An approach to Improving Columnar Permutation Cipher for Wills in Distributed Systems of Law Firms

Nwokedi, E. P
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
nwokedie@gmail.com

Oluwaseun, A. Ojerinde
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
o.ojerinde@futminna.edu.ng

Ojeniyi, A. J.
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
ojeniyija@futminna.edu.com

Adepoju, A. S.
Department of Computer Science, Federal University of Technology, Minna, Niger State, Nigeria
solo.adepoju@futminna.edu.ng

ABSTRACT

With the evolution of cryptography in the twentieth century, classical ciphers (transposition ciphers) are gradually being pushed out because it now possesses low security ratings, however we can still salvage them, as they have other desirable and admirable qualities which include: easy of design, medium technical know-how and low computational power and it is to achieve this that this study; "A three layer permutation Cryptosystem using a modification of Transposition cipher and two layers content permutation for Wills" was carried out . The aim of this study is to make columnar transposition more secure and relevant so that companies with low technology budget and know-how be secured from known cryptosystem attack. The method used to achieve the above aim is adding to columnar transposition the technique of rail cipher, this affected the sequence of transposition, and lead to a new encryption equation and function. Cryptanalysis was carried out using various tools (Cryptool 2, Dcode and Countwordsfree) and parameters, using a transposition decoder the cipher text gotten using the traditional transposition cryptosystem decrypted with a hundred percent word and character accuracy whilst using the improved system gave a thirty percent accuracy.

KEYWORDS

Index Terms: Cryptography, encryption, permutation, transposition

ACM Reference Format:
Nwokedi, E. P, Oluwaseun, A. Ojerinde, Ojeniyi, A. J., and Adepoju, A. S.. 2021. An approach to Improving Columnar Permutation Cipher for Wills in Distributed Systems of Law Firms. In *The 5th International Conference on Future Networks & Distributed Systems (ICFNDS 2021), December 15, 16, 2021, Dubai, United Arab Emirates.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3508072.3512287

ICFNDS 2021, December 15, 16, 2021, Dubai, United Arab Emirates

ACM ISBN 978-1-4503-8734-7/21/12…$15.00
https://doi.org/10.1145/3508072.3512287

1 INTRODUCTION

Information is very vital and should be kept secured through networks [1], however the threats to devices in a networked environment keeps on metamorphosing because of the variety in network devices, protocols, and configuration [2]. This is particularly more difficult for industries who are not in the technology industry but make use of electronic data.

Cryptographic algorithms play an important role in the security architecture of any communication network [3]. With the rapid growth of Internet, global information tide expends the application of information network technology. It also brings about great economic and social benefit along with the extensive use of this technology. However, because Internet is an open system which faces to public, it must confront many safe problems. The problems include network attack, hacker intruding, interception and tampering of network information which lead huge threat to Internet [4]. Information encryption and decryption systems are used to move information security forward making data secured from external attacks, this provides a higher level of guarantee, such that the data that are encrypted cannot be gotten and altered by unauthorized parties in the event of theft, loss or interception.

Cryptography, which is the broad terminology that houses encryption and decryption, is the science and art of making communication systems secured from attacks. The term is gotten from the Greek words: 'kryptos' means "hidden" and 'graphos' [5], [6]. There are two common approaches used to create ciphers systems, they are; substitution and permutation. Substitution substitutes plaintext characters or strings of letters by letters or numbers or symbols. Permutation uses the plaintext message letters but repositions their order [7] therefore the characters in the ciphertext are the same amount with those in the plain text, they are just put in different positions .

In cryptography, a transposition or permutation cipher is a cipher in which the order of the letters are altered, some sort of permutation, therefore instead of replacing the letters with other symbols as in substitution ciphers [8], [9]. Permutation cipher works by dividing a message into a fixed size blocks, and then reordering the letters within each block based on a fixed permutation, say P. The key to the transposition cipher is simply the permutation P. So, the transposition cipher has the property that the encrypted message, that is to say that the, ciphertext contains all the characters that

were in the plaintext message. It can be said that, the unigram statistics for the message are unchanged by the encryption process [5].

The size of the permutation is called the period. Looking at an example of a transposition cipher that has a period of six 6, and a key P= {4,2,1,5,6,3}. In this case, the message is broken into blocks of six characters, and after encryption the fourth character in the block will be moved to position 1, the second remains in position 2, the first is moved to position 3, the fifth to position 4, the sixth to position 5 and the third to position 6 [5].

To achieve authentication and non-repudiation using cryptography, digital signatures are used. In other words, to assure that a specific person/device has sent a specific message, it needs to be digitally signed, just like letters would be imprinted with a special seal and signed by hand of the sender in former times. A digital signature is a method for digitally signing data with, perhaps even more, certainty of identity than a handwritten letter. Formally, this authenticates the message sent, ensures that the sender cannot deny having sent it and also ensures senders identity [10]. There are essentially two types of digital signature algorithms, those that require the original message as input for the verification algorithm, and those that do not. In the latter case, the original message is recovered from the signature itself [10]. Other researchers have tried to improve the encryption security of transposition cipher and have managed to improve results.

Even though the world has enjoyed tremendous advancement in technology, and by extension cryptography over the years [11] the end for classical cryptography is not yet here, hybridizing classical ciphers [12], [13] would be key to keeping them relevant. This paper is divided into four sections, section 1, which would introduce the subject, give a background to the study and review related literature, section 2 shows the methodology used to achieve the results gotten from testing which is what the third section is about, finally the fourth section is the conclusion and further works.

2 RELATED WORKS

A. Cryptography - Data Encryption

Datum (plural Data) in its simplest form of understanding refers to information (Bard) that is collected together for reference and analysis, but it goes beyond that as information is actually processed data. Raw data also referred to as source data are data that has not been processed. There are different forms of data which include Big Data, Time-stamped data, Machine data. Encryption is the process of converting information or a message which is referred to as plaintext into a difficult unreadable form called ciphertext by using an encryption algorithm. [14], [15] .

Cryptography or cryptology (from Ancient Greek krypts “hidden, secret” and graphein, “to write”, or “study”, respectively) is the practice and study of techniques for secure communication in the presence of third parties. [6], [16]–[18] .The method of encrypting any text in order to conceal its meaning and readability is called cipher. It is derived from the Arabic word sifr, meaning zero or empty. In addition to ciphers meaning in the context of cryptography, it also means a combination of symbolic letters as in letters for a monogram which is a symbol made by combining two or more letters [17]. Cryptography is one way to conceal a message (confidential data) so that it is not easy to read or understood by people who are no right to access it [12]. The term “Confidential data” typically denotes data classified as restricted, according to a specific data classification scheme needs to be properly secured via any secured mechanism that will not reveal it presence to an unauthorized party, if measures are not put in place to secure data then an attacker can take compromise the data. [19], [20].

It is important to note that security does not prevent unauthorized access to a system; it only makes such access much difficult and this is what cryptography is known for. In today’s unsafe and increasingly wired world, cryptography plays a vital role in protecting communication channels, databases, and software from unwanted intruder [25].

Below are the four parts of all cryptographic process.

Plaintext: Clear text or unscrambled text to be sent to another person or entity over the network. It could be a simple text document, personal information, a simple text document to be transmitted over the network.

Cipher text: Cipher text refers to information that have been scrambled and difficult to understand by others unless with the knowledge of the correct key e.g. encrypted text to be transmitted over the network.

Key: This refers to formula, mathematical value or process that can be used to encode or decode a message. Keys are used to convert messages or information to a cipher text.

Cryptographic Algorithm: This could take a form of formula which can be used to encrypt or scramble a plain message into a form that cannot be easily understood by anybody unless with the knowledge of the key [22].

B. Columnar Transposition

Columnar transposition is arguably the most commonly studied of the transposition ciphers [27].To encrypt a plaintext, first copy the plaintext, character by character, into a rectangle (m by n matrix). The width of the rectangle becomes the length of the key. At the top of the rectangle, enter in the keyword, and on top of the keyword, write down the numerous corresponding numerical characters. Note that sometimes the last row of the rectangle is incomplete, this makes the transposition is longer (by one row). This situation is known as an incomplete Irregular Columnar or transposition rectangle Transposition. The case where all columns are of the same span, and all the rows are filled up, this is known as the Complete Columnar Transposition (CCT) [8].

To encrypt: Plaintext is written horizontally in k columns, and is then transliterated vertically column- by-column,

Example: Encrypt NOTHING IN THE WORLD IS MORE DANGEROUS THAN SINCERE IGNORANCE AND CONSCIENTIOUS STUPIDITY with a secret key of k = 9 columns.

Solution: Write down the plaintext in a horizontally format occupying 9 columns as follows:

N O T H I N G I N
T H E W O R L D I
S M O R E D A N G
E R O U S T H A S
I N C E R E I G
N O R A N C E A
D C O N S C I E N
T I O U S S T U
I D I T Y

The cipher text is therefore: ***NTSES NDTIO HMRIO CIDTE OONRO OIHWR UCANU TIOES ENSSY NRDTR CCSGL AHEEI TIDNA IAEUN IGNGN NP*** [28].

Transposition ciphers are stronger, more robust than simple substitution ciphers. Nevertheless, if the secret key is short in length and the message is long in length, then numerous cryptanalysis techniques can be applied to break such ciphers [29]. This argument applies to the columnar cipher, however rather than direct transpositioning of the columns, the rows would be divided into equal or near equal parts, depending on the average length of paragraph, line or string in the plaintext, and texts would be concatenated across paragraphs till it equals the number of the first paragraph, this would not yield the plain text if when the cipher text is arranged according to the key.

1. Rail Fence Cipher

Historically, Rail Fence is one of the classic cryptosystems worked by substituting the position of the characters, it also called Transposition Cipher by some researchers [8]. Transposition ciphers rearrange the letters of plaintext without replacing them with another character [9], [30]. It is called Rail fence because of its fencelike appearance, this cryptosystem was used in the early years of cryptography [27].

Rail Fence cipher was gotten from Polybius square modeling. However, in Rail Fence, the ciphertext does not follow the Polybius regulation. He formed his trajectory, this trajectory shaped Zig Zag. That is why this method is also often called the Zig Zag Cryptography. The Rail Fence is a simple example of the transposition ciphers and very weak encryption system which means it can be easily cryptanalyzed [30] .

Example: Encrypting NOTHING IS AS IT SEEMS by first writing it in a dualistic line, which will result to a zig-zag pattern which is also called a rail fence. The ciphertext is produced by transcribing the first row followed by the second row.

N T I G S S T E M
O H N I A I S E S

Cipertext: NTIGS STEMO HNIAI SES

To decrypt, write half the letters on one line, half on the second. (Note that if there are an odd number of letters, include the "middle" letter on the top line [28].

Researchers [7] [14] [15] have proposed a combination of Rail cipher with other ciphers (Caesar and substitution respectively) to improve its security. In this study the researcher is proposing a merger of columnar cipher with the technique of rail cipher.

2. Wills

A will is a legal document that is written by an individual (the testator or will-maker) that dictates how the property or/and assets will be distributed upon the death of the individual. A will also directs any estate taxes that you may owe, appoints a person to administer your estate based on your requests or state law (executor/executrix), and appoints a guardian for minor children among other things. If you have any assets, you should create a will to ensure that those assets go to the people you intend to have them [31], [32]

2.1 Electronic Will.

An 'electronic will' is a last will and testament created on a computer, authenticated with a digital identifier, and stored on electronic media rather than putting it on pen and paper. The testator signs the will electronically and then the witnesses sign electronically and remotely. The will is then notarized electronically and presumably stored electronically. [33], [34]

An electronic will is created and maintained in an electronic record and includes the date and electronic signature of the testator. Additionally, the will must include either an authentication characteristic of the testator, an electronic signature and seal from a notary public, or electronic signatures from two or more attesting witnesses. An authentication characteristic is defined as a characteristic unique to a certain person and "capable of measurement and recognition in an electronic record as a biological aspect of or physical act performed by that person. Authentication characteristics include the following: "a fingerprint, a retinal scan, voice recognition, facial recognition, video recording, a digitized signature or other commercially reasonable authentication using a unique characteristic of the person." [35], [36]

2.2 Advantages of Electronic Will

Electronic will execution could offer many advantages. An electronic document may be more conveniently executed as it does not require travel, the prospect of which may prevent certain groups such as individuals with disabilities or the elderly from executing or updating a will altogether. Electronic documents can be easily located and may be accessed from anywhere with just a few clicks, which is significantly more convenient than attempting to locate estate planning documents in a decedent's home or safety deposit box [37].

2.3 Electronic Signatures for electronic will

Although Morse code and the telegraph were used to electronically accept agreements from the mid-1800s, the use of electronic signatures (as we now known them) first arose in the mid-1990s. The internet was gaining popularity, and becoming a common arena in which to conduct business. The lack of regulations, and the rise of differing rules to govern online transactions, created confusion, and the legality of online agreements was constantly being questioned [38].

Countries around the world quickly responded by introducing legal frameworks for the use of electronic signatures. From 1998 onwards, many countries began introducing electronic and digital signatures legislation and, in 2001, the United Nations Commission on International Trade Law released the UNCITRAL Model Law on Electronic Signatures (the Model Law). This model law aims to 'assist States in establishing a modern, harmonized and fair legislative framework to address effectively the legal treatment of electronic signatures and give certainty to their status.'

In 1999, the Australian government passed the Electronic Transactions Act 1999 (Cth) as 'part of its strategic framework for the development of the information economy in Australia'.43 The Electronic Transactions Act was based on the Model Law. Each Australian state and territory government promptly followed suit [38].

A digital signature is an electronic signature that uses an encrypted digital certificate to authenticate the identity of the signer, and guarantees that the contents of a message have not been altered in transit. The signature is bound to the document with encryption, and everything can be verified using underlying technology known as public key infrastructure (PKI) [38].

2.4 Digital Signatures

To achieve authentication and non-repudiation using cryptography, digital signatures are used. In other words, to assure that a specific person/device has sent a specific message, it needs to be digitally signed, just like letters would be imprinted with a special seal and signed by hand of the sender in former times. A digital signature is a method for digitally signing data with, perhaps even more, certainty of identity than a handwritten letter. Formally, this authenticates the message sent, ensures that the sender cannot deny having sent it and also ensures senders identity [10].

There are essentially two types of digital signature algorithms, those that require the original message as input for the verification algorithm, and those that do not. In the latter case, the original message is recovered from the signature itself [10].

C. Cryptanalysis

Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems with a view to finding sequences, statistics and weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm. This is known as breaking the cipher, cipher text, or cryptosystem. The word breaking the cipher can be interchangeably used with the term weakening the cipher. That is to find a property or fault in the design of the encryption algorithm which would help the attacker to reduce the number of keys that he should try while performing brute force attack to break the code. For example, consider a symmetric key algorithm that uses a key of length 2∧128 bits which implies that a brute force attack would require the attacker to try all 2∧128 possible combinations to be certain of finding the correct key to convert the cipher text into plaintext, which is not possible since it will take thousands of years to try out each and every key. However, a cryptanalysis of the cipher text reveals a method that would allow the plaintext to be found in 2∧20 rounds. While it is yet not broken, it is now much weaker and the plaintext can be found with comparatively very less number of tries [39]. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

1. Ciphertext-Only Attack

In this case, the attacker knows only the ciphertext and the algorithms used. This is the most difficult scenario for an attacker. Based on the ciphertext, techniques such as the frequency analysis can be used to gain information about the plaintext. If a simple substitution was used on an English plaintext of reasonable length, the attacker can perform a frequency analysis. This is because the statistical information in the plaintext leaks through a simple substitution [18].

From statistics, the letter 'E' is the most common letter. The attacker can compute frequency counts in the obtained ciphertext. Based on this frequency counts, the most commonly seen letter in the ciphertext is an 'E'. So, the attacker can try to guess a few letters based on frequency until some words are recognized [18].

2. Known Plaintext Attack.

In a known plaintext attack, the attacker also knows some plaintext along with the ciphertext and the algorithms. This increases the probability of success of the attack, compared to the ciphertext only case. In general, the complete plaintext is not known and only a part of the plaintext is known. The attacker probably knows some words or letters and their the corresponding ciphertexts. The goal is to attack the system using these known plaintexts. This is a practical attack, because in the real-world situations the attacker is likely to know some plaintext. For example, the encrypted email header. As email uses a stereotypical header, the attacker can guess some plaintext corresponding to come ciphertext [18]. As some of the plaintext is known, the attacker need not perform an exhaustive key search as in the ciphertext? only case. The work factor is lesser than an exhaustive search.

3. Chosen Plaintext Attack.

This is an attack when the attacker has an option to use the plaintext of his choice to be encrypted and observe the corresponding ciphertexts. This provides more information to the attacker and hence, reduces the security of the cryptosystem. It is the best case from the attacker's perspective to figure the key. This type of attack is feasible in real world. A variant of the chosen? plaintext attack is the lunch time attack. Suppose that an authorized user forgets to log out of the system during a break, the attacker can gain access to a system and conduct this attack. An adaptively chosen? plaintext attack is also possible, in which the attacker selects the current plaintext based on the previous ciphertext. This would make the attacking the cipher much more simpler [18].

3 METHODOLOGY

A. Modified Columnar Transposition Encryption Algorithm

Create an N by N matrix

Input plaintext

Pick a key P which would equal the number of columns you would want to split text to.

Create cyphertext, rather than assembling text sequentially for each row as in columnar cipher, you assemble the first line from all the paragraphs till it reaches the original amount of characters

Therefore, if it is reversed in a columnar format it wouldn't make intelligible text as in columnar cipher.

B. Mathematical Model of New Approach

Encryption function:

$$\begin{aligned} &P_1Q_1 + P_3Q_1 + P_5Q_1 + P_7Q_1 + P_9Q_1 + P_2Q_1 + P_4Q_1 + P_6Q_1 \\ &+P_8Q_1 \cap P_1Q_2 + P_3Q_2 + P_5Q_2 + P_7Q_2 + P_9Q_2 + P_2Q_2 + P_4Q_2 \\ &+P_6Q_2 + P_8Q_2 \cap P_1Q_n + P_3Q_n + P_5Q_n + P_7Q_n + P_9Q_n \\ &+P_2Q_n + P_4Q_n + P_6Q_N + P_8Q_N \end{aligned} \tag{1a}$$

$$\sum_{(n=1)}^{k} \left[\sum_{(i=1)} \left[P_{(2i-1)}Q_n \right] + \right] \sum_{(i=2)} \left[P_{(2n)}Q_n \right] \tag{1b}$$

Two layers of content permutation would be applied, the individual permutated cipher texts would be permutated two again, with separate sequences for each iteration and unique keys for each part and sequence. These set of keys are kept with the primary beneficiaries, delivered to them through a secure channel such that

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
P1	N	O	T	H	I	N	G	I	N
P2	T	H	E	W	O	R	L	D	I
P3	S	M	O	R	E	D	A	N	G
P4	E	R	O	U	S	T	H	A	N
P5	S	I	N	C	E	R	E	I	G
P6	N	O	R	A	N	C	E	A	N
P7	D	C	O	N	S	C	I	E	N
P8	T	I	O	U	S	S	T	U	P
P9	I	D	I	T	Y				

Figure 1: Ciphertext= NSSDITENT OMICDHROI TONOIEORO HRCNTWUAU IEESYOSNA NDRCRTCS GAEILHET INIEDAAU NGGNINNP

even if their cipher text is gotten, it would still need those set of keys to decrypt.

Encryption Function =

$$P = P_{i1} + P_{ii1} + _{iii1} = P_{1'i.ii.iii} \tag{2a}$$

Two Layer Content Encryption=

$$P_{1'i.ii.iii} = P_{1'i.iii.ii} = P_{1'ii.iii.i} \tag{2b}$$

Decryption Function.

$$P = \sum_{n=1}^{k} \sum_{i=1} R_{2i-1}\ C + \sum_{1=2} R_{2n}\ C_n \tag{3a}$$

Using Plaintext;

NOTHING IN THE WORLD IS MORE DANGEROUS THAN SINCERE IGNORANCE AND CONSCIENTIOUS STUPIDITY

Divide text into strings of nine characters, which will result in an m by n matrix

In Section 3.0 Java was used to implement mathematical formula. See Figure 2 below

4 RESULT AND TESTING

In order to get a better overview of this research, the Will used was an extract from a mock up gotten from a legal chambers in Lagos south-western Nigeria, since it is an extract just a part of it was taken hence the numbering starting from 5.The section of the Will is stated below;

5. I hereby bequeath my real estate property at No 20 Jaiye Oyedotun Street, Magodo GRA 2, Lagos State to my son, Mr. Jeffery Omeike (Front House).

6. I hereby bequeath my house which Papa gave me at Emuhu Delta State to my brother, Mr. Sunday Omeike.

7. I hereby bequeath my land at Old Lagos-Asaba road, Emuhu, Delta State to my son, Mr. Greg Omeike absolutely.

Spaces would be taken out from text to make encryption across cryptosystems uniform thereby making the number of characters the same (for space counting and none space counting systems, matrix and non-matrix systems), this would also increase accuracy of decryption.

5.IHEREBYBEQUEATHMYREALESTATEPROPERTYATNO20 JAIYEOYEDOTUNSTREET, MAGODOGRA2,LAGOSSTATETOMYSON, MR.JEFFERYOMEIKE(FRONTHOUSE). 6.IHEREBYBEQUEATH-MYHOUSEWHICHPAPAGAVEMEATEMUHUDELTASTATETO-MYBROTHER,MRSUNDAYOMEIKE. 7.IHEREBYBEQUEATHMY-LANDATOLDLAGOSASABAROAD, EMUHU, DELTASTATETO-MYSON,MRGREGOMEIKEABSOLUTELY.

```
C:\Users\Emeka Nwokedi\Downloads>java ColumnarCipher
Original Text
[I, h, e, r, e, b, y, b, e, q]
[u, e, a, t, h, m, y, r, e, a]
[l, e, s, t, a, t, e, p, r, o]
[p, e, r, t, y, a, t, N, o, 2]
[0, J, a, i, y, e, O, y, e, d]
[o, t, u, n, S, t, r, e, e, t]
[,, M, a, g, o, d, o, G, R, A]
[2, ,, L, a, g, o, s, S, t, a]
[t, e, t, o, m, y, s, o, n, ,]
[M, r, ., J, e, f, f, e, r, y]
[O, m, e, i, k, e, (, F, r, o]
[n, t, H, o, u, s, e, ), ., I]
[h, e, r, e, b, y, b, e, q, u]
[e, a, t, h, m, y, h, o, u, s]
[e, w, h, i, c, h, P, a, p, a]
[g, a, v, e, m, e, a, t, E, m]
[u, h, u, D, e, l, t, a, S, t]
[a, t, e, t, o, m, y, b, r, o]
[t, h, e, r, ,, M, r, S, u, n]
[d, a, y, O, m, e, i, k, e, .]
[I, h, e, r, e, b, y, b, e, q]
[u, e, a, t, h, m, y, l, a, n]
[d, a, t, O, l, d, L, a, g, o]
[s, -, A, s, a, b, a, r, o, a]
[d, ,, E, m, u, h, u, ,, D, e]
[l, t, a, S, t, a, t, e, t, o]
[m, y, s, o, n, ,, M, r, G, r]
[e, g, O, m, e, i, k, e, a, b]
[s, o, l, u, t, e, l, y, .]
```

Figure 2: Putting Will in Matrix for Encryption

A. Encryption of Will using three-layer encryption system

In the Figure 1 below we find the will converted to matrices for encryption, closely followed by Figure 2 that shows the first layer of encryption using the data in Figure 1 above using the improved columnar cipher.

CIPHERTEXT;Il0,tOheutIddmsupo2MnegadusleheJMemewhhha, yoeet,rtaatae-tgesaaterhueetEslaruL.HtveyaAaOrtigoieiDrrOmouttna JohetOtsSmeayomkbce,elunthySgeummomhatebedyeyhlMbdh,

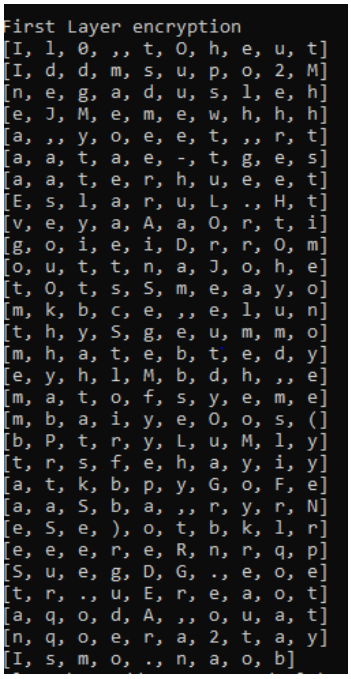

Figure 3: First Layer of Encryption using Improved Columnar Cipher technique

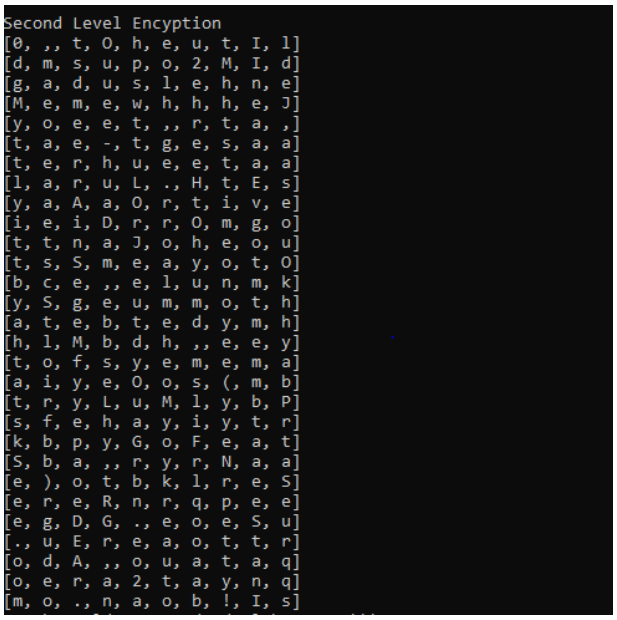

Figure 4: Second level of encryption using cipher text from first level as plaintext and content permutation and cryptosystem

ematofsyemembaiyeOos(bPtryLuMlytrsfehayiyatkbpyGoFeaaSba, ryrNeSe)otbklreeereRnrqpSuegDG.eoetr.uEreaotaqodA,ouatnqoera2 tayIsmo.naob

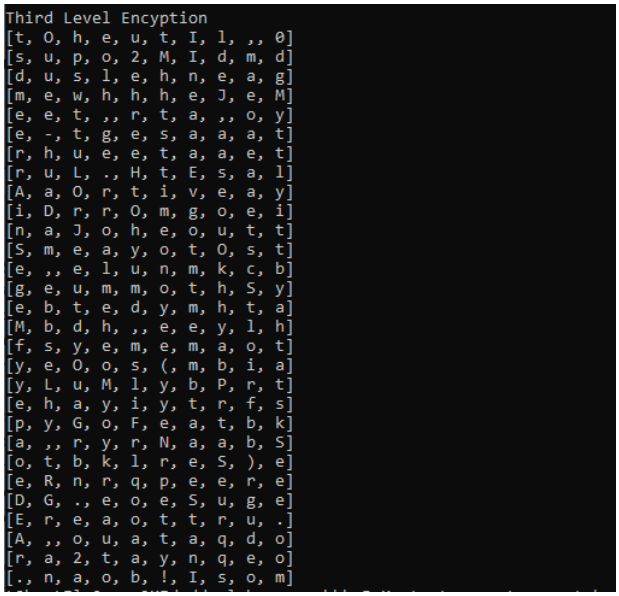

Figure 5: Third Level of encryption

CIPHERTEXT; 0,tOheutIldmsupo2MIdgaduslehneMemewhhhe Jyoeet,rta,tae-tgesaaterhueetaalaruL.HtEsyaAaOrtiveieiDrrOmgottna JoheoutsSmeayotObce,elunmkySgeummothatebtedymhhlMbdh, eeytofsyememaaiyeOos(mbtryLuMlybPsfehayiytrkbpyGoFeatSba, ryrNaae)otbklreSereRnrqpeeegDG.eoeSu.uEreaottrodA,ouataqoera2 taynqmo.naob!Is

FINALCIPHERTEXT;tOheutIl,0supo2MIdmdduslehneagmewhhhe JeMeet,rta,oye- tgesaaatrhueetaaetruL.HtEsalAaOrtiveayiDrrOmgoeina JoheouttSmeayotOste,elunmkcbgeummothSyebtedymhtaMbdh, eeylhfsyememaotyeOos(mbiayLuMlybPrtehayiytrfspyGoFeatbka, ryrNaabSotbklreS)eeRnrqpeereDG.eoeSugeEreaottru.A,ouataqdora2 taynqeo.naob!Isom

B. Analysis of performance of Researches Cryptosystem Against other popular Crypto systems used for last Will and Testament

Digital signatures, Transposition, Caesar and public key cryptosystems, for testing in this phase we would use Caesar, transposition cipher and public key crypto system (RSA) against the new system using the same will from IV.. Encryption would be done using CrypTool 2.0.

In this layer of testing brute force testing is used for cryptanalysis of all the ciphertext.

CIPHER TEXT GOTTEN FROM CAESAR CIPHER

5. S roboli loaeokdr wi bokv ocdkdo zbyzobdi kd Xy 20 Tksio Yionydex Cdbood, Wkqyny QBK 2, Vkqyc Cdkdo dy wi cyx, Wb. Toppobi Ywosuo (Pbyxd Ryeco).

6. S roboli loaeokdr wi ryeco grsmr Zkzk qkfo wo kd Owere Novdk Cdkdo dy wi lbydrob, Wb Cexnki Ywosuo.

7. S roboli loaeokdr wi vkxn kd Yvn Vkqyc-Kcklk bykn, Owere, Novdk Cdkdo dy wi cyx, Wb Qboq Ywosuo klcyvedovi.

KEY: 10, KEY MAPPING; A->K

CIPHER TEXT GOTTEN FROM TRANSPOSITION SYSTEM

IRYQAMEEAPPTT2AEETSEMOG2GSTOSMEEOIFNOEHEBUTYU WCAGEAMULSTOBTRSDOI7EBEEHLDOLOSAAMULSTOSMROIA

Table 1: Analysis of Performance of Proposed System against other system

s/n	Cryptosystem	Crypt Analysis scheme	Decryption key	Time taken to decode(secs)	% Similarity of characters	Difference of characters (Symbols)	%word accuracy
1	Caesar Cipher	Known Cryptosystem attack	Test all possible offsets (brute force)	2.98	100	0	100
2	Transposition Cryptosystem	Known Cryptosystem attack	Try all permutations (Brute force up to size 6)	9.32	92.62	22	100
3	2 Layer Transposition Cryptosystem	Known Cryptosystem attack	Try all permutations (Brute force up to size 6)	3.90	2.68	544	0
4	3 Layer Transposition Cryptosystem	Known Cryptosystem attack	Try all permutations (Brute force up to size 6)	4.92	1.59	557	0
5	Proposed system 3 – layer Encryption	Known Cryptosystem attack	Try all permutations (Brute force up to size 6)	3.69	0.71	563	0

OTY5EBEEHRLTEORAOJYYONRTGOAASATYNJFYEEOHSIRYQ
AMOEIPAVEEHEAATYOERNYEEHEBUTYNTDGABOEHEAATY
NGGEESULHEBUTYASTREYN0IODUTEADRLOTEMORFRMKR
TU6EBEEHHSHHP AMTUDTTEMRHMUAMKIRYQAMAALAS
ARDUDTTEMOREMKBLE

KEY: key = $(2,1,3)^{-1}$

CIPHER TEXT GOTTEN FROM 2-LAYER TRANSPOSITION

RAEP2EEGSSEFEBYCEUTTD7ELLAUTMITEELOOYROSYFESY
MIVHAONEBYDBHANEUETSE0DERTORR6EHHMDEHAIQAARD
ERKEIQEPTESOGOEIOETWGMSBSIBHOSMSSOO5EREAYN
GATJEHRAEAEAYREETTAEAYGSHUARNOTDOMFK UBH-
HAUTRUKYMLAUTOMLYMATATM2TMONH UUAALOROEE-
DOALORAYBHTRJOTAANYOIQOPEETEYHUNGOETGELBYTY-
IUALERMTEESPTTMMMRAASDTMEB

KEY: key = $(2,1,3)^{-1}$, key = $(2,1,3)^{-1}$

CIPHER TEXT GOTTEN FROM 3-LAYER TRANSPOSITION

A2GEBETEAMEORYSIAEDAUSDTRHDAADKQTOEEGBBSS5E
NTHEAETASAOOKHUUMUMMA2OUAREARBRTNIPTHGTLT
UETSTMATBRPESECT7LTTLYSEMHNYHET0RREMHQRRIPS
OOWSIOSORYAEAERTEGUNDFBARYAOYTMMHAOEOOYT
OAOOEYNEEYILMETMADEEESFYUDLUIEOOFYVOBBNEEE
O6HEIAEEEEGITMSHMOEAGJRAYEAYHRTMUHTKLTLAT
TNULODLAHJAYQEEUOGBYAREPMRSM

KEY: key = $(2,1,3)^{-1}$, key = $(2,1,3)^{-1}$, key = $(2,1,3)^{-1}$

From the table above the researcher discovered that there is no correlation direct between time taken to decode and the percentage similarity of the characters in multi-layer transposition ciphers, this goes to say that the fact that it took a longer time does not mean it would decrypt more and vice versa. However, correlation goes across board, in the sense that the percentage similarity of characters affects directly the characters difference and word accuracy.

5 CONCLUSION

In this paper the researcher has presented how to implement increase the security of columnar cipher by merging it the rail cipher technique.

Although both ciphers on their own are weak a combination of both techniques as the researcher has shown above would increase the security of the system with about ninety percent, it can also be deduced that time taken to decrypt seems to have no direct relationship with the number of layers.

This study indicates that an improvement in the columnar transposition system and combining it with two layers of computation brings the similarity of text, that is accuracy of character placement when tested on real life wills to less than one percent (0.71 to be exact), whilst other systems score above one percent, the lowest being 1.59%. This is consistent with [47] who believes that multiple layers increases security, [48]who supports the use of slightly different layers and [39] who supports using modified cryptosystems to improve security, finally it shows that classical ciphers can be improved to reduce statistical properties that make them easy to cryptanalyze, which according to [49] was a major drawback.

ACKNOWLEDGMENTS

This paper presentation project is supported by the Royal Academy of Engineering UK Grant under the Higher Education Partnership in Sub-Sahara Africa (HEP-SSA) Programme with project ID HEP-SSA1921 3 88

REFERENCES

[1] O. Oluwaseun, "Strategies for Managing Information Flow in Nigeria Healthcare System Strategies for Managing Information Flow in Nigeria Healthcare System," no. October, 2015, doi: 10.5120/ijais2015451443.

[2] O. S. Akanji, O. A. Abisoye, S. A. Bashir, and O. A. Ojerinde, "A Survey on Slow DDoS Attack Detection Techniques," *ITED2020*, vol. 3, 2020.

[3] S. A. Khan, "Design and Analysis of Playfair Ciphers with Different Matrix Sizes," *Int. J. Comput. Netw. Technol.*, vol. 3, no. 3, pp. 117–122, 2015, doi: 10.12785/ijcnt/030305.

[4] K. K. M, M. A. S, and S. Rasool, "Efficient Digital Encryption Algorithm Based on Matrix Scrambling Technique," *Int. J. Netw. Secur. Its Appl.*, vol. 2, no. 4, pp. 30–41, 2010, doi: 10.5121/ijnsa.2010.2403.

[5] A. T. Sadiq and L. Ali, "Attacking Transposition Cipher Using Improved Cuckoo Search," no. March 2014, 2015.

[6] M. El–Beheiry, "StegoCrypt: Arithmetic and Rudin – Shapiro Sequence – Based Bit – Cycling and 3DES Bachelor Thesis," 2019.

[7] C. Christensen, "Spring 2015 Chris Christensen MAT/CSC 483," 2015.

[8] G. Lasry, M. Hayarden, and N. Kopal, "Cryptanalysis of the Columnar Transposition Cipher with Long Keys," pp. 1–20, 2015.

[9] A. Mishra, "Enhancing Security of Caesar Cipher Using Different Methods," *Int. J. Res. Eng. Technol.*, vol. 02, no. 09, pp. 327–332, 2013, doi: 10.15623/ijret.2013.0209049.

[10] J. Bergquist, "Blockchain Technology and Smart Contracts: Privacy-preserving Tools," no. 17023, p. 62, 2017.

[11] I. I. and A. M. S. Ojeniyi, Joseph A, Bolaji O. Adedayo, "Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques," no. April, pp. 22–30, 2018, doi: 10.5815/ijigsp.2018.04.03.

[12] F. I. Lubis, H. F. S. Simbolon, T. P. Batubara, and R. W. Sembiring, "Combination of caesar cipher modification with transposition cipher," *Adv. Sci. Technol. Eng. Syst.*, vol. 2, no. 5, pp. 22–25, 2017, doi: 10.25046/aj020504.

[13] R. B. Lee, Z. J. Shi, Y. L. Yin, R. L. Rivest, and M. J. B. Robshaw, "On permutation operations in cipher design," *Int. Conf. Inf. Technol. Coding Comput. ITCC*, vol. 2, pp. 569–577, 2004, doi: 10.1109/ITCC.2004.1286714.

[14] R. Hackworth, "Data encryption," *Itnow*, vol. 37, no. 5, pp. 12–13, 1995, doi: 10.1093/combul/37.5.12.

[15] M. J. Sobol, "Data encryption," *Inf. Syst. Secur.*, vol. 3, no. 3, pp. 27–31, 1994, doi: 10.1080/10658989409342465.

[16] J. K. Ambulkar, "Poly Substitution Method for Encryption and Decryption," vol. 02, no. 05, pp. 1810–1812, 2010.

[17] A. Jain, R. Dedhia, and A. Patil, "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication," *Int. J. Comput. Appl.*, vol. 129, no. 13, pp. 6–11, 2015, doi: 10.5120/ijca2015907062.

[18] R. B. Muralidhar, "Substitution Cipher with NonPrefix Codes," 2011.

[19] I. Idris, O. E. Oche, and J. K. Alhassan, "An Infallible Technique for Hiding Confidential Data in Compressed Video using LSB and RSA Algorithm," no. Icta, pp. 1–5, 2016.

[20] A. O. Isah, J. K. Alhassan, and S. S. Olanrewaju, "Enhancing AES with Time-Bound and Feedback Artificial Agent Algorithms for Security and Tracking of Multimedia Data on Transition," vol. 6, no. 4, pp. 162–178, 2017.

[21] R. Gupta, P. K. Sadh, and P. Gautam, "A Study of Implemented Classical Cipher," vol. 5, no. July, pp. 1270–1275, 2018, doi: 10.22214/ijraset.2017.8180.

[22] J. K. Alhassan, I. Ismaila, V. O. Waziri, and A. Abdulkadir, "A Secure Method to Hide Confidential Data Using Cryptography and Steganography," no. Icta, pp. 105–110, 2016.

[23] O. Osho, Y. O. Zubair, J. A. Ojeniyi, and L. O. Osho, "A SIMPLE ENCRYPTION AND DECRYPTION SYSTEM," *Int. Conf. Sci. Technol. Educ. Arts, Manag. Soc. Sci. iSTEAMS*, pp. 77–84, 2014.

[24] A. A. Adedipe, "Nigerian Internet Fraud: Policy / Law Changes That Can Improve Effectiveness," 2016.

[25] R. Jamal, Z. Hussein, and S. By, "Transposition Cipher Text," pp. 1–43, 2012.

[26] M. Heydari, G. L. Shabgahi, and M. M. Heydari, "Cryptanalysis of transposition ciphers with long key lengths using an improved genetic algorithm," *World Appl. Sci. J.*, vol. 21, no. 8, pp. 1194–1199, 2013, doi: 10.5829/idosi.wasj.2013.21.8.22.

[27] C. Christensen, "Transposition Ciphers," pp. 1–31, 2010.

[28] R. Frost, "Rail Fence Cipher Keyword Columnar Transposition," vol. 124, no. Winter, 2009.

[29] M. Sokouti, B. Sokouti, and S. Pashazadeh, "An approach in improving transposition cipher system," *Indian J. Sci. Technol.*, vol. 2, no. 8, pp. 8–15, 2009, doi: 10.17485/ijst/2009/v2i8/29502.

[30] A. S. Utama, "Rail Fence Cryptography in Securing Information," *Int. J. Sci. Eng. Res.*, no. July, 2016.

[31] R. Stout, "Where There ' S a Will," pp. 1–95, 1938.

[32] A. Gadzo, "Types of Wills," pp. 39–41, 2021.

[33] K. B. Gee, "Chapter 1: Electronic Wills and the Future: When Today ' s Techie Youth Become Tomorrow ' s Testators," vol. 105, no. June 2009, 2005.

[34] B. J. Lebowitz, "Electronic Wills: No Longer in a Galaxy Far , Far Away," vol. 64, no. 1, 2017.

[35] N. Krueger, "LIFE , DEATH , AND REVIVAL OF ELECTRONIC WILLS LEGISLATION IN 2016 THROUGH 2019," vol. 1298, no. 2017, 2019.

[36] S. Snail and N. Hall, "Electronic wills in South Africa," *Digit. Evid. Electron. Signat. Law Rev.*, vol. 7, no. 0, pp. 67–70, 2014, doi: 10.14296/deeslr.v7i0.1925.

[37] S. Eva, "Are electronic wills on the way?," 2021.

[38] K. Martin, "TECHNOLOGY AND WILLS – THE DAWN OF A NEW ERA COVID-19 special edition," 2020.

[39] A. J. Ronak Dedhia, Abhijit Patil, "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication," *Int. J. Comput. Appl.*, vol. 129, no. 13, 2015, doi: 10.5120/ijca2015907062.

[40] T. Wu, Y. Chen, and H. Lin, "Design and Construction of Secure Digital Will System," vol. 13, no. 5, pp. 523–530, 2016.

[41] G. Samid, "The Ultimate Transposition Cipher (UTC).," *IACR Cryptol. ePrint Arch.*, vol. 2015, p. 1033, 2015.

[42] H. Lin, "Toward Secure Strong Designated Verifier Signature Scheme from Identity-Based System," vol. 11, no. 4, pp. 315–321, 2014.

[43] H. Ali-Pacha, N. Hadj-Said, A. Ali-Pacha, M. A. Mohamed, and M. Mamat, "The six-dos transposition cipher based on the rubik's cube," *Int. J. Adv. Technol. Eng. Explor.*, vol. 8, no. 75, pp. 258–273, 2021, doi: 10.19101/IJATEE.2020.762150.

[44] B. Thakkar and B. Thankachan, "A Multilevel Approach of Transposition Ciphers for Data Security over Cloud ISSN NO: 1869-9391 A Multilevel Approach of Transposition Ciphers for Data Security over Cloud," no. May, 2021.

[45] M. S. Hossain Biswas *et al.*, "A systematic study on classical cryptographic cypher in order to design a smallest cipher," *Int. J. Sci. Res. Publ.*, vol. 9, no. 12, p. p9662, 2019, doi: 10.29322/ijsrp.9.12.2019.p9662.

[46] J. Yi and J. Yi, "Cryptanalysis of Homophonic Substitution- Transposition Cipher," 2014.

[47] E. Antal, P. Zajac, and O. Grošek, "Diplomatic Ciphers Used by Slovak Attaché During the WW2," *Proc. 3rd Int. Conf. Hist. Cryptol. HistoCrypt 2020*, vol. 171, pp. 21–30, 2020, doi: 10.3384/ecp2020171004.

[48] D. Rachmawati, S. Melvani Hardi, and R. Partogi Pasaribu, "Combination of columnar transposition cipher caesar cipher and lempel ziv welch algorithm in image security and compression," *J. Phys. Conf. Ser.*, vol. 1339, no. 1, 2019, doi: 10.1088/1742-6596/1339/1/012007.

[49] G. Lasry, "A Methodology for the Cryptanalysis of Classical Ciphers with Search Metaheuristics," 2017.