ISSN 2250-3153

An ASCII value based text data encryption System

Udepal Singh*, Upasna Garg**

*Computer Science & Engineering, Guru Kashi University (Talwandi Sabo), INDIA.
** Computer Science & Engineering, Guru Kashi University (Talwandi Sabo), INDIA.

Abstract- Encryption is a process of generating secrect text from the input text using a secret key and a encryption algorithm. Input text is refered to as plain text and the secret text generated is known as cipher text. Encryption algorithms are mainly divided into two categories which are symmetric key encryption algorithm and asymmetric key encryption algorithm. In Symmetric key encryption algorithm the same key is used by both sender and receiver but in asymmetric key algorithm sender and receiver both uses the different keys. In this paper, we present a technique based on symmetric key encryption algorithm which uses ASCII vales of input text to encrypt the data. Text data encryption techniques are very useful in data communication where one user want to send some secret messages to another users.

Index Terms- Encryption, Decryption, ASCII, Symmetric Encryption, Plain Text, Cipher Text

I. INTRODUCTION

Cryptography or cryptology; from Greek meaning “hidden, secret”; and “writing”, or “study” respectively; is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

There are two main types of cryptography. Those are public-key and symmetric-key. Public-key is a form of cryptography in which two digital keys are generated, one is private, which must not be known to another user, and one is public, which may be made available in public. These keys are used for either encrypting or signing messages. The public-key is used to encrypt a message and the private-key is used to decrypt the message. However, in another scenario, the private-key is used to sign a message and the public-key is used to verify the signature. The two keys are related by a hard one-way (irreversible) function, so it is computationally infeasible to determine the private key from the public key. Since the security of the private key is critical to the security of the cryptosystem, it is very important to keep the private key secret. This public-key system has the problem of being slow.

On the other hand, the system has powerful key management and, even more importantly, public-key cryptography has the ability to implement digital signatures in an efficient way. However, symmetric-key is a form of cryptography in which two parties that want to communicate can share a common and secret key. Each party must trust the other not to tell the common key to anyone else. This system has the advantage of encrypting large amount of data efficiently. However, the problem arises when it comes to key management over large number of users.

II. Research Elaborations

In this system we are using ASCII values of text data and a random key of 4 charcters to encrypt the data for communication purpose. The key by which plain text is encrypted is generated randomly by our system. Various transformations are applied to encrypt this plain text with the help of randomly generated key and the result becomes ciphertext. To decrypt the ciphertext reverse transformations are applied and the result becomes the original plain text. We are using visual C# to implement the algorithm.

Table I: A table for ASCII values for text data.

Character	ASCII Value	Character	ASCII Value
A	97	n	110
B	98	o	111
C	99	p	112
D	100	q	113
E	101	r	114
F	102	s	115
G	103	t	116
H	104	u	117
I	105	v	118
J	106	w	119
K	107	x	120
L	108	y	121
M	109	z	122

An algorithm to encrypt the data for our system is as follows :

Step I : Input the plain text and store it.

Step II: Find the ASCII values for each characters of the input.

Step III : Find the minimum ASCII value from the data.

Step IV: Perform the modulus operation on each ASCII content value with the minimum value find in the step no. III . i.e. (ASCII Content % minimum value) If the value of mod content is greater than 16 then again perform modcontent %16 and record the positions where the value of mod content is greater than 16.

Step V: Generate a random key of 4 characters by the system.

Step VI : Find the ASCII values of the key generated.

Step VII :Find the minimum value from the ASCII values of step VI.

Step VIII : Perform the modulus operation on key ASCII values with the minimum value obtained in step VII.

Step IX : Right shift the key one time.

Step X : Add minimum ASCII value from step III to mod key values to obtain the final key.

Step XI : Add mod contents of data to the final key obtained in step X.

Step XII : Generate the ciphertext from the ASCII values obtained from step XI

Algorithm to decrypt the data:

Step I : Input the ciphertext and find mincipher.

Step II: Obtained the ASCII values of this ciphertext and find mincipher.

Step III: Find the ASCII values of final key.

Step IV : Find the minimum value of final key.

Step V: calculate the difference of ASCII values of ciphertext and ASCII values of final key and add 16

To the stored positions where the modcontent value is greater then 16.

Step VI : Add the minchiper to the difference to obtain the plaintext ASCII values.

Step VII: Generate the text with the help of ASCII values.

III. Results

Below figures and table shows the results obtained by our porposed algorithm. We use input data of various lengths with fixed length key to generate the cipher text. The system is adequate to generate cipher text with this variable length input data.

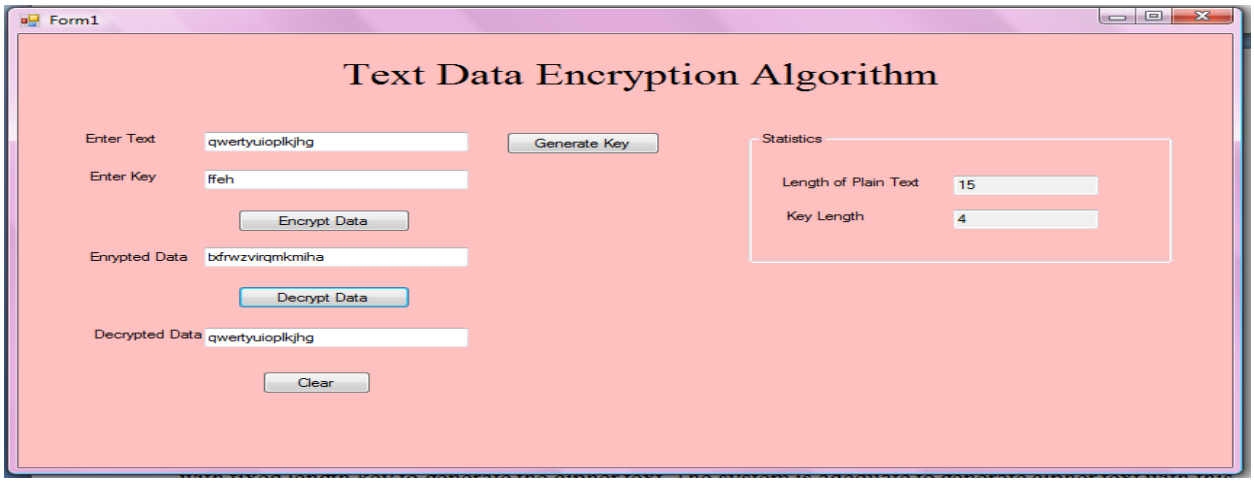

Figure 1: Output screen for 15 characters input.

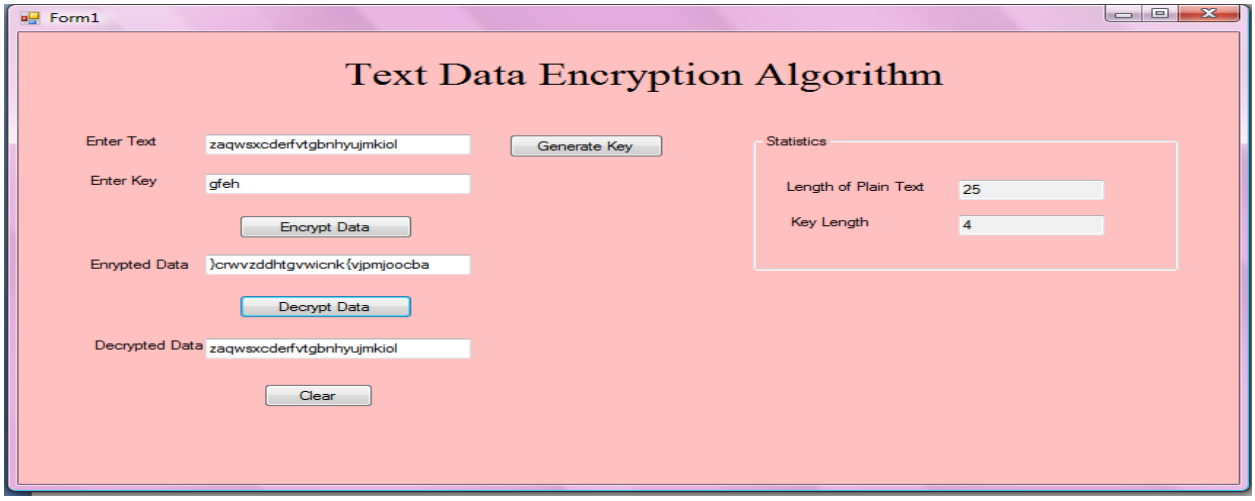

Figure 2: Output screen for 25 characters

Table II: The table which shows the result of the input data

Input data (Plain Text)	**Symmetric Key (generated by system)**	**Out put Data (Cipher Text)**
qwertyuiop	gaed	t}evwumrvac
asdfghjklmnbvcx	kjfg	bxhfhmnkmnbwhla
qwertyuioplkjhgfdsac	gijl	vwguyywltpnnohiiiscf
abcdefghijklmnopqrstuvwxy	glhl	fbhejflinjpmrntqvrxuzv|y~afb

IV. Conclusion

In this paper, we proposed an algorithm to encrypt and decrypt the data base on symmetric key encryption technique. The proposed system is generating very good results. In future, **:** the system can be further improved by using variable length key. System can be made to encrypt the data on the basis of Unicode values. It also can be improved for to decrypt the sentence form of data. so that it can be accepted globally

References

[1] Akanksha Mathur, "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 No. 09 Sep 2012"

[2] Ajit Singh and Upasana Jauhari," Data Security by Preprocessing the Text with Secret Hiding, Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012"

[3] Dr. Anwar Pasha Abdul Gafoor Deshmukh, Dr. Riyazuddin 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"

[4] Matthew M. Shannon, "Forensic Relative Strength Scoring: ASCII and Entropy Scoring,International Journal of Digital Evidence Spring 2004, Volume 2, Issue 4"

[5] Joyshree Nath, Asoke Nath, "Advanced Steganography Algorithm using Encrypted secret message, International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011"

[6] Majdi Al-qdah, Lin Yi Hui,"Simple Encryption/Decryption Application, International Journal of Computer Science and Security, Volume (1) : Issue (1)"

[7] Verma, Sharad Kumar, Ojha, D. B., "An application of data encryption technique using random number generator, International Journal of Research Studies in Computing 2012 April, Volume 1 Number 1, 35-42"

Authors

First Author – Udepal Singh, M.Tech (Computer Science & Engg.), Guru Kashi University (Talwandi Sabo), INDIA, udepalsingh87@gmail.com

Second Author – ER. Upasna Garg, M.Tech (Computer Science & Engg.), CDLU, SIRSA.

Astt. Prof. (CSE Deptt.), GKU (Talwandi Sabo), INDIA. Upasna.garg44@gmail.com