A new efficient encryption and decryption method using a Lossless Data Compression Scheme

Abid Sultan[1]
Department of Computer Science & IT
University of Sargodha Sub-Campus Bhakkar
Bhakkar, Pakistan
abidsultan006@gmail.com

Muhammad Azhar Mushtaq[2]
Department of Computer Science & IT
University of Sargodha Sub-Campus Bhakkar
Bhakkar, Pakistan
azhar.mushtaq@uos.edu.pk

Muhammad Faheem Nazir[3]
Department of Computer Science & IT
University of Sargodha Sub-Campus Bhakkar
Bhakkar, Pakistan

Munaza Saleem[4]
Department of Computer Science & IT
University of Sargodha Sub-Campus Bhakkar
Bhakkar, Pakistan

Javeed Altaf[5]
Department of Computer Science & IT
University of Sargodha Sub-Campus Bhakkar
Bhakkar, Pakistan

Muhammad Junaid[6]
Department of Computer Science & IT
University of Sargodha Sub-Campus Bhakkar
Bhakkar, Pakistan

DOI: 10.29322/IJSRP.10.12.2020.p10867
http://dx.doi.org/10.29322/IJSRP.10.12.2020.p10867

Abstract—With the advancement in internet technologies, data communication via the internet has been increasing day by day. Everybody, who is on the global network, may anguish about the safety of there sensitive data, information security, and privacy. Therefore, security threat has become the global complication in the world and this complication is increased continuously. The previous researcher proposed algorithm was not much efficient and time saving that's why we proposed a time saving a little bit more reliable algorithm. Cryptography is the component of information security that is used for message authentication, privacy, and certification. In this paper, we have described a new symmetric technique using shuffling, High-frequency latter, forward &backward function, and also old methods of cryptography which are already defined. The combination of all these makes the algorithm efficient and also time-saving

Keywords—Encryption; decryption; mean; cryptography

INTRODUCTION

Our world such as our lifestyle, way of thinking, way of working each and everything has changed due to digitalization. Every person who wants to send, receive information, data, service and it's all communication must have to require security, privacy, and protection. Network security plays a vital role in data protection and security from hacking. [1].

When hacking has become a big complication, the requirement of a cryptography mechanism to avoid threats of integrity, confidentiality, and availability is increased. The cryptography mechanism is a combination of several techniques that helps to control security problems. It also makes secure communication and provides high protection to data from the reach of hackers[2].

In cryptography, one thing that is mostly being used for both encryption and decryption is the symmetric key. It means that the same key is used for decryption and encryption. This key helps you to shared information between the two parties over the internet that is possible when the sender and receiver know the secret key. The main deficiency in the symmetric key is shared among the people publicly on the second-hand asymmetric key used different keys for encryption and decryption[3].

Cryptography depends upon some other factors such as Plain text, ciphertext, secret key. Plain text is the form of text or information that every person can understand easily. This information is a combination of characters, symbols, etc. The secret key performs a vital role in the cryptographic algorithm, it is used for encryption and decryption.

Encryption is the process, which is used for the translation of the simple text into un-understandable text and increase the security of a message or text. The Ciphertext is the result of an encryption process that is difficult to understand and read.it. Decryption is the reverse of the encryption which is used for converting cipher text into original text [4][5][6].

This paper is categorized into different sections. The first section is related to the basic knowledge of network security and cryptography analysis. In the second section, we describe the related work that has been already defined by many

researchers and scholars in the field of network security. The third portion contains a complete description of an algorithm that is being proposed in this paper. The next and last portion of this paper is related to the future work that we will cover in the future.

RELATED WORK

The following proposed algorithm that is defined in this paper is the mixture of different already proposed techniques and some cryptography information. This portion defines some early proposed techniques.[2].

Chachapara, K. et al [7] performed protected sharing with cryptography in encrypted cloud computing is also meant the architecture used uses the algorithm like RSA, along with AES which is the most secure algorithm in the field of cryptography. The Cloud controllers created keys for each user to have related privileges to access their files.

Orman, H. [8] describe several techniques on the development of cryptography, according to the author that the hash function plays an important internal role in cryptography, providing almost any data number, and in the MD5 drawbacks became known, it directed toward undoubted influences how the hash function is calculated.

Gennaro R. [9] defined the classification of cryptography and described that the randomness was the outcome of the unfamiliar steps, said to be the cause of why the important is cryptography. The attacker could not find or predict about original information.

Preneel, B. [10] clarifies cryptographic techniques and in the environment of the Snowden period where he talked about the crowds, it also studies the implementation and security of IT systems such as knowledge of the methods of attack where assassins can cross or unreasonably withdraws.

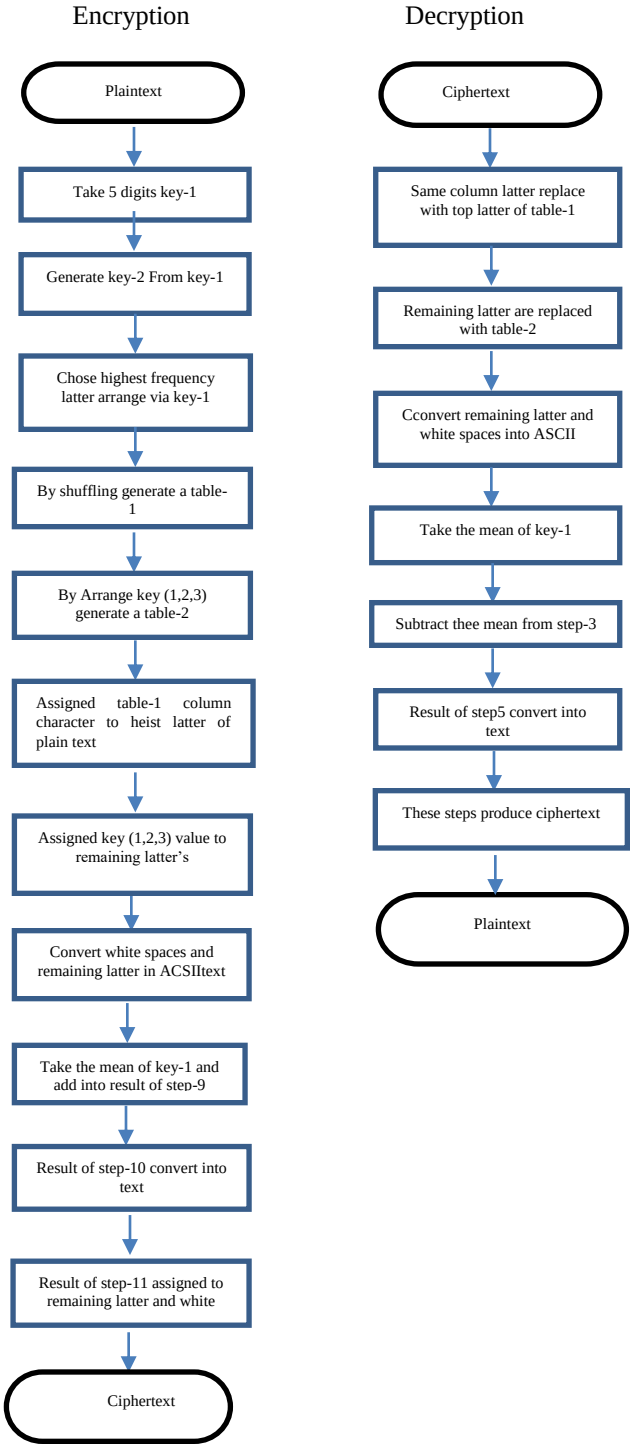
Sadkhan, S. B. [11] demonstrates the principles and procedures in cryptography where Julius Cesar'describing the current situation of Arab industrial and efforts for education in this region and is about a review for a new filtering system for information security.

Muhammad Azhar Mushtaq, Abid Sultan .et all[12] defined a new coin-flipping-based algorithm. the proposed technique is based on coin flipping and ASCII values. CFA is a more efficient technique that was used in this algorithm because ciphertext is difficult to break than other proposed techniques. Moreover, the randomly key created is equal to the size of the plaintext block due to growing security.

In this paper, Muhammad Azhar Mushtaq, Abid Sultan .et all[13] developed a cryptographic algorithm that was based on ASCII value and gray code. Before Gray code is not used in any cryptography techniques. AGS is a strong algorithm because the size of encrypted text is less than then original text. The shifting operation is performed on both randomly key generated and plain text. The Block size of plain text is equal to the key therefore increasing the level of security.

PROPOSED WORK

This paperer aims to define a more effective and complex algorithm. The proposed algorithm has a little bit more reliable encryption and decryption process than the previously proposed algorithms. The previous algorithm was much time-consuming so we proposed a time-saving algorithm.



Flowchart.1 Ecryption and Decryption

A. Encryption

The proposed algorithm is divided into two parts.

The first part is related to the keys.

Step1:

Take a 5-dights key from the user.

Step2:

Generate a new 5-dights key from key-1 with forward and back shuffling called key-2.

Step3:

Chose the highest frequency latter from alphabets and arrange via key-1. The resultant is called key-3.

The second part is related to creating a table and generating a ciphertext.

Step4:

By Shuffling of the highest frequency latter, we generate a table called table-1.

Step5:

Assigned keys (key-1-2-3) values respectively to table-1 characters which are a result as a table-2.

Step6:

Chose the highest frequency latter from plain text and assigned the column characters of table-1 to the highest frequency latter of plain text in forwarding manner first column latter to the first occurrence then move on.

Step7:

Repeat Step6 for the top 5highest frequency latter of plain text.

Step8:

Assigned keys (key-1-2-3) value to the remaining latter's which Belongs to table-2.

Step9:

Convert white spaces and remaining latter into ASCII.

Step10:

Take the mean of key-1 and add to the ASCII value of the existing white spaces and remaining latter.

Step11:

The result of step 10 converts into text.

Step12:

The result of step 11 is assigned to the existing white spaces and remaining latter of plain text.

Step13:

These steps 1 to 12produces a ciphertext.

B. Decryption

Step1:

Replace the same column characters with their top latter of table-1.

Step2:

The remaining chipper text latter's is replaced according to table-2 latter.

Step3:

Convert remaining latter and white spaces of ciphertext into ASCII.

Step4:

Take the mean of key-1.

Step5:

Subtract the mean from the result of step 3.

Step6:

The result of step5 converts into text.

Step7:

These steps produce plain text.

EXAMPLE

C. Encryption

The proposed algorithm is divided into two parts. The first part is related to keys

Key: 53142F1B3

Plain text: "I am happy because All is well in my life"

Step1:

Take a 5-dights key from the user with forward and back.

Key: 53142F1B3

Step2:

Generate a new 5-dights key from key-1 with forward and back shuffling called key-2.

F=1 & B=3

5+1-3=3

3+1-3=1

1+1-3=-1+9=8

4+1-3=2

2+1-3=0+9=9

KEY-2=31829

Step3:

Chose the highest frequency latter from alphabets and arrange it via key-1. The resultant is called key-3.

"E, U, A, O, N"

Arranged form: "N, A, E, O, U"

The second part is related to creating a table an generating a ciphertext.

I	J	K	P	Q
R	T	V	W	Y
R	T	V	W	Y

Step4:

After the Shuffling of the highest frequency letter table-1 is generated.

TABLE-I SHUFFLING OF THE HIGHEST FREQUENCY

E	U	A	O	N
B	D	F	G	H

Step 5:

Assigned keys (key-1-2-3) values respectively to table-I characters which are the result as a table-II.

TABLE II. (assigned keys to table-1)

B	D	F	G	H	I	J	K	P	Q	R	T	V	W	Y
5	3	1	4	2	3	1	8	2	9	N	A	E	O	U

Step 6,7:

Chose the highest frequency latter from plain text and assigned the column characters of table-1 to the highest frequency latter of plain text in a forwarding manner (first column latter to the first occurrence then move on). Repeat this step for the top 5 letters of plain text.

TABLE III(assigned frequency latter to plain text)

I		A	m		h	a	p	p	y			b	e	c	a	u	s	E		a	L	l		I	s		w	e	l	l		I	n		m	y		l	I	f	e
		F				k							b		v	d		I		F								r					h								b

Step 8:

Assigned keys (key-1-2-3) value to the remaining latter's which Belongs to table II.

TABLE IV (assigned keys value to remaining plain text latter)

I		A	m		h	a	p	p	y		b	e	c	a	u	s	e		a	L	l		I	s		w	e	l	l		I	n		m	y		l	I	f	e
3					2		2	2	u		5												3			O				3				u			3	1		

STEP 9:

Convert white spaces and remaining latter into ASCII.

Character	ASCII
M	77
C	67
S	83
L	76
Space	32

Step10:

Take the mean of key-1 and add to the ASCII value of the existing white spaces and remaining latter.

$$m = \frac{sum\ of\ the\ terms}{number\ of\ the\ terms}$$

$$m = \frac{5+3+1+4+2}{5}$$

m=3

Character	ASCII+mean
M	77+3=80
C	67+3=70
S	83+3=86
L	76+3=79
Space	32+3=35

ASCII+mean	Character
77+3=80	P
67+3=70	F
83+3=86	V
76+3=79	O
32+3=35	#

Step11:

The result of step 10 converts into text.

Step12:

The result of step 11 is assigned to the existing white spaces and remaining latter of plain text.

TABLE V (existing white spaces converting)

I		a	m		h	a	p	P	y		b	e	c	a	U	s	e		A	L	L		I	s		w	e	l	l		I	n		m	y		l	I	f	e
	#		p	#						#			f			v		#		o	o	#		v	#			o	o	#			#	p		#						

Step13:

These steps 1 to 12 produces a ciphertext.

TABLE VI (ciphertext)

I		a	m		h	a	p	p	y		b	e	c	a	u	s	e		A	L		l		I	s		w	e	l	l		I	n		m	y		l	I	f	e
3	#	f	p	#	2	k	2	2	u	#	5	b	f	v	d	v	I	#	F	o	#	o	#	3	v	#	o	r	o	o	#	3	h	#	p	u	#	o	3	1	b

Ciphertext: "**3#fp#2k22u#5bfvdvi#fo#o#3v#oroo#3h#pu#o31b**"

D. Decryption

Ciphertext: **3#fp#2k22u#5bfvdvi#fo#o#3v#oroo#3h#pu#o31b**

Step1:

Replace the same column characters with the top letter of table1.

TABLE VIII. RESULT OF DECRYPTION STEP 1

		f				k						b		v	d		I		F							r					h								b
I		a	m		h	a	p	p	y		b	e	c	a	u	s	e		A	L	l		I	s		w	e	l	l		I	n		m	y		l	I	f	e

Step2:

The remaining ciphertext letter's replaced according to table 2 letter.

TABLE IX. RESULT PRODUCED FROM DECRYPTION STEP 2

3					2		2	2	u		5											3			O					3				u			3	1	
I		a	m		h	a	p	p	y		b	e	c	a	u	s	e		A	L	l		I	s		w	e	l	l		i i	n		m	y		l	I	f	e

Step3:

Convert remaining letter and white spaces of ciphertext into ASCII.

$$m = \frac{5+3+1+4+2}{5}$$

m=3

Step4:

Take the mean of key-1.

$$m = \frac{sum\ of\ the\ terms}{number\ of\ the\ terms}$$

Step5:

Subtract the mean from the result of decryption step 3.

Step6:

The result of step5 converts into text chracters.

TABLE X. CIPHER AFTER STEP 3 of DECRYPTION

Character	ASCII
M	77
C	67
S	83
L	76
Space	32

TABLE XI. STEP5 RESULT

ASCII-mean
80-3=77
70-3=67
86-3=83
79-3=76
35-3=32

TABLE XII. TEXT CONVERSION

ASCII	Character
77	M
67	C
83	S
76	L
32	space

Step7:

Finaly plain text is generated.

TABLE XII. PLAIN TEXT

3	#	f	p	#	2	K	2	2	u	#	5	b	f	v	d	v	I	#	F	o	o	#	3	v	#	o	r	o	o	#	3	h	#	p	u	#	o	3	1	b
I		a	m		h	A	P	p	y		b	e	c	a	u	s	e		a	L	l		I	s		w	e	l	l		I	n		m	y		l	I	f	e

“I am happy because All is well in my life”

IMMPLEMENTATION & CALCULATIING EXECUTION TIME

as highlighted in figure1 the implementation of the proposed algorithm is performed in java.net. This takes input from the user as a plain text and the secret key with forward and back shuffling to encrypt and decrypt the data. Finally this implementation also calculates the execution time of the algorithm in a microsecond.

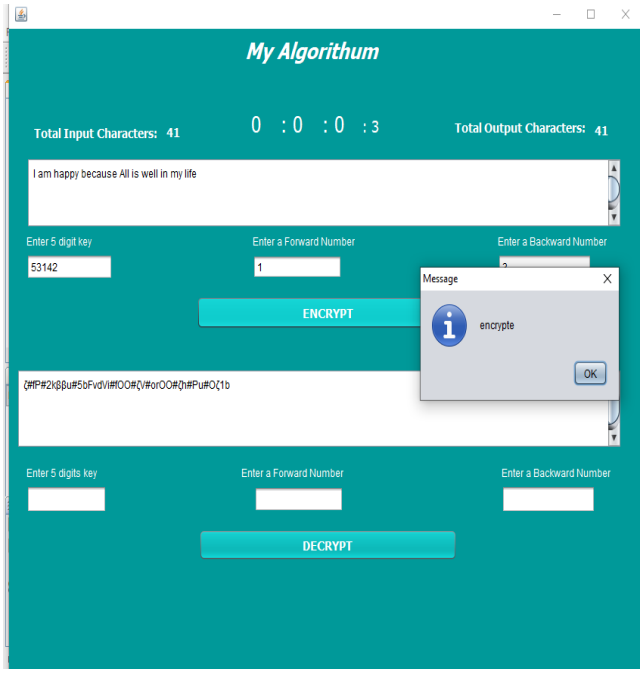


Figure.1 Algorithm Interface

TABLE XIII. EXECUTION TIME

Characters	Execution time
41	0:0:0:3
280	0:0:0:30
560	0:0:0:60
1120	0:0:0:120

Table 13 represents the exection time of the proposed algorithm based on different length of plain text block.

I. CONCLUSION

In this paper after analyzing the disadvantages of multiple substitution techniques, we proposed a new method which is the mixture of existing algorithms. The currently proposed technique is secure than the prevoius methods and it produce relative ciphtertext in less execution time. Our main focus is to improve security and decarese execution time as compared to already prposed methods. In the future, we will work on white spaces, charatcter cases and utalization of memory

REFERENCES

[1] “What Is Network Security? - Cisco.” [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-network-security.html. [Accessed: 17-Dec-2019].

[2] A. K. Vatsa, T. Mohan, and S. Vatsa, “Novel cipher technique using substitution method,” Int. J. Inf. Netw. Secur., vol. 1, no. 4, 2012.

[3] “What is a Symmetric Key? | Symmetric Key Encryption | Thales eSecurity.” [Online]. Available: https://www.thalesesecurity.com/faq/key-secrets-management/what-symmetric-key. [Accessed: 18-Dec-2019].

[4] A. Mathur, “A Research paper : An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms,” Int. J. Comput. Sci. Eng., vol. 4, no. 09, pp. 1650–1657, 2012.

[5] A. Vijayan, T. Gobinath, and M. Saravanakarthikeyan, “OPEN ACCESS ASCII Value Based Encryption System (AVB),” vol. 6, no. 4, pp. 8–11, 2016.

[6] S. R. Shinge and R. Patil, “An Encryption Algorithm Based on ASCII Value of Data,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 6, pp. 7232–7234, 2014.

[8] H. Orman, "Recent Parables in Cryptography," IEEE Internet Computing, vol. 18, no. 1, pp. 82-86, 2014.

[9] R. GENNARO, "IEEE Security & Privacy," IEEE Security & Privacy, vol. 4, no. 2, pp. 64 - 67, 2006

[10] B. Preneel, "Cryptography and Information Security in the PostSnowden Era," in IEEE/ACM 1st International Workshop on TEchnical and LEgal aspects of data pRivacy and SEcurity, Florence, 2015.

[11] S. B. Sadkhan, "Cryptography : current status and future trends," in International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, 2004

[12] M. A. Mushtaq, A. Sultan, A. Razzaq, Ehsaan-Ur-Rehman, and M. Inaam-Ur-Rehman, “New cryptographic algorithm based on CFA,” ACM Int. Conf. Proceeding Ser., no. September, pp. 203–208, 2019.

[13] M. A. Mushtaq, A. Sultan, A. Razzaq, Ehsaan-Ur-Rehman, and M. Inaam-Ur-Rehman, “New cryptographic algorithm based on CFA,” ACM Int. Conf. Proceeding Ser., no. September, pp. 203–208, 2019.

[7] K. Chachapara and S. Bhadlawala, "Secure sharing with cryptography in cloud," in 2013 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, 2013.