JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 109-115
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1446

Use of Mathematical Concepts to Achieve High Levels of Security in Cryptography

Rakesh Chandra Bhadula
Department of Mathematics, Graphic Era Hill University, Dehradun, Uttarakhand, India 248002

Abstract

Encryption, the process by which plaintext (readable information) is transformed into ciphertext (meaningless symbols), was essentially equivalent with cryptography until the advent of modern computing (decryption). To prevent unauthorized access, a sender of an encrypted (coded) communication only reveals the decryption (decoding) method to the intended receivers. Changing the letter or number on the outer disk with the letter right beneath on the inner disk is all that's needed to encode a message. The proposed work creates a novel cryptographic technique where the key is the number of multiples of mod n using Laplace transforms. The Laplace transform has recently found a new use in the world of cryptography, which we describe here. In this research, By encrypting the plaintext using the Laplace transform of an appropriate function and decrypting it with its inverse, we provide a revolutionary iterative method to cryptography. Encryption is frequently employed by organizations and even governments to protect confidential information online. The techniques of cryptography owe a great deal to the contributions of mathematics.

Keywords: Cryptography, Mathematical, Security, Private-Public Key, Laplace transform

Introduction

The basic notions and theories behind cipher systems think of the set of all potential messages as a series of transformations into the set of all possible cryptograms. Cryptography, the science of developing protocols for enforcing security on digital systems like computers and networks, is based exclusively on discrete mathematics. One reason for this is because digital data is sent in "bits," which are essentially independent units. In order to design and crack numerical passwords, cryptographers rely on number theory, a subfield of discrete mathematics. Cryptographers need a strong foundation in number theory to demonstrate they can create safe passwords and encryption techniques due to the high stakes and sensitive nature of the data being protected.

Cryptographic algorithms in the modern era are built on the foundation of mathematical theory and computer science practice, with the goal of making it as difficult as possible for an opponent to break them in practice. While it is conceivable in theory to crack a well-designed system, doing so in reality is very unlikely. The term "computationally safe" is used to describe such systems if they have been constructed effectively; nonetheless, theoretical advances and faster computer technology need the ongoing reevaluation and, if necessary, adaption of these designs. Although information-theoretically secure schemes, such as the one-time pad, are invulnerable to attack, the best theoretically breakable but computationally secure techniques are much simpler to implement in practice. The proliferation of cryptography tools in the Internet Age has prompted a slew of new legal questions. Because to its potential for espionage and sedition, several countries have restricted or outright banned the use and export of cryptography, seeing it as a weapon. Keys to encrypted documents crucial to an investigation may be demanded by law enforcement in a number of nations according to recent laws. Cryptography is also crucial in digital media copyright infringement disputes and digital rights management.

Literature Review

Vincent P M, Durai & Iqbal, S.A. & Bhagat, K. & Kushwaha, K.K. (2013) The purpose of networking is to allow devices located in different physical locations to interact with one another and exchange data and other resources. These days, networking is utilized for everything from online shopping and banking to social media and newsgroup discussions to file sharing and the dissemination of important information. The administrator restricts access to these networks by implementing and enforcing a set of rules and regulations known as network security. The term "network security" is used to describe any measure taken to safeguard a network. Having a safe and secure network is a powerful and fruitful convenience. Each time there is concern that security may be compromised or a weakness could be exploited, a danger occurs. Instead of relying on a single layer of protection, which may be breached at any moment, our method uses numerous levels of security to secure sensitive data.

Adhikari, Mahima & Adhikari, Avishek (2014) Chapter 12 discusses applications and kicks off a study of cryptography. The term "cryptography" is common parlance in today's fast-paced digital culture. Several sites regularly use various forms of encryption, whether intentionally or not. From logging onto a computer to sending an email to using a PIN to withdraw cash from an ATM to sending a text message to making an online purchase to moving money digitally from one bank account to another, encryption is used in almost every aspect of modern life. In all such situations, secrecy in either the conveyance of information or its concealment is required. So, cryptography is related to safety in some way. Questions like "What is cryptography?" are to be expected. What role does it play in typical situations? In this chapter, we are introduced to cryptography and given an understandable and mathematical overview of the topic along with its main aim. Specifically, Ancient ciphers all the way up to contemporary ideas like public-key encryption, signature systems, secret sharing, oblivious transmission, and more are shown here using mathematical approaches mostly based on modern algebra. Finally, we discuss some of the difficulties in using the free software SAGE to build the RSA, ElGamal, and Rabin public key cryptography systems.

Srungaram, Vasundhara (2016) Number theory has a rich history of theoretical investigation. The primary motivation for these studies, which date back centuries, is improved comprehension of the abstract theory. As an understanding of the qualities of numbers is crucial to the advancement of not just mathematics but all sciences, this is an area in which additional research is desperately needed. Incredible progress has been made. Connections between, on the one hand, classical mathematics and, on the other, new ways for attaining improved security of data transmission, are among the surprising elements of contemporary technological breakthroughs. In this study, we explain how current cryptography, including public key cryptography and private key cryptography, may be used to secure sensitive information.

Silverberg, Alice (2013) We introduce mathematicians to completely homomorphic encryption. With the encrypted data Enc (m1),..,Enc (mt) and any efficiently computable function f, an unauthorized third party may generate an encrypted version of f(m 1,,m t) without having access to the decryption key or the original data m1,…,mt. Using concepts from algebraic number theory and the geometry of numbers, Craig Gentry has just found a solution to this issue. We provide some context for the development of cryptography, demonstrate various completely homomorphic encryption algorithms, and talk about the challenging mathematical difficulties at the heart of cryptography's security.

Sikha, M. Suchithra, P. Prabha, & P. Pinchu (2014) found that although many engineering and computer science curricula include at least two security-related courses, students often have little opportunity to apply what they learn into practice. Security-solving cryptographic algorithms rely on niches of mathematics like modular arithmetic, probability theory, and number theory. However, students have trouble grasping the ideas because of the advanced mathematics that underlies them; this calls for a radical overhaul of our pedagogical approach. It is important to integrate interactive pedagogical tools gradually alongside traditional information in a manner that facilitates learning of both. This paper details an Excel-based interactive visualization tool that explains the mathematics underlying popular cryptographic protocols to students. Students with varying mathematical abilities are taught how to use a Microsoft Excel spreadsheet to conceptualize and apply complex mathematical concepts, and many well-known public key methods are covered.

Private and Public Key Cryptography

To grasp the significance of mathematics in cryptography, it is necessary to first familiarize oneself with it use in certain cryptographic procedures. The difference between private and public key cryptography is crucial, but understanding it requires looking closely at what a key is and why it's used. A key is a piece of data that allows both the sender and the recipient to encrypt and decode a communication. Go back to the Caesar cipher we discussed before as an example. Each letter in this cipher is shifted to the right by 23 positions. The cipher key is thus the number 23. In contrast to the encryption key, the decryption key is disguised in this case. Keeping in mind that there are 26 letters in the English alphabet, remember that moving each letter to the right by 23 is the same as shifting each letter to the left by 3. If you move each letter in the encrypted message three times to the right, you'll be back to the original letters. Thus, the answer to deciphering this message is 3. The recipient usually just needs the decryption key to understand the message. In order to encrypt using a private key, only one key has to be used. This key serves as both a means of protection and decryption. As a more secure alternative to private key encryption, public key encryption makes use of a pair of keys: a public and a private one.

Finite Fields

Say we have a set S, and that the set of ordered pairs (s,t) where both s and t are in S → S ×S. S is mapped into itself through the binary operator, *. Remember that the corresponding (s,t) in S ×S must itself be a part of S. A group G is a set with the following characteristics:

- **Associativity:** For any a, b, $c \epsilon G$, $a * (b * c) = (a * b) * c$.
- **Identity:** It is true that for each a ϵ G, there is an element e such that $a * e = e * a = a$
- **Inverse:** There is a corresponding inverse element, a $^{-1}$, for each a ϵ G. $a + a^{-1} = a^{-1} + a = e$.

If the following property also holds, we refer to the group as an abelian group:

- **Commutativity:** For any a, $b \epsilon G$, a $*$ b = b $*$ a.

A ring is a set R satisfying the following conditions for its binary operations + and ·

i. With +, R is an abelian group.

ii. The logical negation · is associative in binary.

iii. The principle of distribution holds. This means that any

$a, b, c \epsilon R, a \cdot (b + c) = a \cdot b + a \cdot c$

If the following also true for a given ring, we refer to it as a field:

- Commutativity of the binary logical operation ·.
- As a group, the non-zero components of R fall under

A field with an infinite number of elements is not considered finite. The set of all finite fields mod p is called the finite field $\mathbb{F}p$.

Key Exchanges over Finite Fields

Many crucial uses in cryptography may be found for the finite field $\mathbb{F}p$. The discrete logarithm issue is very important. Keep in mind that the powers of a primitive root, denoted by g, create the complete group $\mathbb{F}p$. Finding an $x\epsilon\mathbb{F}p$ such that g ^{x} = h (mod p), where g is a primitive root, and h is any non-zero integer in $\mathbb{F}p$, is known as the discrete logarithm problem. The formula for the discrete logarithm is x = log$_g$ h. If you multiply g by itself x times, you'll find that h = $g \cdot g \cdot \ldots \cdot g$ $(mod\ p)$. Finding log$_g$h is equivalent to determining how many times g must be multiplied by itself to get h. The discrete logarithm may be calculated in a straightforward manner by iteratively trying different powers of g until one is found for which g^i = h (mod p). Checking the powers of 2, 2^0, 2^1, . . . 2^7 yields the result that 2^7 = 7 (mod 11), hence this is one way to identify and a such that 2^x = 7 (mod 11). Unfortunately, any huge prime number makes this approach exceedingly challenging. Discrete logarithm problems are at the heart of the calculations behind both the Diffie-Hellman and ElGamal key exchanges.

Number Theory and the Rsa Cipher

The RSA Cipher is a great illustration of how concepts from basic number theory may be put to use in the real world. You'll notice as you read this part that we've excluded a lot of contexts for the definitions and theorems presented, leaving just the essentials for later memorization when we master the RSA cipher. There are a lot of great resources out there if you want to learn more about any of these issues.

Definition 1. Let's pretend a and b are two numbers with a=0 and b=0. We say that a divides b, or that an is a divisor of b, if there exists an integer c such that b = ac. The symbol a | b, which may be interpreted as "a divides b," will be used often.

Lemma 1. Let's pretend a and b are two numbers that have the common divisor d≠0. In other words, for all positive integers r and s, d | (ra + sb) = d.

Proposition 1. For a=0, if we have two positive numbers a and b, we can find a unique pair of integers q and r with 0 ≤ r < a such that b = aq + r. When we divide b by a, we get q as the quotient and r as the remainder.

When we do long division, we get a quotient and a residual. It is standard practice to write the result of long division as $\frac{b}{a}$= q + $\frac{r}{a}$, however this statement is equal to the one provided in the premise above: b = aq + r.

Definition 2. The biggest integer c that divides both non-zero integers a and b is called their "greatest common divisor." We shall use the old notation throughout this essay, even though the correct form is gcd (a, b) = c. We propose that a and b are relatively prime if and only if their greatest common divisor is 1.

Finding the largest common factor between two positive numbers may be a very helpful calculation. The Euclidean algorithm is the name for this method. Given that a and b are positive integers and that a > b, we may write d = gcd of a and b. (a, b). Using Proposition 1, we can express b = aq1 + r1 for every 0 ≤ r1 < a. It follows that d | r1 because r1 = b-aq1, given that d | a and d | b. Hence, d is a factor of both a and r1. Following this, we may express an as a formula: a = r1q2 + r2. Because d | a and d | r1, we may write r2 = a-r1q2 to get d | r2. We may draw the same conclusion for d, which is a common divisor of both r1 and r2. We repeat this procedure until we find a point where r_{k+1} = 0. Hence, d = rk follows. As the remainders are decreasing with each iteration while being non-negative by definition, we know that the process will end when the residual becomes zero. While it's obvious that rk is a divisor of both a and b, we're going to skip over the demonstration that it's also the greatest common divisor. Let's go through several instances to get a feel for this method.

Example: Find gcd(522, 213). First divide 522 by 213.

522 = 213(2) + 96

Next, proceed to divide 213 by the remaining 96.

213 = 96(2) + 21

96 = 21(4) + 12

21 = 12(1) + 9

12 = 9(1) + 3

9 = 3(3) + 0.

So gcd(522, 213) = 3.

Theorem 2. (Arithmetical Primacy Theorem) For each positive integer n, there exists a unique product of primes that expresses n.

Examples: 10 = 2 · 5, since 2 and 5 are prime. 7800 = 23 · 3 · 5 2 · 13 because 2, 3, 5, Nevertheless, 13 is also a prime number. As 23 is prime, 23 equals 23.

Definition 3. If two numbers $m|(a-b)$ have the same remainder when divided by our modulus, we say that they are congruent modulo m, where m is a positive integer. For this, we use the symbolic notation a ≡b (mod m), which may be interpreted as "a is congruent to b mod m."

Examples: Because 10 | (23-3) = 20, the number 23 is equal to 3 modulo 10. Because 13 | (59 -(—6)) = 65, we also get 59 ≡6 (mod 13). Nevertheless, 5 ∤ (7 -3) = 4 leads us to the result 7 6 ≢3 (mod 5).

Definition 4. For any pair of positive integers n and a, the multiplicative inverse of an is the number d such that ad 1 (mod n). (mod n). $d = a^{-1}$ is a common symbolic representation of this d.

Finding multiplicative inverses modulo n may be made easier with the help of the Euclidean Algorithm that we discussed before. Using the technique, we may prove that gcd(a, n) = 1 as a first step toward our goal. Next, we use the obtained equations to figure out which values of d and c would result in 1 = ad + nc. If this is the case, we will know that a modulo n has multiplicative inverse equal to d. As proof, we may look at the solution set for the equation 1 = ad + nc modulo n and see that:

1 ≡ ad + nc ≡ ad + 0 ≡ ad (mod n)

Example: Determine 9 modulo 32's multiplicative inverse. In the left-hand column below, you'll see the results of using the Euclidean Algorithm to prove that gcd(32, 9) = 1. The right-hand column below displays the residual from each step as we answer the problem. These equations involving the remainder are then given labels in the opposite order.

32 = 9(3) + 5 → 5 = 32 − 9(3) (1)

9 = 5(1) + 4 → 4 = 9 − 5(1) (2)

5 = 4(1) + 1 → 1 = 5 − 4(1) (3)

We will now solve these equations in reverse order. To begin, let's take the third-to-last equation, which gives us 1 = [5-4(1)]. Next, we plug in the solution from the second-to-last equation (2), where 4 = [9- 5(1)], into the original formula. Our words are then grouped and distributed to provide the formula 1 = 9j + 5k for any values of j and k. Finally, to get the required equation in terms of 32 and 9, we will substitute 5 = [32-9(3)] (1) and again group our terms.

1 = [5 − 4(1)] (4)

= 5 − [9 − 5(1)] (5)

= 5 − 9 + 5 distribute

= 9(−1) + 5(2) group terms

= 9(−1) + 2[32 − 9(3)] (6)

= 9(−1) + 32(2) + 9(−6) distribute

= 32(2) + 9(−7) group terms

As a result, we may deduce that $9^{-1} \equiv -7 \equiv 25 \pmod{32}$. 9(−7) ≡ −63 ≡ 1 (mod 32) is a valid proof of this (mod 32).

New Mathematical Modeling for Cryptography

Definition 5: If the sender, the recipient, and anybody else with access to the message can all understand it, then it is plain text.

Definition 6: Cipher text is defined as the outcome of encoding a plaintext message using an appropriate scheme.

To create the Laplace Transform, we first need to ensure that f (t) is a function defined for all positive values of t.

$$L\{f(t)\} = F(s) = \int_0^\infty e^{-st} f(t)dt \quad (7)$$

if and only if the integral can be calculated. In this case, s is a real or complex integer serving as a parameter. When the Laplace transform is reversed, you get

$$L^{-1}\{F(s)\} = f(t)$$

Theorem: One kind of linear transform is the Laplace transform. If, that is.

$$L\{f_1(t)\} = F_1(s), L\{f_2(t)\} = F_2(s), \cdots L\{f_n(t)\} = F_n(s) \quad (8)$$

Then

$$\begin{aligned} &L\{c_1 f_1(t) + c_2 f_2(t) + \cdots c_n f_n(t)\} \\ &= c_1 F_1(s) + c_2 F_2(s) + \cdots + c_n F_n(s) \end{aligned} \quad (9)$$

Where the constants c1, c2,..., cn apply.

Some Standard Results of Laplace Transform

The Laplace transform of every function analyzed here is assumed to exist. Additionally, let's pretend that the letter N stands for the set of natural numbers. The subsequent Laplace transform solutions are considered:

1. $$\begin{aligned} &L\{\sinh kt\} = \frac{k}{s^2 - k^2}, \\ &L^{-1}\{\frac{k}{s^2 - k^2}\} = \sinh kt. \end{aligned} \quad (10)$$

2. $$L\{t^n\} = \frac{n!}{s^{n+1}}, \quad L^{-1}\{\frac{n!}{s^{n+1}}\} = t^n, \quad n \in N \quad (11)$$

3. $$\begin{aligned} &L\{t^n f(t)\} = \left(\frac{-d}{ds}\right)^n F(s), \\ &L^{-1}\{\left(\frac{-d}{ds}\right)^n F(s)\} = t^n f(t) \end{aligned} \quad (12)$$

Conclusion

Mathematics plays a crucial role in today's cryptography. In this paper, Here, we'll explore the mathematical applications of many distinct classes of cryptographic ciphers. As one examines the many cryptographic methods out there, the influence of mathematics becomes very obvious. But, as mathematics advances and security improve with each new cryptographic approach, so do the capabilities and understanding of potential attackers. Unlike other symmetric encryption techniques, Laplace Transform-based encryption is very secure. Algorithm implementations may be modified as needed. So, the use of mathematics in cyber security must also develop, just as mathematics itself develops through time. There are benefits and drawbacks to each encoding and decoding procedure outlined in the various cryptography methods.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 9, No. 1, 2018, p. 109-115
https://publishoa.com
ISSN: 1309-3452
DOI: https://doi.org/10.52783/jas.v9i1.1446

References

1. Vincent P M, Durai & Iqbal, S.A. & Bhagat, K. & Kushwaha, K.K. (2013). Cryptography: A Mathematical Approach. Indian Journal of Science and Technology. 6. 5607-5611. 10.17485/ijst/2013/v6i12.12.
2. Adhikari, Mahima & Adhikari, Avishek. (2014). Introduction to Mathematical Cryptography. 10.1007/978-81-322-1599-8_12.
3. Srungaram, Vasundhara. (2016). International Journal of Mathematics And its Applications Cryptographic Protocol.
4. Silverberg, Alice. (2013). Fully Homomorphic Encryption for Mathematicians. 10.1090/conm/606/12143.
5. Sikha & M, Suchithra & Prabha, Pinchu. (2014). An Interactive Visualization Tool for the Interpretation of Mathematical Concepts behind Public Key Cryptography. International Journal of Computer Applications. 90. 10.5120/15572-4199.
6. Sujitha S., Applications of Laplace Transforms in Cryptography, International Journal of Mathematical Archive, 4(3), 2013, 67-71.
7. Sukalyan S., Moumita S., DNA Secret Writing with Laplace Transform, International Journal of Computer Applications, Vol. 50 – No.5, July 2012, 44-50.
8. Vyavahare S., Bani Upmanayu, A, Cryptographic Scheme using Infinite Series and Laplace transform, Global Research Analysis, Vol.2, No.6 June 2013, 60-61.
9. Hiwarekar A.P., A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, 3(3), 1193-1197, (2012).
10. Hiwarekar A.P., A new method of cryptography using Laplace transform of hyperbolic functions, International Journal of Mathematical Archive, 4(2), 208-213, (2013).