

# A New Encryption Method for Secured Message Passing by Sorting Technique

S. Muthusundari<sup>1</sup> and S. Santhosh Baboo<sup>2</sup>

<sup>1</sup> Sathyabama University  
Chennai, India

<sup>2</sup> Department of Computer Science  
D.G.Vaishnav College, Chennai, India

nellailath@yahoo.co.in, santhos2001@sify.com

**Abstract.** Generally, in encryption or decryption process some of the characters are inter changed by using some encryption and decryption algorithms with key. This paper puts focusing a safe mechanism for secured message passing to tackle the security problem of information. We propose a new technique to encrypt the text message by sorting technique. In our method, the encryption process which is carried out by the plain text is arranged in to alphabetical order by sorting procedure and produces the cipher text. The proposed encryption technique needs the ASCII value of the characters. This technique has two advantages over traditional schemes. First, the encryption and decryption procedures are very simple, and subsequently, much faster. Second, the security level is very high due to the ASCII value substitutions of alphabetic characters. In this paper, the encryption and decryption procedures are explained.

**Keywords:** Encryption, Decryption, Plain text, Cipher text, ASCII value, sorting technique.

## 1 Introduction

Encryption is a mechanism by which a message is translated into another form so that only the sender and receiver can see. When a message is *encrypted*, that means that it is transformed into a form 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 and that is not readable. When a message is *decrypted*, it will get the original sent message. Encryption can provide strong security for data in the transmission. In general, cryptography concept is for maintaining the secured message passing system. Encryption, a cryptographic implementation, is the conversion of data into mixture of characters that, when viewed, cannot be read as simple text. Simple text is defined as standard written text, by the sender. The encrypt data is called a cipher, or cipher text which is in the other form of given data [1], while unencrypted data is called plaintext. Decryption is the process of converting encrypted data (cipher text) back into its original form (plaintext), so it can be readable.

The Network security is concerned with the security of information. [Good security means that the system and users are protected from attacks originating from inside the network just as well as they from outside attacks.] Security – guarding against interference by entities external to a system. The main aim is to protect the information, which is sent from one system to another through network. The information security is defined as follows.

Information security = Confidentiality + integrity + availability+ authentication. There can be no information security without confidentiality. Confidentiality ensures the unauthorized users do not intercept copy or replicate the information. The integrity is necessary so that the accurate information can flow over the network. The information security is also required during the retrieval of the data. The users should be authenticated to retrieve data and the information is not secure without authentication. There is no such thing as a completely secure computer network. Fig 1: shows the basic cryptographic system which uses the encryption and the decryption process based on the key.

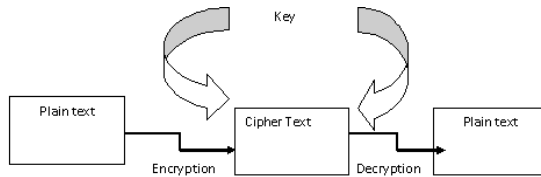


Fig. 1. Basic cryptographic system

## 2 Existing Techniques

All the encryption algorithms are based on two methods: the first one is substitution, in which each element in the plaintext (bit, letter and group of bits or letters) is associated with another element and the second is transposition, the elements of the plaintext have simply been re-arranged in another form; their position have been changed.[2]

### 2.1 Transposition Cipher

These ciphers are block ciphers, which changes the position of particular characters or bits of the input block. For the encryption, the plaintext is broken into n symbols and a key specifies one of (n!-1) possible permutations. The deciphering is accomplished by using an inverse permutation which restores the original sequence. [3] Transposition ciphers preserve the frequency distribution of single letters destroy the diagram and higher-order distributions. These techniques are also combined with other ciphers to produce a more secure product cipher. The simplest such cipher is the rail fence technique, in which the plain text is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message—we are discovered flee at once—with a rail fence of depth 3, we write the following

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 . .

The encrypted message: WECRLTEERDSOEFEFAOCAIVDEN

**2.2 Substitution Ciphers**

A substitution technique is one in which the letters of plain text are replaced by other letters or by numbers or symbols. The well known substitution cipher was invented by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with three positions. [4]For example: Plaintext: task completed

Cipher text: wdnv frpsohwhg. In this technique alphabet are wrapped around for the alphabets x, y and z so that the letter following Z is A. We can define the transformation as follows Plain: 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: 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 Proposed Methodology**

The system deals with security by using sorting technique for encryption and decryption.

**3.1 Encryption Algorithm**

The encryption process of  $C = E(K, P)$  using the proposed algorithm consists of three steps.

Steps

1. Assign the ASCII numeric values for the alphabets from the figure 2.
2. Arrange the numeric values by ascending order by any other sorting technique.
3. Substitute the alphabets for the ordered set.

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
64	40	@	80	50	P	96	60	`	112	70	
65	41	A	81	51	Q	97	61	a	113	71	p
66	42	B	82	52	R	98	62	b	114	72	q
67	43	C	83	53	S	99	63	c	115	73	r
68	44	D	84	54	T	100	64	d	116	74	s
69	45	E	85	55	U	101	65	e	117	75	t
70	46	F	86	56	V	102	66	f	118	76	u
71	47	G	87	57	W	103	67	g	119	77	v
72	48	H	88	58	X	104	68	h	120	78	w
73	49	I	89	59	Y	105	69	i	121	79	x
74	4A	J	90	5A	Z	106	6A	j	122	7A	y
75	4B	K	91	5B	[	107	6B	k	123	7B	z
76	4C	L	92	5C	\	108	6C	l	124	7C	{
77	4D	M	93	5D	]	109	6D	m	125	7D	
78	4E	N	94	5E	^	110	6E	n	126	7E	}
79	4F	O	95	5F	_	111	6F	o	127	7F	~

Fig. 2. ASCII value for the characters

### 3.2 Working Principle of Encryption

#### Step 1:

The encryption process involves taking each character of data and comparing it against a key. For example, one could encrypt the string “GOD IS GREAT” of data in any number of ways, for example, one may use a simple letter-number method. In this method, each in the alp number encryption (i.e.,ASCII( A)= 65,ASCII ( B)=66,ASCII( C)=67, and so on), this data is translated into the following numbers: 71 79 68 73 83 71 82 69 65 84 .

#### Step 2:

Arrange the series of step 1 with ascending order by using with any sorting technique. In this method we are applying the basic bubble sort technique to arrange the series.

Input of step 1 series: 71 79 68 73 83 71 82 69 65 84

Output after the bubble sort: 65 68 69 71 71 73 79 82 83 84

#### Step 3:

Now the output of step 2 is substituted with the corresponding alphabets.

Substitution of alphabets: ADEGGIORST.

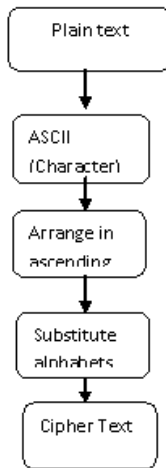


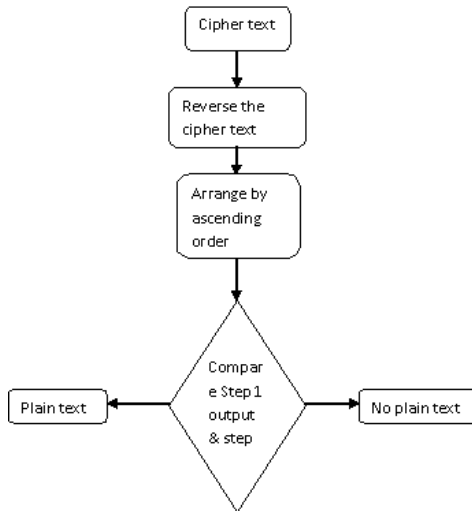
Fig. 3. Encryption Block Diagram

## B Decryption Algorithm

The decryption algorithm performs the reverse operations of encryption such that  $P = D(K, C)$ . It is done in three steps. The steps are as follows,

1. Reverse the cipher text. Then substitute the ASCII value.
2. Arrange the step 1 result by ascending order by using any sorting technique.

3. Match with the cipher text, if it is match with cipher text then it will display the plain text, otherwise it will give us error report. i.e the plain text will not be identified by the receiver.



**Fig. 4.** Decryption Block Diagram

### 3.3 Working Principle of Decryption

**Step 1:** Reverse the cipher text from the encryption process.

Cipher Text: ADEGGIORST

Reverse the cipher text: TSROIGGEDA

**Step 2:** Arrange the reverse of the cipher text in ascending order by using with bubble sort technique.

Now the output is as: ADEGGIORST

**Step 3:** Compare the output of step 1 and step 2. It is matches then the plain text will be displayed from the file. Otherwise it will not display the plain text. The receiver will not identify the plain text. Once he knows the key process only he can decrypt the message.

Step 1 output = step 2 output

ADEGGIORST = ADEGGIORST hence the receiver can decrypt the text message and he can get the plain text.

Decrypt message: GOD IS GREAT

### 3.4 Case Study of Encryption Process and Decryption Process

#### Case 1: Encryption Process

Consider the plain text as a single word: MILITARY

Step 1: Assign the ASCII Value of each alphabet in the plain text. Now we get,

ASCII (M) = 77	ASCII (I) = 73	ASCII (L) = 76
ASCII (I) = 73	ASCII (T) = 84	ASCII (A) = 65
ASCII (R) = 82	ASCII (Y) = 89	

PLAIN TEXT	M	I	L	I	T	A	R	Y
ASCII VALUE	77	73	76	73	84	65	82	89

STEP 2: Arrange the ASCII value by bubble sort technique

ASCII value :	77	73	76	73	84	65	82	89
Ascending Order:	65	73	73	76	77	82	84	89

Step 3: Substitute the alphabets for the ascending order.

Ascending Order:	65	73	73	76	77	82	84	89
Cipher Text :	A	I	I	L	M	R	T	Y

PLAIN TEXT: M I L I T A R Y  
CIPHER TEXT: A I I L M R T Y

#### Case 1: Decryption Process

Step 1: Get the cipher text from the encryption process and reverse the cipher text.

CIPHER TEXT: A I I L M R T Y  
Reverse Cipher Text: Y T R M L I I A

Step 2: Arrange the output of reverse the cipher text in ascending order by bubble sort technique.

Reverse Cipher Text: Y T R M L I I A  
Ascending order: A I I L M R T Y

Step 3: Match the cipher text and step 2 output. If both are match then the receiver will get the plain text from the index file, otherwise he will not get the plain text . The cipher text will not decrypted by the receiver. Hence security provides by the algorithm.

CIPHER TEXT: A I I L M R T Y is equal to  
Ascending order: A I I L M R T Y Hence the receiver will get the plain text.  
PLAIN TEXT: M I L I T A R Y

### Case Study of Encryption Process and Decryption Process:

#### Case 2: Encryption Process

Consider the plain text as a single sentence: WELCOME TO THE STAGE

Step 1: Assign the ASCII Value of each alphabet in the plain text. Now we get,

ASCII ( W ) = 87	ASCII ( E ) = 69	ASCII ( L ) = 76
ASCII ( C ) = 6	ASCII ( O ) = 79	ASCII ( M ) = 77

ASCII (E) = 69            ASCII (T) = 84            ASCII (O) = 79  
 ASCII (T) = 84            ASCII (H) = 72            ASCII (E) = 69  
 ASCII (S) = 83            ASCII (T) = 84            ASCII (A) = 65  
 ASCII (G) = 71            ASCII (E) = 69

PLAIN TEXT: W E L C O M E T O T H E S T A G E  
 ASCII VALUE: 87 69 76 67 79 77 69    84 79    84 72    69    83    84    65 71    69

Step 2: Arrange the ASCII value by bubble sort technique

ASCII VALUE: 87 69 76 67 79 77 69    84 79    84 72    69    83    84    65 71    69  
 Ascending order: 65 67 69 69 69 69 71    72 76    77 79    79    83    84    84    84    87

Step 3: Substitute the alphabets for the ascending order.

Ascending order: 65 67 69 69 69 69 71    72 76    77 79    79    83    84    84    84    87  
 Cipher Text: A C E E E E G H L M O O S T T T W  
 PLAIN TEXT: W E L C O M E T O T H E S T A G E  
 Cipher Text: A C E E E E G H L M O O S T T T W

## Case 2: Decryption Process

Step 1: Get the cipher text from the encryption process and reverse the cipher text.

CIPHER TEXT: A C E E E E G H L M O O S T T T W  
 Reverse Cipher Text W T T T S O O M L H G E E E E C A

Step 2: Arrange the output of reverse the cipher text in ascending order by bubble sort technique.

Reverse Cipher Text W T T T S O O M L H G E E E E A  
 Ascending order: A C E E E E G H L M O O S T T T W

Step 3: Match the cipher text and step 2 output. If both are match then the receiver will get the plain text from the index file, otherwise he will not get the plain text. The cipher text will not decrypted by the receiver. Hence security provides by the algorithm.

CIPHER TEXT: A C E E E E G H L M O O S T T T W  
 is equal to

Ascending order: A C E E E E G H L M O O S T T T W

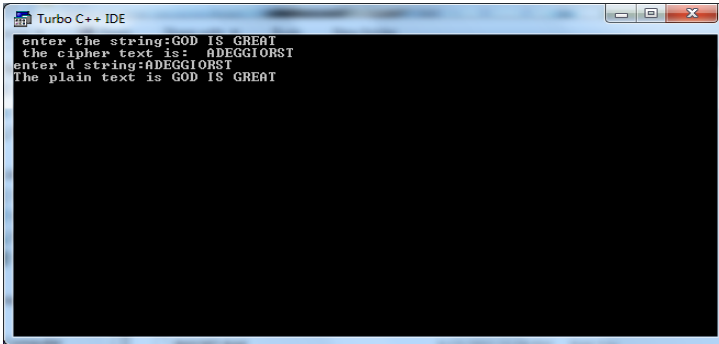
Hence the receiver will get the plain text.

PLAIN TEXT: W E L C O M E T O T H E S T A G E

## 4 Simulation and Experimental Results

We present here results generated from practical implementation of our algorithm. A plain text is taken as the input to the algorithm. The various steps involved in the encryption algorithm are carried out.

The sample test data is given below from the implementation of C program.



```

Turbo C++ IDE
enter the string:GOD IS GREAT
the cipher text is: ADEGGIORST
enter d string:ADEGGIORST
The plain text is GOD IS GREAT

```

#### 4.1 Implementation Procedure

The plain text which is transformed in to its ASCII value and then ASCII value will be arranged in to ascending order by using Bubble sort technique, then for the value the corresponding characters will replace and hence produce the Cipher text.

The Cipher text are given as input to the receiver than the receiver decrypt by reverse the cipher text and again by the same reverse process of encryption it is substitutes its ASCII value then arrange in ascending order by using Bubble sort technique. Then it match with cipher text and the ascending order substitutes data, if both are match then it takes the plain text from the file and display. On any other way it will not decrypt the plain text. Hence security is higher than any other encryption methods. Even though we know the key for the decryption process also the receiver cannot able to attain the plain text. If receiver cannot then definitely no one can attain the plain text. So 100% security message passing is produced.

The results shown here are implemented by using bubble sort technique. Hence the system is implemented successfully

### 5 Conclusion and Future Work

The Encryption algorithm, presented above, is a simple, direct substitution algorithm using sorting technique. Consequently, it is very fast and suitable for high speed encryption applications. The ASCII value translations give strength to this encryption algorithm. The combination of alphabetic substitution, sorting makes the decryption process very simple.

In future work, to improve the performance of the encryption and decryption process by using a novel sorting technique D-Shuffle method is going to be proposed , in place of Bubble sort. The performance and the efficiency of our proposed algorithm will be more benefited for secure message passing system.



## References

1. Wikipedia, "Encryption",  
<http://en.wikipedia.org/wiki/Encryption>  
(modified on December 13, 2006)
2. Lee, M.H.: Bounds on Substitution Ciphers. *IEEE Information Theory* 6, 2294–2296 (2007)
3. Stinson, D.R.: *Cryptogrphy Theory and Practice*, 2nd edn.
4. Kaufman, C., et al.: *Network Security Private Communication in a Public World*. Prentice Hall of India Private Limited (2003)
5. *Information Technology Journal* 4(3), 204–221 (2005)
6. *Information Technology Journal* 4(3), 204–221 (2005)
7. Shannon's, C.: *Communication Theory of Secrecy Systems*
8. Yang, K.-H., Niu, S.-J.: *Data Safe Transmission Mechanism Based on Integrated Encryption Algorithm*. Staffordshire University
9. Chen Tao, X.Y.: Design and implementation of encryption algorithm based on dimension magic cube. *Journal of Information* 2, 13–14 (2005)