers to design secure and efficient cryptographic protocols. By examining the mathematical foundations of cryptographic algorithms, this article underscores the critical role of number theory in safeguarding digital communication, financial transactions, and personal information in the modern age.

Keywords : Number Theory, Cryptography, Prime Numbers, Modular Arithmetic, Elliptic Curve Cryptography.

1 Introduction

The application of mathematics in the form of cryptography is now commonplace. Cryptography is a subfield of mathematics. Cryptography is the study of developing safe and efficient codes. To send and receive secret communications, it employs a variety of methods that are together referred to as cryptosystems. Cryptography, which first appeared in ancient civilizations, is playing an increasingly important part in contemporary life. A security method that is constructed from a cryptosystem is applied every time a credit card is swiped or a computer is used. Matters pertaining to cyber and national security are the ones in which it is most significant. The study of numbers, sometimes known as number theory, is a discrete subject of mathematics that is deeply ingrained in the operations of cryptography. The project's primary emphasis will be placed on those applications of Number Theory that may be directly related to cryptography.

The fight to protect people's right to privacy in their electronic conversations is an age-old one. The development of contemporary cryptography may be traced back to the utilization of techniques such as code pads, vanishing inks, and buried text. The name ”cryptography” comes from the Ancient Greek word ”kryptos,” which literally means ”to hide.” The study of methods that enable messages or information to be encoded (obscured) in such a way that it is extremely difficult to read or understand encoded information without having a specific key (i.e., procedures to decode) that can be used to reverse the encoding procedure is at the core of cryptography. Cryptography can be thought of as the study of procedures that allow messages or information to be encoded (obscured). It is possible for encryption systems to entail only the straightforward substitution of letters for numbers, or they may involve the utilization of ”one-time pads,” commonly referred to as Vernam ciphers, which are extremely safe. One-time pad encryption provides the only known type of cryptography that is secure against cracking. This is due to the fact that one-time pad codes and keys can only be used once. One-time pads, on the other hand, are unsuitable for broad usage because of the large number of codes and keys that are required. The capability of one combatant or country to read the purportedly secret signals being sent by its adversaries has been a deciding factor in a great number of conflicts and diplomatic discussions. During World War II, for instance, the Allied Forces acquired significant strategic and tactical advantages as a result of their ability to intercept and decipher the secret messages that Nazi Germany had encoded using a cipher system known as Enigma. These signals had been sent in code by Nazi Germany. The United States of America got a significant edge over the Imperial Japanese troops as a result of the invention of operation MAGIC, which deciphered the codes that Japan employed to safeguard its communications. This gave the United States a decisive victory. in tandem with the continued development of computing technology and the diminishing use of manual record keeping methods such as paper and pen. The second half of the 20th century saw a rise in the significance of cryptography as a field of study. There was a steady increase in the amount of data that could only be permanently stored in the computer’s memory. Even if the technological revolution and the emergence of the Internet posed their own set of unique security issues, there were also challenges to the fundamental security of the increasing amounts of information that was only kept and sent in electronic form. Because of this growing dependence on electronic communication and data storage, there has been an increased demand for advances in cryptologic research. After initially being used primarily by the military and diplomats, cryptography has since found widespread application in the private communication of businesses and private individuals who value their right to confidentiality. For the purpose of securing their databases and email, governments, companies, and individuals all required cryptologic systems that were not only more secure but also easier to use. In addition to improvements made to cryptologic systems based on information made public from classified government research programs, international scientific research organizations dedicated exclusively to the advancement of cryptography (such as the International Association for Cryptologic Research, or IACR), began to apply applications of mathematical number theory to improve the privacy, confidentiality, and security of data. This was done in addition to the improvements made to cryptologic systems based on information made public from classified government research programs. The applications of number theory were utilized in the development of algorithms (i.e., step-by-step procedures for resolving mathematical issues), which became increasingly complex over time. Not only was it becoming increasingly important to keep information confidential as commercial and personal use of the internet increased, but it was also becoming increasingly important to be able to verify the identity of the person sending the message. The use of certain types of algorithms known as ”keys” enables information to be restricted to a specific and limited audience whose identities can be authenticated. This is made possible through the utilization of cryptographic techniques. Encryption can be achieved in some cryptologic systems, for instance, by selecting particular prime numbers and then using the products of those prime numbers as the basis for further mathematical operations. In addition to developing such mathematical keys, the data itself is divided into blocks of a specific and limited length. This is done to ensure that the amount of information that can be obtained even from the form of the message is restricted. In most cases, decryption can be achieved by following a complicated reconstruction process that, in and of itself, involves performing special mathematical operations. In some circumstances, the process of decryption is carried out by carrying out the inverse mathematical operations that were carried out during encryption.

2 Main Result

Objective

1. Study On Mathematics In The Form Of Cryptography

2. Study On Cryptographic Technique That Is Considered To Be One Of The Oldest

Basic Terminology

Crytography utilizes a wide variety of specialized terms, all of which should be thoroughly understood. It is common practice for two persons, commonly referred to as Alice and Bob, to attempt communication in such a way that it is incomprehensible to a third party, sometimes referred to as Eve. In an ideal scenario, the cryptosystem should be designed in such a way that even if Eve is able to read the message, she or he is unable to figure out what it says. Because of this, it is very necessary for a cryptosystem to be both effective and safe.

Encryption

The act of taking a piece of information in its plaintext form and encoding it in such a manner that the message can only be received and understood by its intended receiver is what we refer to as encryption. The plaintext is sent to an algorithm to be encoded, and the result is called a cipher text.

Decryption

The process of uncovering a ciphertext is referred to as decryption. Using a special method called a reverse algorithm, the message is found and then converted back into its original plaintext form.

Keys

The algorithm that is used to encrypt and decode information frequently makes use of a key. Public and private keys are the two categories under which keys can fall. A key that is considered to be public is one that is not only known to the two parties involved in the communication but also to any third party. One communicating member at a time is the only one who can utilize a private key. It is a well guarded secret, both among the other members and among outsiders. In practice, cryptographic systems frequently make use of a hybrid mix of public and private keys. Throughout the entirety of the project, we will proceed on the assumption that the message space is constituted of integers, integers modified by a positive integer, or vectors of integers.

Cryptography on the Internet

Imagine that two people, Alice and Bob, are trying to have a private discussion, but anyone who wants to can listen in on what they are saying. How are they able to pull this off? We have previously seen how they could accomplish this in Example 9, and we have also seen how certain difficulties may occur as a result of espionage. There is a further issue that we have neglected to discuss. What if Alice and Bob don't have a key K that only the two of them know the secret to? The use of cryptography on the internet solves this problem. This makes use of something called ”public-information algorithms”: It is not necessary for Alice and Bob to have previously communicated in confidence because everything is carried out in public. There are two different strategies that are used.

1. Even if there is another person listening in on Alice and Bob's chat, the two of them are still able to come up with a secret key. In this procedure, Alice and Bob typically perform roles that are comparable to one another; hence, we refer to this as symmetric encryption.

2. Alice has the ability to broadcast data to the globe that enables others to encrypt communications for her while simultaneously making it difficult for anyone other than herself to decrypt such messages. Bob is capable of doing the same. This method is known as public key cryptography because the key is information that is readily available to the general public.

These methods are dependent on something that is referred to as a trapdoor function. A trapdoor function is an invertible function g with the property that it is difficult to compute x when given the value of g(x). Such functions are also referred to as one-way functions; however, this name can be somewhat misleading because it gives the impression that g cannot be inverted. The protocols that make use of two distinct trapdoor functions will be discussed here.

Example number 15 (Separate logs and improved encryption) Even with knowledge of both the plaintext and the ciphertext, it may be difficult to decipher the key even if the system has been designed in a number of different ways. The approach that we will outline in this section is not the one that is actually implemented, but it will help set the stage for the next illustration. 117 may be readily converted into the numerical value 19487171 if you use a calculator. If you already know that the number 19487171 has the form 11x, then all you need to do to find x is use your calculator like you normally would. You should recall that x equals log11 (19487171) from when you were in high school. In all likelihood, you would perform that computation by using either the LOG or the LN button on your calculator, as seen below: LOG(19487171) divided by LOG(11) is 7. In any event, it is not really difficult. However, a change that at first glance does not appear to be significant can make this type of computation extremely challenging in many contexts. If we compute 11t% 163 for t = 0, 2,..., 161, we will obtain each of the numbers 1, 2,..., 162 precisely once; however, they will be in an illogical sequence. Let's compute 117 percent of 163 rather than 117 itself. 32 is the correct answer. Even though we are aware that there is a single value for x that falls between 0 and 161, the equation 32 = 11 x% 163 is proving to be rather difficult to solve. It is possible to achieve it for such tiny numbers by testing all of the numbers from 0 to x plus 162. However, using any of the currently known approaches, it appears to be very hard to do so for large numbers that contain hundreds of digits. The process of recovering an exponent from an exponentiated expression after it has been reduced modulo some integer is referred to as the discrete logarithm problem, and the term "discrete logarithm" is used to refer to the exponent. The following is an example of how discrete logarithms might be used to make it extremely difficult for Joe's espionage when Alice and Bob have access to a secret key K. We go with a big modulus p that is fixed throughout the process. When someone wishes to send a message with the prefix P, the computer selects a "base" b at random and then calculates b K% p. Let's denote the outcome of this calculation with the letter L. L is utilized by the computer in order to encrypt P utilizing the particular encryption method that is now being utilized. Therefore, the computer arrives to the conclusion that $fL(P) = C$. It also conveys the letter C. After computing b K% p to produce L, the computer at the opposite end of the connection uses this value to decode the message. What are Joe's capabilities as a spy? Let's say the method of encryption is the same as the one used in Example 10: Simply put, we convert L into a binary number and then bitwise add it to the message that is P. We are going to proceed on the assumption that Joe is aware of the value of the modulus p. As in the past, Joe asks his buddy to send a message, and as a result, he has P, C, and b for this specific message; we will refer to them as P1, C1, and b1, respectively. Joe is able to obtain L1 by using P1 and C1. P2 then receives a communication from a third party at a later time. The computer selects an arbitrary value for b2 and then calculates b K 2% p = L2 and C2. Joe obtains b2 and C2 by listening in on conversations.

1. To decrypt the message, Joe needs to find L2 so that he can add it bitwise to C2.

2. To get L2 he needs K because L2 = b K 2 (mod p) and he knows b2.

3. To get K he needs to solve the discrete log problem because he has b1 and L1 and b K 1 = L1 (mod p).

Joe decides not to continue since this is too difficult. There was nothing particularly noteworthy about bitwisely adding L to P. Joe would still have the goal of recovering K regardless of the technique that was employed, and in order to do so, he would need to follow out the procedures described in the paragraph before this one.

Assume that the values of b and p are already established and unchanging. Many people believe that the function g, which may be expressed as g(n) = bn% p, is a trapdoor function. Calculating the discrete log of b n is another name for the process of finding n using $g(n)$. As was said in the example that came before this one, calculating the discrete log is thought to be highly challenging. As a result, it is thought that g is a trapdoor function. Let's say Alice and Bob want to conduct a private conversation over the internet but they don't have a key that they both know. Despite the fact that Joe can read their messages, they had to find some way to create K.

Number Theory and Cryptography

The RSA protocol is presented here. Let's say Joe manages to catch C by listening in on him. (The number 26, in this instance, served as the value.) What options does he have? If he knew that $d = 37$, his life would be much easier since he would be able to decode the message in the same way as Alice has. To the best of our knowledge, in order to compute d, he would need to be able to factor N, which is a very difficult task. Is there anything else that he could do? Nobody is aware of anything that Joe is capable of doing that would not be challenging. Since Joe observed Me% N, some of you may be under the impression that he needed to find a solution to the discrete log problem rather than the factoring problem. We already have the value of M and are looking for e in the discrete log issue for Me mod N. The situation is exactly the opposite for Joe; he is aware of e but is looking for m. It is thought that this is a challenging problem, and it is also thought that it is comparable to factoring. How come Alice's method of decryption is successful? In general, she is given the value C, which is calculated as Me% N, and she determines C d as (Me) d equals Med (mod N). You may remember that ed equals 1 (mod (N)). Therefore, ed equals 1 plus some integer k multiplied by N. as a result.

$$M^{ed} = M^{1+k\phi(N)} = M \times \left(M^{\phi(N)}\right)^k$$

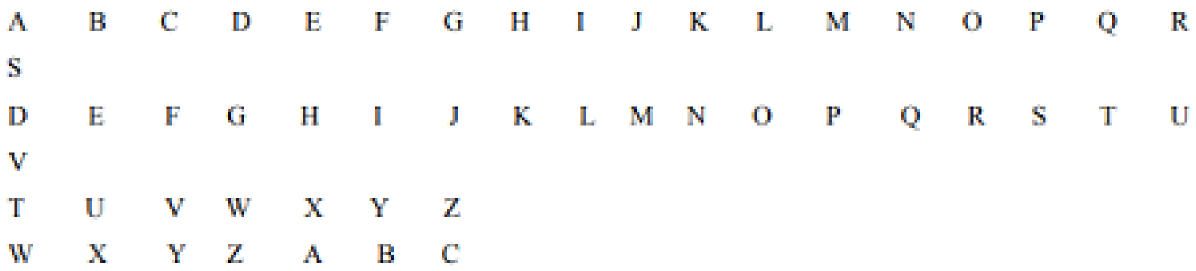
Since $gcd(M, N) = 1$, M is a unit (see Example 14) and so, by the property at the end of Example 14, $M\varphi(N) = 1 \mod N$. Thus

$$M^{ed} = M \times (1)^k = M(\mod N)$$

Due to the fact that 1 less than M is less than N, we have successfully retrieved M rather than ”mod N.” The RSA protocol is not a good scheme for amateurs to set up for themselves, and setting it up on their own is not recommended. Both p and q must have a large number of digits in their prime forms. Careful consideration needs to go into the selection of e and d. We need to be certain that the value of gcd(M, N) is 1. Because (N)/N = (1 1 p)(1 1 q), it is quite near to 1 for p and q that are very big. Therefore, the likelihood of picking a message M that is incorrect—that is, a message that is not relatively prime to N—is fairly low.

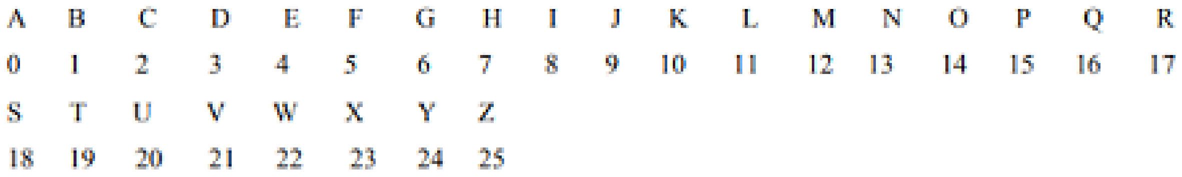
Caesar Cipher Key Cryptography

Around the year 50 B.C., the famous Roman ruler Julius Caesar utilized a cryptographic technique that is considered to be one of the oldest. Caesar spoke with Marcus Cicero through the use of a simple substitution cipher. In this cipher, each letter of the alphabet is substituted with a letter that appears three positions farther down the alphabet. with the most recent three letters returning to the initial three letters in the sequence. Below the letter that represents the plain text, the substitution alphabet for the Caesar cipher is presented as:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S																	
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V																	
T	U	V	W	X	Y	Z											
W	X	Y	Z	A	B	C											

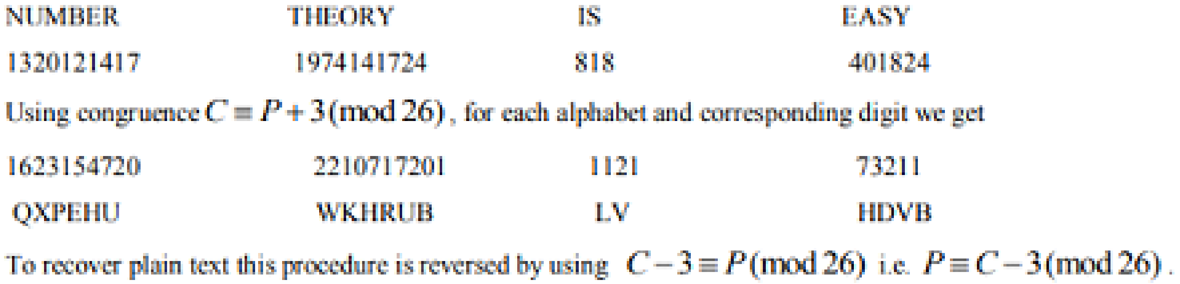
For Example: The phrase NUMBER THEORY IS EASY is altered to read as QXPEHU WKHRUB LV HDVB. The Caesar cipher may be defined in great detail with the use of congruence theory. The first step in representing any plaintext numerically is to convert the characters in the text into digits using a correspondence system such as



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
S	T	U	V	W	X	Y	Z										
18	19	20	21	22	23	24	25										

Now if P is the plain text and C is the cipher text then $3(\mod 26) + P \equiv C$.

For Example:



NUMBER	THEORY	IS	EASY
1320121417	1974141724	818	401824

Using congruence $C \equiv P + 3(\mathrm{mod}\ 26)$, for each alphabet and corresponding digit we get

1623154720	2210717201	1121	73211
QXPEHU	WKHRUB	LV	HDVB

To recover plain text this procedure is reversed by using $C - 3 \equiv P(\mathrm{mod}\ 26)$ i.e. $P \equiv C - 3(\mathrm{mod}\ 26)$.

Uses of Cryptography

Cryptography has maintained its significance over the ages, serving mostly as a means of communication for militaries and diplomatic missions with the emergence of the internet and electronic trade. The use of cryptography has grown more important to the operation of the global economy. Sensitive information such as bank records, credit card reports, passwords, and private information is encrypted and then updated in such a manner that, hopefully, it is only comprehensible to the individuals who should be authorized to have access to it, and it is undecipherable to anybody else. Cryptography is another method that is known to be both effective and practical in securing information that is sent via public communication networks. These networks may include those that use telephone lines, microwaves, or satellites.

3 Conclusion

In this article, we come to the conclusion that every instrument in the field of number theory plays an important part in the process of cryptography to hide information. In cryptography, several of the techniques from number theory, such as prime numbers, divisors, congruencies, and Euler's 'function, play a vital part in the protection of sensitive information. Both Caesar ciphering key cryptography and RSA public key cryptography make advantage of the congruencies in their respective processes. In the context of algebra and number theory, this provides an overview of cryptosystems.

References

[1] B. Beckett, *Introduction to cryptology*, Blackwell Scientific, (2010).

[2] A. Menezes, P. Van Oorschot and S. Vanstone, *Handbook of applied cryptography*, CRC Press, (2009).

[3] J. Seberry and J. Pieprzyk, *Cryptography: an introduction to computer security*, Prentice-Hall, (2006).

[4] R. P. Burn, *A pathway into number theory*, Second edition, Cambridge University Press, (2007).

[5] K. H. Rosen, *Elementary number theory and its applications*, Addision-Wesley, (2012).

[6] David M. Burton, *Elementary Number Theory*, 2nd Edition, UBS Publishers.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th Ed., Clarendon Press, (2013).

[8] Gilles Brasssard, *Modern Cryptography : A Tutorial*, Lecture Notes in Computer Science, Vol.325, Springer-verlag, (2013).

[9] Niven Zuckerman and Montgomery, *An Introduction to the Theory of Numbers*, 5th Ed., New York: John Wiley and Sons, (2011).

[10] Neal Koblitz, *A course in Number Theory and Cryptography*, New York: Springer Verlag, (2010).

[11] R. Cramer and V. shoup, *A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Cipher text Attack*, Springer-Verlag, Berlin, (2010).

[12] Simon Singh, *The codebook*, Anchor Books, (2008).

[13] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag (New York), (2009).