International Multidisciplinary Research Journal 2012, 2(7):08-12
ISSN: 2231-6302
Available Online: http://irjs.info/

INTERNATIONAL MULTIDISCIPLINARY
RESEARCH JOURNAL

Reveiw of effective data encryption and decryption technique

Ramalingam Sugumar[1], Tamilenthi.S[2]* and Gurunathan.M[1]

[1]Dept .of Computer Science and Application, Christhuraj College, Panjappur,Trichy- 620012, India
[2]Department of Earth Science, Tamil University, Thanjavur- 613 010, India

Abstract

The requirements of information security within an organization have undergone two major changes in the last several decades. Before the wide spread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means. The collection of tools designed to protect data and to thwart hacker is computer security. Network security measures are needed to protect data during their transmission. This technique for encryption and decryption process to combine two methods ceaser cipher and transposition cipher, ceaser cipher is one of the substitution techniques. A substitution technique is one in which the letters of plain text are replaced by other letter or by numbers or symbols. if the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns. The encryption process is two stages first, to convert the given plaintext into cipher text using ceaser cipher text technique, second stage the cipher converted using transposition technique, the final output is cipher text, The Decryption is the reverse process of the Encryption.

Keywords: Encryption, Decryption, Caesar cipher and transposition cipher.

INTRODUCTION

Cryptography is the science of writing in secret code and is an ancient act. Cryptography is not only protect data from theft or alternation, but can also be used for user authentication. An original message is known as the plaintext. The encoded message is called cipher text. The process of converting from plain text to cipher text is known as Enciphering(or)Encryption. The process of converting from cipher text to plain text is Deciphering (or) Decryption. The many schemes used for encryption constitute the area of study known as Cryptography. Such a scheme is known as Cryptographic system or a cipher. Technique used for deciphering details falls into the area of Cryptanalysis. Cryptnalysis is what the layperson calls “Breaking code”. The area of cryptography and cryptanalysis together called Cryptology.

Wikipedia(2012),Encryption is the most effective way to achieve data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. Freeman et al.(1998) stated , the purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data. Encryption occurs when the data is passed through some substitute technique, shifting technique, table references or mathematical operations. All those processes generate a different form of that data. The unencrypted data is referred to as the plaintext and the encrypted data as the cipher text, which is representation of the original data in a difference form .

Received: May 10, 2012; Revised: June 18, 2012; Accepted: July 20, 2012.

*Corresponding Author

Tamilenthi.S
Department of Earth Science, Tamil University, Thanjavur- 613 010, India

Email: rst_edu2010@yahoo.com

Beth .T. and Gollmann.D (1989) and IBM(1994),Key-based algorithms use an Encryption key to encrypt the message. There are two general categories for key-based Encryption: Symmetric Encryption which uses a single key to encrypt and decrypt the message and Asymmetric Encryption which uses two different keys – a public key to encrypt the message, and a private key to decrypt it. Currently, there are several types of key based Encryption algorithms such as: DES, RSA, PGP, Elliptic curve, and others but all of these algorithms depend on high mathematical manipulations .

Wikipedia(2012),One simple and good way to encrypt data is through rotation of bits or sometimes called bit shifting. But, rotation of bits is more advanced than simple bit shifting. In rotation of bits operation, the bits are moved, or shifted, to the left or to the right. The different kinds of shifts typically differ in what they do with the bits .

According to Vivek Thakur(2006),There are several kinds of Encryption software in the market categorized by their functions and target groups. For example, some are single Encryption applications for files and database security; some are for messenger security or email Encryption applications that hide the actual text in the medium between the sender and the receiver.

Neekprotect is a software in the market right now with the ability to make Encryption on any files in the window platform, a key is set when one try to encrypt a files and the key will be used again when someone else trying to open the files been decrypted through decryption on the certain files .

William Stallins(2004), In open networked systems, information is being received and misused by adversaries by means of facilitating attacks at various levels in the communication . According to the Charless (2004),Data encryption is sought to be the most effective means to counteract the attacks. Jose .J(2005) states that there are two classes of encryption in use, which are referred to as i) Symmetric-key encryption using secret keys and ii) Asymmetric-key encryption using public and private keys. Public-key algorithms are slow, whereas Symmetric-key algorithms generally run 1000 times faster . Dragos Trinica(2006) worked out on Symmetric key cryptography, has been and still is extensively used to solve the Traditional problem of communication over an insecure channel.

REVIEW OF CAESAR CIPHER

In Cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known techniques (Wikipedia 2012). It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, would be replaced by D, B would become E, and so on. The method is named after Julius Caesar who used it in his private correspondence.

The encryption step performed by a Caesar cipher is often incorporated as part of more complex schemes, such as the vigenere, and still has modern application in the ROT13 system. As with all single alphabet substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communication security.

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places (the shift parameter, here 3, is used as the key:

```
Plain text:   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
```

```
Cipher Text:  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
```

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line. Deciphering is done in reverse.

```
Cipher text: WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB
GRJPlain  text :  the quick brown fox jumps over the lazy dog
```

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1, Z = 25. Encryption of a letter x by a shift n can be described mathematically as,

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

(There are different definitions for the modulo operation. In the above, the result is in the range 0...25. I.e., if *x+n* or *x-n* are not in the range 0...25, we have to subtract or add 26.)

TRANSPOSITION CIPHER

In cryptography, a transposition cipher is methods of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

Rail fence cipher

The rail fence cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom. The message is then read off in rows. For example, using three "rails" and a message .The study identified flee at once, the cipherer writes out:

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

Then reads off:

```
WECRL TEERD SOEEF EAOCA IVDEN
```

(The cipherer has broken this cipher text up into blocks of five to help avoid errors.)

Route cipher

In a route cipher, the plaintext is first written out in a grid of given dimensions, then read off in a pattern given in the key. For example, using the same plaintext that we used for rail fence.

```
W R I O R F E O E
E E S V E L A N J
A D C E D E T C X
```

The key might specify "spiral inwards, clockwise, starting from the top right". That would give a cipher text of:

```
EJXCTEDECDAEWRIORFEONALEVSE
```

Route ciphers have many more keys than a rail fence. In fact, for messages of reasonable length, the number of possible keys is potentially too great to be enumerated even by modern machinery. However, not all keys are equally good. Badly chosen routes will leave excessive chunks of plaintext, or text simply reversed, and this will give cryptanalysts a clue as to the routes.

An interesting variation of the route cipher was the Union Route Cipher, used by Union forces during the American civil war. This worked much like an ordinary route cipher, but transposed whole words instead of individual letters. Because this would leave certain highly sensitive words exposed, such words would first be concealed by code. The cipher clerk may also add entire null words, which were often chosen to make the cipher text humorous.

Column transposition

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. Both the width of the rows and the permutation of the columns are usually defined by a keyword. For example, the word ZEBRAS is of length 6 (so the rows are of length 6), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "6 3 2 4 1 5".

In a regular columnar transposition cipher, any spare spaces are filled with nulls; in an irregular columnar transposition cipher, the spaces are left blank. Finally, the message is read off in columns, in the order specified by the keyword. For example, suppose we use the keyword ZEBRAS and the message in a regular columnar transposition, we write this into the grid as.

W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

Providing five nulls (QKJEU) at the end. The cipher text is then read off as:

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

In the irregular case, the columns are not completed by nulls:

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E					

This results in the following cipher text:

EVLNA CDTES EAROF ODEEC WIREE

To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length. Then he can write the message out in columns again, and then re-order the columns by reforming the key word.

Columnar transposition continued to be used for serious purposes as a component of more complex ciphers at least into the 1950s.

METHODOLOGY

In this study, combination two techniques i.e. Caesar cipher and transposition technique to produce a new method, and to develop an algorithm for the new method.

Caesar cipher is a substitution techniques a substitution technique is one in which the litters of plaintext are replaced by other letters or replaced by other letters or by numbers or symbols.

- The original message is called plain text, The plain text is converted in to cipher text called Encryption
- In this method, we combine two methods Caesar Cipher and Transposition Cipher

Encryption process

Step 1:

- The given plain text is converted as cipher text using caesar cipher

Step 2:

- The second stage is converted text given to the input as column transposition cipher. It is complex is to write the message column by column
- Depending on the message length the matrix is created and write the message in a rectangle row by row
- Apply the key, depending on the key order to read meassage column by column, The final output is cipher text

Decryption process

Step 1:The cipher text are numbered from 0 to n.The text is arranged in ascending order.

Step 2:Then the cipher text is again converted using caesar cipher,so that the plain text is discovered.

Hardware Requirements:

System	: Pentium IV 2.4 GHz.
Hard Disk	: 40 GB.
Floppy Drive	: 1.44 Mb.
Monitor	: 15 VGA Colour.
Mouse	: Logitech.
Ram	: 512 Mb.

Software Requirements:

Operating system	: Windows XP.
Coding Languag	: ASP.Net with C#
Data Base	: SQL Server 20**05**

ANALYSIS

In existing method, the study encoded message using Caesar cipher or Transposition cipher,

The Plain Text: Hello How are you
Converted as cipher text using Caesar cipher
The cipher Text: khoor krz bubhrx
It converted using Column transposition cipher

3	1	2	4
H	E	L	L
O	H	O	W
A	R	E	Y
O	U	*	*

Cipher text: e h r u l o e * h o a o l w y *

But in this new method the Plain text is converted in to cipher text using caesar cipher is first stage, again it is converted to using column transposition technique.

Plain text: Hello How Are You
Step 1: Caesar cipher
Khoor krz dubhrx
Again it is converted using column transposition technique.

3	1	2	4
k	h	o	o
r	k	r	z
d	u	h	b
r	x	*	*

Cipher text: hkux orh* krdr ozb*

Caesar cipher

It was developed by Julius Caesar; the Caesar cipher involves replacing each letters of the alphabet with the letter standing three places farther down alphabet.

Plain text : 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
Cipher text : 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

Plain text :	Hello	How	Are	You
Cipher text:	khoor	krz	duhbrx	

The Caesar cipher algorithm:

Let us assign a numerical equivalent to each letter

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	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Then the algorithm can be expressed as follows.
Where: c=E (3ip) = (p+3) mod 26
= (p+k) mod 26
C= cipher tent P=plain text K=constant

The decryption algorithm
P=(c-k) mod26
P= plain text K= constant C= cipher text

The new method, combine two method's Caesar cipher and transposition method.

Encryption process:

The encryption process is two stages.

First stage:

The given plain text is converted as cipher text using Caesar cipher.
Plain text: HELLO HOW ARE YOU
Cipher text: KHOOR KRZ DUH BRX

Second text:

It is more complex scheme is to write the message in a rectangle, row by row and read the message column by column.

STEP 1: depending on the length the matrixes is created and writes the message in a rectangle row by row.

STEP 2: Apply the key, then depending on the key order to read the message column by column.

STEP 3: At the same time the letter are numbered from 0 to n.
Plain text: hello how are you.
Khoor krz duhbrx
uses the key: 2 4 1 3

$$\begin{pmatrix} k & h & o & o \\ R & k & r & z \\ D & u & h & b \\ R & x & * & * \end{pmatrix}$$

To read the message column by column depending on the key.
Orh*kr Kdrozb*h kux
Now plain text is
Hello how are you
Cipher text:
Orh*kr dro zb*h kux
It can be more secure by performing more than one stage. The result is more complex.

Foe Ex:

$$\begin{pmatrix} 2 & 4 & 1 & 3 \\ O & r & h & * \\ K & r & d & r \\ O & z & b & * \\ H & k & u & x \end{pmatrix}$$

Cipher text: hdbu okoh *r*xr rzk
Decryption process:
The decryption process is very simple. Already the cipher texts are numbered from 0 to n. so that the text arranged an ascending order.

$$\begin{pmatrix} 2 & 4 & 1 & 3 \\ k & h & o & o \\ 0 & 1 & 2 & 3 \\ r & k & r & z \\ 4 & 5 & 6 & 7 \\ d & u & h & b \\ 8 & 9 & 10 & 11 \\ r & x & * & * \\ 12 & 13 & 14 & 15 \end{pmatrix}$$

o	r	h	*	k	r	d	r	o	z	b	*	h
	k	u	x									
2	6	10	14	0	4	8	12	3	7	11	15	1
	5	9	13									

Ascending order

Khoor krz duhbrx **
Then the cipher text is again converted using Caesar cipher, so that the plain text discovered.
Khoor krz duhbrx **
P=(c+k)mod 26
Hello how are you

Encryption:

Plain text : hello how are you.
Cipher text : orh*kr dro zb*h kux.
(or)
Hdbuo koh*r*xr rzk.

Decryption:

Cipher text : orh*kr dro zb*h kux.
Plaintext : hello how are you

CONCLUSION

Cryptography plays a vital role in Network security. The original message is converted cipher text known as Encryption and cipher text is converted as plain text known as Decryption. Two Cryptography techniques are (1) substitution techniques (2)Transposition techniques. There are several substitution techniques, Caesar cipher is one of the earliest substitution techniques, in which the plain text converted as cipher text it involves replacing each letter of alphabet with the letter standing three places further down the alphabet. In column transposition technique, is more complex scheme to write the message in a rectangle row by row, depending on the key it read the message column by column. In this new method, is very effective and very difficult to find the plain text because in this method we combined two encryption and decryption techniques called Caesar cipher and Transposition cipher.

REFERENCE

[1] Wikipedia, 2012 "Encryption", http: //en. wikipedia. org/wiki/ Encryption, accessed on 14 th July, 2012.

[2] Freeman J., Neely R., and Megalo L. 1998. "Developing Secure Systems: Issues and Solutions". *IEEE Journal of Computer and Communication,* Vol. 89, PP. 36-45.

[3] Beth T. and Gollmann D. 1989. "Algorithm Engineering for Public Key Algorithms". IEEE *Journal on Selected Areas in Communications;* Vol. 7, No 4, PP. 458-466.

[4] IBM. 1994."The Data Encryption Standard (DES) and its strength against attacks". *IBM Journal of Research and Development,* Vol. 38, PP. 243-250.

[5] Wikipedia ,2012. "Bitwise operation", http: //en. wikipedia. Org /wiki/Bitwise_operation , accessed on 14 th July, 2012.

[6] Baraka H., El-Manawy H. A., and Attiya A. 1998. "An Integrated Model for Internet Security Using Prevention and Detection Techniques". *IEEE Journal of Computer and Communication* Vol. 99, PP. 25-33.

[7] Vivek Thakur , 2012. "NeekProtect", http: //neekprotect. sourceforge.net , accessed on 14 th July, 2012.

[8] http://en.wikipedia.org/wiki/Transposition_cipher, accessed on 14 th July, 2012.

[9] William Stallings, 2004. "Network Security Essentials (Applications and Standards) " *Pearson Education*, pp. 2–80.

[10] Charles P. 2004.Pfleeger, Shari Lawrence Pfleeger. "Security in computing" *Pearson Education*,pp. 642-666.

[11] Jose J. Amador, Robert W. Green, 2005. "Symmetric-Key Block Ciphers for Image and Text Cryptography",*International Journal of Imaging System Technology*, Vol. 15 – pp. 178- 188.

[12] Dragos Trinca, 2006."Sequential and Parallel Cascaded Convolution Encryption with Local Propagation:Toward Future Directions in Cryptography", Proceedings of The third International Conference on information TechnologyNew Generations. (ITNG'06), *IEEE Computer Society.*