International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Develop Coding Operations by Improving Applications of Matrix Algebra in Cross Mathematical Notation

Azhar Malik

Submitted: 08/11/2022 **Revised:** 15/01/2023 **Accepted:** 10/02/2023

Abstract : Currently encryption methods are much more sophisticated , among them the most used is the RSA algorithm, created by Rivest, Shamir, Adleman pblished in 1977 in the journal Scientific American, based on prime numbers of great magnitude, the which uses the model of a public and a private key (asymmetric encryption) . The reliability offered by the RSA algorithm allowed Phil Zimmerman in 1991, develop PGP (Pretty Good Privacy) which is an encryption algorithm that works easily on home computers. PGP uses classical cryptography concepts and combines them with the RSA algorithm .

In most classical ciphers, the algorithms developed are based on mathematical foundations, for example, modular arithmetic, the fundamental theorem of arithmetic and its applications to prime numbers, such as the Euler function and the Chinese remainder theorem, among others. others. For the transposition encryption system, an encryption and decryption algorithm can be determined whose mathematical basis is based on matrix algebra .

Keywords*: mathematical notation, RSA algorithm, encryption*

1. Introduction

Cryptography is the science that studies the methods and procedures, through mathematical algorithms, that allow reliability, integrity and confidentiality of information. in this work: matrix applications to cryptography, the points out: "there are various methods to encrypt a message" [1], it is commonly divided into three groups, which constitute classical cryptography: transposition cipher, substitution cipher, and symbol substitution cipher. A classic cipher is a channel to hide a message, known as a plain message, where letters are replaced or transposed by other letters, pairs of letters, and sometimes by many letters [2]. In cryptography, classical encryption was used historically and currently most of them are developed through computer applications [3]. The most modern methods use computers or other digital technologies, which operate with bits and bytes. Many classic ciphers were used by well-known figures [4], who created their own ciphers that have since been popularly used, many of which have military origins, other mechanical or electromechanical machines, such as Enigma [5], are sometimes grouped together with classical ciphers.[6]

This article proposes an algorithm to encrypt and decrypt messages by the double transposition system based on the pillars of linear algebra, which would represent a mathematical model based on matrix algebra for the encryption method of this classical cryptosystem [7],[8].Through the development of the mathematical foundations based on matrix algebra and its implementation in encryption and decryption by means of the double transposition system, a new methodology is proposed for the generation of algorithms and encryption and decryption functions based on matrix factorizations or decompositions. [10],[11-12]. , as is the case of the PALU factorization. For this purpose, this article is divided in such a way that the reader can find in chapter two, the development of the transposition encryption system for the particular case of encryption by the method known as double transposition, based on matrix algebra. The additional considerations that allow to generate new applications of the special factorizations in matrices for the development of new encryption and decryption algorithms are treated in detail in chapter three, for the applied case of the PALU factorization. In chapter four are the conclusions.

2. The System Of Encryption By Transposition

In the transposition encryption system, the letters of a message encrypted using this methodology remain the same as in the plain message, however they are reorganized according to a previous model or defined method, thus generating an anagram. A famous example of the latter is the pseudonym Avater, which, according

Computer Engineering Department / University of Technology-Iraq
Azhar.M.Alnaseri@uotechnology.edu.iq

to one theory, was chosen because it was an anagram of Raeatv, with the consideration that i and j are the same letter, just like u and v, as in Latin. From a cryptanalyst point of view, for a 26-characters alphabet (as is the case of the English alphabet, incorporating the n), if five letters are chosen to establish a linear ordering access key without repetition, the number of dispositions (word key, since it indicates the importance of the linear order) of letters that are possible to generate, or permutation, according to the principle of choice (or the product) is 26!/(26-5)!=8,688,600 possible linear arrangements without repetition. Impressive!, if you remember that you are only considering the choice of five letters from an alphabet of 26. Unlike the first case, the number of arrangements (linear) of the four letters of the word BALL is 12 and not 4! = 24. The reason is that you don't have to order four different letters. If the two letters L are distinguished as L1, L2, then the permutations of distinct objects can be used ; with the four symbols B, A, L1, L2, thus obtaining 4! = 24 permutations. However, each arrangement in which the letters L are indistinguishable corresponds to a pair of permutations with different letters L. Consequently, we have permutations with repetition: if there are n objects with n_1 of a first type, n_2 of a second type, ... and *n_r of an rth* type (objects of the same type are indistinguishable), where $n_1+n_2+ ...+nr = n$, then there are *n!/ (n1! n2! .. nr!)* (linear) arrangements of the given n objects.

The speed with which the values of n! grow is brilliantly recounted: “it can be calculated that 10! = 3,538,800, and this is precisely the number of seconds in six weeks. Consequently, 11! is greater than the number of seconds in a year, 12! exceeds the number that there is in 12 years, and 13! exceeds the number of seconds in a century.” The foregoing demonstrates that the transposition method is a system that requires prior agreement at all ends of the cryptosystem.

2.1. Transposition encryption techniques: the double transposition method.

This method consists of ordering the plain text of the message by rows and columns, creating a table that can be completed with null letters (a key can be established on the alphabet, which can be numerical, to encrypt the letters according to their order in the same). Once all the letters (or numbers) that represent the text of the message have been arranged, forming the table, permutations are made by rows and columns, one or more times. This would give us what is known as the double transposition method. In the following example considering the double transposition encrypted message. The message is passed to a square table with 5 x 5 entries (since there are 25 letters in the message), numbered by rows and columns.

Table 1. Plain message table: double transposition cipher.

0	1	2	3	4	5
1	W	A	Y	Q	O
2	C	B	X	R	J
3	E	A	Y	A	F
4	V	M	D	U	Z
5	T	B	C	R	T

Next, the order of the columns is swapped randomly, knowing that the receiver of the message knows the final arrangement in which it will be left. Assuming that the chosen order is (4-2-5-1-3). In addition to the order of the columns, the order of the rows must also be changed, following the same numbering order, just for this example. Both layouts (rows and columns) correspond to the keys of the cryptosystem k_1,k_2, these being presented in numerical form or by means of the word associated with the numerical assignment of the alphabet used, which for this example, the layout (4-2-5-1-3) corresponds to k_1=k_2= WCEVT. A swap only in column order or row order is known as a simple transpose method. The following table shows the proposed permutations.

Table 2. Table of the message in the clear encrypted by double transposition with key (4-2-5-1-3) (in rows and columns).

0	4	2	5	1	3
4	Q	A	O	W	Y
2	R	B	J	C	X
5	A	A	F	E	Y
1	U	M	Z	V	D
3	R	B	T	T	C

The encryption of the message is obtained by transcribing from left to right and from top to bottom, by rows, the letters of this last table. Presenting, for example, in a group of some depth. Using groups of five characters, the encrypted message looks like this:

QAWOY RBJCX AAFEY UMZVD RBTTC

The encrypted message obtained contains 25 letters of which there are repetitions, such as B, R, S, D, A, N with a frequency of two, i with a frequency of three, or with a frequency of four and finally the letters T,V, O, X and E with only one appearance in the plain message. The number of repeating, linear permutations (or arrangements) of the message is (2!5/2!6·3!·4!)=1.680.102, hence the importance of the key! However, by laying out the message in a table, the possible permutations of rows and columns that can be generated are (parsing the number of linear

arrangements). This method is also vulnerable to frequency analysis.

2.2. Matrix mathematical foundations in the formulation of the encryption method by double transposition.

One of the first objectives of this article is to mathematically formalize the double transposition encryption system through the use of matrix algebra. To do this, it starts with the following definitions and types of special arrays,

Definition 2.1 Upper Triangular Matrix (U): Let $U = [u_{k,j}] - (n\text{^}2)$ be a square matrix of order n. U is said to be an upper triangular matrix if:

$$u_{k,j} \quad \begin{matrix} = 0 \; xk \;\; k > j \\ \neq 0 \; xk \;\; k \leq j \end{matrix} \qquad \text{.....(1)}$$

Definition 2.2 Lower Triangular Matrix (M): $M = [m_{k,j}] - (n\text{^}2)$ be a square matrix of order n. L is said to be a lower triangular matrix if:

$$m_{k,j} \quad \begin{matrix} = 0 \; xk \;\; k < j \\ \neq 0 \; xk \;\; k \geq j \end{matrix} \qquad \text{.....(2)}$$

Definition 2.3 Diagonal Matrix (O): $O = [o_{k,j}] - (n\text{^}2)$ square matrix of order n. D is said matrix diagonal if:

$$o_{k,j} \quad \begin{matrix} = 0 \; xk \;\; k \neq j \\ \neq 0 \; xk \;\; k = j \end{matrix} \qquad \text{.....(3)}$$

A particular case of a diagonal matrix is the identity matrix of order n, denoted by *I_n*, which has unit values on its main diagonal.

Definition 2.4 Elementary operations: Let Amxn be a matrix of m rows and o columns (or dimensions m x o). On the matrix A, three operations called elementary are defined:

1. Swap row (or column) k for row (or column) j. Symbolically, the notation for the permutation of rows and columns is adopted, respectively, by $F_k \updownarrow F_j$, $C_k \updownarrow C_j$.
2. Multiply row (or column) i by a scalar a≠0. Symbolically, aF_k, aC_j for the case of applying the scalar to a column.
3. Add i times row (column) k to row (column) j, k≠j. Symbolically $(F_k+i)*(Fj, C_k+k*Cj)$.

The elementary operations (operations- elementary) allow to define the elementary matrices.

Definition 2.5 Elementary Matrix: An elementary matrix is that square matrix that is obtained from the identity matrix, by applying a single fixed elementary operation or column according to (2.2) on In, which is denoted by E_k and F_j , respectively.

An elementary matrix is nonsingular.

In (elementary-operations) are the mathematical foundations for the matrix formulation of encryption and decryption by double transposition. The elementary operations and matrices are calculated to the example considered in the transposition cipher section by the double transposition method to the double transposition encrypted message passed to a 5 x 5 square matrix (table). The order of the columns and rows arranged in random way is (4-2-5-1-3). The operations and associated elementary matrices are given by:

$$F_1 \updownarrow F_5,\ C_5 \updownarrow C_1,\ C_1 = A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$F_2 \updownarrow F_3,\ C_3 \updownarrow C_2,\ C_2 = A_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$F_3 \updownarrow F_5,\ C_5 \updownarrow C_3,\ C_3 = A_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

To finish the analysis of matrix algebra in terms of the mathematical foundations in encryption by transposition using the double transposition method, in relation to the definitions (elementary-operations) and (elementary-matrix) the following results are proposed.

Definition 2.6 Matrix congruence relation: If a finite sequence of elementary operations is carried out on $A \in M$ mxn, a matrix $B \in M$ mxn is obtained which is said to be congruent with matrix *A* and is denoted by *A~B*.

Theorem 2.1. The relation (2.2) is an equivalence relation between matrices.

That is: let $A \in M\_(m \; x \; n)$ *(R)* and *E* be an elementary matrix that comes from *I_m*, the multiplication from the left of *A / E* performs the same elementary operation on the rows of *A* as the one performed on the identity matrix for obtain *E*. Analogously, the right multiplication of *A / F* performs the same elementary operation on the columns of *A* as the one performed on the identity matrix to obtain *F*.

In conclusion: the table associated with the plain message arranged in rows and columns by means of a double transposition cipher, and then the application of permutations of rows and columns, correspond to elementary operations of permutation of rows and columns (elementary-operations) on the table seen as an array of the message to encrypt. That is a finite mapping

of elementary matrices (matrix-elementary) from the left and from the right.

Continuing with the example of the application of elementary operations and matrices on the table (table-example-double-transposition) we obtain, Thus obtaining the matrix of the encrypted message:

0	1	2	3	4	5
1	W	A	Y	Q	O
2	C	B	X	R	J
3	E	A	Y	A	F
4	V	M	D	U	Z
5	T	B	C	R	T

$$\begin{matrix}1&0&0&0&0\\0&0&0&1&0\\0&0&1&0&0\\0&1&0&0&0\\0&0&0&0&1\end{matrix}\qquad\begin{matrix}0&0&0&0&1\\0&0&0&1&0\\0&1&0&0&0\\0&0&1&0&0\\1&0&0&0&0\end{matrix}\qquad\begin{matrix}0&0&0&0&0\\0&0&0&1&0\\0&0&1&0&1\\0&1&0&0&0\\1&0&0&0&0\end{matrix}$$

Which according to (encrypted-example-message) checks the application. (non-singularity-theorem) allows the inversion of each permutation matrix, which solves the problem of deciphering the encrypted message to obtain the plain message.

The following chapter proposes the generalization of the application of matrices in the encryption of messages in a cryptosystem. This application consists of the PALU special factorization.

3. Encryption Using Special Matrix Factorizations: Encryption By Palu Factorization

This method consists of ordering the text of the plain message by rows and columns, creating a matrix that can be filled with null characters or symbols to generate a square matrix. Each entry in this array is uniquely assigned a character from the corresponding alphabet used by the ends of the cryptosystem. If *(n∈Z^)* corresponds to the length of the alphabet, then n must be prime. It is assigned to each character of this ordered alphabet an element of the set *(Zn+ 0)*, which has structure of body for n prime. This consideration allows generalization of the alphabet used in other classic cryptographic systems, for example, the possibility of considering the space between the words that make up the message, differentiation between upper and lower case letters, numbers or accented letters, among other possibilities, enrich the encoding of the message in clear and thereby hindering the work of the cryptanalyst.

Once all the numbers that represent the plain text of the message formed in the matrix have been arranged, the encryption consists of the permutations of rows and/or columns, one or several times, which is known as the double transposition method and the elimination of part of this message by transforming by equivalence the matrix of the message in clear in an upper triangular matrix (upper-triangular) associated with matrix *A* is obtained by the product thus achieving an encrypted message of shorter length: *E-1*E-1…E-1*E-1... Ei* matrices are triangular ,than the original message and with a triple security key, two associated with the double transposition method and one corresponding to reduction by staggering. lower, with ones on its main diagonal, therefore also *E -1∀i=1,2,…,j* are also lower triangular and the product of lower triangular is known to be lower triangular, therefore *L is a*

Let be the matrix of the plain message A=[a] mod(n), lower triangular matrix with ones on its diagonal k,j where *m2=m×m,m∈Z^+* corresponds m^2 to the number ofmajor. However, and according to the above, the *elements (lk,j= -rk,j for k > j. For k=j, lk,j=1 and k < j, lk,j=0).*rows (and columns) of the matrix A squared. Applying the PALU factorization algorithm as follows:

checks that the element dij=aij,i=j (element of the main diagonal of the matrix) called element pivot is not zero. If so, row permutation is applied, according to the elementary operations (elementary-operation}) defined. If it is different from zero, the elements of column j below the pivot are eliminated, for this, they are defined for each row.

This matrix configures what is called the decryption key matrix and is delivered through the factors (Table 3) organized as elements of a lower triangular matrix for its inverse application through (Table 3). Finally, the permutations carried out on the representative matrix of the message in the clear generate the permutation matrices P , P that is constructed

k=j+1,j+2,…,m-1, m the factors or multipliers, for *1*, *2* each column (fixed) j. Since *a_kj∈Z ∀k,j and (Z ,+,·)*

according to what was revised for the double method n transposition (table-example-double-transposition).
has an algebraic body structure, the existence and uniqueness of the symmetric elements for both operations defined on the set is ensured. Let *(-akj)* be the symmetric element with respect to *(Zn,+)* or additive inverse of *akj and dj-2* the symmetric element with respect to *(Zn,·)* or multiplicative inverse (reciprocal) of dj, thus defining the multiplier for each row i, for a column j,
Elementary operations (elementary-operations) are applied using the following algorithm: all elements below the main diagonal of column j will cancel, the other elements of the matrix below row j will also be affected according to the operation ,
The reduction algorithm ends when the matrix A is represented as an upper triangular matrix denoted by U (for Up). The reduction of a square matrix to one of the triangular forms can be achieved by successive left (or right) multiplications of suitable elementary matrices. That is, if *A* can be reduced to an upper triangular matrix *U* by elementary row operations, then
The permutations in rows that generate the matrix P1 and columns P2 establish the first two keys of the system, respectively.

3.1. Encryption application by PALU factorization.
Considering the message matrix in clear ENCRYPTION APPLYING PALU FACTORIZATION,

Table 3. Matrix of the message in plain ENCRYPTION APPLYING PALU FACTORIZATION.

0	1	2	3	4	5	6
1	W	y	d	Q	H	P
2	C	b	J	v	R	I
3	A	A	L	C	I	e
4	O	u	f	Z	O	Y
5	M	S	r	R	T	k
6	a	D	P	A	L	U

Table 4. Matrix with the numerical assignment with Z59 arithmetic of the message in the clear (Table 3).
The double transposition encryption is applied to the matrix (numeric-table-example-LU), by means of a permutation in rows and columns, thus generating the first two keys k_{1},k_{2}, respectively of the encryption: k_{1}=(6,3,4,5,2,1)= DATEHBCD and k_{2}=(4,3,6,1,2,4)=CHBFCED. The matrix *P1 AP2*, where
the permutation matrices *P1,P2* are modeled by the matrix formulation of the double transposition method.
Table 5. Matrix (Table 4) with the application of permutations in rows and columns.
The encrypted message is obtained by transcribing from left to right and from top to bottom, by rows, according to the numerical assignment of the alphabet used. Thus, the message is given by PNU enl gtr AIY DER ytr rrpo. Presenting in blocks of three characters, as is usual for sending, it is as follows:

0	4	3	6	1	2	4
6	11	31	41	18	28	0
3	45	24	12	21	36	23
4	15	11	27	35	3	13
5	43	24	18	3	29	26
2	26	S	17	39	17	0
1	2	15	38	43	31	42

The third encryption key k3 corresponds to the collection of factors (or multipliers) r_kj, which allow the determination of the lower triangular matrix associated with the LU factorization. According to its position in the matrix (k,j) transcribing from left to right and from top to bottom, by rows, we have for this application: ZHYTREDweuthRETH
From the cryptanalyst point of view, there are algorithms in such a way that the matrix U and the matrix L remain in the same square matrix. The strategy lies in the fact that being all the elements of the main diagonal of U ones, the space to store them is not required. This procedure can be applied under the field structure of (Zn,+,·) for n primes. There are also ways to program the algorithm so that the permutation matrices, which governs the double transposition method P1, P2, are presented by a single vector (independently, of course) with n values, numbered, indicating how the arrays should be permuted. identity rules. This is very convenient because the matrices Pi is such that of its n2 values all are zero except n which are 1. Using these storage techniques required by the algorithm of
PALU factorization can be reduced from *3n*2 to n2+n* floating point numbers, which means a space saving of about 66%. Regarding the modular arithmetic used, the determination of the additive and multiplicative symmetric elements in *(Zn,+,·)* has a degree of complexity of the order of $(Log\,2^{a})^{3}$, *where* $a \in Zn$ is the class to which its symmetrics are needed. The foregoing, because in the use of the extended Euclid's algorithm numbers decay by half (at least) every two steps.

4. Conclusions

The encryption and decryption method, with mathematical foundations developed in the matrix algebra proposed in this article, begins with the revision of the transposition system, specifically with the double transposition method. This methodology allows extrapolation to new encryption techniques. PALU matrix factorization is one of these new proposed methodologies. Among the scope is the possibility of generalizing the alphabet by incorporating new characters. The possibility of hiding and substituting part

of the message that is to be communicated in the cryptosystem allows to raise the degree of security and integrity of the information, in this way an improvement in the efficiency of the encryption methods in the line of the communication systems is obtained. transposition, also incorporating a greater number of keys. The result obtained shows us a good encryption performance, due to the length of the alphabet used, the orders of the matrix calculations and the use of modular arithmetic.

Reference

[1] B. Stroustrup, OOPS Messenger, 1995, an addendum to the OOPSLA '95 Proceedings.

[2] J. R. Cary, S. G. Shasharina, J. C. Cummings, J. V. W. Reynders, and P. J. Hinker, Comput. Phys. Commun. ~submitted!; available at http:// jove.colorado.edu/˜ cary/CompCPP–F90SciOOP.html.

[3] Y. Dubois-Pe`lerin and Th. Zimmermann, Comput. Methods Appl. Mech. Eng. 108, 165 ~1993!.

[4] J-L. Liu, I.-J. Lin, M.-Z. Shih, R.-C. Chen, and M.-C. Hseih, Appl. Numer. Math. 21, 439 ~1996!.

[5] Th. Zimmermann, Y. Dubois-Pe`lerin, and P. Bomme, Comput. Methods Appl. Mech. Eng. 98, 291 ~1992!.

[6] L. Machiels and M. O. Deville, ACM Trans. Math. Softw. 23, 32 ~1997!.

[7] Th. Zimmermann and D. Eyheramendy, Comput. Methods Appl. Mech. Eng. 132, 259 ~1996!. 14. D. Eyheramendy and Th. Zim

[8] P. Moyer, Are we having fun yet? How teachers use manipulatives to teach mathematics, Educ. Stud. Math. 47 (2) (2001) 175–197, http://dx.doi.org/10.1023/A:1014596316942.

[9] P. Moyer, G. Salkind, J. Bolyard, Virtual manipulatives used by K-8 teachers for mathematics instruction: The influence of mathematical, cognitive, and pedagogical fidelity, Contemp. Issues Technol. Teach. Educ. 8 (3) (2008) 202–218.

[10] J.L. Cross, B. Brewer, E. Hamner, L. Zito, S. Speer, M. Tasota, Pilot results of a digital manipulative for elementary mathematics, in: AERA Annual Meeting, San Francisco, CA, 2020, URL http://tinyurl.com/sxgvcuy Conference Cancelled.

[11] S. Suh, M. Lee, E. Law, How do we design for concreteness fading? Survey, general framework, and design dimensions, in: Proceedings of the Interaction Design and Children Conference, in: IDC '20, Association for Computing Machinery, New York, NY, USA, ISBN: 9781450379816, 2020, pp. 581–588, http://dx.doi.org/10.1145/3392063.3394413.

[12] Mirghafoori S H, Sayyadi Toranlu H, Dehghani Ashkezari J. Provision of a Model to Spread the Use of Information Technology in Serving. sjis 2020; 2 (1) :1-6