Ministry of Higher
Education and
Scientific Research
University of Diyala
College of Sciences

"Encryption by Caesar and Hill"

By

Mustafa Sabah Jarullah
Ammar Ali Hassan

Supervisor by

Dr. Khaled Mohammed Safar

June, 2020 IRAQ Dhul Qi'dah, 1441

Dedication

To a strong and gentle soul

To whom taught me to trust in Allah

To whom made me believe in hard work and that so much could be done with little

To my mother

To whom work hard for earing an honest living for use

To whom supporting and encouraging me to believe in my self

To my father

Acknowledgments

Thanks be to ***Allah*** *for all things which led me into the light during the critical time.*

I would like to express my deep thanks and gratitude to my supervisors ***Dr. Khaled Mohammed Safar*** *for their supervision, encouragement and efforts during preparation of this work.*

Special recognition of help to ***My Brother and My Sister***

ABSTRACT

All the world uses data a lot. This data has evolved and has become very large in size. Programs have been developed to preserve this data. One of the most important of these programs is encryption, which is a very important program in maintaining and maintaining data security. Among the most important means and types of encryption used are Symmetric Encryption,

In this research substitution method are use, it can replacing the original text with different letters helps to protect the data from penetration and also strengthens the code and does not penetrate easily. The code cannot be expected by the penetrator and it is difficult for him to determine the number of characters of the code, one of its disadvantages of this method that the text is made up of one or two words, because several times a number of letters will be deleted and it is insecure due to less number of keys, and it is more prone to attacks**.**

Several coding methods have been used in this program, which by is (Caesar method, Hill method). This program provides data protection from penetration. The program was designed using Visual basic 0.6

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER ONE
INTRODUCTION

1.1 Introduction

We are living in cyber age where data and information is the biggest wealth. Our personal, professional and organizations data is available in the devices which are connected with the Internet. Data Hacks and threats in computer networks are growing day by day which demands more security and reduction in both the time for data transmission and the space requirement for data storage. This can be achieved by encryption and compression; such kind of system is called compression-crypto system [1].

Cryptography is powerful tool which provides authenticity, privacy, integrity, and limited access to data. For the reason that networks often involve even greater risks, data is often secured with encryption, plausibly in combination with other controls. The content owner encrypts the actual data using an encryption key which converts the data into cipher text. The cipher text is an intermediate data which is unreadable form which can be shared amount other users and can be stored in the various storage media.
The cipher text can be converted into the actual data using the same encryption key in case of symmetric key encryption or using different key in case of asymmetric key encryption [1].

The most significant type of cryptography is the symmetric key encryption. In the symmetric key encryption, encryption and decryption process both uses the same key thus key should be private to avoid any data breaches. Symmetric key algorithms are high speed and do not consume too much of computing resources. Although there are scope of improvement, thus in this work researchers are focusing on various symmetric key encryption algorithms like Data Encryption Standard (DES), Triple Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish etc. and their throughputs and memory consumptions and proposing high speed new Enhanced Simplified Symmetric Key Encryption Algorithm (in short authors are going to call it proposed algorithm subsequently) which can be useful for the devices with low memory and processing capabilities[1].

1.2 Objective Of Research

- Protects personal data such as passwords.
- Provides for confidentiality of private information.
- Safety of data
- Ensures that a document or file has not been altered.
- Prevents denial or plagiarism.

1.3structural of research

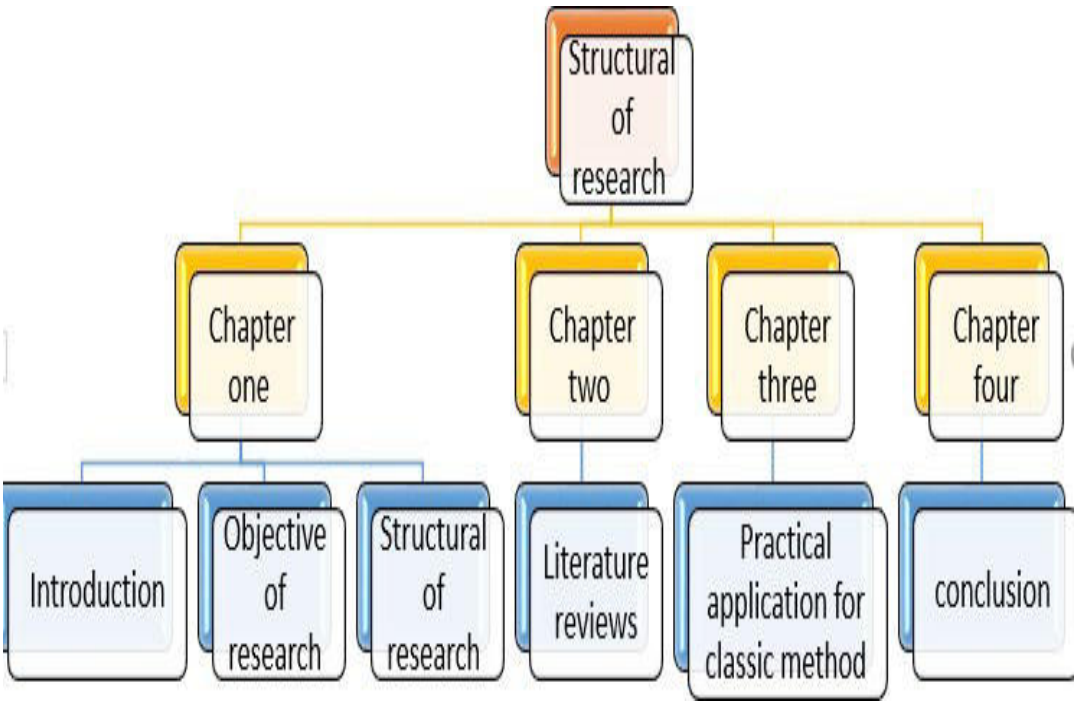


Figure 1 structural of research

CHAPTER TWO
Cryptography Methods

2.1Introduction

Nowadays, the use of internet are growing increasingly across the world, security becomes a prime concern of issue for the society. Earlier security was a major issue for military applications but now the area of applications has been enhanced since most of the communication takes place over the web. Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called Encryption/ Decryption. Cryptography ensures that the message should be sent without any alterations and only the authorized person can be able to open and read the message. A number of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography- Symmetric and Asymmetric **[**2]**.**

2.2 Cryptography

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications.

In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, particularly the Internet. Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext [3].

2.3 Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography [2].

1. Confidentiality
Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

2.Authentication
The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

3.Integrity
Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

4.Non-Repudiation
Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

5.Access Control
Only the authorized parties are able to access the given information

2.4 Types of Encryption

The encryption algorithms are basically classified into two types based on the keys used for the encryption; these are the Symmetric and Asymmetric key encryption.

1.Symmetric Encryption
In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus, the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH [4,5].

2. Asymmetric key encryption is the technique in which the keys are different for the encryption and the decryption process. They are also known as the public key encryption. One of these keys is published or public and the other is kept private. Diffie-Hellman key agreement algorithm, Rivest Shamir Adleman (RSA), Elliptic Curve Cryptography (ECC), El Gamal and Digital Signature Algorithm (DSA) are most popular asymmetric algorithms[4,5].

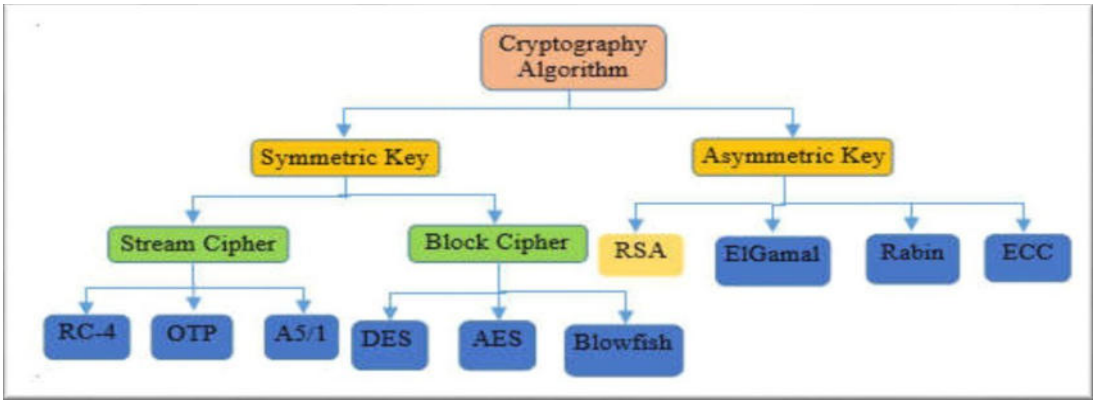


Figure (2) classification of cryptography[3]

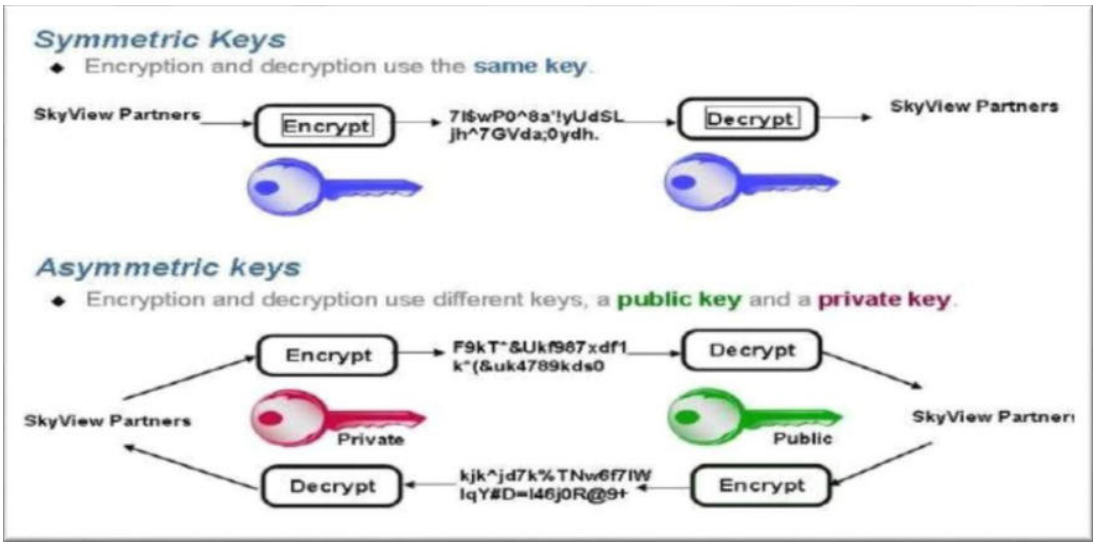


Figure (3) the Symmetric and Asymmetric key encryption.

2.5 Classical Method

The old Encryption and Decryption techniques before the implementation of computer systems are called Classical techniques, while those invented and implemented for the computer systems are called modern techniques. However, cryptography system (whether Classical or Modern) are generally classified along three independent dimensions:

The **type of operations** used for transforming plaintext to cipher text. All encryption algorithm are based on general principle:

(a)Substitution,
(b)Transposition,
(c) XOR.

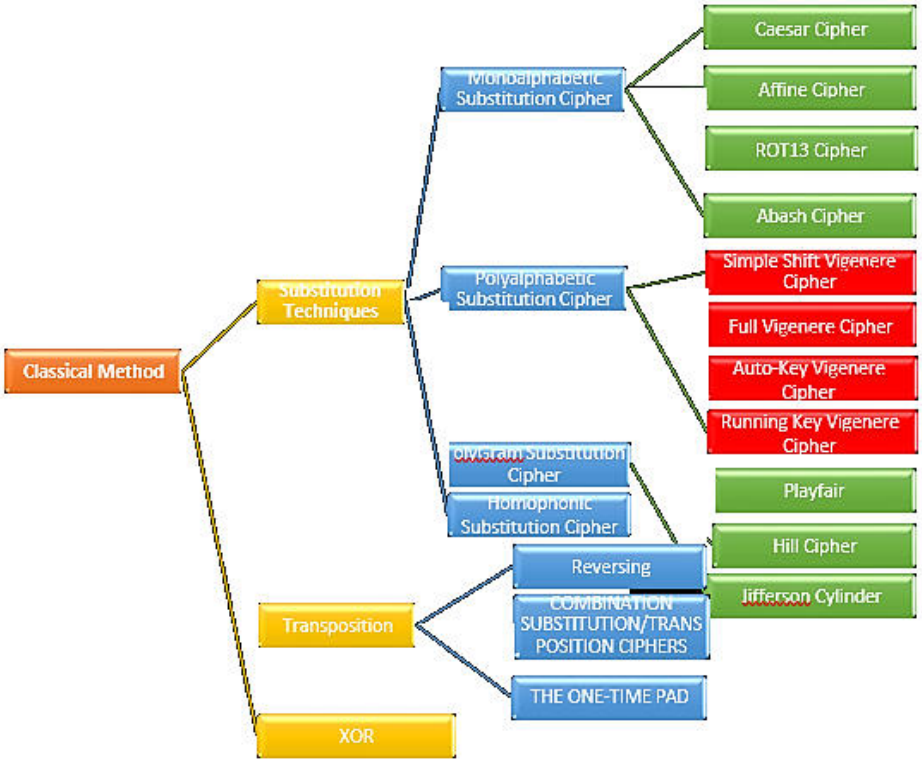


Figure (4) classification of Classical Method

2.6 History of Caesar Cipher

Caesar's code is considered in classic cryptography as a means of coding texts, this code was widely used in the past and it is believed that Julius Caesar was the first to use this method and that was between 58 BC. AD Until 51 BC, the encryption algorithm was very simple as it used to replace the letter to be encoded with the third letter that followed it, that is, if he wanted to encode the letter "A" he would write the place "w" and so on. When August took over, the displacement was only two characters!
According to modern standards, this type of encryption is completely unsafe since it is from the cipher text that the original text can be derived, because the distribution of letters in the text does not change and therefore according to the original distribution of the original language the original text can be derived, this type of attack is called: the cipher text attack only[4].

The Caesar cipher is named after Julius Caesar, who, according to Suetonius, used shift cipher with a constant left shift of 3 to encrypt important military messages during the war. Hence it is also known as shift cipher, Caesar's cipher or Caesar shift. It uses a substitution method to evolve the encrypted text. Consider an Example,

Plain text:
ZYXWVUTSRQPONMLKJIHGFEDCBA
Cipher text:
WVUTSRQPONMLKJIHGFEDCBAZYX
When encrypting, an individual looks up each letter of the text message in the "plain text" and writes down the corresponding letter in the "cipher text". Deciphering is done in exactly reverse manner, with a right shift of 3. This could also be represented using modular arithmetic by transforming the

letters into numbers, as per the scheme, a→0, b→1, c→2 … x→23, y→24, z→25. Now, if a letter (x) is to be encrypted, it is expressed as: En (x) = (x + n) mod 26. Decryption is performed similarly: Dn (x) = (x – n) mod 26. The replacement is same for entire text to be encrypted, thus Caesar cipher is classified as monoalphabetic substitution. The major drawbacks of Caesar cipher is that it can easily be broken, even in cipher-text only scenario. Various methods have been detected which crack the cipher text using frequency analysis and pattern words. One of the approaches is using brute force to match the frequency distribution of letters. This is possible because there are only limited number of possible shifts. (26 in English).

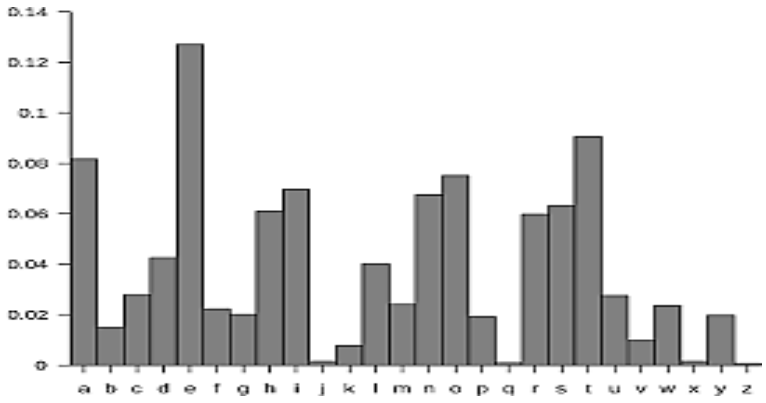


Figure (5)Typical Frequency Distribution of English Alphabets[4].

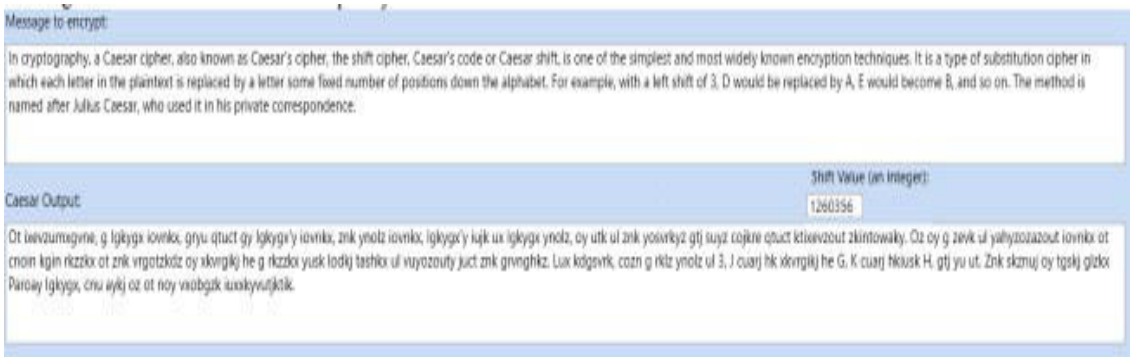
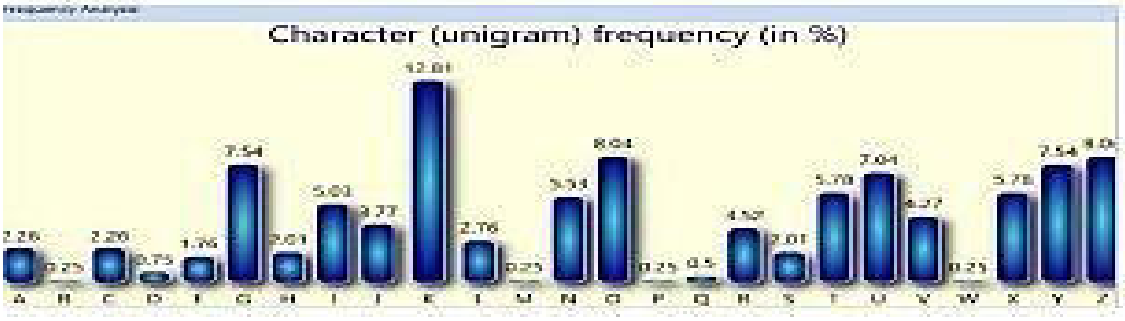


Figure (6) An Example of Encryption using Traditional Caesar Cipher[4]

The distribution of letters in a typical sample of English language text has a very distinct and predictable shape. A Caesar shift "rotates" this distribution, and it is possible to determine the shift by examining the resultant frequency graph. This is the easiest way to break Caesar cipher. Lets take an example to illustrate this weakness[4].

This is a text message which is encrypted using a key of 1260356.The encryption technique used is Caesar cipher. The resultant cipher text is also given. Now assume an attacker gets this encrypted cipher text but does not know the key. So to generate a plaintext he tries various cryptanalysis techniques on the cipher text. Suppose, he uses frequency analysis technique to break it. The frequency distribution graph obtained by analyzing this cipher text is shown in Figure 7.



Figure(7)Frequency Distribution of Characters in Cipher Text[4].

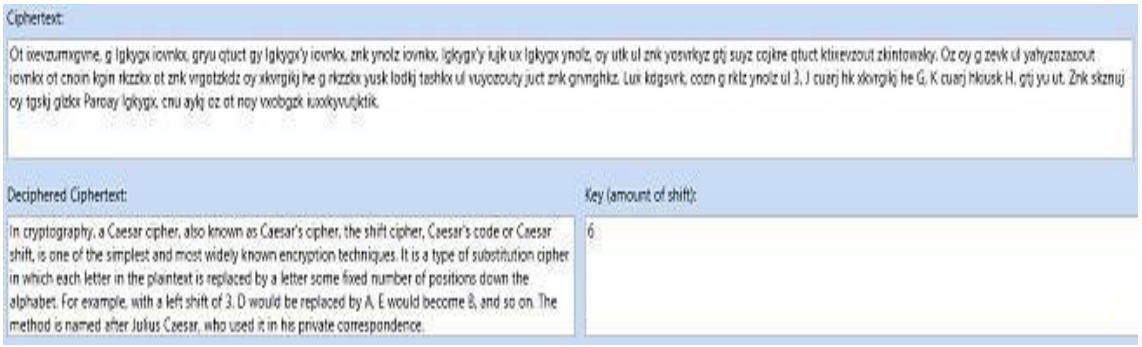


Figure (8) Decryption of the Cipher Text using Cryptanalysis technique of Frequency Analysis[4].

On comparing this with the normal frequency distribution of characters in English language (see Figure 4)it is found that the shift is of 6 characters, since K is repeated most in this graph whereas generally E is repeated. Thus, on reverse shifting by 6 characters (as shown in Figure 7), anybody can successfully get the actual plain text and thus the attacker has successfully attacked the system and obtained the actual message. cryptanalyst that the text has been encrypted.

2.7 History Hill cipher

The Hill cipher is a historic polygraphic substitution cipher invented by Lester S. Hill in 1929. It was the first substitution cipher to allow operations on groups of more than three plaintext characters at a time.

The Hill cipher is based on linear algebra, specifically matrix multiplication. It works by mapping the plaintext letters into numbers, dividing the resulting number sequence into blocks of n numbers, each of which is interpreted as an n element vector and multiplied with an invertible $n \times n$ key matrix (using modular arithmetic) to obtain the corresponding block of cipher text. Decryption works the same way, except that the key matrix is replaced with its.

On its own, the Hill cipher is insecure, being vulnerable to a simple known plaintext attack: an attacker who knows the plaintext corresponding to at least n blocks of cipher text can solve a system of linear equations to (with high probability) recover the full key matrix. In U.S. patent 1,845,947, describing a mechanical implementation of the cipher for $n = 6$ (with a fixed key matrix), Hill recommended combining the cipher with a non-linear monographic substitution to thwart such attacks.[6]

This cryptographic technique was created in order to be able to create a cipher that cannot be solved using frequency analysis techniques. Hill Cipher does not replace each of the same alphabets in plaintext with the same alphabet in ciphertext because it uses matrix multiplication by encryption and decryption. Hill Cipher which is a polyalphabetic cipher can be categorized as a block cipher because the text to be processed will be divided into blocks of a certain size. Each character in one block will influence the other characters in the encryption and decryption process so that the same character is not mapped to the same character. Hill Cipher is included in classical cryptographic algorithms which cryptanalysts are very difficult to solve if done only by knowing the cipher text file only. However, this technique can be solved quite easily if the cryptanalyst has a cipher text file and a piece of the plaintext file. This cryptanalysis technique is called a known-plaintext attack. The basis of the Hill Cipher technique is modulo arithmetic to the matrix. In its application, Hill Cipher uses matrix multiplication techniques and inverse techniques for matrices. The key to Hill Cipher is the matrix n x n with n is the block size. The K matrix that becomes this key must be an invertible matrix, which has inverse K-1 so that the key must have an inverse because the K-1 matrix is the key used to decrypt[6].

The stages of the Hill Cipher encryption algorithm are as follows

Organize character alphabetically with numeric A → 1, B → 2, ..., Z → 26 or in ASCII (256 characters)

1. Create a key matrix measuring m x m

$$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix}$$

1. Matrix K is an invertible matrix that has multiplicative inverse K−1 so that K. K−1 = 1 4. Plaintext P = p1 p2 ... pn, blocked with the same size as the row or column column K

$$P_{qxm} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ p_{q1} & p_{q2} & \cdots & p_{qm} \end{bmatrix}$$

5. Transpose matrix P and became

$$P^t_{mxq} = \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \cdots & p_{qm} \end{bmatrix}$$

6. Multiply matrix K with transposed P in modulo 26 or 256

$$C^t = K_{mxm} P^t_{mxq}$$

$$C^t = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \cdots & p_{qm} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ c_{1q} & c_{2q} & \cdots & c_{mq} \end{bmatrix}$$

7.Then transpose to

$$C = (C')^t = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1q} \\ c_{21} & c_{22} & \cdots & c_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ c_{m1} & c_{m2} & \cdots & c_{mq} \end{bmatrix}$$

8.Change the result of step 7 into the alphabet using alphabetical correspondence with numeric in step 1 to obtain the ciphertext

CHAPTER THREE
Practical Application For Classic Method

3.1 Introduction

In this chapter, we will look at two classical encryption algorithms, and we will explain how they are represented in visual Basic, along with an explanation of the most important codes included in each method. The two classical encryption algorithms are Caiser and Hill cipher method.

Visual Basic language was used in the implementation of the practical aspect of the research project because of the advantages of this language such as graphical interfaces and direct orders in the implementation of procedures for the program.

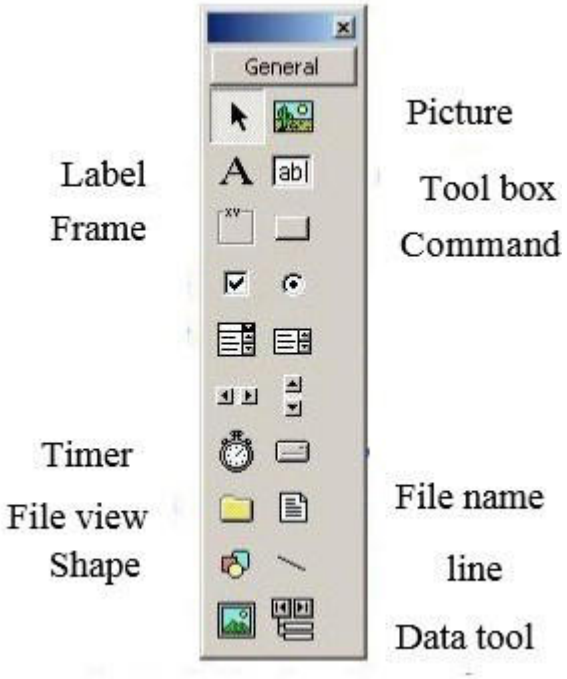


Figure (9) main control tools

Picture : This tool is used to display images with the extension Ico, Wmf, Jpg, Gif, Dib, Cur

Text Box : It is used to write texts and make modification on them, as well as display texts from files and has the ability Writing by the user

Label : You write texts in it and these texts cannot be modified by the user, but the programmer does modify these texts or make them fixed

Command : It is used so that if the user presses it, he executes a certain command

Frame: The frame contains the tools that are placed inside it so that if the frame moves, the tools inside it do not their places change as their places are fixed inside the frame

3.2 Properties Box

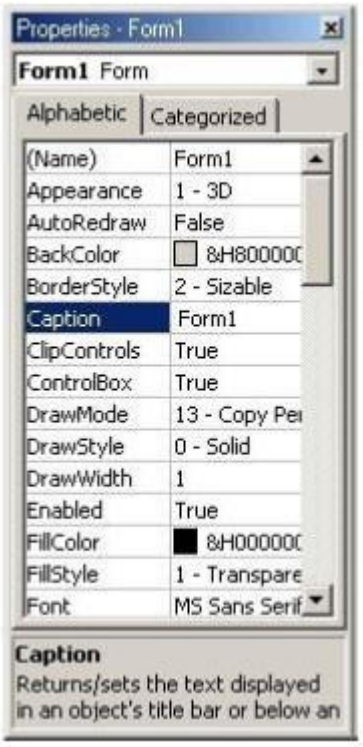


Figure (10) properties box

The following is an explanation of the commonly used

properties: - Back color: to change the background color

Caption property: to write a visible title of an item as the programmer see appropriate

The Alignment feature is used to align left or right scripts according to the

values for the tool itself

Font property: Controls the font size and

type Font color property: Controls the font color

3.3 Method of write codes

By double-clicking the left mouse button on the tool where you want to write codes, the code writing window will appear for you and you can write codes in it

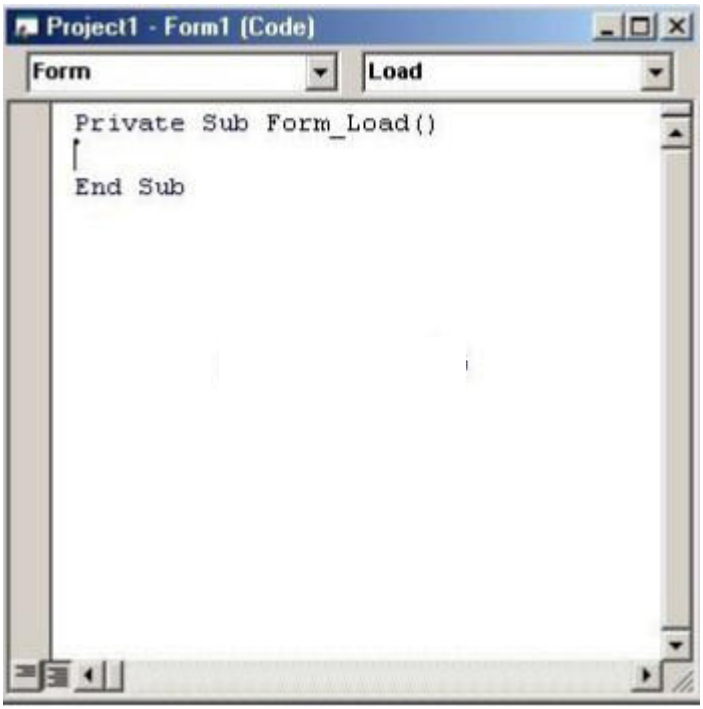


Figure (11) windows of write code

The code is written between the two written lines. Ready functions used in

the program:

1. Mid $ (X, I, J) to deal with the letter of a letter from the sentence where X represents the written sentence and I represents a counter usually equal the number of letters of the word or sentence and J represents the amount of deduction from the sentence one or two letters or more.

2.Asc Convert the letter to its numeric value, which corresponds to it, to easy handling, by increasing or decreasing it to change it to another letter

3.Chr $ Converts a numeric value into an equivalent letter or an

alphanumeric character

4. Len (X) is a ready function to place the number of component letters of a word including spaces in a given variable where X represents the word

5- Mod 26 to take the remainder of the division for any calculation that results when dealing with letter values to stay within the range of English letters

In this chapter, we will look at two classical encryption algorithms, and we will explain how they are represented in visual Basic, along with an explanation of the most important codes included in each method and the two methods are:

1- Caiser Cipher Method

```
Dim t, c, y, b As String
Dim k, l, j, a, e As Integer
Private Sub Command1_Click()
k = Input Box (" enter the key")
t = Text1.Text
l = Len(t)
For j = 1 To l
m = Mid$(t, j, 1)
If m < > " Then"
a = Asc (m)
e = (((a - 97) + k) Mod 26) + 97

c = Chr $(e)
y = y + c
End If
Next j
Text2.Text = y
End Sub
Private Sub Command2_Click()
k = Input Box (" enter the key")
```

```
l = Len(y)
For j = 1 To l
m = Mid$(y, j, 1)
a = Asc (m)
e = (((a - 97) - k) Mod 26) + 97
c = Chr $(e)
b = b + c
If (e < 0) Then
e = e * -1
End If
Next j
Text3.Text = b
End Sub
Private Sub Command3_Click()
End
End Sub
```

2) Hill Sipher Method

```
Dim s, x, x1, h, g, y1, y2, h1 As String ... hill.
Dim a, b, k, i, c, d, e, f, s1(1 To 2, 1 To 2) As Integer
Private Sub Command1_Click()
s = Text1.Text
Print "enter the key consist of 4 number"
For i = 1 To 2
For j = 1 To 2
s1(i, j) = Input Box ("enter key")
Next j, i
a = Len(s)
k = 1
For i = 1 To a
y1 = Mid$(s, i, 1)
If y1 < > " " Then
ss = ss + y1
End If
Next
a = Len(ss)
For i = 1 To a Step 2
y1 = Mid $(ss, i, 1)
x = y1
y2 = Mid$(ss, i + 1, 1)
x1 = y2
c = Asc (x)
 d = Asc (x1)
e = (s1(1, 1) * (c - 97)) + (s1(1, 2) * (d – 97))
f = (e Mod 26) + 97
g = Chr $(f)
```

```
h = h + g
e = (s1(2, 1) * (c - 97)) + (s1(2, 2) * (d – 97))
f = (e Mod 26) + 97
g = Chr $(f)
 h = h + g
Next
Print h
End Sub

Private Sub Command2_Click()
s = h
Print "enter the key consist of 4 number"
For i = 1 To 2
For j = 1 To 2
s1(i, j) = Input Box ("enter key")
Next j, i
a = Len(s)
k = 1
For i = 1 To a
y1 = Mid$(s, i, 1)
If y1 < > " " Then
ss = ss + y1
End If
Next
a = Len(ss)
For i = 1 To a Step 2
y1 = Mid$(ss, i, 1)
x = y1
y2 = Mid$(ss, i + 1, 1)
x1 = y2
c = Asc (x)
d = Asc (x1)
```

```
e = (s1(1, 1) * (c - 97)) + (s1(1, 2) * (d – 97))
f = (e Mod 26) + 97
g = Chr $(f)
h1 = h1 + g
e = (s1(2, 1) * (c - 97)) + (s1(2, 2) * (d – 97))
f = (e Mod 26) + 97
g = Chr $(f)
h1 = h1 + g
Next
Print h1
End Sub

Private Sub Command3_Click
End
End Sub
```

CHAPTER FOUR
CONCLUSION

All classic encryption methods use one key, to encode and then decode with the same key. Classical encoding can be done in two ways: either replacing the original text with different letters, or switching the locations of the original text and changing their arrangement according to the method used in coding**.** Substitution is very simply used for encryption in cryptography, it is having more than one benefit, such as replacing the original text with different letters helps to protect the data from penetration and also strengthens the code and does not penetrate easily. The code cannot be expected by the penetrator and it is difficult for him to determine the number of characters of the code, one of its disadvantages is that the text is made up of one or two words, because several times a number of letters will be deleted and it is insecure due to less number of keys, and it is more prone to attacks**.**

Referenc

1. K. Shrivas, A.B. Boasiako, S.Krishanan , and T. Yeboah, " Enhanced Simplified Symmetric Key Encryption Algorithm" Texila International Journal of Academic Research Volume 3, Issue 2, Dec 2016

2. Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques," International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

3. Mithil P. Gharat and Dilip Motawani " Overview on Symmetric Key Encryption Algorithms" Mithil P. Gharat Int. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, Vol. 4, Issue 9 (Version 3), September 2014, pp.123-126

4. Jain, A., Dedhia, R. & Patil, A. (2015). Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication. International Journal of Computer Applications (0975 – 8887), 129, 6-11. Retrieved from http:// www.ijcaonline.org

5. M. Ebrahim, S. Khan, and U. bin Khalid, "Symmetric algorithm survey: A comparative analysis," International Journal of Computer Applications, vol. 61, no. 20, pp. 12–19, 2013.

6. M.D.L Siahaan and A.P.U Siahaan " Application of Hill Cipher Algorithm in Securing Text Messages" international journal for innovative research in multidisciplinary field issn: 2455-0620 volume - 4, issue - 10, oct – 2018

ملخص

في الوقت الحاضر ، يتزايد استخدام الإنترنت بشكل متزايد في جميع أنحاء العالم ، ويصبح الأمن الشغل الشاغل للقضية بالنسبة للمجتمع. كان الأمن السابق قضية رئيسية للتطبيقات العسكرية ولكن الآن تم تحسين مجال التطبيقات حيث أن معظم الاتصالات تتم عبر الويب. التشفير هو مجال علوم الكمبيوتر تم تطويره لتوفير الأمان للمرسلين وأجهزة الاستقبال لإرسال واستقبال البيانات السرية عبر قناة غير آمنة عن طريق عملية تسمى التشفير / فك التشفير. يضمن التشفير إرسال الرسالة بدون أي تعديلات ولا يمكن لغير الشخص المفوض فتح الرسالة وقراءتها. عدد من يتم تطوير تقنيات التشفير لتحقيق اتصال آمن. هناك أساسا اثنين تقنيات التشفير - متماثل وغير متماثل. يقدم هذه البحث دراسة لمعظم تقنيات التشفير المتماثل مع مزاياها وقيودها على بعضها البعض أحد عيوب هذه الطريقة أن النص يتكون من كلمة أو كلمتين ، لأن عدة مرات عدد من الأحرف سيتم حذفه وهو غير آمن بسبب عدد المفاتيح الأقل ، وهو أكثر عرضة للهجمات.

تم استخدام العديد من طرق الترميز في هذا البرنامج ، والتي هي (طريقة قيصر ، طريقة هيل). يوفر هذا البرنامج حماية البيانات من الاختراق. تم تصميم البرنامج باستخدام Visual basic 0.6.

وزارة التعليم العالي
والبحـــث العلـــمي
جامعـــــة ديـــالى
كليـــــة العلوم

" التشفير بطريقة قيصر و هيل "

من قبل
مصطفى صباح جارالله
عمار علي حسن

باشراف
م.د خالد محمد صفر

ذوالعقدة، ١٤٤١ هـ العراق حزيران، ٢٠٢٠ م