International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 8, pp.3202-3216
doi: 10.25147/ijcsr.2017.001.1.214
https://stepacademic.net

Short Paper*

An Enhancement of Text Encryption Algorithm with Hybrid Two-Square Cipher and Columnar Transposition Cipher

Mary Grace O. Ostia
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
mgoostia2020@plm.edu.ph
(corresponding author)

Alessa L. Crisostomo
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
alcrisostomo2020@plm.edu.ph

David Jhozel R. Lucas
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
djrlucas2020@plm.edu.ph

Francis Arlando L. Atienza
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
faatienza@plm.edu.ph

Raymund M. Dioses
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
rmdioses@plm.edu.ph

Jamillah S. Guialil
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
jsguialil@plm.edu.ph

Leisyl M. Mahusay
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
lmocampo@plm.edu.ph

Jonathan Morano
Computer Science Department, Pamantasan ng Lungsod ng Maynila, Philippines
jcmorano@plm.edu.ph

Date received: May 7, 2024
Date received in revised form: July 11, 2024; July 15, 2024
Date accepted: July 15, 2024

Recommended citation:

Ostia, M. G. O., Crisostomo, A. L., Lucas, D. J. R., Atienza, F. A., Dioses, R. M., Guialil, J. S., Mahusay, L. M., & Morano, J. (2024). An enhancement of text encryption algorithm with hybrid two-square cipher and columnar transposition cipher. *International Journal of Computing Sciences Research, 8*, 3202-3216. https://doi.org/10.25147/ijcsr.2017.001.1.214

**Special Issue on International Research Conference on Computer Engineering and Technology Education (IRCCETE). Guest Associate Editors: Dr. Roben A. Juanatas (National University-Manila) and Dr. Nelson C. Rodelas (University of East).*

Abstract

Purpose – Enhance the Two-Square Cipher's effectiveness by developing an algorithm to address vulnerabilities in plaintext variations, character set limitations and encryption performance.

Method – Proposed adjustments include expanding the grid to 14x14, using table shuffling instead of random character insertion, and strategically inserting random special characters in odd-length plaintexts.

Results – The algorithm demonstrated improved encryption, producing more random ciphertext sequences and successfully recovering original characters during decryption.

Conclusion – The developed algorithm outperforms the current Two-Square Cipher, enhancing encryption security and adaptability to different plaintexts.

Recommendations – Further enhance the algorithm to address specific issues such as character transformation, while maintaining the grid size at 14x14.

Research Implications – Contributes to advancing cryptographic techniques, highlighting the importance of addressing vulnerabilities in existing ciphers to strengthen data security.

Keywords – two-square cipher, columnar transposition, text encryption, cryptography, block and stream cipher

INTRODUCTION

One of the biggest challenges in the digital world is data security. Unauthorized access to private data may result in negative outcomes (Budiman, Rachmawati, & Parlindungan, 2018). Information security focuses on privacy and privacy protection,

using cryptographic encryption techniques to prevent unauthorized deciphering of data. Its main goal is to reduce security lapses and misuse of private data by unauthorized parties. (Kester, 2013).

The history of cryptography dates back two millennia, to a prehistoric use by Julius Caesar. Caesar, realizing the need to protect military communications, devised a simple substitution cipher in which he substituted one letter for another, thus establishing the first example of cryptography in action (Lopez, 2018).

Using two 5 × 5 sets of alphabets organized either horizontally or vertically, the Two Square cipher stands out as a classic symmetric algorithm (Kumar & Sharma, 2017) (Rachmawati et al., 2018; Es-Sabry et al., 2018). The two square cipher relies on 25 uppercase letters in plaintext, causing difficulties in decryption and omission of one letter. It also ignores spaces, leading to their exclusion. The introduction of "X" ensures a uniform strategy in odd-numbered plaintexts (Es-Sabry et al., 2018).

The two-square cipher, along with a modified columnar transposition cipher, enhances security in the encryption process by adding complexity to the straightforward transposition cipher (Abbasi & Singh, 2021).

Classically ciphers that rearranged the letters of plaintext were called transposition ciphers. They can be recognized because ciphertext letter frequencies are the same as plaintext letter frequencies (Christensen, 2015). Transposition ciphers in cryptography encrypt plaintext by shifting unit locations, creating a ciphertext permutation. Columnar transposition reads messages column by column, choosing columns in unpredictable order, and arranging messages in predetermined length rows (Kester, 2013). Writing the plaintext in rows and extracting the ciphertext column by column is known as columnar transposition (Zafar, 2023).

The issues were resolved by expanding the grid to 10x10, removing the 'X' letter when the word's length was odd, and introducing a pseudo-random character (Calumbiran & Camangian, 2022).

Despite the aforementioned improvements or adjustments, the algorithm still displays limitations. Because the 10x10 grid cannot handle all ASCII characters, the algorithm has certain weaknesses when it comes to encryption and decryption, which might result in omissions and compromised security. A significant problem also occurs with pseudo-random character production, which makes a specific character more predictable. Accurate decryption is further challenged by appending a random character based on a key (n) value after encryption. To overcome these problems, a 14x14 grid with all ASCII characters is proposed. Additionally, character insertion is made random by including special characters on the dataset for increased security, and the key function is changed to shuffle the grid to optimize columnar transposition.

LITERATURE REVIEW

The encryption and decryption process involves obtaining plaintext and encryption keys, segmenting them into digraphs wherein random characters are inserted if the plaintext is odd, and creating a character matrix. The Transposition Columnar method is used to reorganize the matrices, and the Two-Square Cipher is used to encrypt data. The decryption process is similar, starting with ciphertext extraction, random character removal, matrix column rearrangement, and pad character elimination.

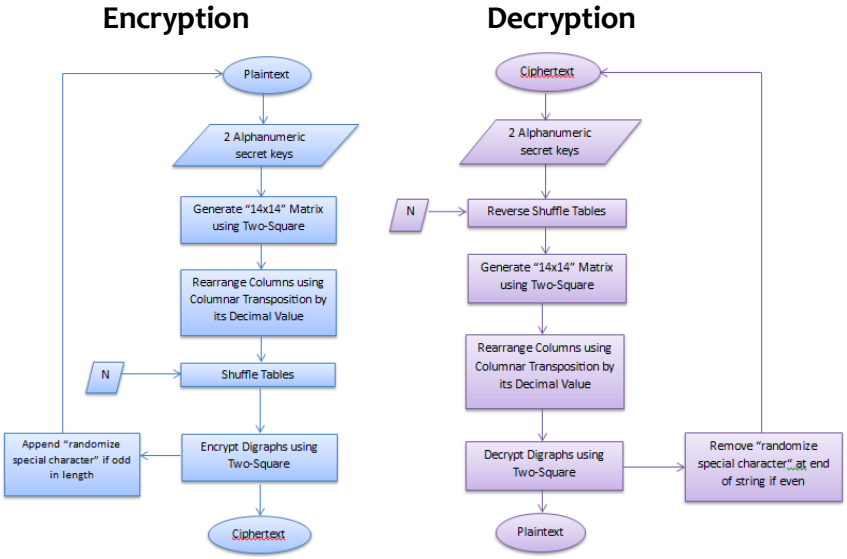

Figure 1. Encryption and Decryption of the Proposed Algorithm

Composition of Cryptography

As stated by Ronald (1990), cryptography is the discipline committed to protecting the confidentiality of information. Cryptography, which often involves two parties, tries to promote safe data communication while preventing attackers from collecting any sensitive information (Qadir & Varol, 2019; Rubinstein-Salzedo, 2018). Symmetric cryptography, a traditional cryptographic method, uses secret-key cryptosystems to ensure information secrecy by utilizing cryptographic algorithms.

a) A message space (m), also called plaintext, can be any type of data, including text, numerical data, executable programs, and other types of data (Delfs & Knebl, 2015).
b) A key space (k), or a set of characters that are given to the encryption algorithm along with the plaintext.
c) A ciphertext space (c), or the encrypted plaintext.

d) An encryption algorithm (E) mapping k X m into c, or the process that converts m into c.

e) A decryption algorithm (D) mapping k X c into m, the process that converts c into m.

Symmetric cryptography uses the same secret key for both encryption and decryption, hence D(k, E(k, m)) = m. Wherein the plaintext (m) is encrypted into ciphertext, c = E(k, m), before being transmitted, which is then decrypted once received, m = D(k, c).

Diffie and Hellman established public-key cryptography, also known as asymmetric cryptography, in 1976, solving the long-standing problem of safe key exchange and setting the framework for the development of digital signatures (Delfs & Knebl, 2015). Asymmetric cryptography uses two distinct, mathematically related keys, the public key (pk) and the secret key (SK), for encrypting and decrypting plaintext. The public key is accessible to the general public, while the secret key is kept confidential for decrypting ciphertext. Anyone can encrypt a message using the public key, but decrypting the ciphertext without the secret key is practically impossible (Delfs & Knebl, 2015).

Symmetric cryptography, known for its simplicity and efficiency, is commonly used for encrypting large volumes of data, while asymmetric cryptography is used for system requirements (Delfs & Knebl, 2015). The Two-Square Cipher is a good example of symmetric cryptography.

Existing and Proposed Algorithm

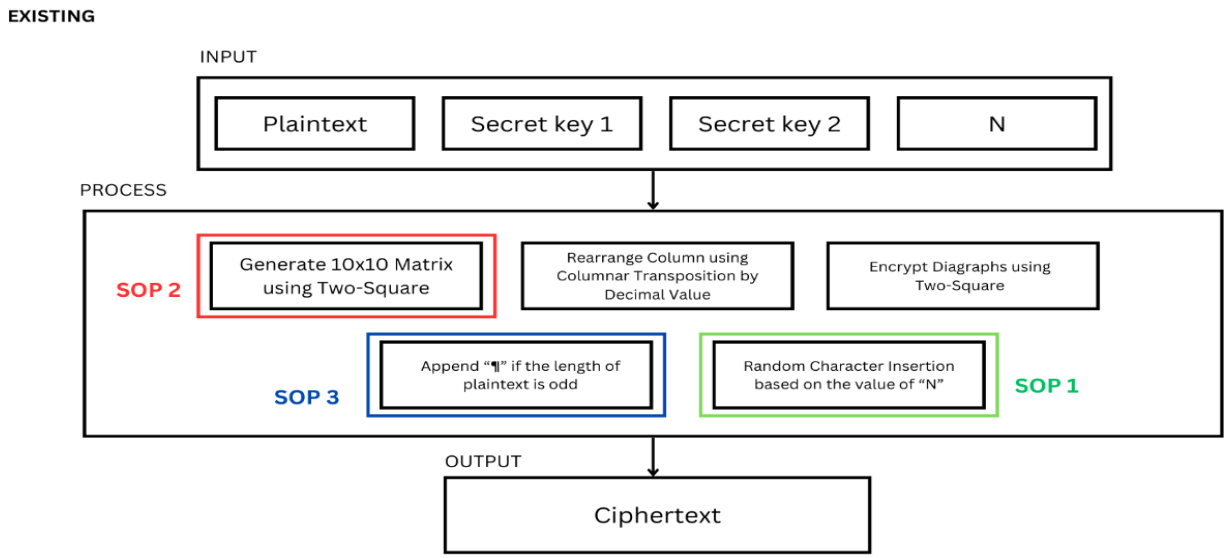

Figure 2. Existing Text Encryption

In the Existing Text Encryption, the first step in the encryption process is entering the plaintext, secret keys, and n value (Figure 1). Next, two 10x10 grids are created, rows are filled in using the keys first followed by the remaining characters from the data set, and a specific character (¶) is added if the plaintext length is odd. After that, the plaintext is split into digraphs, and the letters are switched around according to where they appear on the grids. The user-inputted number 'n' is then used to determine the random characters introduced into the ciphertext.

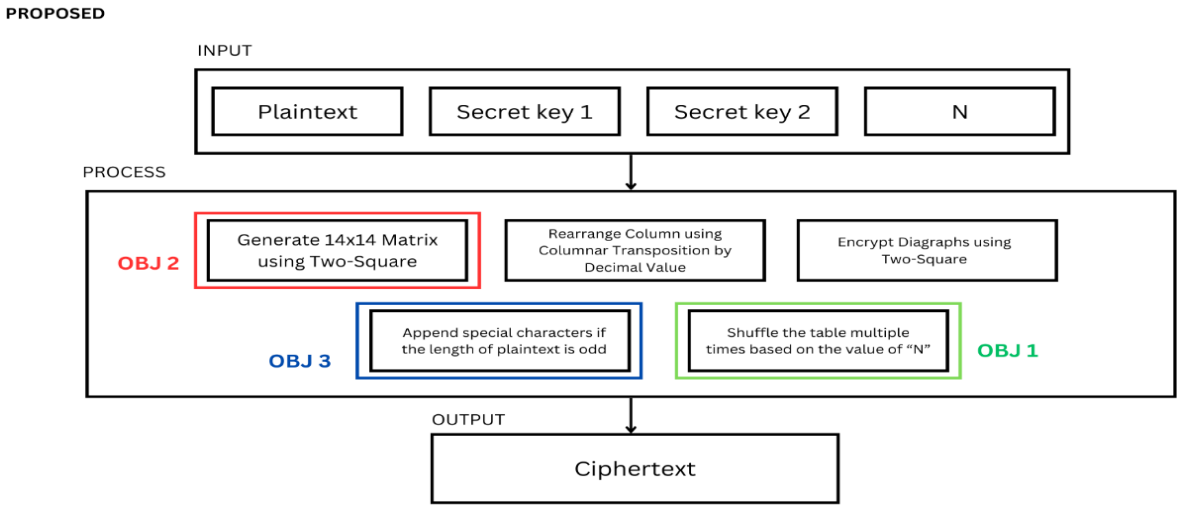

Figure 3. Proposed Text Encryption

The Proposed Text Encryption algorithm outlined above represents a more advanced version than the existing text encryption algorithm provided earlier (Figure 2 and Figure 3). It introduces several enhancements such as using larger grids (14x14), replacing the use of the value of 'n' wherein it is now used to shuffle columns of the matrices, and appending a random special character to the plaintext if its length is odd, thereby enhancing the security and complexity of the encryption process.

The study compares the current algorithm and its improved version using a comprehensive flowchart. The flowchart demonstrates the grid's expansion from 10x10 to a more comprehensive layout, highlighting the optimal application of the columnar transposition technique. It also highlights the deliberate transition from appending specific characters to random characters, enhancing the algorithm's security protocols.

METHODOLOGY

The study implies a hybrid Two-Square Cipher and modified Simple Columnar Transposition Cipher, as well as alphabet extension for flexibility, to overcome the limitations of the original Two-Square Cipher.

Alphabet Extension

The grids or tables within the structure of the Two-Square Cipher are constrained by a

limited character set, consequently restricting the number of characters that can be encrypted using this cipher. To overcome this limitation, a proposed improvement involves expanding the alphabet to encompass all ASCII characters, inclusive of extended ASCII characters. This expansion aims to populate the two 14 x 14 grids, totaling 196 characters, as depicted in the image below (Figure 4).

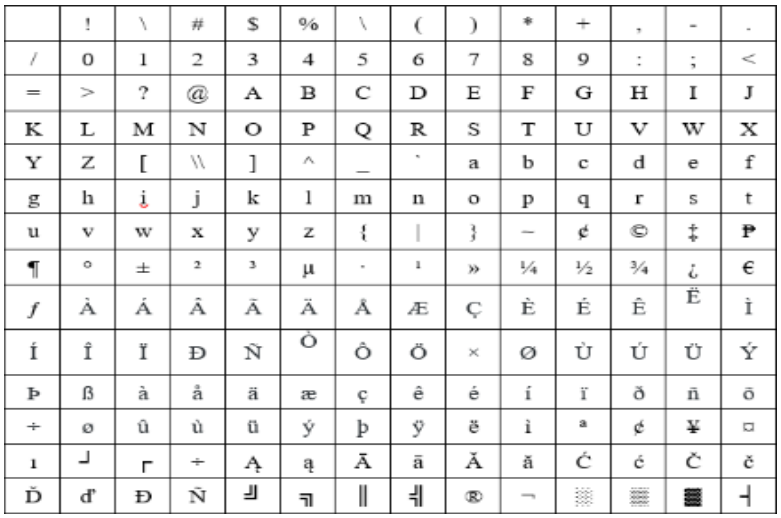

Figure 4. 14 x 14 ASCII Characters

Hybrid Two-Square Cipher and Columnar Transposition Cipher

The Two-Square Cipher, a widely used encryption method, has been refined to enhance its security by expanding its character set, integrating it with the full Columnar Transposition Cipher, and incorporating random characters. This method requires users to input plaintext and three keys into the encryption algorithm. The detailed procedure for the proposed method is outlined below.

Design

This study aims to enhance the security of encrypted text files by examining current encryption methods, detecting potential weaknesses, and applying robust measures to enhance the overall protection of sensitive data.

This enhances the encryption capabilities of an existing algorithm by increasing its grid size from 10x10 to 14x14, supporting all ASCII characters, and utilizing the columnar transposition approach for full cryptographic potential. Additionally, random special characters are introduced for odd text lengths to address a weakness in the encryption process, reducing risk from predictable patterns. These goals aim to improve efficiency, safety, and flexibility in processing diverse textual data.

The algorithm uses a numerical key, two secret keys, and plaintext to function. The remaining characters are inserted in each table without repeating any characters after the two secret keys are placed. Columns are shuffled using a number key, mimicking a

columnar transposition key. The two-square cipher verifies even letters in the plaintext, appending a random special character for odd-numbered characters. The ciphertext is generated by matching the letters from the first table to the other.

RESULTS

Existing Two-Square Cipher Algorithm

Eleven plaintext messages of varying lengths were encrypted, decrypted, and subjected to testing using the existing two-square cipher. The Arithmetic Mean Test and Monobit Test were employed to assess the encryption's effectiveness.

Table 1. Existing Two-Square Cipher Encryption

PLAINTEXT LENGTH	PLAINTEXT	ARITHMETIC MEAN TEST (mean value > 0.5)	MONOBIT TEST (p-value > 0.01)	RESULT
20	With the higher wind	0.4943181818181818	0.8801684549067255	}hYhDjzheZx%ighex/isdn
26	Dance with joy, my friend!	0.45689655172413796	0.18916127259520793	|NQdm%bishD7Zz%E$$#sZ vigEqd$c
44	Sunshine kisses gently, birds sing joyfully.	0.4819734345351044	0.407867043902164	"nanshidoZ¶Bwifo&IgentA"s$ $big7&lHfsdqZz%Eskll:/
44	The quick brown fox jumps over the lazy dog.	0.45663265306122447	0.08593180021994952	GeX%bquicl!;lh%C$lsex]jump&l%Bqhvjzhej !j¶/ne8b
50	Mist hills silent pines, an alone owl hoots softly	0.5089285714285714	0.7054569861112734	^ZYstZxwblsyjywbqdz/fEgdo. sM¶$lkb(q7%b%C"lvevqF&ls osj"s
58	The stars shimmer brightly in the velvety night sky above.	0.4819734345351044	0.407867043902164	4eX%bstkh&l^frwccox/lhrigvj "sZy$lhhD%bho"pqjl¶/dsghz/ fu5¶/ab%B6b
83	The ancient oak tree stood majestically, its branches reaching towards the heavens.	0.48097826086956524	0.30202822810977686	]eX%bkdciqdez/TG!lvDee7jy vAe7j!ajoqihEQkll\EKZyvEZ VGdmwhe&lgAcahi(dqjz%Ck hnihjzheZxTkhons&\
85	In the quiet forest, a stream murmurs softly, its melody soothing the weary traveler.	0.48774193548387096	0.49492274940962633	8qJjzhejwgsyqjZvqDqi0EeM ¶jyvDTk#l1muu6ur&IsoBsj"s $$wj&l¶colo$ijyqA]hDwdxbh D%b>iokh¶/vD!fqbqh&\
97	With a swift breeze, blossoms dance, painting the spring air with shades of pink	0.47282608695652173	0.14036866077167334	_hYhDM¶jyisXsjZ gA%j-irZ lossq6&laSkdm-ijvaiBntwdxb hD%b‡spgEdqM¶wh: wwjzbfradrqij#&bfEdu
118	Underneath the starry night, waves whisper secrets, and the moonlight unveils a world of dreams on the tranquil beach.	0.48365384615384616	0.2917477655212689	LsTdeu7TkhDljzhejyWGuD.¶ /dsgh0E w_!fqi whispIqhjyecgAvEg$$kd$bh D%baomq7bsghz/5unhowb& l!bTwou/$beBZ"9gAkc&lq7jz ~hejzVGnqgs"lbeca9b
216	In the heart of the ancient forest, symphony of rustling leaves and birdsong serenaded the lush surroundings, as sunlight filtered through the dense canopy, illuminating the tranquil scene of nature's timeless beauty	No Output	No Output	No Output
	Average Result =	0.432494469569656 (FAILED)	0.390552000544983	

Table 1 reveals that the existing two-square encryption, while passing the monobit test with its p-value higher than 0.01 which proves its randomness, does not meet the arithmetic mean test requirements, as it is below 0.5, making it easier to breach. The average results are inconsistent and there is an algorithmic flaw, particularly when dealing with characters not in the dataset. For example, the system cannot provide an output due to an apostrophe (') in plaintext.

Table 2. Existing Two-Square Cipher Decryption

PLAINTEXT LENGTH	PLAINTEXT	RESULT
22	}hYhDjzheZx%ighex/isdn	With the higher wind
29	|NQdm%bishD7Zz%E$$#sZvigEqd$c	Dance with joy, my friend!
48	"nanshidoZ¶Bwifo&IgentA"s$$big7&lHf sdqZz%Eskll:/	Sunshine kisses gently, birds sing joyfu3ux\
48	GeX%bquic!l;lh%C$lsex]jump&l%Bqhvjzhej !j¶/ne8b	The quick brown fox jumps over the lazy 6i"k
67	^ZYstZxwblsyjywbqdz/fEgdo.sM¶$lkb(q 7%b%C"lvevqF&lsosj"s	Mist hills silent pines, an alone owl hoots softly
64	4eX%bstkh&l^frwccox/lhrigvj"sZy$lhhD %bho"pqj!¶/dsghz/fu5¶/ab%B6b	The stars shimmer brightly in the velvety night sky above
92	]eX%bkdciqdez/TG!lvDee7jyvAe7j!ajoqi hEQkll\EKZyvEZ VGdmwhe&lgAcahi(dqjz%CkhnihjzheZ xTkhons&\	The ancient oak tree stood majestically, its branches reQkhing towards the heave.n¶\
94	8qJjzhejwgsyqjZvqDqi0EeM¶jyvDTk#l1 muu6ur&lsoBsj"s$$wj&l¶colo$ijyqA]hD wdxbhD%b>iokh¶/vD!fqbqh&\	In the quiet forest, a stream murmurs softly, its melody soothing the weary travlg0d¶\
88	_hYhDM¶jyisXsjZ gA%j-irZ lossq6&laSkdm-ijvaiBntwdxbhD%b‡sp gEdqM¶wh: wwjzbfradrqij#&bfEdu	With a swift breeze, blossoms dance, painting the spring air with shades of pink
129	LsTdeu7TkhDljzhejyWGuD.¶/dsgh0E w_!fqi whisplqhjyecgAvEg$$kd$bhD%baomq 7bsghz/5unhowb&l!bTwou/$beBZ"9gAk c&lq7jz~hejzVGnqgs"lbeca9b	Underneath the starry night, waves whisper secrets, and the q6onlight unveils a world of dreams on the tranquiblec2j"k
	No Output	

Table 2 shows that the message does not return to its original characters during the decryption process, which might lead to misspellings or, in certain situations, make the message incomprehensible. It is also noticeable that the arithmetic mean test and monobit test were not performed in the decryption process since what it does is to revert the encrypted text into its original form.

Proposed Two-Square Cipher Algorithm

Eleven plaintext messages of various lengths were encrypted and then deciphered to see if the suggested algorithm had passed the tests and fixed the limitations and weaknesses in the existing algorithm.

Table 3. Proposed Two-Square Cipher Encryption

PLAINTEXT LENGTH	PLAINTEXT	ARITHMETIC MEAN TEST (mean value > 0.5)	MONOBIT TEST (p-value > 0.01)	RESULT
20	With the higher wind	0.5560165975103735	0.08199556442374521	ïû÷=ëJ{Wë=òK{W¾<î[‡V
26	Dance with joy, my friend!	0.5135135135135135	0.641938220405063	wd'‡U³Kî[÷=ë?,@¼u.OsJö>îR²L
44	Sunshine kisses gently, birds sing joyfully.	0.501010101010101	0.964149827094507	"ù÷WñM‡Wë@òWse°YzW÷X-O¼uëM©H°Yë[÷Kë?,@'KõPĆ?
44	The quick brown fox jumps over the lazy dog.	0.5112474437627812	0.6188807818388096	ìú³K0K|U¼KëV,>¿KiSµY+KöT°Y,=îVëJ{WëA0þÀ<íSþN
50	Mist hills silent pines, an alone owl hoots softly	0.5058236272878536	0.775233561700436	õčëfë=òPõWëlòPîR¿<õ>‡WùZsE¿Køþô D³K,>½KñSôJ°YëaïX-O
58	The stars shimmer brightly in the velvety night sky above.	0.49928263988522237	0.9697851923488126	ìú³KëføĄ°YëZòQ©W¾<ëVòKñX-Oë>¿K÷=³Kve-LîXÀ<÷MõL¿<ë]À<₱Ă,=üN
83	The ancient oak tree stood majestically, its branches reaching towards the heavens.	0.5126903553299492	0.425702993814263363	ìú³KøÃiMîR¿<~E¼K÷HwWël÷E~HëCøüîW÷>uSõPĆ=ë>÷IsF©E‡U{W°Y©l₱ăñM÷KëJ,>øĄîWëJ{Wë=wSve÷Wèv
85	In the quiet forest, a stream murmurs softly, its melody soothing the weary traveler.	0.5056294779938587	0.7248973758103097	ñĎëJ{WëGî[îXsJôHîWą=sEël÷HwS¾K.KöCìd°YëaïX-O¼uòX°Y©WõS$OëlôE÷=òR¶K÷=³KweøĄÀ<÷H0úîPîV_w
97	With a swift breeze, blossoms dance, painting the spring air with shades of pink	0.5121693121693122	0.4543455281852 3816	ïû÷=sEëlî[îXsF©l%PüLsFõSëeôC°YvS‡UüLëFøû÷XòR¶K÷=³Këbö>÷KsEòV">òX·KëZ₱Ąî WëEµKõ>÷O
118	Underneath the starry night, waves whisper secrets, and the moonlight unveils a world of dreams on the tranquil beach.	0.4924187725631769	0.5725638111101173	íÃvWõDwS÷=ëJ{Wël‡EöHÀ<÷MõLą=">0úîW">ñMëbîVëlwU©l÷l¼uøÃ²K÷=³KöSôDõMõL¿<ì`veòP°YÀùîaöA²K~JsH©løÿ°YôDëJ{WëJ©E÷Ui[½KsW₱ăÿN
216	In the heart of the ancient forest, symphony of rustling leaves and birdsong serenaded the lush surroundings, as sunlight filtered through the dense canopy, illuminating the tranquil scene of nature's timeless beauty	0.4959254947613504	0.6791101779478186	ñĎëJ{Wë=wSöJëEµK÷=³KøÃiMîR¿<ïS©lëf¼u"]òTñS/OëEµK.<ëfõM÷KëAwSve°YøÃ²KëM©Hëa÷KëlîVîR₱ĄwVëJ{WëAìe·K"YöH,<‡VòRðW¼uøąëlì`õMõL¿<ïMõXîVwVëJñV,<ðLëJ{WsHîRsesGøÃôFĆ=ë>õPi_òRøĆòR¶K÷=³K÷HøÃ0KòPëluW‡WëEµK‡S/<©lï‡ëJòQîPîW°YsW0ù÷>îWru
	Average Result =	0.509611576 (Passed)	0.628054821 (Passed)	

Table 3 shows that consistent p-values greater than 0.01 for all eleven ciphertexts demonstrate that the suggested algorithm produces ciphertext that is more random than the existing Two-Square Cipher. The results were also consistent, making the tests reliable. Furthermore, these ciphertexts are more challenging to decipher with a mean value of more than 0.5 which is greater than the ones generated by the existing algorithm.

Table 4. Proposed Two-Square Cipher Decryption

PLAINTEXT LENGTH	PLAINTEXT	RESULT
20	xß‡úsĆ·Ûsú|Ï·ÛĄùwi¿Ú	With the higher wind
26	³}¿ÙüÏwi‡úsüLýÃëNÓ°Ć©ûwÖüÐ	Dance with joy, my friend!
44	?Ý‡Û{Ñ¿Ûsý|Û°sùg¶Û‡ÜMÓÄësÑ¾Ąùgsi‡ÎsüLýEĬ¢ÔēÜ	Sunshine kisses gently, birds sing joyfully.
44	uÞüÏQÏ¹ÙÃÏsÚLûąĬx×ýgKĬ©ØùgLúwÚsĆ·ÛsþQâĆüv×ČÒ	The quick brown fox jumps over the lazt dog.
50	¢wstsú|Ô¢Ûsą|ÔwÖąù¢ü¿Ûćh°ãąĬÞâ~ÃüÏLûäĬ{×~ĆùgsoxÜMÓ	Mist hills silent pines, an alone owl hoots softly
58	uÞüÏstÞèùgsh|Õ¾ÜĄùsÚ|Ï{ÜMÓsûąĬ‡úüÏ²sMÐwÜĆù‡ÑzĐąùskĆùÀæLúVÔ	The stars shimmer brightly in the velvett night skt above.
80	ÓÑÛ,Ý4Ï:ÒMÓêÝ5è:üâCÞÝ5ÜåÏWØ2ćKßåéçCÞĬ5ÜÑÛëÔäČÝÚ,ĆŸĬTÚ-ÛÝÝ4Õèü-ÖêčŸĬLêÚÒéĬ4ćÝÜ-Ûá	With a swift breeze, blossoms dance, painting the spring air with shades of pink
84	ÐĐĆŸÜÖĐßÒäē+æ4ĐÝÛ9àéĬ:Û4æ9Ĭ2ÜÒÒéÚ-ÞáÙây,Ĭ-Ü:Ý5ė4éçãéćKè:êÙÕßÛŸĬ;Ã-ÜÚÑéĬ;ãéĬ,àåßWÛéöÁ	The ancient oak tree stood majestically, its branches reaching towards the heavens.°
86	ÕDĬ;ãéĬ8ĐMÒêÝ;Ø9Òét,Ý4Ĭ:Û9àåĒÝĄŸÚ2ĐVćKĬSÓëäàĐÁÖëćKėéÙåûáĬ:Ø4Ü,ÖäČŸÛ,ĆŸàWÜÚē+Û9ĆĐÒâÒėëË	In the quiet forest, a stream murmurs softly, its melody soothing the weart traveler.c
118	ÑÖßéÚ3àåÛ,Ï;ãéĬ:é4Ú9ē+ÛßÔÞt,ù-ĆĐÒéù-ÕßĬTÒëĬ:àçè:Ü:ĐÁÜÖčÝÛ,ĆŸÚåØ3ÜßÔÞē+ĐRßWÖâćKēĬÒSÚ1čÝæ;Ý9è:ÜÕćKØ3Ĭ;ãéĬ;é4ÚçĐMđÝÝéêÙPà	Underneath the starrt night, waves whisper secrets, and the moonlight unveils ` world of dreams on the tranquil beach.
216	ÕDĬ;ãéĬ,àåÚ;Ĭ4ćÝÛ,ĆŸÜÖĐßÒäē+Óåė:ĬXĐÁùOÚæÕåąáĬ4ćŸĄ+ĬXÙßÛŸĬ1àáßWćKÜÖčŸĬßè9ĬSÛŸĬ:ÒèÒäēÚàėĬ;ãéĬ1ĐWčÝùKÚ9Ã+éèÕäÔéĐÁÜÜĬ:ĐRÜßÔÞē+ÓßÙêÒèàėĬ;ÕèÃ+ÔÞĬ;ãéÝ9ÒäŸWŸ8ÜÖØ5y,Ĭ-ÙâĐQÖäÜÜÖäČÝÚ,ĆŸÚ9ÜÖĆÝÖäĬ:Þéėéĭ4ćÝéåą+ė:ÓĬĬ;ÖāÒâÒéćKÝéĆĬą0	In the heart of the ancient forest, symphony of rustling leaves and birdsong serenaded the lush surroundings, as sunlight filtered through the dense canopy, illuminating the tranquil scene of nature's timeless beauty

Table 4 shows that almost all of the original characters can be successfully recovered throughout the decryption procedure. It is also noticeable that the arithmetic mean test and monobit test were not performed in the decryption process since what it does is to revert the encrypted text into its original form.

DISCUSSION

The cryptographic strength of the proposed algorithm is thoroughly assessed by precise cryptanalysis using techniques like the arithmetic mean test and the Monobit test. These tests are necessary to evaluate how reliable encryption techniques are. The arithmetic mean test divides the total number of ones and zeros by the binary length to determine how difficult it is to decrypt encryption, as highlighted by Yellapu (2018), Gaire et al. (2019), and Dionisio et al. (2014). A mean that is more than 0.50 shows that the algorithm is more resilient to cryptographic attacks and can endure possible dangers. An essential component of the encryption's security and unpredictability is the balanced bit distribution, which is ensured by this statistical measure. The algorithm's overall cryptographic strength is increased by showing strong resistance to decoding attempts by keeping a mean greater than 0.50.

An additional important technique to assess the cryptographic strength of the suggested algorithm is the Monobit test. With p-values greater than 0.01 signifying unpredictability, this test calculates the ratio of ones to zeros in a bit sequence. A bit sequence with a high degree of randomness is a good sign that the method is resistant to cryptanalysis attempts. Achieving a p-value above this threshold indicates that the bit sequence does not display any noticeable patterns, which makes it harder for attackers to exploit predictable structures, as noted by Yellapu (2018), Gaire et al. (2019), and Dionisio et al. (2014). By combining these tests, a thorough examination of the algorithm's security characteristics is possible, guaranteeing that sensitive data is adequately shielded from potential breaches and unauthorized access. Therefore, the Monobit test is essential for confirming that the encryption technique produces genuinely random sequences, which is the foundation of a strong cryptographic defense.

All things considered, the improved text encryption algorithm shows a notable increase in data security. The algorithm satisfies digital regulatory requirements and preserves confidentiality by passing both the arithmetic mean and Monobit tests. This lowers the likelihood of data breaches and unauthorized access. This in-depth analysis demonstrates how the algorithm may improve data security, which makes it a dependable option for protecting sensitive data in an increasingly digital environment. Users are highly assured of the integrity and security of their data because of the rigorous application of these cryptanalysis techniques, which guarantee that the encryption is resilient to changing cyber threats. As such, the algorithm provides a strong defense mechanism in the field of digital security, guaranteeing that private data is safe from malicious parties.

CONCLUSIONS AND RECOMMENDATIONS

The researchers provide an overview of their interpretation and findings from the study, which are based on the simulation results. It discusses the objectives achieved and delves into the researchers' suggestions for further enhancing the developed algorithm.

The study aims to improve the Two-Square Cipher's effectiveness by introducing a

14x14 grid structure and expanding the character set to all ASCII characters. Strategic enhancements include a complete columnar transposition cipher, table shuffling based on user input keys, and selective inclusion of special characters in odd-length plaintexts. This new algorithm provides a robust and secure alternative for protecting sensitive data, setting a new standard for data protection and accommodating a wider range of plaintexts.

The researchers recommend after a thorough examination of the study's findings and conclusion:

1. Further enhancement of the algorithm should be done as the letter "y" in some cases transforms into the letter "t", while the letter "a" becomes an apostrophe " ' ".
2. Given that the dataset already contains the ASCII characters that can be used in a message, it is advised that the grid remains at 14x14.

ACKNOWLEDGEMENT

The researcher expresses gratitude to God for His daily guidance and assisting them in their study, providing strength, health, and courage to face challenges, and to everyone who assisted them during the development and planning phases.

FUNDING

The study did not receive funding from any institution.

DECLARATIONS

Conflict of Interest

All authors declare that they have no conflict of interest in this study.

Informed Consent

This study did not directly involve human subjects, thus informed permission was not necessary. All data utilized in this study came from publicly available sources and academic reviews.

Ethics Approval

This study did not require ethical approval because it did not include any human or animal participants, nor did it contain any data that may identify individuals. The study was based exclusively on publicly accessible data and a literature evaluation.

REFERENCES

Abbasi, F. & Singh, P. (2021) Cryptography: Security and Integrity of Data Management. *Journal of Management and Service Science,1*(2), 4, 1-9. https://doi.org/10.54060/JMSS/001.02.004

Budiman, M. A., Rachmawati, D., & Parlindungan, M. R. (2018). An implementation of super-encryption using RC4A and MDTM cipher algorithms for securing PDF files on Android. *Journal of Physics: Conference Series*, *978*, 012090. https://doi.org/10.1088/1742-6596/978/1/012090

Calumbiran & Camangian (2022). *Text Encryption*. Pamantasan ng Lungsod ng Maynila

Christensen, J. (2015). *Columnar transposition*. Retrieved from https://www.nku.edu/~christensen/1402%20Columnar%20transposition.pdf

Delfs, H., & Knebl, H. (2015). Symmetric-key cryptography. In *Information security and cryptography* (pp. 11–48). Springer. https://doi.org/10.1007/978-3-662-47974-2_2

Rachmawati, D., Budiman, M. A., & Atika, F. (2018). PDF file encryption on mobile phones using super-encryption of Variably Modified Permutation Composition (VMPC) and two square cipher algorithm. *Journal of Physics Conference Series*, *978*, 012115. https://doi.org/10.1088/1742-6596/978/1/012115

Es-Sabry, Mohammed & el Akkad, Nabil & Merras, Mostafa & Saaidi, Abderrahim & Satori, Khalid. (2018). A Novel Text Encryption Algorithm Based on the Two-Square Cipher and Caesar Cipher. 10.1007/978-3-319-96292-4_7.

Gaire, R., Ghosh, R., Kim, J., Krumpholz, A., Ranjan, R., Shyamasundar, R., & Nepal, S. (2019). Crowdsensing and privacy in smart city applications. In *Smart Cities Cybersecurity and Privacy* (pp. 57-73). Elsevier.

Kester, Q. A. (2013). A hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher. *arXiv preprint.* Retrieved from https://arxiv.org/ftp/arxiv/papers/1307/1307.7786.pdf

Kumar, Sachin & Sharma, Rajendra. (2017). Securing color images using a Two-square cipher associated with Arnold map. Multimedia Tools and Applications. 76. 10.1007/s11042-016-3504-1.

Lopez, A. (2018). *Modern cryptography* (Master's thesis). California State University, Los Angeles, USA. Retrieved from https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1810&context=etd&fbclid=IwAR0nhsC7zRBQzjN-0olUrwxHg5MwMb-paItInGQWkIilkaFrgRDEtIzELzY

Qadir, A. M., & Varol, N. (2019, June). A review paper on cryptography. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE. https://ieeexplore.ieee.org/document/8757514

Rachmawati, D., Budiman, M. A., & Atika, F. (2018). PDF file encryption on mobile phones using super-encryption of Variably Modified Permutation Composition (VMPC) and two square cipher algorithm. *Journal of Physics: Conference Series*, *978*, 012115. https://doi.org/10.1088/1742-6596/978/1/012115

Sruthi, B., & Radhakrishna, V. (2015, September). Secure data transmission using MS-extended 8-bit ASCII character set. In *Proceedings of the International Conference on Engineering & MIS 2015* (pp. 1-8). ACM. https://doi.org/10.1145/2832987.2833073

Yellapu, G. (2018). Necessity of frequency (Monobit) test for pseudo-random bit generators.

Journal of Information and Optimization Sciences, 39(1), 1-4. https://doi.org/10.1080/02522667.2016.1231969.

Zafar, A. (2023, January). *Columnar transposition cipher.* Retrieved from https://www.geeksforgeeks.org/columnar-transposition-cipher/amp/?fbclid=IwAR13XArwJTRCGSyu8yJnUmPFVWSOMYb5NfHCTmQJFXK9zAvwzfxQJn6bIR0

Author's Biography

Born on August 9, 2001, Alessa L. Crisostomo is a fourth-year student at Pamantasan ng Lungsod ng Maynila, majoring in Computer Science. Alessa's commitment to excellence was evident as she graduated with high honors from senior high at the Philippines College of Criminology.

David Jhozel R. Lucas is a fourth-year (4th) computer science student from Pamantasan ng Lungsod ng Maynila (PLM). He completed his secondary education at San Jose Academy with honors. Throughout his twenty-one (21) years of existence, Lucas has been known for having a diverse set of interests, ranging from arts-related interests to sports and technology. All these interests have shaped him into a well-rounded individual with a passion-driven personality.

Mary Grace O. Ostia is a fourth-year Bachelor of Science in Computer Science student at Pamantasan ng Lungsod ng Maynila (PLM). She is also a former officer of the PLM Computer Science Society (CSS). She graduated Senior High School with Honors and has consistently been on the Dean's List throughout her college years.

Francis Arlando L. Atienza is a professor of Pamantasan ng Lungsod ng Maynila.

Jamillah S. Guialil is a professor of Pamantasan ng Lungsod ng Maynila.

Leisyl M. Mahusay is a professor of Pamantasan ng Lungsod ng Maynila.

Jonathan Morano is a professor of Pamantasan ng Lungsod ng Maynila.

Raymund M. Dioses is a professor and chairperson of the Computer Science Department at Pamantasan ng Lungsod ng Maynila.