International Journal for Research in Applied Sciences and Biotechnology

ISSN: 2349-8889
Volume-9, Issue-3 (May 2022)

www.ijrasb.com

https://doi.org/10.31033/ijrasb.9.3.18

Cryptological Mathematics

Dr. Kaushal Rana
Assistant Professor, Department of Mathematics, Dau Dayal Institute of Vocational Education, Dr. Bhimrao Ambedkar University, Agra, Uttar Pradesh, INDIA

Corresponding Author: rana.kaushal1966@gmail.com

ABSTRACT

The basis of cryptography is the requirement for different parties to share information, and only those international recipients have moved to the data. It is possible to achieve this in many other ways; the most common is to physically hide the data transmitted to all except those intended to receive it. Cryptography encompasses all methods of hiding the contents of messages, even if unauthorized third parties take over the message. It is possible to conclude that practices like disguised ink or small pin puncture over specified personality could be classified as cryptography. But this isn't the case as the attacker has not discovered the data that makes up the message but simply an additional disguise. These techniques, such as disguised ink, fall under the steganography umbrella. So, cryptography tries to provide the contents of a message inaccessible to any person who might intercept it but allows those who are intended to receive it to understand the significance of the content. The sender is able to encrypt the message while the recipient decrypts it. Apart from the security achieved through encryption, there are various other aspects of information security, such as authenticity, data integrity, and non-repudiation. Together, the fields that encompass various information security techniques are known as cryptography. The techniques and methods designed to attempt to reduce the effectiveness of cryptography are called cryptanalysis. Cryptology is a field of study that encompasses both cryptanalysis and cryptography. In the field of study of modern cryptology, it's important to know the strategies used in the field and the mathematical concepts utilized to study and improve the area. A large portion of applied mathematics in the modern age and, in particular, applied math has been centered on creating algorithms through which two parties can safely exchange information. Many of these algorithms have been released in the last 30 years; certain algorithms have been deemed insecure, while others have escaped examination for a long time. The algorithms, called key agreements, are particularly important due to their effectiveness for secure, fast encryption.

Keywords- Cryptological maths, cryptography, algorithms

I. INTRODUCTION

The evolution and usage of cryptology were slow and were developed independently across different cultures. Kahn provides a comprehensive description of the history of cryptology. It is very difficult to determine the precise date for the beginning of cryptanalysis. The inscriptions carved onto a wall of Khnumhotep II principal room, Khnumhotep II's burial chamber Khnumhotep II provide early evidence for deliberate modification to writing. The tomb is located within the village of Menat Khufu bordering the Nile in Egypt. The writings date back to about 1900 BC. The motivation behind the modifications made by the scribe was not one of concealment but to show authority and respect. The existence of these deliberate transformations indicates that the basic concepts that were underlying cryptography began to evolve within the society. In tombs built around 1900 BC, the process of transformation got more complex and intricate and more frequent. Different forms of writing were reportedly used in India. The Artha- 's-Astra was an important work on statecraft, which is believed to be written by Kautilya and was written between 321 BC and 300 BC. The work suggests that institutions of espionage exchange information with their spies through secret writing. Secret writing was mentioned in V-Vatsyayana's famous book on sexuality, known as the Kama-sutra, among the 64 different arts (or yogas) that women must learn and master. Another method of communication that is secret that originated during the time of India can be described as "nir-abh-asa." It is a communication using a fingers system in which the phalanges stand for consonants, and joints represent vowels. Traders and moneylenders still employ this type of communication. It also serves as the foundation for the use of sign language, which deaf and dumb people employ. Contrary to India, China did not achieve the same level of cryptographic abilities. This is due to the differences in literacy levels between the two nations. Comparatively to the case of China, India has an extremely high level of literacy. In China, writing was practised for a considerable period of time, but due to the low literacy level, cryptography became popular significantly later. A wise observation was given by prof. Owen Lattimore of the University of Leeds, "Although writing is very ancient in Chinese culture; literacy was limited to a tiny minority that writing anything was, to a certain degree, similar to writing in code." Therefore, it's reasonable to conclude that the primary driving reason for the rise in cryptography lies in individuals' need to communicate in a secure manner. Another reason for the growth of cryptography is to safeguard intellectual property. In Mesopotamia, an

ISSN: 2349-8889
Volume-9, Issue-3 (May 2022)

https://doi.org/10.31033/ijrasb.9.3.18

ancient tablet dating to 1500BC was discovered that contained the first known formula to make ceramic glazes. To protect this secret of the trade, it was written down in an encrypted version of Cuneiform. This encryption method demonstrates that the writer was trying to hide the information contained in the message written on the tablet. The technique relies on modifications to the message's text using correlations between phonetic sounds and their written equivalent. As the knowledge of glaze-making grew, the requirement for secrets dwindled as later formulas or descriptions were written with plain text. Since cryptography can be used to secure a secret, it's not surprising that unintentional recipients may try to discover why the message has been encrypted. The first example of active cryptography originates in the Arabs during the 7th century. Methods that were formalized, such as letter frequency analysis, were created in the next couple of hundred years. The concept of letter frequency analysis was widely known before it was when Subh al-a'sha (a massive 14-volume encyclopedia) was published in 1412. The data in Cryptography was due to Ibn ad-Duraihim, who lived between 1312 and 1361. He held various teaching and official positions across Syria and Egypt. The first cryptographic systems depended on modifications to the plaintext messages done by the individual who composed the text. When the difficulty of techniques grew, it was imperative to design tools or machines that could perform the cryptographic function. The first device specifically designed to be used for cryptography is referred to as "the scytale." The device was developed in the Fifth Century BC during the time of the Spartans who were among the most abrasive among the Greeks and was created to boost their military. It is composed of a wooden staff that is covered by an extended strip of leather or papyrus that is wrapped tightly in a way. It is possible to write secret messages on all the width of the staff. The strip is then cut and sent to the person intended to receive it. The words printed on the strip won't be understood until it's wrapped in batons of similar thickness. Another method was clever ways to use an astragal disk with holes that correspond to every letter of the alphabet. The thread moves through holes from one hole to the next, and the message is then written out. The receiver must reverse the process to discover what message it is, as threads are removed from the holes. Then, they must change the content. Modern cryptosystems use digital computers to perform hundreds of algorithms necessary to perform the most modern cryptographic conversions. In some cases, general-purpose computers don't suffice to handle the demands of modern cryptography, so specially designed hardware is created to handle the enormous volume of data to be encrypted and decrypted. In the middle ages, cryptology was tarnished by a stigma that persists in the present day - the belief that is ingrained in the minds of a lot of individuals that it is an art that is black. The practice of cryptology was associated with magic, as "spells" and recipes to cure curses were usually encoded. It also has a lot in common with divination because it is, to the uninitiated, it is apparent that extracting an understandable message from ciphertext is something similar to studying tea leaves or the length and interconnections of lines that one holds. Even in 1940, the U.S. referred to its Japanese diplomatic cryptanalysis with the magic of the code name. Contrary to the mystical view that surrounded the field of cryptology in the mid-century, the field of cryptology has been steadily progressing, though slowly. The 1600s witnessed a significant breakthrough with the introduction of words as a mnemonic to help mix an alphabet used to cipher. The increasing number of diplomatic messages sent out across the world's west, and the demands of military organizations required constant advancement. The importance of cryptology for the military continues to grow. There are numerous instances of wars where the outcome has been drastically changed based on the information obtained through the analysis of messages intercepted by cryptanalysis. In the same way, there are numerous scenarios that could not occur if the information were not protected by cryptography. The year 1914 was the first time England stressed the significance of data when their initial offensive action in the war against Germany was to cut off the transatlantic cables that connected Germany. Germany was required to communicate using radio or enemy-controlled cables. The only defense was to safeguard the communications by using cryptography. At the time, England had no department that dealt with cryptograms sent by enemies. The department was eventually able to help when Sir Alfred Ewing began to rally expertise to cryptanalysis German messages. The initial progress was slow even with the aid of a German codebook, which was found from a shipwreck within the Baltic. The department was later referred to as "Room 40." After the war, it was believed that between October 1914 and February 1919 Room 40 was able to solve more than fifteen thousand German intercepts. A single of the more well-known intercepted messages, which was later decrypted, was referred to as the "Zimmermann Telegram." The telegram was written through German Foreign Minister Arthur Zimmermann. German Foreign Minister Arthur Zimmermann, on 16 January 1917, to an unnamed German ambassador to the United States. After "Room 40" solved the telegram just over a month later, the English military was informed that Germany would be preparing to conduct an unrestricted war on submarines, and they would not cease when this would provoke the United States into joining the war. Instead, they offered to bring Mexico into an alliance so that Mexico could take back the territory it had lost. After the U.S. was informed, this led them to take action, and they abandoned their neutrality and became a part of the war.

The result was a tipping point for Germany Mathematical and Cryptology As we've seen earlier, the first cryptographic systems utilized very simple

ISSN: 2349-8889
Volume-9, Issue-3 (May 2022)

www.ijrasb.com https://doi.org/10.31033/ijrasb.9.3.18

techniques. They typically used codes that can be used as direct substitutions for phrases or words in the text message. As time passed, methods began to utilize rules that describe the transformations of specific characters, e.g. the Caesar cipher outlines a simple transformation rule: a D, b – E, . . . Z C. The most significant innovation included the usage of words that determined the results of the transformation rules. The cryptographic function can remain unchanging and be made public by using keywords. Security is contingent on the secret keyword. It has been established that the attacker knows the whole functioning of the security system. Security is based on the principle of keeping secrets about the key. This is commonly referred to as Kerckhoff's principle. Along with improvements to the cryptosystems and the techniques to analyze were enhanced. Initially, this was made possible through improvements in language analysis that led to the application of analysis based on the frequency of letters and the development of methods that use phonetic relationships of the language employed. As cryptology grew, it became more mathematical. The majority of cryptographic functions originate from mathematical issues which are difficult to resolve. These are issues that stem from various disciplines, including the mathematics of geometry and number theory, and the lattice concept. The outcomes of various fields are also able to enhance encryption procedures in the event that reasonable assumptions are made. This can be seen in the evolution of modern block ciphers, pseudorandom numbers generators, and various cryptographic primitives.

Furthermore, the methods used to analyze messages with cryptography benefit from mathematical expertise and techniques. Probability theory is extensively used and is essential to the investigation and creation of the area of non-deterministic threats. Recent developments in the area of the theory of numbers have led to more efficient systems based on the difficulty of factoring out the results of large primes, also known as the discrete logarithm question. This subject is a part of a variety of mathematical fields and has served as the source of inspiration for some of the most innovative mathematical concepts. In this article we will give short descriptions of the basics of cryptography and cryptanalysis through reference and using the fundamental mathematical concepts.

II. THE CONCEPTS

The primary function of cryptosystems is to permit two people, Alice and Bob (as they are generally depicted in literature) to communicate through an unsecured channel in order to prevent their adversary, Oscar, from being in a position of understanding the conversation. To achieve the purpose, Alice transforms her original textual message into one that is only understood only by Bob and the encryption. This is referred to as encryption. Suppose an attacker is determined to penetrate a cryptosystem designed to breach the encryption of messages in a detrimental or negative manner. In that case, it is possible to attack every cryptographic protocol, algorithm, or implementation. The focus of this chapter is the cryptographic algorithms. However, when we look at the process of cryptanalysis in future chapters, there are a variety of methods employed to target this protocol.

The algorithms employed to create key cryptographic encryption are among the foundations for the security of cryptosystems. The class of algorithms that is considered most important is the encryption/decryption algorithm. A more comprehensive definition of cryptography can be described in the following way:

A cipher can be described as a 5-tuple (P C, P, E D) comprised of:

1. A finite number of plaintexts. C is a finite set of ciphertexts. The key space K is an infinite key space comprising 4 keys. Each key is characterized by an encryption rule eKE and an equivalent decryption rule dK D, under the requirement that the functions eK C + C and dK C + P satisfy dK(eK(x)), which is an x. So, in order for Alice and Bob the ability to talk, they must choose the appropriate key to utilize. Alice can encode her message with eK , and then send an encrypted text message to Bob via a possible unsecured channel. Once Bob receives the ciphertext it will use dK to extract data from the text. There are many encryption methods available, and it's important to establish broad categories into which different ciphers fall. Different kinds of ciphers exist. Block ciphers work by transforming a block text into encrypted blocks (e.g. DES is a 64-bit cipher operating with blocks). Stream is a cipher that uses plaintext input to produce the output stream with encrypted text (e.g. key-stream generator that creates streams of bits that can be combined together with input streams via an operator or bitwise (denoted by the XOR) making an output stream). The symmetric cipher uses the same encryption key and decryption. The cipher that is asymmetric utilizes different encryption keys and decryption. It's usually paired by the chance that encryption keys may be revealed without affecting any security measures used by the system (e.g. RSA).

We will go over some basic encryption techniques that were employed in the past, but due to advances in computer power and cryptanalysis, these techniques are now considered insecure. These methods could be an excellent starting guide to understanding the basic concepts of ciphers, as well as the many ways they are used for encryption as well as decryption.

Shift Cipher in the ciphertext alphabet, letters are constructed using a plaintext alphabet, increasing the plaintext alphabet and its relationship with the plaintext alphabet by a certain amount. The shift cipher is described using modular algebra. It is essential to note that a corresponds to b modulo M. The cipher (mod

mod) is a (mod m), meaning it is that the m variable is divided in b and in which case the m is within the modus. This is how we define Arithmetic within the Zm Ring. Zm, which is the set{ . . . |, the m-1/m using|1 by using|1 by} two operations that are + and. The calculations are exactly similar to the ones used for real numbers, however, the result is diminished by the number m (i.e. replaced by the remainder after being multiplied by m).

Affine Cipher is a reverse mapping of the alphabet from plaintext to ciphertext with the help of the following type of operations: e(x) = ax + b mod 26, where A as well as B form the keys for the cipher. These operations are referred to as affine functions, and that's why it's the name of this cipher. It is clear that when you have a value greater than 1, the affine cipher can be diminished to one that is an alteration within the encryption. For this function to work as a cipher we have to demonstrate the existence of an inverse function capable of determining the message. We must also demonstrate that the inverse function is exclusive. Thus, we require knowledge of the concept of the affine. It is clear that we need to establish it is true that e(x) has an injective nature, and define the conditions in which this might be the case. To determine what we need to know, we'll examine the math of congruence, specifically linear congruence.

Substitution Cipher:

A substitution cipher is a unique one that has been utilized for many years. In this cipher, the letters in the plaintext are replaced with letters randomly chosen from a permutation plaintext alphabet. The permutation, which is represented by the letter P, serves as the key for the cipher. It also gives an explanation of this cipher for substitution.

The shift cipher and the affine cipher as described previously, are distinct cases of substituting a cipher. The primary feature of the affine or the shift cipher is that it chooses one permutation out of all 26! Permutations that could be possible as well as an explanation of the cipher, which includes an algorithm to construct for the permutation.

Vigenere Cipher:

Through the substitution cipher, as well as the particular cases of it once the key is selected, every letter of the alphabet in plaintext is linked to the same letter from the alphabet in the text of the ciphertext. This is why these ciphers have been called monoalphabetic. For example, the Vigenere cipher, which is named after Blaise de Vigenere in the 16th century, is an alphabetic cipher that is polyalphabetic. The reason is that the same letter of the plaintext alphabet can be assigned to an individual ciphertext letter in accordance with the position it appears within the plaintext.

Hill Cipher can be described as an alphabetic polyalphabetic cipher that was created prior to the ciphers prior to its. Hill created it; Lester S. Hill created the cipher and the specifics of the cipher were initially revealed in a study titled "Cryptography of an alphabetic one" that was published by The American Mathematical Monthly in the months of June and July 1929. The basic idea behind it is to make use of lines of combination to transform plaintext words into the ciphertext block. If characters make every block there is an m-linear equation which will result in the ciphertext block that is made up of the number of letters. To demonstrate this, we change the plaintext into a form of a series of numbers, that is, if the plaintext is derived from 26 letters of the English alphabet, then we could transform it into the equivalent numbers using Z26. Linear numbers can be computed using Z26 with modulo Arithmetic.

III. CRYPTANALYSIS

Cryptanalysis studies methods used to hack into cybersecurity systems for information. The techniques include trying to obtain the plaintext from the ciphertext of a message, without access to an encryption key or trying to retrieve the encryption key, even though only the ciphertext has been identified.

Applications and their implications Cryptanalysis isn't only a theory-based subject. In fact, it's an area that has numerous real-world applications that have real consequences. In the past, many wars, the results have changed dramatically due to the information obtained by analysis of messages intercepted by cryptanalysis. The advancement of cryptanalytic attacks and the speed of implementations of cryptanalytic algorithms have rendered methods like DES unsecure. This has a direct impact on banks as many banks utilize this DES algorithm to protect PIN codes and other sensitive information. So banks that continue to utilize DES could be at risk of fraud. The use of cryptography is not just crucial to military institutions as well as diplomatic communications, or large corporations, but instead, it is now becoming relevant to the average person in a daily civilian setting. It is used to secure the pin number and passcode, as well as to allow information entered on World Wide Web-based forms to be protected and also to stop unintentional listening in on cell phone calls. However, the design of the cryptosystem could result in the application not securing individuals as they were intended to. The majority of mobile phones utilize an algorithm called A5. The algorithm has since been broken, which means that the phones could be "cloned" and an attacker could be able to access the cell phone network, and a victim could be illegally charged for the duration. There is also the possibility for an attacker to decrypt phone call information and recover the complete conversation. In another instance of currently being conducted cryptanalytic experiments one can look at one of the protocols, the Wired Equivalent Protocol (WEP) is a security protocol that is used in the link layer for wireless network cards that utilize the 802.11 standards

it was recently shown to be insecure following the protocol was examined for cryptanalysis and found to have flaws. This WEP protocol is designed to offer wireless 802.11 networks that are secure as an existing network by cables, which cannot be accessed via wire-tapping. This is a problem for the majority of networks that use 802.11 wireless connectivity as there is the possibility to listen in on any communication. To make matters worse it is necessary for the hardware implementation to be upgraded. The ongoing efforts to improve cryptanalytic analysis show the difficulties involved in building secure systems and also how difficult it is to implement security systems. Poor designs or implementations can have negative consequences for individuals as well as organizations. In previous times, the field of cryptology has not become an unchanging field. It's the game of spy against surveillance, where new cryptosystems are created to defend against new attacks and new vulnerabilities are discovered that can cause damage to new cryptosystems. Cryptography is continuing to evolve to meet the requirements of users communicating using new techniques and at new degrees of security. It will also be able to protect against the latest theoretical attacks on cryptanalysis (new methods) and attacks that are made more practical due to advances in related areas in mathematics (e.g. more efficient algorithmic factorization) and computer technology e.g. speed improvement massively parallel computers enormously distributed computer systems, different types of computing, such for quantum computers).

IV. CONCLUSION

Starting with the simplest cryptosystems like affine encryption, and Vigenere encryption, the key principles were explained. I then discussed the idea of cryptanalysis and demonstrated the ways in which techniques can be used to attack cryptosystems that are simple. Based on this information it is possible to hack block encryption. They are the foundation of cryptographic algorithms. By providing brief descriptions of various block ciphers, we can see that the field of study has significantly advanced throughout the second quarter of this century. Following a discussion of fundamental concepts behind block ciphers, I gave an extensive description of the DES algorithm. This is an excellent setting to discuss the ways differential cryptanalysis could be employed to hack blocks of encryption, for example, DES. The methods that are learned from differential cryptanalysis can be used to hack pseudo-random number generators. The principle allows for a greater understanding of other cryptosystems. I also presented an overview of linear cryptography. This technique is, in many ways, equivalent to differential cryptography. Linear cryptography has also led to one of the biggest and most powerful attacks against cryptosystems based upon DES. I also discussed Knapsack cryptosystems. They are founded on the subset-sum formula and provide a fascinating way to make use of the results of theories like lattice theory and integer programming. Pseudo-random generators are vital in many cryptosystems and can be utilized to create encryption keys or trigger the block-ciphering mode. I will discuss PRNGs, among them one is the Blum Blum Shub (BBS) generator which could be thought of as being one of the important algorithms. This BBS generator is built with mathematical principles that have been derived from the area of mathematical theory. This allows for a deep study and understanding which is the reason for this, it's now possible to offer an analysis of mathematical concepts that support an acceptance for BBS generators as a secure PRNG. BBS generator for a safe PRNG. In order to understand the way that cryptosystems function, it is crucial to realize that one of them usually comprises many distinct elements. In addition, a secure system is required to be able to stand up against an array of diverse attacks. Each of these elements or attacks are built on distinct theories and techniques. To provide an overall overview, I have included brief descriptions of a variety of concepts and algorithms. This included the functions of hashing, digital signatures, keys distribution, key agreements, subliminal channels, secret sharing, differential power analysis as well as zero-knowledge proofs. Cryptology is a wide and rapidly growing field. The goal of this review was to provide a general overview of the field that can be used to better understand the way that this field is interconnected and the importance of mathematics to the subject, and also to draw attention to areas that have been deemed as crucial for the advancement of the field. With this information at hand, it will be possible to pinpoint specific subjects of interest or areas that require more study and then begin deeper research.

REFERENCES

[1] Wiles, K. (2021). Explorations and Applications of Modern Cryptology.

[2] Bauer, C. (2021). *Secret history: The story of cryptology*. CRC Press.

[3] Borys, T. of the Paper: Suggestion for an Integration of Cryptology into a Math Curriculum.

[4] Ramazan, E. R. O. L., & SAYGI, E. (2021). The Effect of Using Cryptology on Understanding of Function Concept. *International Journal of Contemporary Educational Research*, *8*(4), 80-90.

[5] Jara-Vera, V., & Sánchez-Ávila, C. (2021). Some Notes on a Formal Algebraic Structure of Cryptology. *Mathematics*, *9*(18), 2183.

[6] Karaçam, C., Algül, F. N., & Tavit, D. (2021). Transmission of Time and Position Variable Cryptology in Fibonacci and Lucas Number Series with Music. *Journal of Mathematical Sciences and Modelling*, *4*(1), 38-50.

[7] Jacox, L. M. (2021). *Using Classical Ciphers to Teach Mathematics in Secondary Education* (Doctoral dissertation, Elizabeth City State University).
[8] Bos, J., & Stam, M. (Eds.). (2021). *Computational Cryptography: Algorithmic Aspects of Cryptology* (Vol. 469). Cambridge University Press.
[9] Boersma, S. (2022). A Cryptologic Dinner Party. *Math Horizons*, *29*(4), 14-17.
[10] Yu, Y., & Yung, M. (2021). *Information Security and Cryptology*. Springer International Publishing.
[11] MATYSIAK, L. (2021). Generalized RSA cipher and Diffie-Hellman protocol. *Journal of applied mathematics & informatics*, *39*(1_2), 93-103.
[12] Hoborski, A., Hordyński, L., Kaszycki, L., Leja, F., Nikodym, O., Rosenblatt, A., ... & Żorawski, K. The Jubilee Congress for the 100th anniversary of the Polish Mathematical Society.
[13] Cheon, J. H., Lauter, K., & Song, Y. (2021). Editor's Preface for the Second Annual MathCrypt Proceedings Volume. *Journal of Mathematical Cryptology*, *15*(1), 1-3.
[14] Kaymak, Ö. Ö. A New Coding/Decoding Algorithm Based on k-Fibonacci Numbers. *ICAMΣ'21*, 147.
[15] Galbraith, S., Panny, L., Smith, B., & Vercauteren, F. (2021). Quantum Equivalence of the DLP and CDHP for Group Actions. *Mathematical Cryptology*, *1*(1), 40-44.
[16] Lauter, K. E. (2021). Private AI: machine learning on encrypted data. *Cryptology ePrint Archive*.
[17] Han, H., Zhu, S., Li, Q., He, Y., Wang, X., & Wang, Y. (2021). The cryptologic characteristics of circulant matrices. *International Journal of Innovative Computing and Applications*, *12*(5-6), 248-254.
[18] Pandey, A., Gupta, I., & Singh, D. K. (2021). Improved cryptanalysis of an ElGamal Cryptosystem Based on Matrices Over Group Rings. *Journal of Mathematical Cryptology*, *15*(1), 266-279.
[19] Bouftass, S. (2021). Symmetric encryption algorithms based on the mathematical structure underlying the three body problem. *Cryptology ePrint Archive*.
[20] Gjergji, M., & Lamagna, E. A. (2021). A web-based toolkit for exploring cryptography. *Journal of Computing Sciences in Colleges*, *36*(8), 53-62.

