ALGEBRAIC GEOMETRY AND MODERN CRYPTOGRAPHY

Dr. Mukesh Punia
Associate Professor
Department of Mathematics
S D (PG) College, Panipat-132103
Haryana

Abstract

The field of linguistics, along with the military and diplomatic spheres, has made use of one of the most significant applications of algebraic geometry, which is known as linguistics. It was stated that the Pharaohs were the ones who were the first to organize a discussion amongst the troops. In addition to that, he added that Arabs had tried their hand at encryption in the past. During the conflict, the Chinese employed a variety of different means to communicate with one another. Their goal was to interpret the signals in the incorrect way. This research is a broad study on science looking for numerous ways in English linguistics, as well as a message and a word of appreciation.

Keywords: *Algebraic, Geometry, Cryptography*

1. Introduction

In this day and age, it is of the utmost need to make use of the "encryption" technology in order to connect its worlds over open networks. And referred to the situation of human rights in Saudi Arabia. It is imperative that the confidentiality of the information be maintained at all times. There have been significant efforts made by people all around the globe to determine the most effective methods in which data flow may be streamlined and data can be concealed from detection. Be an excellent verification tool, developed specifically for all different types of ideas. Because an increase in the speed of the computer implies a reduction in the amount of time required for the computer to break or discover a particular encryption key, there is a need for encryption techniques that are particularly robust because the fast growth of the computer has a negative impact on the security of encrypted data. In addition to this, it utilizes encryption in order to secure sensitive information from unauthorized access attempts. Encryption is a method that may be used to safeguard communication channels as well as physical databases if other preventative measures are ineffective in thwarting an unauthorized access attempt. In addition, throughout European history, codes and codes have been employed to assist in the planning of the overthrow of rulers, the drawing up of war plans, and the sending of critical communications. George was presented for the sake of the American Revolution. Washington is equipped with a system of spies who report on the capabilities and movements of British troops, and they relay this information to Washington's followers. Each secret agent has a symbolic book that contains a series of symbolic numbers. These numbers each stand for a different word. The letter has a string of integers that are intended to provide information on the adversary. In today's contemporary warfare, the

practice to prevent sensitive information from falling into the hands of the adversary. There are various publications that discuss military intelligence during World War II and the process of breaking symbols to disclose enemy intentions. These books may be found in a variety of different formats. Every party made an effort to decipher the symbols used by the opposing side (Yan, Wang, Niu, and Yang, 2010).

Definition

"The science of cryptoanalysis is based on the application of mathematics to the process of encrypting and decrypting data." You are able to store or communicate sensitive information through insecure networks, such as the Internet, with the help of encryption. Because of this, the information cannot be read by anybody other than the person who sent it. The decryption and analysis are necessary in order to protect the information's privacy and confidentiality. It is a flag that can be broken and secure communication may be broken.(Shukla, Khare, Rizvi, Stalin, and Kumar 2010).

Encryption Objectives

"(1) The employment of cryptography is motivated by the pursuit of four primary goals, which are as follows: - An assurance of confidentiality and secrecy A service that is used to hide the contents of information from all individuals, with the exception of those who have been aware of its existence.

2) Data integration

It is a service that protects data from being changed (either deleted, added to, or modified) by anyone who are not allowed to do so.

3) Proof of identity

A service used to authenticate the handling of authorized data.

4) Do not be arrogant

It is a service used to prevent a person from denying something"

How Encryption Works

"An encryption algorithm is a mathematical function that is utilized throughout the encryption and decryption processes." In order to encrypt the read messages, it collaborates with the key, password, number, or phrase that is provided. The same text that can be read may be encoded to many distinct encrypted messages using a variety of keys. The safety of encrypted information is

dependent on two very essential factors. The effectiveness of the encryption algorithm is a closely guarded secret.

Types of Encryption

"Broadcast and symmetric device," also known as "Synaptic Encryption." It encrypts and decrypts the data using the same key both times. The success or failure of this kind of encryption is dependent on keeping the key a secret. In this scenario, the individual who has the key is the actual key. For instance, if Zaid wanted to deliver a secret message to the slaves, this would be an effective method to do it. Any third party has this key on him, as well as his eye, and can decrypt anything that has been encrypted between Zaid and Obaid, as well as other instances of similar kind. (Kahrobaei, Tortora, and Tota, 2011).

Code of Caesar

"It is an old method that was invented by Tsar Julius to work encrypted messages between the different sectors of the army, and it has proven to be effective in his time," But in today's world and with the advancement of computer technology, this method can no longer be utilized for the quick detection of the contents of messages; instead, we will provide two examples of applications based on the code Caesar (Yan & Wang & Niu & Yang, 2010, Hong & Cheon, 2012).

Example

"If we were to code the word "SECRET" and use the value of "3," we would rearrange the characters starting with the third letter, which is "D," such that the arrangement of the letters would be as follows: The letters of the alphabet are: A B C D E F G I J K L M N O P Q R S T U V W X Y Z After pressing the "3" key with its newly assigned value, the letters are in their present shape.

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

Now the value of A = D, B = E, C = F and so on

To provide anybody else the opportunity of reading your encrypted communication, you should transmit him the value of the key "3." In this manner, the word "SECRET" will be "VEFUHW."

Example

If we encode the word "ZYIAD" and apply the value of the key "5", we will alter the position of the letters starting with the letter V, "F," and the order of the letters will be as a result of this modification as follows:

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

After utilizing their new value on the "5" key, the characters are the same as they are now.

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

Now the value of A = F, B = G, C = H and so on

To make it possible for everyone else to read your message, the term "ZYIAD" will be changed into "EDNEF" using this method. You are instructed to transmit the "5" value that is associated with the key.

Standard Data Encryption

"This system was developed by the United States National Security Agency at the tail end of the 1970s, and it is not feasible to use it with the development of computer systems and the faster processing of data because the content of encrypted messages may be detected in a short amount of time."

Measuring Strength of Encryption

"Encryption may be either strong or weak, due to the fact that the strength meter for encryption is the amount of time and resources needed for unencrypted text to discover encrypted messages. Text that is encrypted in such a way that it is difficult to decrypt over time or that gives tools for doing so is said to have strong encryption.

Modern Methods of Encryption, The Decryption Process

"takes plaintext and replaces one character in it with another character to produce encoded text." (In order to open the code, we execute the reverse of the encryption steps). To put it another way, the sequence in which the characters appear is altered. The following are some examples of how the encryption technique is used.

Method of Reverse Message

"In order to generate encrypted text using this type of encryption, the characters in the message are flipped in order to generate the encrypted text. When someone wants to read a text and the language is highly English, it is typical for that person to read the text from left to right, since this is the method that is most acquainted to them when reading any text. characters that are read from left to right in text characters"

Example

" We are assuming that the following message is correct. The meht sucof noitseuq noittarapes question focuses on them before encryption, whereas the separation question looks at them after encryption. Take note that in this example, the punctuation goes "then e then h until the end of the sentence." Note that the encrypted text was generated in this particular example by reading the message from right to left, with the m character activated in the word "them," followed by the letter e, then the letter h, and so on until the conclusion of the phrase.

Example

"If we have the following encrypted text, Eab doog," we may generate clear text by reading the text from right to left, starting from the right of the letter g in the word "doog" and moving left to read o then o then d and so on to produce the text of the sentence. This process is called reading the text from right to left. Text encoded using eab and doog To your bay Clear text after decryption has been performed. Note that the mechanism used to locate the clear text of the encrypted text is the same one used in the encryption process to find the encrypted text. This is something to keep in mind as you go through the process of opening the code. When the encrypted text is being encoded during the encryption process, the text is read from right to left. In other words, the content is encrypted such that it cannot be decrypted. When the text is clearly defined in the process of deciphering the code, the text is also read from right to left, which is the opposite of the message (whether it is plain text or encrypted message).

Method of Engineering Modeling

"In this method, we use the message to create a specific geometry model in the shape of a rectangular box with different dimensions according to the length of the message, and here we must emphasize the necessity of calculating the length of the message prior to the beginning of the encryption process."

Example

"Assume that the following message has been received." HIDE COMMUNICATIONS FROM SAM Therefore, the length of the message is equal to the number of characters it includes, which is 18. The following tests may be used to determine whether or not the message that was just shown can be split into a rectangle.

(1) The letter may be written in two equal rows, and if you read the message horizontally, you'll see that each row has nine characters in it. This is shown in Table1 below.

Table 1. Table CONCEAL SAM MESSAGES

Letter	C	O	N	C	E	A	L	S	A
Characters	M	M	E	S	S	A	G	E	S

(2) The geometrical shape (rectangle) shall be in the form of two equal columns by writing the above letter vertically, one letter as in the following Table2.

Table 2. Table geometrical shape (rectangle)

Letter	C	O	N	C	E	A	L	S	A
Characters	M	M	E	S	S	A	G	E	S

The letter was read in a certain manner in order to create an engineering form. The form required that the first nine letters of the letter be put in the first column, and the second nine letters of the letter be placed in the second column.

Methods of Alternative Coding

"Cryptography is a way of encrypting information in which units of clear text are exchanged for other units of encrypted text within a certain legal framework. These modules might be comprised of one character per unit, two pairs of characters per unit, three characters per unit, or any combination of the aforementioned options. The person who receives the message, often known as the "receiver," is the one who unlocks the code by carrying out the stages in the opposite order. It is possible to draw parallels between the replacement encoder and transposition ciphers. Within the framework of the everlasting encodings, the clear text units are reorganized into a sorted order. Changing the same units in the typical P is difficult but not taken into consideration. In contrast, the plain text units in the encrypted text keep their order and remain in the same sequence when encoded with the alternative encoding, but the text units themselves are plainly altered. Now we will take a look at one kind of encoders, known as simple-instance encryption, and demonstrate an application of encryption via a concrete example.

The Method of Encryption to Replace the Simple

In this approach, just one letter is used, and the following example is detailed in depth in the section that came before this one. (Escala, Herold, Kiltz, afols, & Villar, 2013).

Example

In order to cipher the word "THEORM," we must first isolate each letter from the other letters in the word and then determine the coordinates of each character inside the box polypus, as shown in the accompanying Table3.

Table 3. Table word (THEORM)

T	H	E	O	R	M
44	23	15	34	42	32

Therefore, the number 442315344232 will be the output code for this keyword. "If we wish to open the previous code, which is 442315344232, we will need to extract every two digits of this encrypted text. Because each letter is encoded into two integers, which reflect its numerical coordinates in the array, this is the explanation. As an example, the numbers 44 stand for the four vertical coordinates, but the second set of 4 digits stands for the horizontal coordinate, as was previously established. Return to the Polypus square by going back through the Polypus box. Find these two occurrences at the places where they are intermingled with the letter T, and so on for the remainder of the encrypted word's letters.

Bified Cipher

"The code, known as Bified, encrypts the message by using a polypeous box in such a manner that it is impossible to decrypt the message without first having knowledge of the confidential information. The reason for this is because two characters of the text are used to support each letter of the encoded text. As a direct consequence of this, doing a frequency analysis on the characters becomes more challenging. The code is a form of cryptography that is used in classical coding. This approach links the polypus square via the use of replacement and combines it with relative encryption. In the year 1901, Felix Delastell (Bennett, Brassard, and Breidbart, 2013) (Bennett& Brassard& Breidbart,2010,) In order to demonstrate how this strategy works, we will begin by constructing a matrix with a size of five by five cells that has a unique combination of alphabetical letters. This matrix will not include the letter, as shown in Table4.

Table4. Table Bified Cipher

	1	2	3	4	5
1	B	G	W	K	Z
2	Q	P	N	D	S
3	I	O	A	X	E
4	F	C	L	U	M
5	T	H	Y	V	R

"It is important to take note that the letters in this matrix have been arranged in an erratic fashion; that is, the set of alphabetical characters has not been written in the conventional order, which is the pattern that was adhered to for the arrangement of alphabetical characters in the polypus box. You then put the coordinates vertically beneath each row after the letter has been translated to the matching letter of each letter with its coordinates in the matrix (column number - row number).

Example

The following message is assumed by us. FLEE AT ONCE According to the Bified matrix, the coordinates of the letter characters may be adjusted as indicated in the following Table10 as given in the following Table5.

Table 5. Table Bified matrix

Character	F	L	E	E	A	T	O	N	C	E
Coordinates	14	34	53	53	33	15	23	32	24	53

After that, jot down these coordinates beneath each integer in a vertical format, as illustrated in Table6.

Table 6. Table Bified matrix

F	L	E	E	A	T	O	N	C	E
1	3	5	5	3	1	2	3	2	5
4	4	3	3	3	5	3	2	4	3

"The coordinates of each letter have been used to organize these numbers such that they are vertically placed beneath each letter. As an example, the coordinates of the letter F are 14, and these numbers are printed vertically beneath each letter 1 and 4, and then the numbers are read horizontally to make a sequence of the following numbers: 13553123254433353243 After that, write these numbers in the units of each letter of each unit. To begin, look at the first pair of numbers below, starting from the right. 43 32 35 33 44 25 23 31 55 13 The next step is to take two integers, each of which represents the coordinates of one of the numbers, in order to determine the character that corresponds to these coordinates. Where each of the two numbers represents the coordinates of one of the letters in the matrix that makes up the paveid in order to obtain the result given in Table7.

Table 7. Table letters of the matrix

13	55	31	23	25	44	33	35	32	43
I	R	W	O	H	U	A	Y	N	X

"The coordinates will be read in the following order: first by reading the column number, and then by reading the row number. For instance, the number 25 represents the column number 5, and the number 2 represents the row number; the intersection of these two numbers gives us the letter H; similarly, different coordinates may be expressed using other numbers.

References

[1] Alex, E., Gottfried, H., Eike, K., Carla, R., & Jorge, V. (2010). An algebraic framework for Di_e-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, Advances in Cryptology {CRYPTO 2013, Part II, volume 8043 of Lecture Notes in Computer Science, 129-147. Springer. https://doi.org/10.1007/978-3-642- 40041-4

[2] Bennett, C. H., Brassard, G., & Breidbart, S. (2006). Quantum cryptography II: How to re-use a one-time pad safely even if P= NP. Natural computing, 13(4), 453-458. https://doi.org/10.1007/s11047-014-9453-6

[3] Budaghyan, L., Li, C., & Parker, M. G. (2011). Special Issue on Mathematical Methods for Cryptography. https://doi.org/10.1007/s12095-019-00356-8

[4] Jae Hong, S., & Jung, H. Ch. (2012). Beyond the limitation of prime-order bilinear groups, and round optimal blind signatures. In Ronald Cramer editor, TCC 2012: 9th Theory of Cryptography Conference, volume 7194 of Lecture Notes in Computer Science, pages 133-150. Springer, March 2012. https://doi.org/10.1007/978-3- 642-28914-9

[5] Kahrobaei, D., Tortora, A., & Tota, M. (2011). Multilinear Cryptography using Nilpotent Groups. arXiv preprint arXiv:1902.08777

[6] Nilsson, A., Johansson, T., & Wagner, P. S. (2011). Error Amplification in Code-based Cryptography. IACR Transactions on Cryptographic Hardware and Embedded Systems, 238-258. https://doi.org/10.13154/tches.v2011.i1.238-258

[7] Shukla, P., Khare, A., Rizvi, M., Stalin, S., & Kumar, S. (2013). Applied cryptography using chaos function for fast digital logic-based systems in ubiquitous computing. Entropy, 17(3), 1387-1410. https://doi.org/10.3390/e17031387

[8] Yan, X., Wang, S., Niu, X., & Yang, C. N. (2013). Generalized random grids-based threshold visual cryptography with meaningful shares. Signal Processing, 109, 317-333. https://doi.org/10.1016/j.sigpro.2014.12.002