ISSN:0975-9646

An Encryption Algorithm Based on ASCII Value of Data

Satyajeet R. Shinge[#1] , Rahul Patil[#2]
[#1-2]*Department of Computer Engineering, Pimpri-Chinchwad College of Engineering,*
[1-2]*Savitribai Phule Pune University, India.*

***Abstract*— Encryption is the process of encoding messages or information in such a way that only authorized users can read it. In an encryption algorithm the original message or information called plaintext is given as input to form ciphertext. Decryption is the process of transforming ciphertext into plaintext. Here ciphertext is the input to the decryption algorithm and it generates plaintext as output. Cryptographic algorithms are classified as symmetric and asymmetric. This paper presents a symmetric cryptographic algorithm for data encryption and decryption based on ASCII values of characters in the plaintext. This algorithm encrypts the plaintext using their ASCII values. The secret key is converted to another string and that string is used as a key to encrypt or decrypt the data.**

***Keywords*—Encryption, Decryption, ASCII, symmetric cryptography, plaintext, ciphertext, key.**

I. INTRODUCTION

Cryptographic algorithms are used to encrypt and decrypt messages in a cryptographic system. In simple terms, they protect data by making sure that unauthorized people can't access it. Cryptographic algorithms allow two parties to communicate and prevent unauthorized third parties from understanding those communications. Encryption transforms human readable plaintext into something unreadable, also known as ciphertext [1]. The ciphertext is then decrypted to convert to the original plaintext, making it understandable to the authentic party. Cryptography is constructed by five elements {M, C, K, E, D}, among which Message space M, also called Plaintext space, Cipher text space C, Key space K, Encryption algorithm E and Decryption algorithm D [3].

There are many approaches of cryptographic algorithms, most of them classified as symmetric key and asymmetric key cryptography [2]. In symmetric key algorithm same key is used for both encryption of plaintext and decryption of ciphertext. Symmetric-key encryption can use either stream ciphers or block ciphers. Asymmetric cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message.

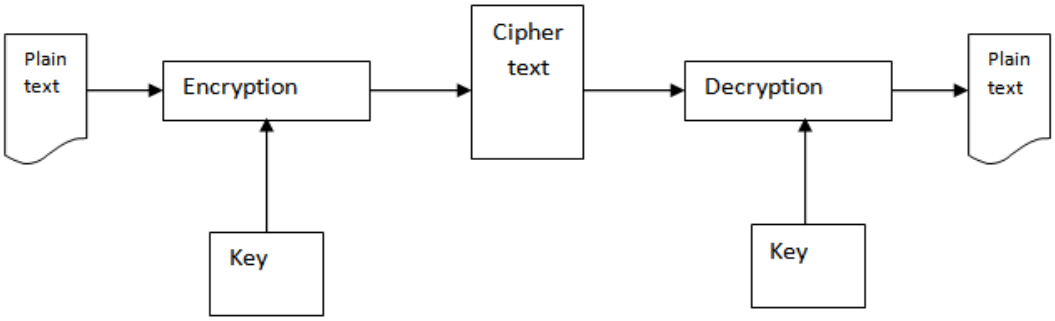

Fig. 1 Symmetric-key encryption Algorithm

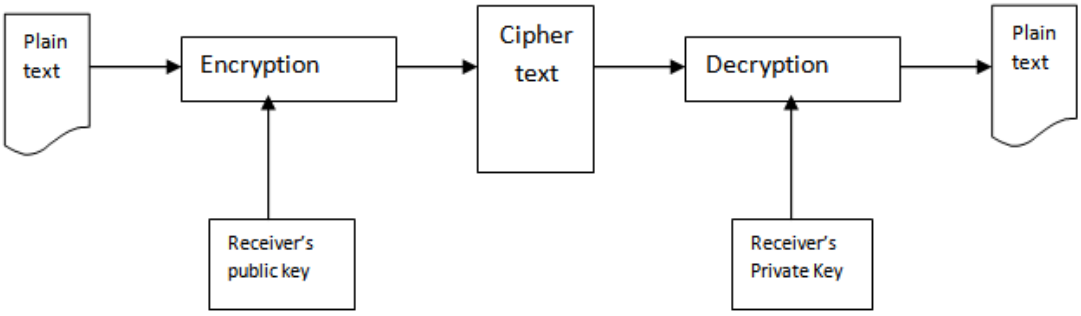

Fig. 2 Asymmetric-key encryption Algorithm

Figure 1 and 2 shows the process of symmetric-key algorithm and asymmetric-key algorithm respectively. As shown in figure 2, encryption algorithm uses the Receiver's public key and decryption algorithm uses the Receiver's private key.

II. RELATED WORK

An existing data encryption algorithm is given in paper [1] which proposes the encryption algorithm based on the ASCII value of message to be encrypted. This algorithm uses the key of length equal to the length of message. This key is encrypted to another key and used for encryption and decryption process. User has to enter the key for this system. If the message has more length, then system asks user to enter key equal to the length of message. It makes a difficult task for the user to enter a large key. Another limitation of this algorithm is that it has more execution time. So, these are the two limitations of existing algorithm.

III. PROPOSED WORK

Encryption and decryption of data performed in an efficient manner is one of the challenging aspects of modern computer science [4]. In this paper we propose an algorithm that uses the ASCII values of the plaintext to encrypt it. This system randomly generates a key for user having length equal to the length of the message or plaintext. The randomly generated key is converted to another key and is used to decrypt the message to original plaintext. As both encryption and decryption processes use the same key, it can be said that this is symmetric cryptographic algorithm. This algorithm takes less execution time as compared to existing algorithm.

A. Algorithm to perform encryption in proposed algorithm

Encryption steps are as follows:

1) Convert all characters of input plaintext into its ASCII values and store it in asciiArray.

Input	h	e	l	l	o
asciiArray	104	101	108	108	111

2) Find minimum value minValue from asciiArray.

3) Now Perform modulus operation on each value of charArray by minValue and store result into charMod array.

asciiArray	104	101	108	108	111
charMod	3	0	7	7	10

4) Automatically generate a key having length equal to the length of plaintext and store it to charKey array.

asciiArray	104	101	108	108	111
charMod	3	0	7	7	10
charKey	R	T	L	J	H

5) Convert all the character from charKey array into ASCII value and save it to asciiKey array.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72

6) Find minimum value minKey from asciiKey.

7) Perform modulus operation on each value of asciiKey by minKey and store result into keyMod array.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72
keyMod	10	12	4	2	0

8) Now add keyMod array into charMod to form encrypted key encKey.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72
keyMod	10	12	4	2	0
encKey	13	12	11	9	10

9) Now add minValue to each value of encKey array to get ciphertext of plaintext.

charKey	R	T	L	J	H
asciiKey	82	84	76	74	72
keyMod	10	12	4	2	0
encKey	13	12	11	9	10
asciiCiphertext	114	113	112	110	111
ciphertext	r	q	p	n	o

B. Algorithm to perform decryption in proposed algorithm

Decryption steps are as follows:

1) Convert all characters of ciphertext into its ASCII values and store it in decArray.

ciphertext	r	q	p	n	o
decArray	114	113	112	110	111

2) Now substract value of final encrypted key encKey from value of decArray.

ciphertext	r	q	p	n	o
decArray	114	113	112	110	111
difference	101	101	101	101	101

3) Add decArray and charMod to generate original plaintext.

ciphertext	r	q	p	n	o
decArray	114	113	112	110	111
difference	101	101	101	101	101
asciiPlaintext	104	101	108	108	111
Plaintext	h	e	l	l	o

IV. RESULTS

Table I show that the proposed algorithm takes less execution time as compared to existing algorithm. Table II shows the results of proposed algorithm for different plaintext and their automatically generated keys.

TABLE I

COMPARISON BETWEEN EXECUTION TIME OF EXISTING ALGORITHM AND PROPOSED ALGORITHM

Size of plaintext	Execution time for existing algorithm in ms	Execution time for proposed algorithm in ms
2	322	15
4	3679	15
6	3861	16
8	4748	16
10	5543	30

TABLE II

RESULTS OF PROPOSED ALGORITHM FOR DIFFERENT PLAINTEXT

PlainText	Automatically generated Key	CipherText
Abcd	BJWU	ajxw
Abcdef	WRGQSL	qmcnqk
Abcdefghi	LCFNAQDMP	ldhqevjtx

V. CONCLUSION

In this paper we proposed a symmetric encryption algorithm using ASCII values of data. The proposed algorithm gives good result in less execution time. This technique generates key automatically to encrypt the message. The automatically generated key is converted to another string and same key is used for encryption and decryption. Hence, we call this algorithm as symmetric key algorithm. In future work we can try to reduce the length of the key which will again reduce the execution time.

REFERENCES

[1] A. Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms", *International Journal on Computer Science and Engineering (IJCSE)*, Vol. 4, pp. 1650-1657, Sep 2012 ISSN: 0975-3397.

[2] U. Singh, U. Garg, "An ASCII value based text data encryption System", *International Journal of Scientific and Research Publications*, Volume 3, pp.1-5, November 2013 1 ISSN 2250-3153.

[3] Z. Yunpeng, Z. Yu, W. Zhong and R. O. Sinnott "Index-Based Symmetric DNA Encryption Algorithm", *2011 4th International Congress on Image and Signal Processing*, pp. 2290-2294,978-1-4244-9306-7/11/$26.00 ©2011 IEEE.

[4] M.P. Uddin, A. Marjan and M.R. Islam , "Developing a cryptographic algorithm based on ASCII conversions and a cyclic mathematical function", *Informatics, Electronics & Vision (ICIEV)*, 2014 International Conference .

[5] G. Singh, A. K Singla and K.S. Sandha, "Throughput Analysis of Various Encryption Algorithms", *International Journal of Computer Science and Technology*, Vol. 2, Issue 3, Septemver 2011.

[6] D.S.A. Elminaam, H.M.A. Kader and M. M. Hadhoud, "Evaluating the Performance of Symmetric Encryption Algorithms", *International Journal of Network Security*, Vol.10, No.3, PP.216–222, May 2010.

[7] Dr. A.P.A.G. Deshmukh, Dr. R. Qureshi, "Transparent Data Encryption- Solution for Security of Database Contents", *(IJACSA) International Journal of Advanced Computer Science and Applications*, Vol. 2, No.3, March 2011"

[8] A. Singh , U. Jauhari, "Data Security by Preprocessing the Text with Secret Hiding", *Advanced Computing: An International Journal (ACIJ)*, Vol.3, No.3, May 2012".