JMETP
Journal for the Mathematics Education and Teaching Practices, 5(1), 23-27, June 2024
e-ISSN: 2717-8587
dergipark.org.tr/jmetp

Young Wise Publishing
youngwisepub.com
gencbilgeyayincilik.com © 2024

Mathematics Instructional Design/Teaching Practice Article

Enhancing digital security through randomized cryptology: a novel algorithm utilizing prime numbers, pi, linear encryption, and matrices

Neslihan Gül[1]

Elazığ Science and Art Center, Elazığ, Turkiye

Article Info

Received: 18 March 2024
Accepted: 27 June 2024
Available online: 30 June 2024

Keywords:
Cryptology
Digital security
Encryption
Information security

Abstract

Recently, the widespread use of computer technology and the development of the internet have facilitated access to information. However, this has also increased the importance of information security. Public and private sector organizations need robust databases to protect their digital assets. For this reason, many security-oriented products and projects are being developed. Especially with the rapid progress of the internet age and the increasing importance of digital security, the field of cryptology has attracted great interest. Cryptology is the science of ciphers. The infrastructure of cryptology is based on mathematics. In order to ensure the security of information in the digital environment, a strong database is needed. This is achieved with strong encryption algorithms. Algorithms that incorporate the principle of randomness and allow repeating letters to take different values are stronger against external attacks. For these reasons, the aim of this study is to create a cryptology algorithm that is resistant to password cracking techniques, adopts the principle of randomness, contains mathematical formulas and has a decryption. In this study, prime numbers, pi number, linear encryption technique and matrices are used. In the encryption algorithm, it is aimed to adopt the principle of randomness with prime numbers and pi number. By using linear encryption technique and matrices, new sequence numbers of each letter were obtained, and it was aimed to strengthen against the frequency analysis method, which is one of the password cracking techniques, by ensuring that the repeating letters take different number values.

To cite this article

Gül, N. (2024). Enhancing digital security through randomized cryptology: a novel algorithm utilizing prime numbers, pi, linear encryption, and matrices. *Journal for the Mathematics Education and Teaching Practices, 5*(1), 23-27.

Introduction

With the development of computer technology, access to information has become easier. However, this situation has brought along certain problems. One of these problems is the protection and secure transmission of information. For these reasons, one of the increasingly important branches of science is cryptology. Cryptology is the science of ciphers and is the transmission of various messages to the recipient in a secure environment by encrypting them with certain methods (Jones, 2005). Cryptology is divided into two sub-branches: cryptography and cryptanalysis (Figure 1). Cryptography is the process of encrypting public data by hiding it (Yılmaz, 2010). On the other hand, cryptanalysis is the process of converting encrypted data into original form (Buluş, 2006).

[1]Mathematics Teacher for gifted students, Master of Science at Math education, Elazığ Science and Art Center, Elazığ, Turkiye. gulneslihan85@gmail.com ORCID: 0000-0003-2137-0206

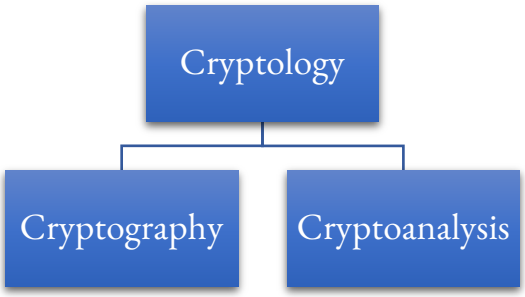

Figure 1. Sub-branches of cryptology

Various encryption methods have been used throughout history. Caesar, zigzag, vigenere, hill, stenagrofi, vernam, linear (affine) encryption are some of the methods used. Linear encryption is a technique applied by selecting (a,b) keys and creating a linear function of the type y=ax+b (mod n) (n being the number of letters in the alphabet). In this technique, the independent variable (x) is given the sequence numbers of the letters and new values (y) are obtained. The important point in this technique is that the numbers a and n must be prime (Mollin, 2007).

Various techniques are used to decrypt ciphertext. One of them is frequency analysis. In every language, each letter has a frequency of use. According to this method, the number of each letter in the cipher text is divided by the total number of letters. Thus, the cipher text is decrypted according to the frequency of letter usage in that language (Coşkun & Ülker, 2013).

Although cryptology seems to be a branch of science in itself, in fact, a large part of its infrastructure is mathematical science. Mathematical concepts such as number theory, prime numbers, matrices and modular arithmetic form the basis of cryptology. As a different teaching material, activities using various encryption techniques have been encountered in mathematics education in recent years (Bahadır & Özdemir, 2012; Chua, 2006; Güler, 2007; Katrancı & Özdemir, 2013; Özdemir & Erdoğan, 2011; Özdemir & Yıldız, 2012; Sahal & Özdemir, 2018; Welsh, 1988). With the developing technology, the security of information has gained importance. Public and private institutions want to have a strong database in order to survive safely in the digital environment. A strong database requires a strong encryption algorithm. In this direction, in this study, the following problem is sought by creating a cryptology algorithm.

- Can an algorithm be created that incorporates the principle of randomness?
- Can an algorithm be constructed that contains more than one mathematical concept and can be adapted to an encryption technique at the same time?

Purpose of the Instructional Activity

Recently, cryptology has emerged as a branch of science that attracts attention. The biggest reason for this is the rapid progress of the internet age and the increasing importance of digital security. For this reason, public and private institutions want to have a strong database in order to survive safely in the digital environment. The strength of encryption algorithms is that they are resistant to cyber-attacks. Every password is cracked sooner or later. The important thing is that this period is long. One of the criteria for a password to be strong is that it incorporates the principle of randomness. For these reasons, the aim of this study is to create a cryptology algorithm that is resistant to password cracking techniques, adopts the principle of randomness, contains mathematical formulas and has a decryption.

Structures of Math Teaching Practice

Information on the Teaching Activity

In this study, prime number, linear (affine) encryption technique, matrix, pi number are used. Pi and prime numbers are chosen because they are resistant to any cracking attacks since they do not have a specific order. The encryption algorithm consists of 4 steps.

Determination of New Sequence Numbers of Letters in the Alphabet Using Linear Encryption Technique

In order to apply the linear encryption technique, two primes (keys) are chosen and a function is created ($f(x) = ax + b \pmod{29}$, where a and b are the chosen primes and $a<b$). Then a character table is created. The table consists of 29 letters

and each letter is numbered starting from 1 (Table 1). For the text to be encrypted, new sequence numbers are determined according to the linear encryption technique using the sequence number of each letter.

For example, for the letter A, the new value f(1)= a.1+b (mod29) is found. Let the letters in the text to be encrypted be c, d, e, f, g, h. Let us consider the new number values as the numbers given in Table 2 by applying the linear encryption technique.

Table 1. Creating Characters and Determining Sequence Numbers

Letter	A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L
Sequence number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Letter	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z	
Sequence number	16	17	18	19	20	21	22	23	24	25	26	27	28	29	

Table 2. New Sequence Numbers of Letters as an Example

Letter	c	d	e	f	g	h
New sequence numbers	5	7	8	9	10	12

Pi Number (π) and Writing the Message to be Sent as a Matrix

The new sequence number of the letter in each word in the message to be sent and the decimal parts of the number pi (π= 3,1415926535897932...) are written in separate matrices (starting from the left and writing from top to bottom) to form mx2 type matrices (m is the number of letters in each word). If there is a blank space in the matrix, zero is written and the result of the operation is determined as the new sequence numbers of the letters (Figure 2). For example, let the letters be c, d, e, f, g, h. The first 6 digits of pi after the comma are 1, 4, 1, 5, 9, 2. These values are written as a matrix and addition is performed (Figure 2).

$$\begin{matrix} 5 & 9 \\ 7 & 10 \\ 8 & 12 \end{matrix} + \begin{matrix} 1 & 5 \\ 4 & 9 \\ 1 & 2 \end{matrix} = \begin{matrix} 6 & 14 \\ 11 & 19 \\ 9 & 14 \end{matrix}$$

Figure 2. Writing as a Matrix

Table 3. New Values of Letters as a Result of Matrix Summation

Letter	**c**	**d**	**e**	**f**	**g**	**h**
New number value according to linear encryption method	5	7	8	9	10	12
Matrix sum result new sequence numbers	6	11	9	14	19	14
According to the matrix sum result, the new equivalents of the letters in the alphabet are	e	ı	ğ	k	ö	k

Sending the Message to the Recipient

For linear encryption, the key values and the ciphertext are written together and sent to the receiver. For example, let the key values be (2,3) and the ciphertext be e, ı, ğ, k, ö, k. To the receiver 2, 3 is transmitted as e, ı, ğ, k, ö, k. If there is more than one word, a comma is placed between the words.

Deciphering the Ciphertext (Deciphering)

The receiver first determines the key values. It then applies a linear encryption technique by substituting the key values for each letter and determines new sequence numbers for each letter. It determines the sequence numbers of the letters in the sent ciphertext from Table 2. Then, for each word, according to the number of letters, it writes the number values of pi after the comma as a matrix and performs subtraction. It decrypts the ciphertext by matching the result with the new sequence number of each letter.

Implementation of Math Teaching Practice

Example; Text to be encrypted: MUTLU

Switches: 2 and 3

Determination of New Sequence Numbers of Letters in the Alphabet Using Linear Encryption Technique

Text to be encrypted: "MUTLU" (Happy) (this word is chosen to show that although there are two letters u, they take different values). The prime numbers 2 and 3 (keys) are taken as the new sequence numbers of the letters. For example, if a linear encryption technique is applied for letter A, f(1)=2.1+3=5 and f(2)=2.2+3=7 for letter B.

Table 4. Application of Linear Encryption Technique to Letters

Letter	**A**	**B**	**C**	**Ç**	**D**	**E**	**F**	**G**	**Ğ**	**H**	**I**	**İ**	**J**	**K**	**L**
Sequence Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Linear encryption technique Application	5	7	9	11	13	15	17	19	21	23	25	27	29	2	4
Letter	**M**	**N**	**O**	**Ö**	**P**	**R**	**S**	**Ş**	**T**	**U**	**Ü**	**V**	**Y**	**Z**	
Sequence Number	16	17	18	19	20	21	22	23	24	25	26	27	28	29	
Linear encryption technique Application	6	8	10	12	14	16	18	20	22	24	26	28	1	3	

Table 5. Application Of Linear Encryption Technique To The Letters In The Word "MUTLU"(Happy)

For the letter M,	f(16)=2.16+3=35, 35=6 (mod29)
For the letter U,	f(25)=2.25+3=53, 53=24 (mod29)
For the letter T,	f(24)=2.24+3=51, 51=22 (mod29)
For the letter L,	f(15)=2.15+3=33, 33=4 (mod29)

Table 6. New sequence numbers of letters in the word "MUTLU" according to linear encryption technique

Letter	Sequence number	New sequence number
M	16	6
U	25	24
T	24	22
L	15	4
U	25	24

Pi Number (π) and Writing the Message to be Sent as a Matrix

With the new values of the letters, the decimal part of pi is written in the matrix and addition is done. In order not to leave any empty space in the matrix, 0 is written in the empty space.

$$\begin{matrix} 6 & 4 \\ 24 & 24 \\ 22 & 0 \end{matrix} + \begin{matrix} 1 & 5 \\ 4 & 9 \\ 1 & 2 \end{matrix} = \begin{matrix} 7 & 9 \\ 28 & 33 \\ 23 & 2 \end{matrix}$$

Figure 3. Matrix Addition of the Letters in the Word "MUTLU" and the Number Pi

Table 7. Matrix sum result new values of letters in the word "MUTLU"

M = 7	U = 28	T = 23	L = 9	U = 33	space = 2

Table 8. New alphabet correspondences of letters in the word "MUTLU"

M	U	T	L	U	Space
F	Y	Ş	Ğ	Ç	B

How to Send to the Recipient

2,3 FYŞĞÇB

Conclusion

In our encryption algorithm, prime numbers, linear encryption technique, matrix, pi number are used. In the algorithm, it is aimed to ensure the principle of randomness by using pi and prime numbers, which do not have a specific order. This will make the algorithm strong against external threats. By using linear encryption technique, the letters were given new sequence numbers and their order was changed. Thus, the algorithm was able to give new values to the new numbers of the letters by adding them with matrices. In this case, the numbers of the letters were removed from the regular formula structure. In addition, repetitive letters in the same word are given different number values to avoid letter repetition. The prime number (key) to be selected in each new message is changed. Thus, the linear encryption technique is strengthened against password cracking techniques such as frequency analysis by changing the sequence number of each letter. In this respect, it can be said to have a strong algorithm.

Limitations

In our encryption algorithm, linear encryption technique is used, but a new encryption algorithm can be created by using a different encryption technique instead. When creating encryption algorithms, care is usually taken to use prime numbers. This is because a strong encryption algorithm is more resistant to password cracking techniques if it has the principle of randomness. Therefore, different sequences of numbers can be used with no particular rule between them.

Biodata of Author

Neslihan Gul is a mathematics teacher for gifted students at the Elazig Science and Art Center. She holds a M.A. in mathematics education from Firat University, and a B.S. in mathematics from Firat University. She is interested in mathematical giftedness, cryptology, mathematics education, and gifted education. Affiliation: Elazig Science and Art Center, Elazig, Türkiye. E-mail: gulneslihan85@gmail.com ORCID: 0000-0003-2137-0206

References

Bahadır, E., & Özdemir, A. Ş. (2012). Examining the applicability of substitution cipher activity and students' opinions about the activity. *KALEM International Journal of Education and Human Sciences, 2*(2), 51-90.

Buluş, H. N. (2006). *Examination of basic cryptographic algorithms and crypto analysis*. Master's Thesis. Trakya University, Edirne, Türkiye.

Chua, B. L. (2008). Harry potter and the coding of secrets. *Mathematics Teaching in the Middle School, 14*(2), 114-121.

Coşkun, A., & Ülker, Ü. (2013). Development of a cryptography algorithm for national information security and reliability determination against letter frequency analysis. *International Journal of Informatics Technologies, 6*(2), 31-39.

Güler, E. (2007). *The effect of encryption activities on mathematics achievement in the teaching of modular arithmetic subject*. Master's Thesis. Marmara University, Istanbul Türkiye.

Jones, A. (2012). Information warfare-what has been happening? *ComputerFraud& Security*, 4-7.

Katrancı, Y., & Özdemir, A. Ş. (2013). Strengthening the subject of modular arithmetic with the help of RSA encryption. *KALEM International Journal of Education and Human Sciences, 3*(1), 149-186.

Mollin, R. A. (2007). *An introduction to cryptography.* CRC Press.

Özdemir, A. Ş., & Erdoğan, F. (2011). Teaching factorial and permutation with encryption activities. *West Anatolian Journal of Educational Sciences, 1*(3), 19-43.

Sahal, M., & Özdemir, A. Ş. (2018). Examination of the activities about enciphering done with fifth grade students and their views about the activities. *International Online Journal of Educational Sciences*, *10*(3), 1-21.

Welsh, D. (1988). *Codes and cryptography*. Oxford University Press.

Yılmaz, R. (2010). *Some statistical tests in cryptologic applications*. Master's Thesis. Selçuk University, Konya, Türkiye