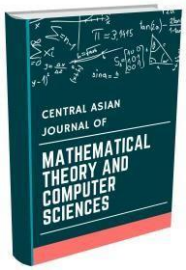

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 05 Issue: 03 | July 2024 ISSN: 2660-5309

Text Encryption and Decryption using Mathematical Functions

Hamza M. Salman*, Mohammed H. O. Ajam, Hawraa Imad Kadhim

Al-Qasim green university, Babylon 51013, Iraq.
* Correspondence: hamza.salman@uoqasim.edu.iq

Abstract: One of the most important challenges that the world is still facing until now is the issue of information security and preservation From breach and change. Cryptography is the answer to this question. This science includes many ancient ciphers (classic), which was used to encrypt phrases and text messages. Among these ciphers are the Playfair cipher and the cipher cipher. Veginer of all kinds. These ciphers help secure the confidentiality of information, but they have the disadvantage that they are easy to break. That's because their algorithms rely on a single key for encryption and decryption. In order to increase the degree of security and confidentiality of the information, the complete VIGENER cipher has been developed in its numerical form to the matrix image to become more complex. And to obtain encrypted messages and phrases as well as re-decrypt them With the fastest time and the least effort, a program designed for the complete Visioner code was used on MATLAB.

Keywords: Cryptographic Theorems, Ciphers, Playfair Cipher's

Citation: **Hamza M. Salman*, Mohammed H. O. Ajam, Hawraa Imad Kadhim**. Text Encryption and Decryption using Mathematical Functions. Central Asian Journal of Mathematical Theory and Computer Sciences 2024, 5(3), 121-131.

Received: 11th June 2024
Revised: 15th June 2024
Accepted: 19th June 2024
Published: 27th June 2024

1. Introduction

Information security is one of the most important issues in various areas of life[1]. There is a lot of information Such as private secret messages and phrases between individuals that no one should see. From that I was born Different ideas for a long time seeking to protect information from penetration and change These ideas have evolved as a result of the acceleration of risks, to form a science in itself, built on foundations and principles Clear sports. This science is known as cryptography (cryptography) (*Cryptography*). One of the branches of applied mathematics, which works according to certain algorithms to hide the concept of text, not to hide it his existence[2]. The text to be encrypted is transformed from the plain image to the encrypted image, by means of a specific method It is called the encryption key agreed between the sender and the receiver. The one-key principle of

encryption and decryption is Basis of classic cipher algorithms. The research aims to[3]:

1) Definition of matrices and operations on them.
2) Introducing encryption, especially classical encryption.
3) Presentation of some types of classic codes such as Playfair code and the simple and complete Visionar code,
   The developer, and the way its algorithms work.
4) The use of MATLAB in the process of encoding and decoding the full Wegener algorithm. search problem:
   The research problem lies in the following:

1) The weakness of the codes and their lack of security.
2) Finding an effective and strong method to ensure confidentiality of information.

Previous studies :

Mridul Suklabaidyaa , Dr. Anupam Dasb , Biswajit Dasc International Journal of Computational Intelligence & IoT, Vol. 2, No. 4, 2018 6 Pages Posted: 28 Mar 2019 A Cryptography Model Using Hybrid Encryption and Decryption Techniques

In his research he used the mathematical model"Hybrid Encryption Decryption (HED)" is proposed which first codify the original texts to cipher texts and then cipher texts to original texts[3]

2. Materials and Methods

Matrices and algebraic operations on it [1]

In this section, we will learn about the most important concepts about matrices and the algebraic operations on them. Well we will know On how to calculate the determinant of the matrix, the elementary transformations, the elementary matrices and the inverse of the matrix[4] .

Definition 2.1.[1] *Arrays are a collection of quantities that may be (complex numbers, variables, real numbers, derivatives, vectors, etc.) arranged as rows of rows and columns of columns in large brackets Such as () a and [], and the matrix is symbolized by one of the capital letters, such as: B, A, C, ... and is subject to operations specific algebraic.*

The general form of any matrix is:-

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots\dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots\dots & 2n \\ \vdots & & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \dots\dots\dots & a_{mn} \end{bmatrix}$$

The matrix can be expressed as:

$$A = [a_{ij}]_{m \times n}$$

Where this formula reads as follows:

A matrix A whose element is in row i and column j where $I = 1,2, \ldots \ldots, m$ and $j = 1,2, \ldots \ldots n$

Definition 2.2.[1] *Let us have a matrix $A = [a_{ij}]$ where the number of rows is m and the number of columns is n, it is said that the order of The matrix* ***Order of Matrix*** *is the number of rows times the number of columns i.e. $m \times n$*

Example 2.3.[1] Let's have the matrix $\mathbf{A} = \begin{bmatrix} \mathbf{8} & \mathbf{0} & \mathbf{1} \\ \mathbf{5} & \mathbf{2} & \mathbf{9} \end{bmatrix}$ ***This matrix has 3 rows and 2 columns, so it is of order (2×3)***

Definition 2.4.[1] *Let's have two matrices $A = [a_{ij}]$ and$B = [b_{ij}]$ We say that matrices A and B are equal* ***Equal Matrices*** *if and only if they are of the same order and the corresponding inputs are equal*

Example 2.5.[1] Set the value of x so that the matrices A and B are equal:

$$\mathbf{A} = \begin{bmatrix} 10 & 3 \\ 2 & 5 \\ 6 & -3 \end{bmatrix} \qquad \mathbf{B} = \begin{bmatrix} 2x^2 + x & \mathbf{3} \\ \mathbf{x} & \mathbf{5} \\ \mathbf{6} & \mathbf{2x - 7} \end{bmatrix}$$

Sol :

For two matrices of the same order to be equal, it is enough that the corresponding elements are equal :

$$2x^2 + x = 10$$

$$x = 2$$

$$2x - 7 = -3$$

So the common solution is $\mathrm{x} = 2$ *so*

$$\mathbf{B} = \begin{bmatrix} 10 & 3 \\ 2 & 5 \\ 6 & -3 \end{bmatrix}$$

Definition 2.6.[1] *Let I_n be a binary matrix. And as we know, the effect of one or more primary transformations is harmful to obtaining Matrix equivalent to In . This equivalent matrix is called an elementary matrix. Also, the initial matrix is considered a non-normal matrix because this matrix is obtained from*

[5]*through a transformation or set of elementary transformations on* I_n*, and that* In *is a no nominal matrix because* $detI_n = 1$

Example2.7.[1] Let $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ ***then the following matrices:***

$$H_{1,3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = K_{1,3}, H_{2,3} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{bmatrix} = K_2(4), H_{1,2}(\mathbf{4}) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

raw matrices.

Remark 2.3.[6] *For short,* $H_{ij}I_n$ *can be written instead of* H_{ij} .

3. Results and Discussion

The process of securing information has become one of the important operations, past and present, in order to preserve Confidentiality and privacy. Therefore, in this chapter, we will learn about concepts about cryptography and study some ciphers classic[6].

3.1. Concepts of cryptography [7]

Cryptography is the science known as cryptography, the word ($Cryptography$) is derived from Greek taken from the two words ($Kryptus$) which means secret, and the word ($graphein$) which means writing, And by that means secret writing.

Definition 3.2.[7] *Defines the plain text is the original understood message or data that constitute the algorithm's input .*

Definition 3.3.[9] *The cipher text is known as (* $Cipher\ Text$ *) and is an unintelligible message generated as an output from The algorithm depends on the plain text and the secret key.*

Definition 3.4.[7] *Encryption is the process of converting information or plaintext into cipher text or Concealer.*

Definition 3.5.[9] *Decryption is the reverse process of encryption, meaning the retransformation of the cipher text to the plain text.*

The following figure shows the encryption and decryption process

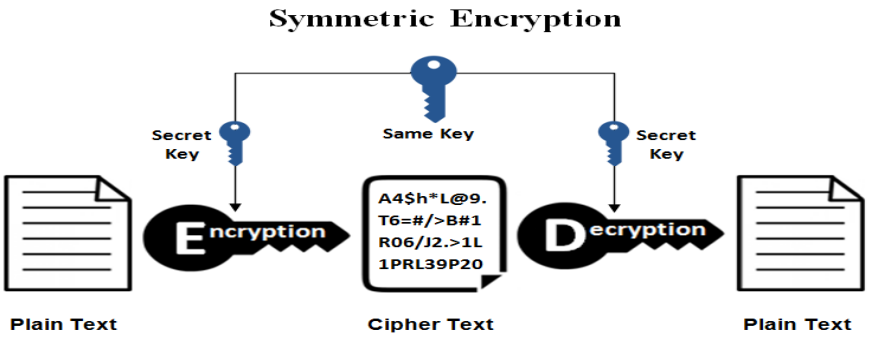

Figure (3.1) shows how encryption and decryption work

Definition 3.6.[4] *The cipher key (Encryption Key) is the means by which we encrypt the original text, and also decrypt the text encoder*[7].

Definition 3.7.[6] *A matrix code is defined as a matrix mathematical function whose variables are matrices A scalar of the order $n \times n$ and a matrix function is more useful than ordinary mathematical functions, because the coding Using regular functions, the text is encrypted letter by letter, while matrix functions encrypt the entire text at once one.*

3.2. Some types of classic blades [5]

There are many classic blades that have been used since time immemorial, and whose work depends on the use of One key encryption and decryption. In this section, we will learn about some of them[8].

3.2.1. Playfair Cipher's [3]

The Playfair cipher is an ancient cipher invented by the British scientist Charles Weston in 1854 AD, as he named it after Playfair's friend. Its method is to make a matrix of 25 cells (5 * 5) and put in each cell an alphabetic letter A, B and so on. Since the number of letters of the alphabet (in the English language) is equal to 26 letters, then there is a letter that has no place, so this code puts the letters J, *I* together in one box always[9]

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*

Matrix form 5*5

Usually, the letters that represent the encryption sentence are written in this matrix.

Example 3.2.2[3] ***Using the*** Playfair ***cipher, encrypt the message,*** *'EESSAGM TESECR'* ***knowing that the key is 'DORKEYW"***

Sol :

1) We divide the message into blocks.
2)

SE	CR	ET	ME	SX	SA	GE

2) We write a 5*5 matrix and fill it with the key and the remaining cells with the rest of the letters that are not in the key[10]

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

3) We notice that both the letter S and the letter E are in a different row and column, so the solution is the intersection of each Among them, as well as the two letters CR that have the same row, so the solution is to replace each letter with the next letter on the other hand. Right, and the letters GE are in the same column, so the solution is to replace each letter with the letter below it[11]

$TEXT$	SE	CR	ET	ME	SX	SA	GE
$CIPHER$	NO	RD	KU	NK	QZ	PC	ND
KEY	$KEYWORD$						

3.2.3.The Vigenere's Cipher [8]

This blade was invented by the Frenchman Blaise de Vigenier in 1553 AD. This blade is considered a Vigenier blade One of the strongest ciphers in classical cryptography, as this cipher was not broken for decades, and they believed that this cipher Unbreakable until the scientist Frederick Caskey broke it[12]

Example 3.2.4[8] Using the simple Vigenier cipher to decrypt the message '$LMZPZXHHF$', noting that key 4375

Sol :

$F - 4 = B \quad H - 3 = E \quad H - 7 = A \quad Z - 5 = U \quad X - 4 = T \quad L - 3 = I$
$M - 7 = F \quad Z - 5 = U \quad P - 4 = L$

Thus, we find that the plain text is **BEAUTIFUL** .

3.2.3.Alphapatic Vigenere's Table [8]

The Vigenier table consists of 26 rows and 26 columns. In each row there are 26 letters of the alphabet written with 26 different ways on different lines, so that each line produces the line before it by shifting the character to The left is one square[13].

Example 3.2.4[8] Using the complete Vigener cipher to decrypt the message 'IIBLSMG' given that the key is *Djqifs*

Sol[14] :

We replace the letters of the word and the key with their corresponding numbers from the Vigenier table, and we get[15]:

8 8 1 11 18 12 6 25: Text

3 9 16 8 5 18: The key

We substitute the values into the numerical function
$f^{-1}(z,y) = x = (z - y + 1) mod 26$
$f^{-1}(8,3) = (8 - 3 + 1) mod 26$
$= 6 mod 26$
$= 6 \rightarrow G$

In the same way we get the following:

$Cipher$	z	y	$x = f^{-1}(x,y)$	$xmod26$	$Plain$
I	8	3	6	6	G

I	8	9	0	0	A
B	1	16	-14	12	M
L	11	8	4	4	E
S	18	5	14	14	O
M	12	18	-5	21	V
G	6	3	4	4	E

Therefore, the original text is : $GAME\ OVER$ which is what we found previously[16].

1. Cryptographic theorems

In this chapter, we will prove that every text can be encrypted through a specific function, and that any text can also be decrypted through another function in a mathematical way[17].

Theorem 4.1. Every clear text can be encoded according to the function

$$Z = f(X, A_k, B) = [A_k(X + B)]mod256 \qquad 4.1$$

Proof :

Let us have the plain text P, which we will assume corresponds to the numerical matrix X, and let us assume for the sake of argument that there is Another text P_1, which corresponds to the numerical matrix X_1, so that the following is achieved[18]:

$$X_1 \neq X \Longrightarrow f(X_1, A_k, B) = f(X, A_k, B)$$

$$\Longrightarrow f(X_1, A_k, B) mod\ n = f(X, A_k, B) mod\ n$$

$$[f(X_1, A_k, B) - f(X, A_k, B) mod\ n = 0\ mod\ n$$

Where 0 represents a zero matrix, thus:

$$[A_k(X_1 + B) - A_k(X + B)] mod\ n = 0\ mod\ n$$

$$A_k(X_1 + B - X - B) mod\ n = 0\ mod\ n$$

$$A_k(X_1 - X) mod\ n = 0\ mod\ n$$

$$(X1 - X) mod\ n = 0\ mod\ n$$

$$X1 mod\ n = X\ mod\ n$$

$$X_1 = X$$

This is contrary to the assumption

$$f(X_1, A_k, B) \neq (X, A_k, B)$$

Therefore, the encryption of any message through function (4.1) is done in a single manner, and from this we conclude that the encryption of any message[19]

Theorem 4.2. Every ciphertext can be decrypted according to the **:**function

$$X = [A - 1.Z - B] mod 256 \qquad 4.2$$

Proof :

Let us have the ciphertext c, which we will assume corresponds to the numerical matrix Z. Let us assume, for the sake of argument, that there is Another ciphertext C_1 which corresponds to the numerical matrix Z_1 such that

$$Z_1 \neq Z \implies X_1 = X$$

$$\implies X1 mod\ n = X\ mod\ n$$

$$[X1 - X] mod\ n = 0\ mod\ n$$

where 0 is the zero matrix and thus:

$$[A - 1Z_1 - B - A - 1 + B] mod\ n = 0 mod n$$

$$A - 1(Z_1 - Z) mod\ n = 0\ mod\ n$$

$$(Z1 - Z) mod\ n = 0\ mod\ n$$

$$Z1 mod\ n = Z\ mod\ n$$

$$Z_1 = Z$$

This is contrary to the assumption

$$X_1 \neq X$$

Therefore, each message is decrypted through function (4.2) in a single manner, and from this we conclude that decryption

REFERENCES

1. T. Radożycki, Solving Problems in Mathematical Analysis, Part I: Sets, Functions, Limits, Derivatives, Integrals, Sequences and Series. books.google.com, 2020. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=W-

7RDwAAQBAJ&oi=fnd&pg=PR5&dq=mathematical+functions&ots=aOaTlE3Obc&sig=r6DzaNC-WKA3ZVTcJBttrC_J3HQ
2. V. Innocente and P. Zimmermann, Accuracy of Mathematical Functions in Single, Double, Double Extended, and Quadruple Precision. homepages.loria.fr, 2021. [Online]. Available: https://homepages.loria.fr/PZimmermann/papers/glibc234-20210907.pdf
3. G. Urcid, R. Morales-Salgado, and M. Mares-Javier, "Analysis and Evaluation of Real-valued Functions in Mathematical Morphology," academia.edu, [Online]. Available: https://www.academia.edu/download/97365813/E12013346.pdf
4. J. García-García, "Mathematical Understanding Based on the Mathematical Connections Made by Mexican High School Students Regarding Linear Equations and Functions," The Mathematics Enthusiast, 2024, [Online]. Available: https://scholarworks.umt.edu/tme/vol21/iss3/7/
5. F. Mainardi, Special functions with applications to mathematical physics. mdpi.com, 2023. [Online]. Available: https://www.mdpi.com/books/reprint/7016
6. T. M. Gataullin and S. T. Gataullin, "Endpoint functions: mathematical apparatus and economic applications," Mathematical Notes, 2022, doi: 10.1134/S0001434622110037.
7. N. E. Ndlovu, "Exploring learners' understanding of mathematical concepts necessary in the learning of grade 11 algebraic functions: the case of three schools in …." 2019.
8. O. Kryazhych and O. Kovalenko, "Examining a mathematical apparatus of Z-approximation of functions for the construction of an adaptive algorithm," Восточно-Европейский журнал …, 2019, [Online]. Available: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vejpte_2019_3(4)__2
9. K. G. Campo-Meneses, V. Font, J. García-García, and ..., "Mathematical connections activated in high school students' practice solving tasks on the exponential and logarithmic functions," EURASIA Journal of …, 2021, [Online]. Available: https://www.ejmste.com/article/mathematical-connections-activated-in-high-school-students-practice-solving-tasks-on-the-exponential-11126
10. M. Hemery, F. Fages, and S. Soliman, "Compiling elementary mathematical functions into finite chemical reaction networks via a polynomialization algorithm for ODEs," … September 22–24, 2021, Proceedings 19, 2021, doi: 10.1007/978-3-030-85633-5_5.
11. F. Mainardi and A. Consiglio, "The Wright functions of the second kind in Mathematical Physics," Mathematics, 2020, [Online]. Available: https://www.mdpi.com/2227-7390/8/6/884
12. V. S. Ilkiv, Z. M. Nytrebych, P. Y. Pukach, and ..., "Analysis of measurement systems mathematical models by using the comparison of functions," Mathematical …, 2019, [Online]. Available: http://jnas.nbuv.gov.ua/j-pdf/mmc_2019_6_2_12.pdf
A. Tabieh, "A teaching model impact of learning outcomes for mathematical content in functions," Opción, 2020, [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3685857
13. L. Siqing and L. Zhou, "AN EXPLORATION OF INTEGRATING MATHEMATICAL MODELING IDEAS IN TEACHING APPLICATION OF FUNCTIONS," researchgate.net, [Online]. Available: https://www.researchgate.net/profile/Lili-Zhou-27/publication/375519330_AN_EXPLORATION_OF_INTEGRATING_MATHEMATICAL_MODELING_IDEAS_IN_TEACHING_APPLICATION_OF_FUNCTIONS/links/654d1c70ce88b87031d8b47e/AN-EXPLORATION-OF-INTEGRATING-MATHEMATICAL-MODELING-IDEAS-IN-TEACHING-APPLICATION-OF-FUNCTIONS.pdf

14. A. Firsova and G. Y. Chernyshova, “Mathematical models for evaluation of the higher education system functions with DEA approach,” … университета. Новая серия …, 2019, [Online]. Available: https://cyberleninka.ru/article/n/mathematical-models-for-evaluation-of-the-higher-education-system-functions-with-dea-approach
15. D. Cattaneo, M. Chiari, G. Magnani, N. Fossati, and ..., “FixM: Code generation of fixed point mathematical functions,” … Informatics and Systems, 2021, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210537920302018
16. K. G. Campo-Meneses and ..., “Mathematical Connections Related to Exponential and Logarithmic Functions: A Literature Review,” RANGE: Jurnal …, 2023, [Online]. Available: http://jurnal.unimor.ac.id/index.php/JPM/article/view/4738
17. K. S. Sørensen, On some differential equations in mathematical-physics and singular functions in probability theory. vbn.aau.dk, 2022. [Online]. Available: https://vbn.aau.dk/files/549497701/PHD_KStudsgaardS_rensen.pdf
18. Kusmaryono, H. Suyitno, D. Dwijanto, and ..., “The Effect of Mathematical Disposition on Mathematical Power Formation: Review of Dispositional Mental Functions.,” International Journal of …, 2019, [Online]. Available: https://eric.ed.gov/?id=EJ1201186
19. Suklabaidya, M., Das, A., & Das, B. (2018). A cryptography model using hybrid encryption and decryption techniques. International Journal of Computational Intelligence & IoT, 2(4).
20. Agbedemnab, P. A. N., Baagyere, E. Y., & Daabo, M. I. (2019, October). A Novel Text Encryption and Decryption Scheme using the Genetic Algorithm and Residual Numbers. In ICICIS (pp. 20-31).
21. Singh, L. D., & Singh, K. M. (2015). Implementation of text encryption using elliptic curve cryptography. Procedia Computer Science, 54, 73-82.
22. Singh, J., Lata, K., & Ashraf, J. (2015). Image encryption & decryption with symmetric key cryptography using MATLAB. International Journal of Current Engineering and Technology, 5(1), 448-451.
23. Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.
24. Patil, P., & Bansode, R. (2020). Performance evaluation of hybrid cryptography algorithm for secure sharing of text & images. International Research Journal of Engineering and Technology, 7(9), 3773-3778.
25. Babaei, M. (2013). A novel text and image encryption method based on chaos theory and DNA computing. Natural computing, 12(1), 101-107.
26. Karudaiyar, G., Karthikeyan, S., & Sainath, B. (2014). Encryption and Decryption Scheme by Using Finite State Machine. Biosciences Biotechnology Research Asia, 11(3), 1867-1872.
27. Goyal, R., & Khurana, M. (2017). Cryptographic security using various encryption and decryption method. International Journal of Mathematical Sciences and Computing (IJMSC), 3(3), 1-11.