Advanced Data Encryption Algorithm Based on ASCII Value

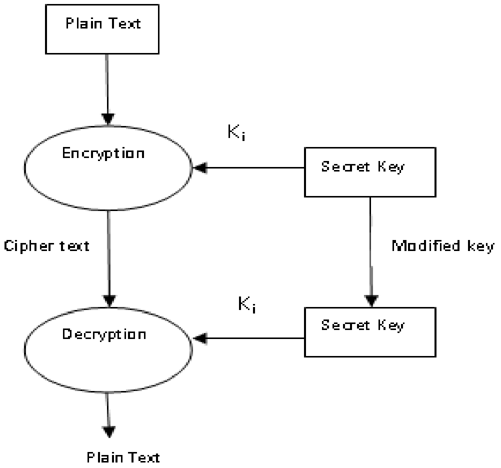
Prof. Dipali V. Patel
Vadodara Institute of Engineering, kotambi

Abstract- *Encryption is the process of converting sensitive data in such a way that only permitted users can access or read it. In which actual data called plaintext is passed as input to form cipher text which is converted code of actual message. Decryption is the process of converting cipher text into plaintext. Here cipher text is taken as input to the decryption algorithm and it produces plaintext as output. This paper presents data encryption and decryption based on ASCII values of characters using symmetric key. This algorithm encode the plaintext using their ASCII values. The secret key is converted to another string using its ASCII value and that string is used as a key for both encryption and decryption of the data.*

Keywords- ASCII, randomly generated key, symmetric encryption, Encryption, Decryption, plain text, cipher text.

I. INTRODUCTION

With the rapid development of modern communications technology and the Internet, the importance of information security becomes highlighted[2]. Cryptography has progressed been put forward to produce many new techniques for secure communication. Cryptography is study of designing or producing the secret message i.e. code or ciphers of the original message for the secure communication between sender and the receiver[1]. They protect data by making sure that unauthorized people can't access it. Encryption is basically a process or algorithm to make information hidden or secret. It is the process to converting the human readable plaintext into some another form that appears to be unintelligible ,random or meaningless , also known as cipher text [3]. The cipher text is then decrypted to convert to the original plaintext, making it understandable to the authentic party[2]. cryptographic algorithms are classified as symmetric key and asymmetric key cryptography. In this paper I have tried to keep data communication secure by using symmetric key. Which will be helpful for keeping data as secure . Here figure 1.1 shows the process of encryption and decryption algorithm:



II. PROPOSED WORK

It is one of the challenging aspects of modern computer science to keep data secure. In this paper I propose an algorithm that uses the ASCII values of the plaintext to encrypt it. In This algorithm, system randomly produces a string for user which is known as key, having length equal to the length of the plaintext. Then this 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 but by slightly modifying it.

A. Algorithm to perform Encryption

Steps:

1) Get the ASCII values of each character of string to be encrypted. i.e. plain text and store it in an ASCII content array
2) Find out the minimum value *mincontent* from the ASCII content array, Where *Mincontent*=avg of two lowest number.
3) Perform the modulus operation on each ASCIIcontent value : ASCII Content[i] %mincontent and save the answer in modcontent array where the value of i ranges up to the length of input. If the value of mod content is greater than 16, then again perform modcontent %16, and

track record the places where changes occur or record the positions where the value of mod content is greater than 16.

4) Perform the modulus operation on each ASCII content value: ASCII Key[i] % mincontent (minimum value of encrypted key)and store the answer in modkey array where the value of i ranges upto the length of key.
5) Find binary values of each value of modkey
6) Do the left circular shifts of binary values n time.(where n is the length of input)
7) Now add min value to each ASCII value of each character of encrypt key after shifting.
8) Add each mod content ()value to the ascii values of final encrypt key and it will generate cipher text.

Example:

1) Get the ASCII values of each character of input string i.e. plain text and store it in an ASCII content array. Eg.:-

Input	n	e	h	a
ASCII Content	110	101	104	97

2) Find out the minimum value *mincontent* from the asciicontent array. Eg.:-Mincontent=avg of min 2 value(97+101/2= 99)
3) Now perform the modulus operation on each asciicontent value as follows i.e. ASCIIContent[i] %mincontent and save the resultants in modcontent array where the value of I ranges upto the length of input.

Input	n	e	h	a
ASCII Content	110	101	104	97
modcontent	**11**	**2**	**5**	**1**

If the value of mod content is greater than 16, then again perform modcontent %16, and record the places where changes occur or record the positions where the value of mod content is greater than 16.

4) Now perform the modulus operation on each ASCII content value as follows i.e. ASCII Key[i] %mincontent (97)(minimum value of encrypted key)and save the resultants in modcontent array where the value of I ranges upto the length of key.

Input	n	e	h	a
ASCII Content	110	101	104	97
modcontent	**11**	**2**	**5**	**1**
Key	a	b	c	d
ASCIIkey	97	98	99	100
modkey	0	1	2	3

5) Take the binary values of each value of modkey.

Input	n	e	h	a
ASCII Content	110	101	104	97
modcontent	**11**	**2**	**5**	**1**
Key	a	b	c	d
ASCIIkey	97	98	99	100
Modkey	0	1	2	3
binary	**0000**	**0001**	**0010**	**0011**

6) Perform the left circular shifts of binary values 4 time .

	0000	0001	0010	0011
left circular shift 1	0000	0010	0100	0110
left circular shift 2	0000	0100	1000	1100
left circular shift 3	0000	1001	0001	1000
left circular shift	0001	0010	0011	0000
Encrypt key after shifting	1	2	3	0

So,

Input	n	e	h	a
ASCII Content	110	101	104	97
modcontent	11	2	5	1
Key	a	b	c	d
ASCIIkey	97	98	99	100
Modkey	0	1	2	3
binary	0000	0001	0010	0011
Encrypt key after shifting	**1**	**2**	**3**	**0**

7) Now add min value(97) to each ASCII value of each character of encrypt key after shifting. So, final encrypt key is-

Input	n	e	h	a
ASCII Content	110	101	104	97
modcontent	11	2	5	1
Key	A	b	c	d
ASCIIkey	97	98	99	100
Modkey	0	1	2	3
binary	0000	0001	0010	0011
Encrypt key after shifting	1	2	3	0
add min value to encrypt key	**98**	**99**	**100**	**97**

8) Now to encrypt the original data (input) or plaintext to generate ciphertext, add each mod content ()value to the ascii values of final encrypt key.

Input	n	e	h	a

ASCII Content	110	101	104	97
modcontent	11	2	5	1
Key	A	b	c	d
ASCIIkey	97	98	99	100
Modkey	0	1	2	3
binary	0000	0001	0010	0011
Encrypt key after shifting	1	2	3	0
add min value to encrypt key	**98**	**99**	**100**	**97**
Final Encrypt key	B+11	C+2	D+5	A+1
ciphertext ascii values	109	101	105	98
Ciphertext	m	e	I	b

B. Algorithm to perform Decryption

Following steps are performed to decrypt the cipher text:-

1) Take cipher text and find out the average of lowest two values from ASCII values of each character of cipher text.
2) Now Perform the subtraction of ASCII values of final encrypt key from asciicipher.(Add 16 to the stored positions where the modcontent value is greater than 16)
3) Add mincontent to each value of difference to generate plaintext.

Example:

1) ASCII values of each character of cipher text.

Ciphertext	M	e	i	b
ASCII Cipher	109	101	105	98

Mincontent is 98+101/2=99.5=99

2) Subtraction of ASCII values of final encrypt key from ASCII cipher

Cipher	m	e	i	b
ASCIICipher	109	101	105	98
asciifinalencrypt	98	99	100	97
difference	11	2	5	1

3) Adding mincontent to each value of difference to generate plaintext:

Cipher	m	e	i	b
ASCIICipher	109	101	105	98
asciifinalencrypt	98	99	100	97
difference	11	2	5	1
asciiplain	110	101	104	97
Plain text	n	e	h	a

III. LIMITATIONS

Length of plain text and Key must be equal.

IV. FUTURE SCOPE

In the future wok related to proposed algorithm, the limitations of proposed algorithm are overcome by encrypting and decrypting data with may or may not be same key length size in comparison with input size.

REFERENCES

[1] Akash 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] 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.

[3] Satyajeet R. Shinge , Rahul Patil,” An Encryption Algorithm Based on ASCII Value of Data”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234, ISSN:0975-9646