

Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication

O.E. Omolara[1], A.I. Oludare[2] and S.E. Abdulahi[3]
[1]Ahmadu Bello University, Department of Mathematics, Zaria, Nigeria
[2]Nigerian Defence Academy, Department of Physics, Kaduna
[3]Ahmadu Bello University, Department of Mathematics, Zaria, Nigeria
Corresponding author: email: styleest2011@gmail.com

ABSTRACT
Many Ciphers have been developed to provide data security. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new modified hybrid way of encryption of plaintext. Using of large key spaces with huge number of rounds with multiple complex operations may provide security but at the same time affects speed of operation. Hence in this paper, a modified hybrid of Caesar Cipher and Vigenere Cipher with diffusion and confusion which Classical ciphers cannot boast of is proposed. The Caesar Cipher and Vigenere Cipher have been modified and expanded so as to include alphabets, numbers and symbols and at the same time introduced a complete confusion and diffusion into the modified cipher developed. Classical ciphers can be made effective and used for providing security by adding the properties possessed by the modern ciphers. In this paper, the characteristics of modern cipher were incorporated to classical cipher. Thus the proposed Scheme is a hybrid version of classical and modern cipher properties in which the modified hybrid of both the Caesar Cipher and Vigenere Cipher is now made a very strong cipher and difficult to break using a frequency method, brute force, etc.
Keywords: Encryption, Decryption, Substitution, Cipher, Random Number, Recursive, Primitive Root, Plaintext, Cipher Text, Optimization

1. Introduction

Secured communication involves encryption process at the sending end and decryption process at the receiving end of the communication system [1]. Over the years, there are many aspects to security solutions on many applications, ranging from secure commerce and payments to private communications and protecting passwords. Cryptography is the practice and study of hiding information. That is cryptography is the science of using mathematics to encrypt and decrypt data. Thus cryptography enables someone to store sensitive information or transmit it across unsecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. The Figure 1 showed types of cryptography.

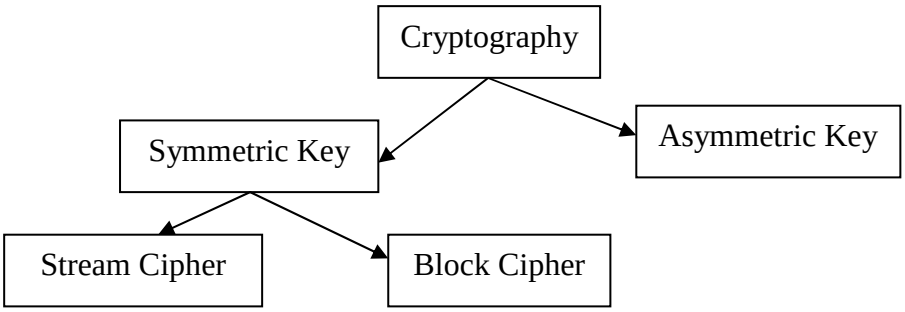

Figure 1. Types of Cryptography

Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords, and electronic commerce, which all depend on cryptography. Cryptography refers to encryption, the process of converting ordinary information (plaintext) into unintelligible cipher text. Cryptography is divided into two types, Symmetric Key Cryptography and Asymmetric Key Cryptography. In Symmetric Key Cryptography a single key is shared between sender and receiver. The sender uses the shared key and encryption algorithm to encrypt the message. The receiver uses the shared key and decryption algorithm to decrypt the message. In Asymmetric Key Cryptography each user is assigned a pair of keys, public key and private key. The public key is announced to all members while the private key is kept secret by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message. The process of converting plain text into Cipher text is called enciphering or encryption while restoring the plain text from the Cipher text is called deciphering or decryption. Decryption is the reverse, moving from unintelligible cipher text to plaintext. A cipher is a pair of algorithms which creates the encryption and the reversing decryption. The detailed operation of a cipher is controlled both

by the algorithm and, in each instance, by a key. This is a secret parameter for a specific message exchange context. Keys are important, as ciphers without variable keys are trivially breakable and therefore less than useful for most purposes. Historically, ciphers were often used directly for encryption or decryption, without additional procedures such as authentication or integrity checks. Encryption has long been used by militaries and governments to facilitate secret communication. The process of encryption and decryption is shown in Figure 2.

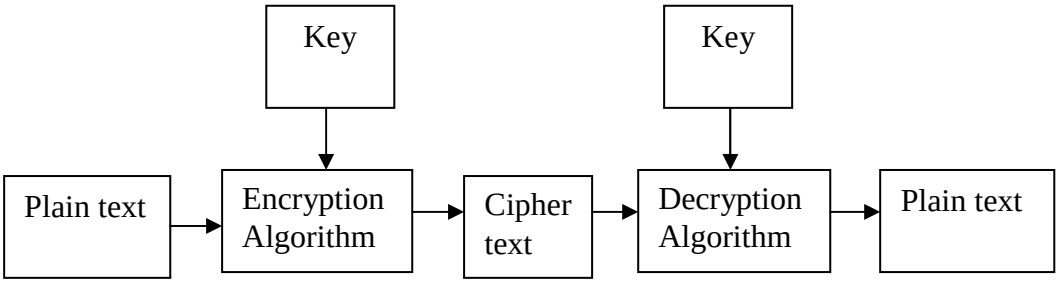

Figure 2.The process of encryption and decryption

It is now commonly used in protecting information within many kinds of civilian systems, banks, etc. For example, the Computer Security Institute in United States reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage[2]. Also, the Computer Security Institute (CSI) reported that the average annual loss reported by U.S. companies in the 2007 CSI Computer Crime and Security Survey is more than doubled, from $168,000 in last year's report to $350,424 in this year's survey. This ends a five-year run of lower reported losses. Financial fraud overtook virus attacks as the source of the greatest financial loss. Virus losses, which had been the leading cause of loss for seven straight years, fell to second place. Another significant cause of loss was system penetration by outsiders[3].

The challenge is that technology is advancing and evolving, and crimes are increasing as well, then data and information need to be well safe and avoid leakages, and loss, therefore, there is need for more research work into the field of encryption and cryptographic for a better secure future. The single most important reason for using encryption is to preserve confidentiality. This means that only an authorized receiver can read the message (the receiver must have the appropriate decryption key). Though there have being several works done to strengthen the classical ciphers such as an algorithm that allowed diffusion was incorporated to the Vigenere stream cipher strengthening it considerably (Phillip I. Wilson and Mario Garcia, 2006) but there are still need for further strengthening since the benefits of Cryptography is to offers individual privacy and confidentiality and in some circumstances also authentication and non-repudiation (e.g. legal ‘signatures’) and Especially important in explicitly Authorization . In this study, we will take advantages of classical or historical cryptography and clubbed it with the important features of modern cryptographic algorithms to create a cipher which we believe is indecipherable except the algorithm and the keys are known.

2. Aim of the Research

The primary goal of this paper is to develop a modified hybrid of Caesar cipher and Vigenere cipher that can prevent unauthorized access to or modification of sensitive information by introducing a large amount of diffusion and confusion into the cipher which classical cipher cannot boast of. This work aim at carrying out a modified hybrid of Caesar Cipher and Vigenere Cipher with 95% diffusion and confusion. “Cryptography is only a small part of the protection needed for "absolute" secrecy”[4], (Terry Ritter, 2006).

2.1 Research Objectives

The research aim to develop a modified hybrid of Caesar cipher and Vigenere cipher and the objectives are;

(i) To introduce a new and better secure confusion and diffusion into two classical ciphers; the Caesar Cipher and the Vigenere Cipher so as to produce a strong algorithm that is devoid of being attacked by brute force or frequency analysis.

(ii) To create an improved cipher where the plain text input determines how the algorithm works. A cipher that does the same work all the time is sensitive to attacks.

(iii) To develop a cipher with high avalanche effect; Avalanche effect refers to a desirable property of cryptographic algorithms where, if an input is changed slightly the output changes significantly (Sriram Ramanujam and Marimuthu Karuppiah, 2011). This will make it impossible to break the cipher if one step of the algorithm is missed thereby introducing a high level of security of the data.

(iv) To create a cipher where the frequency of the letters/symbols produced at the end of the day cannot be used to determine the plaintext unlike the usual Caesar and Vigenere Cipher that could be broken using frequencies of the letters.

3. Statement of Research Problem

It was discovered that originally, cipher text generated with Caesar Cipher algorithms and Vigenere algorithms are prone to be broken easily using brute force, exhaustive search, searching by frequency and many other methods because they lack diffusion and confusion in the algorithms that generate them. Though, the use of cryptography techniques such as encryption and decryption has significantly increase as it seems to promise to be the best method so far for achieving secure communication over a non-secure communications channel globally, which in turn will offers individual privacy and confidentiality and enhance both technological and socio-economical growth of mankind. This non-privacy and non-confidentiality in data communication has been posing very serious and necessary challenges such as ensuring that information is secure and transmitted confidentially. The experts have implemented several tools to transform data via encryption technology to prevent unauthorized access to or modification of sensitive governmental and public information yet intruders and fraudsters are still having their way.

Therefore for more secure communication there is need to,

i) Improve on secure communication technology on data encryption and decryption
ii) Improve on public-key cryptography system in place
iii) Provide adequate security to document or data confidentially and secrecy
iv) Provide more practical solutions to secure document or data confidentially
v) Provide cost-effective, efficient, and secure systems to protect the vast quantity of data stored and communicated by electronic data-processing systems, the growth in electronic fund transfers, instant electronic mail, point-of-sale terminals, home banking, and conferencing through computers, the threat of unauthorized accessibility to this data becomes a pressing concern of our society, hence the need for this type of secure communication. Furthermore, technology is advancing and evolving, and crimes are increasing as well, then data and information need to be well safe and avoid leakages, and loss, therefore, there is need for more research work into the field of encryption and cryptographic for a better secure future.

4. Significant of Study

The significance of this study is:

(i) Introducing a new and better secure confusion and diffusion into two classical ciphers; the Caesar Cipher and the Vigenere Cipher so as to produce a strong algorithm that is devoid of being attacked by brute force or frequency analysis.

(ii) Creating an improved cipher where the plain text input determines how the algorithm works. A cipher that does the same work all the time is sensitive to attacks.

(iii) Developing a cipher with high avalanche effect; Avalanche effect refers to a desirable property of cryptographic algorithms where, if an input is changed slightly the output changes significantly (Sriram Ramanujam and Marimuthu Karuppiah, 2011). This will make it impossible to break the cipher if one step of the algorithm is missed thereby introducing a high level of security of the data.

(iv) Modifying the cipher such that the frequency of the letters/symbols produced at the end of the day cannot be used to determine the plaintext unlike the usual Caesar and Vigenere Cipher that could be broken using frequencies of the letters.

Therefore, there is need to urgently introduce different techniques in securing communication over a non-secure communications channel and introduce open and close innovation conceptions for strategic development of secure communication growth in future.

5. Limitation of the Study

This research work is limited to developing a modified hybrid of Caesar cipher and Vigenere cipher as a means of passing secure information.

6. Scope/delimitation of the Study

To fulfill this goal, the thesis studied behaviour patterns of cryptography techniques and hybrid of Caesar cipher and Vigenere cipher users by questionnaires, results indicating that variables and factors assess in this study can significantly affect communication security.

7. Methodology of the Research

In this work, the methodology of the research is the use of combine modified hybrid Caesar Cipher and Vigenere Cipher for data encryption in an attempt to provide data security. Both methods are used because, one method is not strong enough to secure data as singular method has been easily broken by fraudsters in the past and so they are no longer reliable method for data security or information security. But with combine knowledge of hybrid Caesar Cipher and Vigenere Cipher and the modification of both we can adequately secure our data and have reliable information. Though "hybrid method of both Caesar Cipher and Vigenere Cipher**"** for data security is an

improvement of secure data encryption, they have also been broken by fraudsters in the past. But with combine knowledge of hybrid Caesar Cipher and Vigenere Cipher and the modification of both we can adequately secure our data and have reliable information. The hybrid Caesar Cipher and Vigenere Cipher methods are popularly used in data encryption technique for data security.

8. Related Work

Some related previous works include: "Using Classical Ciphers in Secondary Mathematics"[5],"new concept of symmetric encryption algorithm a hybrid approach of Caesar cipher and columnar transposition in multi stages"[6], "A Poly-alphabetic Approach to Caesar Cipher Algorithm'[7], "Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols"[8]," Implementation of hybrid encryption method using Caesar' Cipher algorithm"[9]. Others are, "Analyzing the Superlative Symmetric Cryptographic Encryption Algorithm"[10] and "A Hybrid Cryptosystem Based On Vigenere Cipher and Columnar Transposition Cipher"[11]. These are some of the papers where the effective used of Cryptographic in data security has been established.

9. Research Design/Approach

The method employs both the use of both Caesar Cipher and Vigenère Cipher in its encryption and decryption process and a little modification was applied on the cipher generated. A Numbered Key and a Lettered Key are generated randomly; A Caesar Cipher was performed on the lettered key using the shift value of the numbered key. The plain text to be encrypted is now operated on using Vigenere cipher and using the new key as the key generated when the Caesar cipher was performed initially. The key was transformed in order to prevent a simple frequency analysis, particularly in short messages. At the end of the process, the binary of the first letter of the resulting cipher text will then be XORed with the binary of the numbered key, the result will be encrypted with the next cipher text and consequently, the result is now converted to their Binary value in the ASCII Table. Finally, a cipher text mixed with numbers, symbols and alphabet is generated as the final outcome of the cipher text. This process will end up making the final cipher text more difficult to be broken using existing cryptanalysis processes.

9.1 Algorithm

The algorithm to encipher a plain text is generated as follows;
a. Two key are needed for the enciphering/deciphering.
The First key is a number from 1-26 (following the Caesar Cipher method)
The Second key is a lettered word or group of words (following the Vigenere method)
b. The first key is used to construct the Caesar cipher table based on the Key shift.
c. The Caesar Cipher algorithm will now be performed on the second key to generate a new key that would be used for the Vigenere table.
The new key generated is now used as the key to generate the Vigenere Cipher on the plain text.
d. After performing all of the above on the plain text, the first key is now converted to its Binary equivalent in the ASCII Table and the key is XORed with the binary equivalent of the first letter of the plain text, the output is now XORed with the binary equivalent of the letter of the next plain text and subsequently till the end of the data.
e. The outputs are now converted back to their values and therefore the cipher text is generated.

The algorithm to decipher a cipher text is generated as follows;
i. The first letter or symbol of the ciphertext is converted to its binary equivalent and it is XORed with the first key, the binary equivalent of the next ciphertext letter or symbol is XORed with the binary equivalent of the previous letter and so on.
ii. The first key is used to construct the Caesar cipher table based on the Key shift.
iii. The Caesar Cipher algorithm will now be performed on the second key to generate a new key that would be used for the Vigenere table.
iv. The new key generated is now used as the key to decrypt the Cipher text using the Vigenere method of decryption after which the original plain text will now be derived.

9.2 Flowchart

The flowchart presented in Figure 8 is a guide used in accomplishing the research goals and objectives:

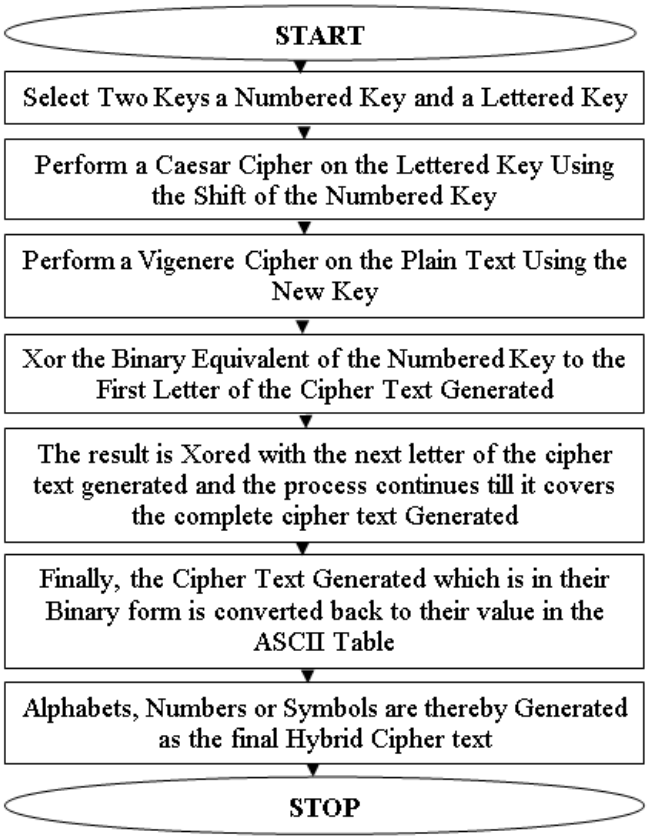

Figure 8: Flowchart for Encryption Using the Modified System

The Figure 9, is the flowchart for decryption using the modified system

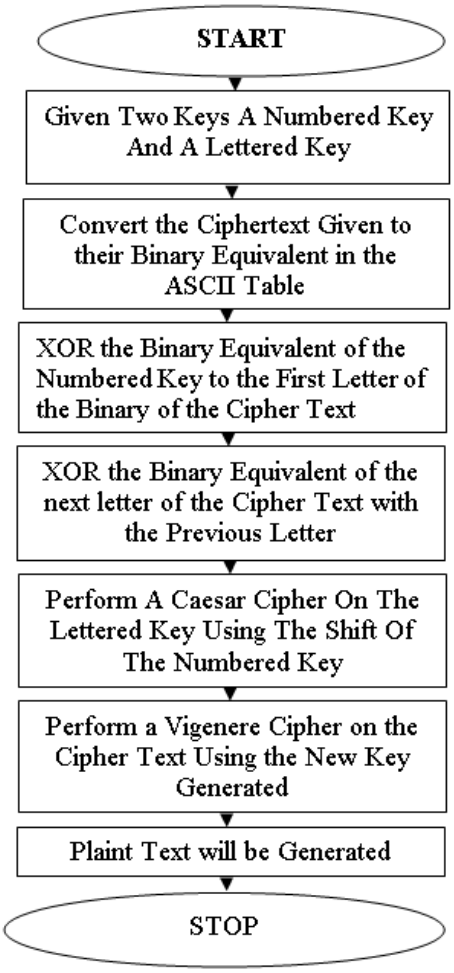

Figure 9: Flowchart for Decryption Using the Modified System

10. Implementation and Experimental Design of Modified Hybrid Approach of Caesar Cipher and Vigenere Cipher

10.1 RESULT AND ANALYSIS

The modified hybrid of Caesar cipher and Vigenere cipher program software give outputs that show the difficulty of breaking the cipher text.

The program written was used to encrypt a message and the result was analyzed by various methods of cryptanalysis.

10.1.1 Results - Plain Text

THE CAESAR CIPHER IS A SIMPLE SUBSTITUTION CIPHER WHERE EACH LETTER OF THE PLAIN TEXT IS REPLACED BY A UNIQUE OTHER LETTER OF THE ALPHABET

Numbered Key-3 which is equivalent to D (Following Caesar Cipher A=0, B=1, C=2…Z=25)

Lettered Key – learn (Following Vigenere Cipher)

If Caesar Cipher is used to encrypt the plain text, the cipher text becomes

WKHFD HVDUF LSKHU LVDVL PSOHV XEVWL WXWLR QFLSK HUZKH UHHDF

KOHWW HURIW KHSOD LQWHA WLVUH SODFH GEBDX QLTXH RWKHU OHWWH URIWK HDOSK DEHW

It is clear that cryptanalysis can be carried out using frequency analysis to deduce that H occurs more in the cipher text and using the frequency table, H will correspond to E, also T occurs most after H in the cipher text and this can be mapped to O. Once a little of the message is matched, the plain text can be gotten. This method is

based upon the fact that the letters in an English text appear with certain abundance. If we sort the letters according to their abundance, we find E,T,A,O,I,N,S,R,H,L,D,C,U,M,F,P,G,W,Y,B,V,K,X,J,Q,Z

Hence, the letter “E” is the most frequent one in an English text followed by “T” and “A”. In order to break a substitution cipher, you first count how often the letters appear in the encrypted text. The most frequent letter is most likely identified with an “E” and the second frequent letter might be a “T”, etc. Though, depending on the amount of text you have at your disposal, only the most frequent letter are identified correctly while the order of less frequent letters might be statistically insignificant.
Instead of relying completely on the abundance of letters, you can also look on the abundance of pairs of letters. Most frequent pairs in an English text are,
th, er, on, an, re, he, in, to, of, in, on, it, by, or, etc.
A brute force can also be used where the 26 keys are tried.

If Vigenere Cipher is used to encrypt the plain text, the cipher text becomes
ELETN PWAIP TTHVE TWAJV XTLVF FFSKV EYTZB YGIGU PVWYR CIERP
SPEKG PVOWG SIPCN TRTVK EMSIR APATR OFYRH YMQLR ZXHVE WITKR
CSFKU PELGU LFEK

It is also clear that since the message is much longer than the key, the key will eventually encrypt the same set of letters previously encrypted by the key. This creates a small pattern of repeating groups of letter. By finding the frequency between the repeating groups and factoring them it is possible to derive the key length. Once the length of the key is known, the key is easily derived by using frequency analysis on each group of Caesar ciphers.

If The Modified Cipher is used to encrypt the plain text, the cipher text becomes
{4|+zZ S[((c:rR_V/n9v/fFF^'o-z9|\-TR
*y z8mM
GZ) ,d*`@JB(~2a'vVT————————————————Z4|,z6cCTG2`)k>uUG\ )j+`9qQ
G^
+m;r<dD_Z"m$l"

The mixture of ASCII Table symbol, numbers and alphabet is enough to deduce that a brute force attack will be confusing. This has introduced complexity and a greater masking to the system and any third person trying to understand the cipher text will find it confusing.
There is no specific frequency of occurrence of digits or other symbols which cause the frequency analysis based cryptanalysis to fail.

The use of symbols apart from the English alphabets makes both the message and the key more complex and less predictable. The cipher text is less understandable and difficult to break as compared to the original Caesar and Vigenère Cipher. In fact the use of other characters causes the frequency analysis attack to fail which was implementable on the original Caesar and Vigenère Cipher.

Therefore the Modified Hybrid of the Caesar Cipher and Vigenere Cipher provide much more security. The three Ciphers have been implemented experimentally on Visual Basic 6.0 software.

The screenshots of the system implementation process are presented in Figure 3 to Figure 3 as follows:

Testing for Caesar Cipher for the Plain Text and Key above

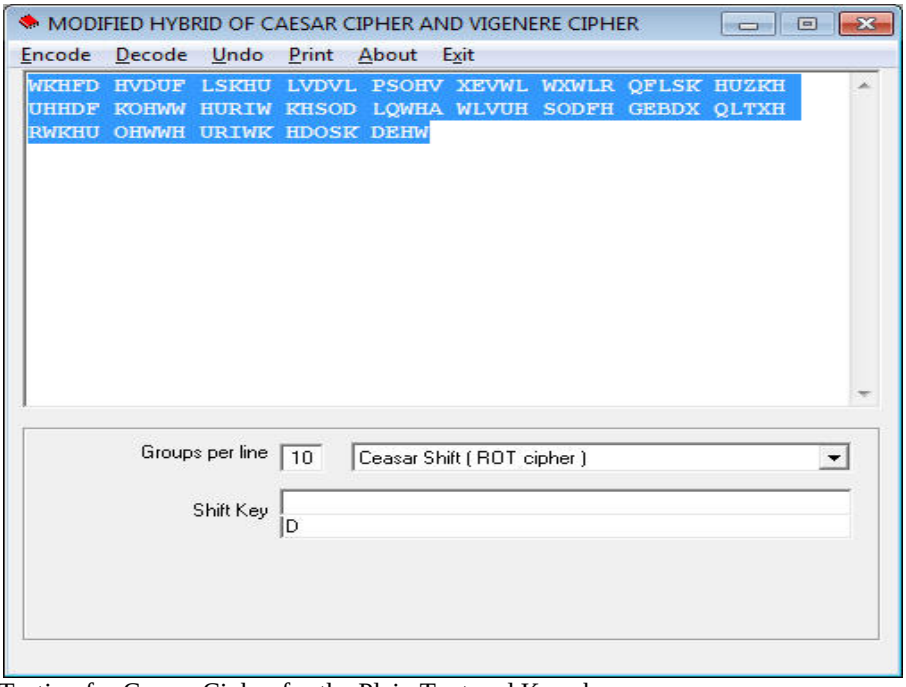

Figure 3: Testing for Caesar Cipher for the Plain Text and Key above

Testing for Vigenere Cipher for the Plain Text and Key above

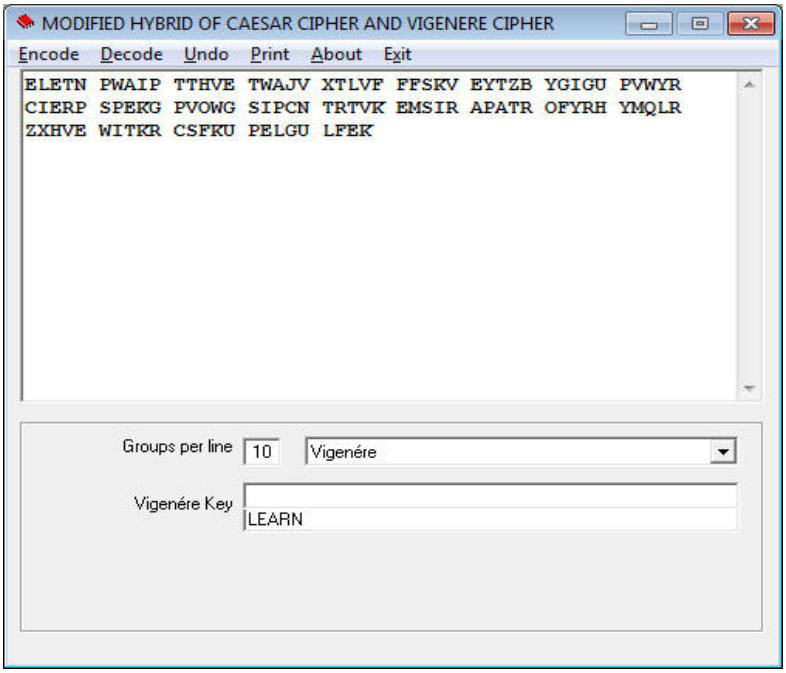

Figure 4: Testing for Vigenere Cipher for the Plain Text and Key above

Testing for the Modified Hybrid of Caesar Cipher and Vigenere Cipher
for the Plain Text and Key above

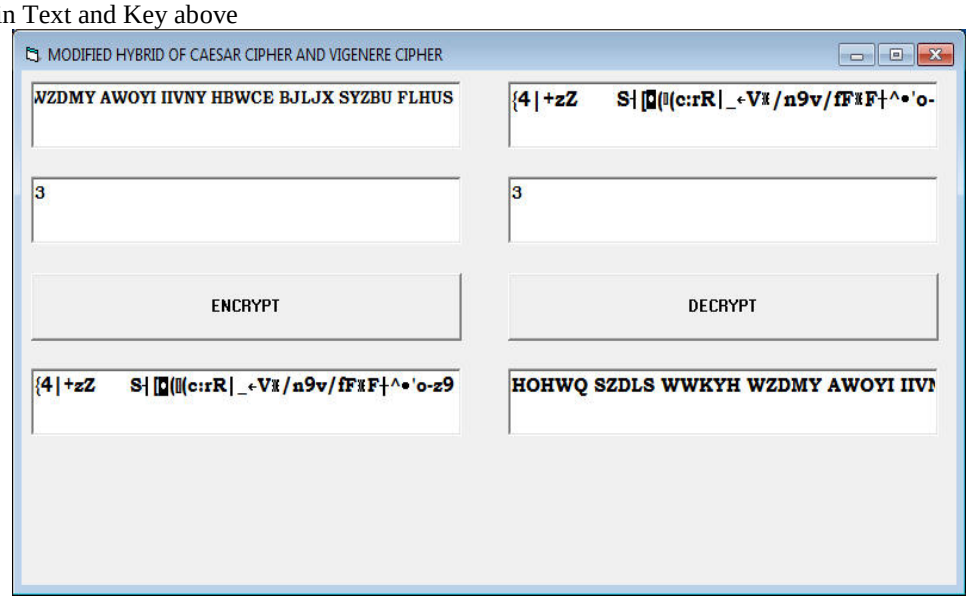

Figure 5: Testing for the Modified Hybrid of Caesar Cipher and Vigenere Cipher
for the Plain Text and Key above

11. Analysis of the Caesar Cipher

To communicate secretly, Julius Caesar wrote to Marcus Cicero, using a cipher that shifts the alphabet three places to the right and wraps the last three letters X, Y, Z back onto the first three letters:

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

Thus, the plaintext message SCHOOL is transformed into the cipher text VFKRRO
The Caesar cipher is probably the easiest of all ciphers to break. Since the shift has to be a number between 1 and 25, (0 or 26 would result in an unchanged plaintext) we can simply try each possibility and see which one results in a piece of readable text. If you happen to know what a piece of the cipher text is, or you can guess a piece, then this will allow you to immediately find the key. If this is not possible, a more systematic approach is to calculate the frequency distribution of the letters in the cipher text. This consists of counting how many times each letter appears. Natural English text has a very distinct distribution that can be used to help crack codes. This distribution is as follows**:**

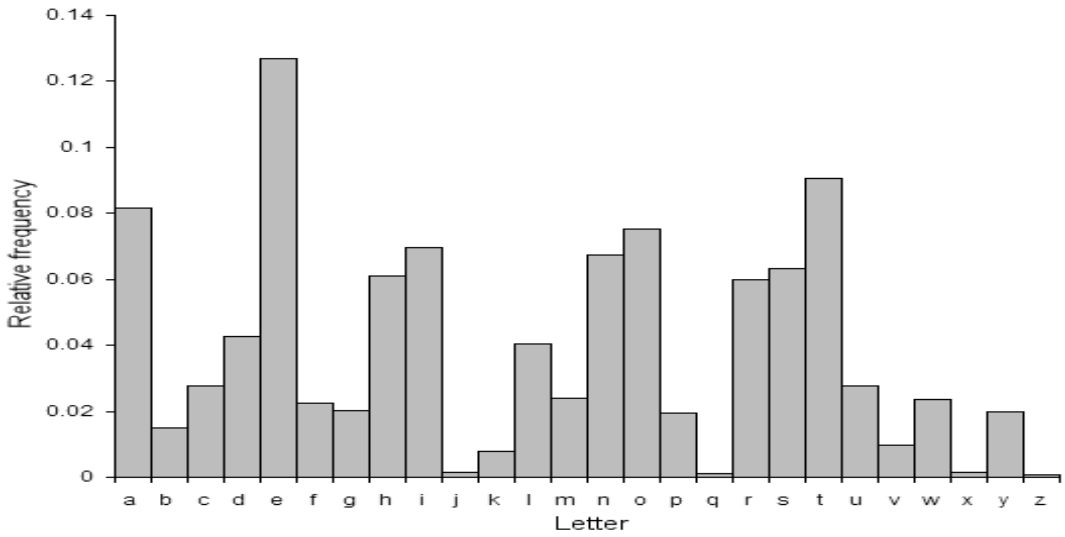

Figure 6: English Letter

Frequencies

This means that the letter 'e' is the most common, and appears almost 13% of the time, whereas 'z' appears far less than 1% of time. Application of the Caesar cipher does not change these letter frequencies, it merely shifts them along a bit (for a shift of 1, the most frequent cipher text letter becomes f). A cryptanalyst just has to find the shift that causes the cipher text frequencies to match up closely with the natural English frequencies, and then decrypt the text using that shift. This method can be used to easily break Caesar Ciphers by hand. Obviously, it had two weaknesses.

The first was that the algorithm was not particularly strong. If trial and error couldn't crack the algorithm, then some simple analysis would. If English text was being encrypted, then it would be relatively simple to compare the frequency of letters in the cipher text against the frequency of letters in Standard English. Statistics would soon reveal patterns that pointed out the probable plain text letter associated with each cipher text letter. Once a single association was found the entire algorithm could be cracked. No message would be secure. This means that the letter e is the most common, and appears almost 13% of the time, whereas z appears far less than 1 percent of time.

Application of the Caesar cipher does not change these letter frequencies, it merely shifts them along a bit (for a shift of 1, the most frequent cipher text letter becomes f). A cryptanalyst just has to find the shift that causes the cipher text frequencies to match up closely with the natural English frequencies, and then decrypt the text using that shift. This method can be used to easily break Caesar ciphers by hand.

Secondly, if there is a sufficiently large ciphertext, it would be solved by comparing the frequency of letters in the cipher text against the frequency of letters in Standard English. If the frequency of the letter in the cipher text is almost the same as the frequency of letters in Standard English, we can find out which letter is substituted for the letter in ciphertext. Then the message would be decrypted.

11.1 Analysis of the Vigenere Cipher

The Vigenere Cipher is a polyalphabetic cipher based on using successively shifted alphabets, a different shifted alphabet for each of the 26 English letters. The procedure is based on the tabula recta and the use of a keyword. The letters of the keyword determine the shifted alphabets used in the encoding process. The description of the tabula recta is as follows**:**

11.1.2 The Vigenere Cipher Table (Tabula Recta)

A tabula recta, Vigenere square or Vigenere table is a table that consists of the English alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

In the 16th century a French diplomat named Blaise de Vigenère developed a new substitution cipher. This cipher relied on using multiple Caesar ciphers based on a key. This polyalphabetic cipher used each letter of the key to determine which Caesar cipher shift to use. Once all letters of the key had been used the cycle begins again by using the first letter of the key. This is illustrated as follows with the key "THREE":

Key: THREET
Message: SCHOOL
Cipher Text: LJYSSE

This cipher solely relies on the confusion methodology for creating cipher text. The repetitive nature of message is not diffused, only camouflaged by the series of Caesar shifts.

The Vigenère cipher was considered unbreakable for nearly 300 years. However, a method to crack it was discovered by Kasiski and Kerckhoff. Both of the methods rely on the fact that the key is repeated and languages in general are relatively repetitive. Given a message is much longer than the key, the key will eventually encrypting the same set of letters previously encrypted by the key. This creates a small pattern of repeating groups of letter. By finding the frequency between the repeating groups and factoring them it is possible to derive the key length. Once the length of the key is known, the key is easily derived by using frequency analysis on each group of Caesar ciphers. The longer the key length is, the more arduous the task of breaking the code. The Vigenere Table 1 is hereby presented[4].

TABLE 2-1 Vigenère Tableau.

	0 a	b	c	d	e	5 f	g	h	i	j	10 k	l	m	n	15 o	p	q	r	s	t	20 u	v	w	x	y	25 z	π
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	0
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	1
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	2
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	3
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	4
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	5
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	6
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	7
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	8
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	9
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	10
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	11
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	12
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	13
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	14
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	15
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	16
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	17
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	18
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	19
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	20
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	21
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	22
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	23
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	24
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	25

In fact, if the key is at least as long as the message, the cipher text is immune from a cipher text only attack. When this occurs it is known as a one-time pad. With the advent of computer the Vigenère cipher has become even easier to break. Most cipher texts can be cracked within a few seconds even with long keys. This cipher is now considered trivial to break and provides no security by today's standards.

12. Analysis of the Modified Hybrid of Caesar Ciphers and Vigenère Cipher

The proposed system the modified hybrid Caesar cipher and Vigenere cipher can be analyze as follows**:**
A good function of modified hybrid Caesar cipher and Vigenere cipher uses three important steps**:**
1. Substitution**:** the replacing of groups of bits or words by others.
2. Fractionation**:** breaking up groups of bytes in smaller parts before relocating.
3. Transposition**:** swap words, bytes or bits from position with each other.

The combination of these three operations results in diffusion. This diffusion is required for any good encryption scheme (Shannon, 2009).
The new algorithm developed boasts one major advantage over the usual classical algorithm. It has the added benefit of diffusion. The diffusion is provided by XORing the first key with the first letter of the word and the

result of XORing the first letter is used in XORing the next letter and subsequent letters till the end of the message using their BINARY and there after converting their binary back to the alphabet or symbol they represent in the ASCII table.
The method used here is called chaining. Each input depends on the output of the previous input to encrypt and vice versa. That way, one encryption/decryption error is fatal to the rest of the message and thus makes the cipher much stronger.
This stage focuses on how the proposed system is to be developed. That is, at this stage the developer translates the set of system requirements into an operational system element known as a program. Here, the developer describes how data structure and software architecture are to be designed, how procedural details are to be represented, how the design will be translated into a program using appropriate programming language and how testing will be performed.
Finally, the uniqueness of the modified hybrid Caesar cipher and Vigenere cipher design defeated brute force, letter frequency and word pattern analysis.

13. Summary/Conclusion

In summary modified hybrid of Caesar cipher and Vigenere cipher algorithm was to test data security on communicated message and it was found to be most secure compared to data security test on Caesar cipher and Vigenere cipher algorithm or that of hybrid Caesar cipher and Vigenere cipher algorithm. It was discovered that originally, cipher text generated with Caesar cipher algorithms and Vigenere algorithms are prone to be broken easily using brute force, exhaustive search, searching by frequency and many other methods because they lack diffusion and confusion in the algorithms that generate them but with the modified hybrid of both the Caesar cipher and Vigenere cipher, there is now a high percentage of diffusion and confusion in the algorithm that generates them making it a very strong cipher and difficult to break.

Contribution to knowledge:

1. This work provides a high degree of secure data encryption of data than Caesar Cipher and Vigenere Cipher methods. Since it is not only a combination of both methods, but a composition of modification of both hybrid Caesar Cipher and Vigenere Cipher methods of data encryption.
2. The developed modified hybrid of Caesar Cipher and Vigenere Cipher provides higher secure key features on encryption of document and easy decryption of information messages to the bearer.

Recommendations

The problem of encryption malpractices can be resolve with the use of modified hybrid of Caesar cipher and Vigenere cipher algorithm as this has been tested globally as the best method. This would ensure that there is secure data communication privately and corporately also locally and internationally.

Suggestions for Further Research

This thesis is based on a scientific study and could be used as a base for further research since Caesar cipher and Vigenere cipher algorithm can be improved upon and the technology of data is still evolving, it would be a good idea for further research to be carried out on both modified hybrid Caesar cipher and Vigenere cipher security features before its implementation.
Since we could not gather enough data to support all our hypotheses, we propose that further research should be done in the area of high rate of data transfer and communication. Moreover, further studies can be conducted as a complement to this paper or as a follow-up on this work and it would be more appropriate; to find out whether the factors proposed in this paper, actually influenced data security. So far, not many researches have been carried out to investigate the fact that both the modified hybrid Caesar cipher and Vigenere cipher security are tamper proof, we here by suggest a further research on the security issues to data communication.

In conclusion, it was discovered that originally, cipher text generated with Caesar Cipher algorithms and Vigenere algorithms are prone to be broken easily using brute force, exhaustive search, searching by frequency and many other methods because they lack diffusion and confusion in the algorithms that generate them but with the modified hybrid of both the Caesar Cipher and Vigenere Cipher, there is now a high percentage of Diffusion and Confusion in the algorithm that generates them making it a very strong cipher and difficult to break.

Acknowledgments

We thank Department of Physics, Nigerian Defence Academy (NDA) Kaduna, Nigeria Atomic Energy Commission, Energy Commission of Nigeria, Department of Mathematics Ahmadu Bello University Zaria, for the material support during the research work. The authors would like to express profound gratitude to anonymous reviewers for their valuable comments and suggestions that improve the presentation of this paper.

References

[1] Srikantaswamy S and Phaneendra H. 2012, “Improved Caesar cipher with random number generation technique and multistage encryption”. Published by International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.4, December 2012

[2] Available at: http://en.wikipedia.org/wiki/Encryption

[3] CSI/FBI 2007, Computer Crime and Security Survey, 9-14-2007. Content Posted by New Media Institute (NMI) Editor. Available at: http://en.wikipedia.org/wiki/Encryption

[4] Terry Ritter, 2006 “Cryptography is only a small part of the protection needed for "absolute" secrecy” Available at: <http://tlindner.macmess.org/wp-content/uploads/2006/09/byte_6809_articles.pdf>

[5] Rigoberto G. 2009, Using Classical Ciphers in Secondary Mathematics. BSc. Thesis McMurry University Abilene, Texas 2009

[6] Dharmendra K. 2012, New concept of symmetric encryption algorithm a hybrid approach of caesar cipher and columnar transposition in multi stages. Journal of Global Research in Computer Science (JGRCS) Copyright Agreement & Authorship Responsibility Vol 3, No. 1 (2012). Available at:http://www.jgrcs.info/index.php/jgrcs/article/view/295

[7] Prachi P. 2013, A Poly-alphabetic Approach to Caesar Cipher Algorithm. International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 4 (6) , 2013, 954-959

[8] Bhardwaj C. 2012, Modification of Vigenère Cipher by Random Numbers, Punctuations & Mathematical Symbols. Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 4, Issue 2 (Sep.-Oct. 2012), PP 35-38 Available at: www.iosrjournals.org

[9] Charomie A. 2010. Implementation of hybrid encryption method using Caesar' Cipher algorithm. BSc. Thesis of Bachelor of Computer Science (Computer Systems & Networking)**,** Faculty of Computer System & Software Engineering Universiti Malaysia Pahang (UMP)**,** April 2010.

[10] Srinivasarao et al. (2011). Analyzing the Superlative Symmetric Cryptographic Encryption Algorithm (ASCEA)” Journal of Global Research in Computer Science Volume 2, No. 7, July 2011.

[11] Quist-Aphetsi Kester 2013. A Hybrid Cryptosystem Based On Vigenere Cipher and Columnar Transposition Cipher. International Journal of Advanced Technology and Engineering Research (IJATER) Vol. 3 Issue 1 pp141-147. July 2013.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Recent conferences: http://www.iiste.org/conference/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar