Advances in Intelligent Systems and Computing 939

Ajith Abraham
Niketa Gandhi
Millie Pant *Editors*

Innovations in Bio-Inspired Computing and Applications

Proceedings of the 9th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2018) held in Kochi, India during December 17–19, 2018

Springer

Advances in Intelligent Systems and Computing

Volume 939

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing such as: computational intelligence, soft computing including neural networks, fuzzy systems, evolutionary computing and the fusion of these paradigms, social intelligence, ambient intelligence, computational neuroscience, artificial life, virtual worlds and society, cognitive science and systems, Perception and Vision, DNA and immune based systems, self-organizing and adaptive systems, e-Learning and teaching, human-centered and human-centric computing, recommender systems, intelligent control, robotics and mechatronics including human-machine teaming, knowledge-based paradigms, learning paradigms, machine ethics, intelligent data analysis, knowledge management, intelligent agents, intelligent decision making and support, intelligent network security, trust management, interactive entertainment, Web intelligence and multimedia.

The publications within "Advances in Intelligent Systems and Computing" are primarily proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

**** Indexing: The books of this series are submitted to ISI Proceedings, EI-Compendex, DBLP, SCOPUS, Google Scholar and Springerlink ****

More information about this series at http://www.springer.com/series/11156

Ajith Abraham · Niketa Gandhi ·
Millie Pant
Editors

Innovations in Bio-Inspired Computing and Applications

Proceedings of the 9th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2018) held in Kochi, India during December 17–19, 2018

Springer

Editors
Ajith Abraham
Machine Intelligence Research Labs
Auburn, WA, USA

Niketa Gandhi
Machine Intelligence Research Labs
Auburn, WA, USA

Millie Pant
Department of Applied Science
and Engineering
Indian Institute of Technology
Roorkee, India

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-030-16680-9 ISBN 978-3-030-16681-6 (eBook)
https://doi.org/10.1007/978-3-030-16681-6

Library of Congress Control Number: 2019936144

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Welcome to the Proceedings of the ninth International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2018) and seventh World Congress on Information and Communication Technologies (WICT 2018). Conferences are held at Toc H Institute of Science and Technology (TIST) during December 17–19, 2018. Last year, IBICA 2017 was held in Marrakech, Morocco, and WICT 2017 was held in New Delhi, India.

The aim of IBICA is to provide a platform for world research leaders and practitioners, to discuss the full spectrum of current theoretical developments, emerging technologies, and innovative applications of bio-inspired computing. Bio-inspired computing is currently one of the most exciting research areas, and it is continuously demonstrating exceptional strength in solving complex real-life problems. WICT 2018 provides an opportunity for the researchers from academia and industry to meet and discuss the latest solutions, scientific results, and methods in the usage and applications of ICT in the real world. Innovations in ICT allow us to transmit information quickly and widely, propelling the growth of new urban communities, linking distant places and diverse areas of endeavor in productive new ways, which a decade ago was unimaginable. Thus, the theme of this World Congress is “Innovating ICT For Social Revolutions.”

IBICA–WICT 2018 brings together researchers, engineers, developers, and practitioners from academia and industry working in all interdisciplinary areas of intelligent systems, nature-inspired computing, big data analytics, real-world applications and to exchange and cross-fertilize their ideas. The themes of the contributions and scientific sessions range from theories to applications, reflecting a wide spectrum of the coverage of intelligent systems and computational intelligence areas. IBICA 2018 received submissions from 10 countries, and each paper was reviewed by at least five reviewers in a standard peer-review process. Based on the recommendation by five independent referees, finally 25 papers were accepted for the conference (acceptance rate of 37%). WICT 2018 received submissions from 12 countries, and each paper was reviewed by at least five reviewers in a standard peer-review process. Based on the recommendation by five independent referees, finally 25 papers were accepted for the conference (acceptance rate of 35%).

Many people have collaborated and worked hard to produce the successful IBICA–WICT 2018 conference. First, we would like to thank all the authors for submitting their papers to the conference, for their presentations and discussions during the conference. Our thanks go to program committee members and reviewers, who carried out the most difficult work by carefully evaluating the submitted papers. Our special thanks to Oscar Castillo, Tijuana Institute of Technology, Tijuana, Mexico; Florin Popentiu Vladicescu, University Politehnica of Bucharest, Romania; and Sheng-Lung Peng, National Dong Hwa University, Taiwan, for the exciting plenary talks. We express our sincere thanks to the session chairs and organizing committee chairs for helping us to formulate a rich technical program.

Ajith Abraham
Preethi Thekkath
General Chairs - (IBICA-WICT 2018)

Millie Pant
Simone Ludwig
Antonio J. Tallón-Ballesteros
N. Vishwanath
Rasmi P. S.
Program Co-chairs

Organization

Patrons

K. Varghese	Toc H Public School Society, India
Alex Mathew	Toc H Public School Society, India

General Chairs

Ajith Abraham	Machine Intelligence Research Labs (MIR Labs), USA
Preethi Thekkath	Toc H Institute of Science and Technology, India

Program Co-chairs

Simone Ludwig	North Dakota State University, USA
Millie Pant	Indian Institute of Technology, Roorkee, India
Antonio J. Tallón-Ballesteros	University of Seville, Spain
N. Vishwanath	Toc H Institute of Science and Technology, India
Rasmi P. S.	Toc H Institute of Science and Technology, India

International Advisory Board

Achuthsankar S. Nair	University of Kerala, Thiruvananthapuram, India
Albert Zomaya	University of Sydney, Australia
Andre Ponce de Leon F. de Carvalho	University of Sao Paulo at Sao Carlos, Brazil
Bruno Apolloni	University of Milan, Italy

Francisco Herrera	University of Granada, Spain
Imre J. Rudas	Óbuda University, Hungary
Janusz Kacprzyk	Polish Academy of Sciences, Poland
Marina Gavrilova	University of Calgary, Canada
N. Krishnan	Manonmaniam Sundaranar University, Tamil Nadu, India
Patrick Siarry	Université Paris-Est Créteil, France
Ronald Yager	Iona College, USA
Salah Al-Sharhan	Gulf University of Science and Technology, Kuwait
Sankar Kumar Pal	ISI, Kolkata, India
Sebastian Ventura	University of Cordoba, Spain
Vincenzo Piuri	Universita' degli Studi di Milano, Italy
Vrinda V. Nair	APJ Abdul Kalam Technological University, India

Publication Chairs

Azah Kamilah Muda	UTeM, Malaysia
Niketa Gandhi	Machine Intelligence Research Labs (MIR Labs), USA

Web Service

Kun Ma	Jinan University, China

Publicity Committee

Atta Rahman	University of Dammam, Dammam, Saudi Arabia
Chinmay Chakraborty	Birla Institute of Technology, Jharkhand, India
G. Sudha Sadasivam	PSG College of Technology, Coimbatore, India
Meera Ramadas	University College of Bahrain, Kingdom of Bahrain
Marjana Prifti Sk'nduli	University of New York, Tirana
Mayur Rahul	C.S.J.M. University, Kanpur, India
Neeraj Rathore	Jaypee University of Engineering and Technology, Guna, MP, India
Nesrine Baklouti	University of Sfax, Tunisia
Sanju Tiwari	National Institute of Technology, Kurukshetra, Haryana, India

Shikha Mehta	Jaypee Institute of Information Technology, Noida, India
Sourav Banerjee	Kalyani Government Engineering College, West Bengal, India

Organizing Chairs

Babu John	Toc H Institute of Science and Technology, India
Sreela Sreedhar	Toc H Institute of Science and Technology, India
Rasmi P. S.	Toc H Institute of Science and Technology, India
N. Vishwanath	Toc H Institute of Science and Technology, India

Local Organizing Committee

Jesna Anver	Toc H Institute of Science and Technology, India
Saira Varghese	Toc H Institute of Science and Technology, India
Leda Kamal	Toc H Institute of Science and Technology, India
Elsaba Jacob	Toc H Institute of Science and Technology, India
Abin Oommen Philip	Toc H Institute of Science and Technology, India
Ceira Sara Cherian	Toc H Institute of Science and Technology, India
Mima Manual	Toc H Institute of Science and Technology, India
Ashly Joseph	Toc H Institute of Science and Technology, India
Rinu Rose George	Toc H Institute of Science and Technology, India
Mithu Mary George	Toc H Institute of Science and Technology, India
Anju Kuriakose	Toc H Institute of Science and Technology, India
Anuraj C. K.	Toc H Institute of Science and Technology, India

International Program committee

Abid Hussain Wani	University of Kashmir, India
Alberto Cano	University of Córdoba, Spain
Andries Engelbrecht	University of Pretoria, South Africa
Arun Kumar Sangaiah	Vellore Institute of Technology, India
Aswani Kumar Cherukuri	Vellore Institute of Technology, India
Azah Muda	UTeM, Malaysia
Cesar Hervas	University of Córdoba, Spain
Christian Veenhuis	HELLA Aglaia Mobile Vision GmbH, Germany
Daniel Valcarce	University of A Coruña, Spain
Daniela Zaharie	West University of Timisoara, Romania
Denis Felipe	Federal University of Rio Grande do Norte, Brazil

Dilip Pratihar	Indian Institute of Technology Roorkee, India
Eiji Uchino	Yamaguchi University, Japan
Elizabeth Goldbarg	Universidade Federal do Rio Grande do Norte, Brazil
Francisco Chicano	Universidad de Málaga, Spain
Frantisek Zboril	Brno University of Technology, Czech Republic
Giovanna Castellano	Università degli Studi di Bari Aldo Moro, Italy
Gregorio Sainz-Palmero	Universidad de Valladolid, Spain
Igor Silva	Federal University of Rio Grande do Norte, Brazil
Isabel S. Jesus	Instituto Superior de Engenharia do Porto, Portugal
Janmenjoy Nayak	Sri Sivani College of Engineering (SSCE), India
Jaroslav Rozman	Brno University of Technology, Czechia
Jerry Chun-Wei Lin	University of Kansas, USA
Jerzy Grzymala-Busse	University of Kansas, USA
José Everardo Bessa Maia	University of Oviedo, Spain
José Ramón Villar	University of Córdoba, Spain
José Raúl Romero	Universidad de A Coruña, Spain
Jose Santos	Instituto Superior de Engenharia do Porto, Portugal
Jose Tenreiro Machado	ISEP, Portugal
Joseph Alexander Brown	Innopolis University, Canada
Juan A. Nepomuceno	University of Calcutta, India
Kaushik Das Sharma	University of Calcutta, India
Leandro Maciel Almeida	Jinan University, China
Lin Wang	Jinan University, China
Mario Giovanni C. A. Cimino	University of Pisa, Italy
Meera Ramadas	University College of Bahrain, Kingdom of Bahrain
Mohammad Shojafar	Sapienza University of Rome, Italy
Niketa Gandhi	Machine Intelligence Research Labs (MIR Labs), USA
Oscar Castillo	Instituto Tecnológico de Tijuana, Mexico
Oscar Gabriel Reyes Pupo	University of Central Oklahoma, USA
P. E. S. N. Krishna Prasad	S V College of Engineering, Tirupati, India
Patrick Siarry	South Asian University, Delhi, India
Prabukumar Manoharan	Vellore Institute of Technology, India
Pranab Muhuri	South Asian University, Delhi, India
Radu-Emil Precup	Politehnica University of Timisoara, Romania
Ricardo Tanscheit	PUC-Rio, Brazil
Rubén Salado-Cid	University of Córdoba, Spain
Sarika Jain	National Institute of Technology, Kurukshetra, Haryana, India
Simone Ludwig	North Dakota State University, USA

Sylvain Piechowiak	Université de Valenciennes et du Hainaut-Cambrésis, France
Terry Trowbridge	York University, Canada
Thanasis Daradoumis	Open University of Catalonia, Greece
Thatiana C. N. Souza	Federal University Rural Semi-Arid, Brazil
Thomas Hanne	University of Applied Sciences Northwestern Switzerland, Switzerland
Varun Ojha	ETH Zurich, Switzerland

Contents

Transfusion of Extended Vigenere Table and ASCII Conversion for Encryption Contrivance

Sakshi[1], Prateek Thakral[2](✉), Karan Goyal[1], Tarun Kumar[1], and Deepak Garg[1]

[1] National Institute of Technology, Kurukshetra, Haryana, India
[2] Jaypee University of Information Technology, Waknaghat, Solan, India
18.prateek@gmail.com

Abstract. In the field of cryptography, to make cryptosystem more secure an evaluation of modulus operations on integral values followed by ASCII value generation on plain text characters have been deeply explored in this research paper. On the basis of this an extended algorithm has been proposed. In this, the Encryption technique consists of an extended combination of Vigenere and Caesar cipher which is the main key feature of this algorithm and then decryption of text along with ASCII algorithm and substitution methodology has been done. The Algorithm is initiated on the basis of inspection of various research papers, furthermore, reviews have been made for proving this system more reliable. In the proposed algorithm modified Vigenere table and ASCII values are taken into consideration for decreasing the steps to reduce complexity and making a more secure way of cryptography.

Keywords: Computer security · ASCII value · Cryptography · Cryptology · Multiplicative cipher · Random key · Symmetric key

1 Introduction

Network security comprises various strategy and application that are taken to avoid and check unintended access, alteration, misuse, or refusal of a network and other network resources that are accessible [1]. With each passing year, the security dangers confronting computer systems have turned out to be all the more, in fact, modern, better sorted out and harder to recognize. A great part of the data imparted every day must be kept private. Data, for example, monetary reports, worker information and therapeutic records should be conveyed in a way that guarantees secrecy and honesty [2]. The issue of unsecured correspondence is exacerbated by the way that quite a bit of this data is sent over people in general Internet and might be handled by outsiders, as in email or texting Presently, cryptography is recognized as a part of computer science as well as of science and mathematics, and is connected closely with, computer security, information concept, and engineering. Encryption simply means to change the message, also known as plaintext, to make it unreadable to any user who is not an authorized user [2]. In other words, we can say the whole procedure of encryption is to discover a protected

A. Abraham et al. (Eds.): IBICA 2018, AISC 939, pp. 36–45, 2019.
https://doi.org/10.1007/978-3-030-16681-6_4

mechanism by means of which just the valid or the authorized user has the access to the message sent by the sender. Cryptography is termed as “Hidden Secrets” and is mainly deals with encrypting the data [3]. It is useful for inspecting those conventions, which are related to various perspectives in information security, for instance, verifying data, ordering of data, non-dissent and data uprightness. The authorization secures and sustains the interest of both the parties i.e. the person who is sending message as well the authorized receiver [4].

There are various security aspects for a cryptographic technique including Authentication, Confidentiality, Integrity, and Non-Repudiation [5]. Authentication is only a procedure of demonstrating one’s personality. Furthermore, if privacy or secrecy is taken into the picture it is tied in with confirming that no one else can read the information except for the intended user. To confirm that the received message has not been altered at all from its original content, is keeping up the Integrity. Non-Repudiation describes a system that shows that message or information received is from a valid user [6].

2 Related Work

The current work done in this field can be analyzed in this section briefly by experiencing the proposed model and various algorithm proposed by the different authors.

Mathur [7] proposed an algorithm that performs modulus operation on the plain text message and the secret key by using ASCII based conversion mechanism. The minimum value of both is stored in separate arrays. A binary conversion of the minimum key value is performed and right shifting is done. The shifted encrypted key is added to the minimum value of plain text characters and the final cipher text is produced. Saraswat et al. [8] proposed an algorithm that brings the new version for the vigenere table having the 26 alphabets (A–Z) as well as the 10 numeric digits (0–9). The alphanumeric cross-section of the rows and columns of the table provides the intersection text on which advance version of Caesar cipher is performed to get the final cipher text. Krishna [9] proposed a new algorithm that is totally different from symmetric, asymmetric or hashing function. The algorithm changes the input plain text into small sized packets of constant length and then stored in a binary matrix. The binary matrix has the 8 bit equivalent of every plain text characters’ ASCII value. It uses rotational mathematical method and conversion of radix on the text repeatedly. The encrypted text is rotated by the cyclic function. The final cipher text is in the form of unprintable characters below ASCII value 32.

Bhargava et al. [10] proposed a new algorithm that incorporates the features of transposition and substitution cipher mechanism. It uses Multiplicative cipher techniques and Rail fence cipher techniques. In multiplicative cipher technique a secret key is selected such that taking its product with any other character would give another changed character for every plain text character. The final cipher text is a sequence of special characters that is formed by performing the algorithm on plain text. Gupta et al. [11] proposed a symmetric key encryption algorithm that takes plain text and two different keys. A modified Vigenere table is used that consists characters from ASCII table and values ranging from 33–126. An intersection text is produced by plain text and key 1 from the table. The Intersection text is then added with second key using modified Caesar cipher and modulo 26 arithmetic. It gives the final cipher text.

3 Proposed Algorithm

The algorithm that is being proposed here comes with the fusion of ASCII conversion and mathematical modification concept. Since the ASCII values are valid values for the numbers, characters, and other special symbols. The proposed algorithm will be coming up with the fulfillment of the shortcomings of the existing work and it will efficiently apply the ASCII values to produce the cipher text [12].

If we examine the ASCII table, we can draw conclusion that ASCII values from 33–126 depict the numeric values, alphabetical characters and special characters that are mostly used in day to day conversation while typing. These 94 characters are the printable characters that are available on every keyboard. In this algorithm the sender begins with the plain text message and a randomly generated key of length equivalent to the plain text.

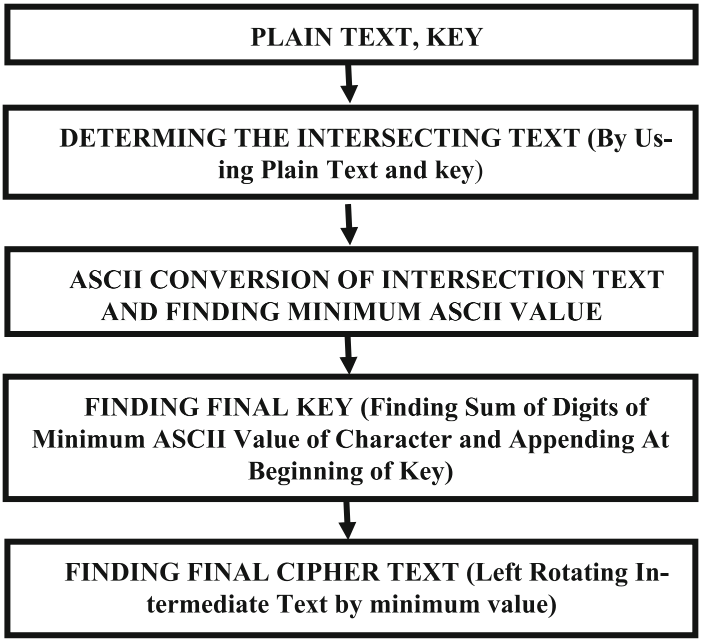
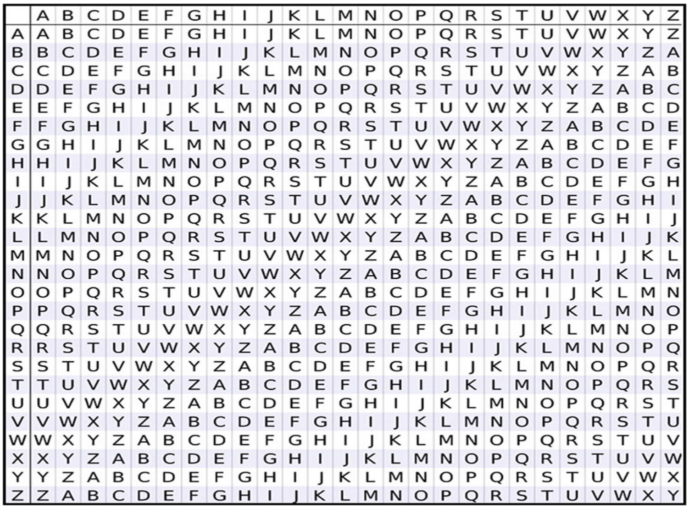

PLAIN TEXT, KEY
DETERMING THE INTERSECTING TEXT (By Using Plain Text and key)
ASCII CONVERSION OF INTERSECTION TEXT AND FINDING MINIMUM ASCII VALUE
FINDING FINAL KEY (Finding Sum of Digits of Minimum ASCII Value of Character and Appending At Beginning of Key)
FINDING FINAL CIPHER TEXT (Left Rotating Intermediate Text by minimum value)

Fig. 1. Flowchart for the processing of the proposed algorithm

The entire operation can be understood by having gone through the proposed algorithm sequentially. The proposed algorithm can be viewed by the Fig. 1.

3.1 Step 1: Determining the Intersecting Text

This part is mainly affected by using the Vigenere table and is further extended to include the numeric values and the special characters. The below Fig. 1 presents the vigenere cipher table. The Vigenere cipher table contains only alphabets both in horizontal and vertical axis. The horizontal axis represents the plain text and the vertical axis represents the key. The intersection of these axis values i.e. the plain text character value and key character value gives the cipher text. The form of ordering used in the vigenere table will be used for ordering the characters for the table in the proposed algorithm (Fig. 2).



	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
A	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
B	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	A
C	C	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
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Fig. 2. Vigenere table

Similar to this vigenere table, a new and extended table i.e. the extended version of previous Table is designed that not only contains the alphabetical characters but also the numeric and special characters. For Table 1 the horizontal axis depicts the plain text and the vertical axis depicts the key. The Table 1 is a matrix of 94 rows and columns for which the records start with the character whose value start with the ASCII value 33 with character "!" and it moves on till character whose ASCII value is 126 with character "∼" in both the horizontal and vertical axis. This table consist of all 94 printable characters that contains all the capital letters (A–Z), small letters (a–z), numeric values (0–9) and remaining are the special printable characters. The following Table 1 i.e. the extended vigenere table will be used for the proposed algorithm.

The determination of the intersection text can be understood by the next example. Let us take the plain text that needs to be sent be "ABC12#" and the key be "SA4$#*". Now we will see how Intersecting Text is calculated.

Table 1. The extended vigenere table

	!	“	#	$	%	&	‘	(	)	*	And up to ∼
!	!	“	#	$	%	&	‘	(	)	*	
“	“	#	$	%	&	‘	(	)	*	+	
#	#	$	%	&	‘	(	)	*	+	,	
$	$	%	&	‘	(	)	*	+	,	-	
%	%	&	‘	(	)	*	+	,	-	.	
&	&	‘	(	)	*	+	,	-	.	/	
‘	‘	(	)	*	+	,	-	.	/	0	
(	(	)	*	+	,	-	.	/	0	1	
)	)	*	+	,	-	.	/	0	1	2	
*	*	+	,	-	.	/	0	1	2	3	
+	+	,	-	.	/	0	1	2	3	4	
,	,	-	.	/	0	1	2	3	4	5	
-	-	.	/	0	1	2	3	4	5	6	
.	.	/	0	1	2	3	4	5	6	7	
/	/	0	1	2	3	4	5	6	7	8	
0	0	1	2	3	4	5	6	7	8	9	
1	1	2	3	4	5	6	7	8	9	:	
2	2	3	4	5	6	7	8	9	:	;	
Up to till ∼											

We can calculate Intersecting Text from table by finding the entry which is cross section point of plaint text character and key characters. Below gives the table showing the calculation of intersection text (Table 2).

Table 2. Working of proposed algorithm

Plain text	A	B	C	1	$	#
Key	S	A	4	$	#	*
Intersection text	S	B	V	4	&	,

Intersection text can also be calculated by using the mathematical formula. The formula for calculation intersection text is:

$$\mathrm{I.T} = (\mathrm{PT} - 33) + \mathrm{K} \tag{1}$$

Where I.T = ASCII value of Intersection Text, PT = ASCII value of Plain Text, K = ASCII value of Key.

```
    IF (I.T > 126) THEN
{
I.T = I.T – 94;                                   (2)

}
```

This technique is applied so that the ASCII value of intersecting text is between the ranges of 33–126.

3.2 Step 2: Finding Minimum Value from the Intersection Text

In this step the ASCII values of the characters of the Intersection text are stored in an array and then sorted in ascending order. Now the smallest value among them is taken into consideration and stored in a separate variable (Table 3).

Table 3. Finding the minimum value from intersection text and sorting

Intersection text	S	B	V	4	&	,
ASCII value	115	98	86	52	38	44
Sorted ASCII values	38	44	52	86	98	115

Minimum (ASCII_VALUES) = 38, Store it in MIN. MIN = 38

Adding the digits of MIN recursively up to a single digit and store it in variable SUM.

SUM = 2.

3.3 Step 3: Final Cipher Text Determination

This step goes with determination of final cipher text. The ASCII values of the Intersection text are circularly sifted by the value of SUM (Table 4).

Table 4. Circular shifting

Intersection text	S	B	V	4	&	,
ASCII value	115	98	86	52	38	44
Circularly shifted ASCII values	86	52	38	44	115	98
Intermediate text	V	4	&	,	S	B

CIPHER TEXT: V4&,sb

The intermediate text obtained by the circular shift is the ultimate cipher text. Hence,

Plain Text	ABC1$#
Key	SA4$#*
Cipher Text	V4&,sb

4 Encryption and Decryption Algorithm

Encryption:

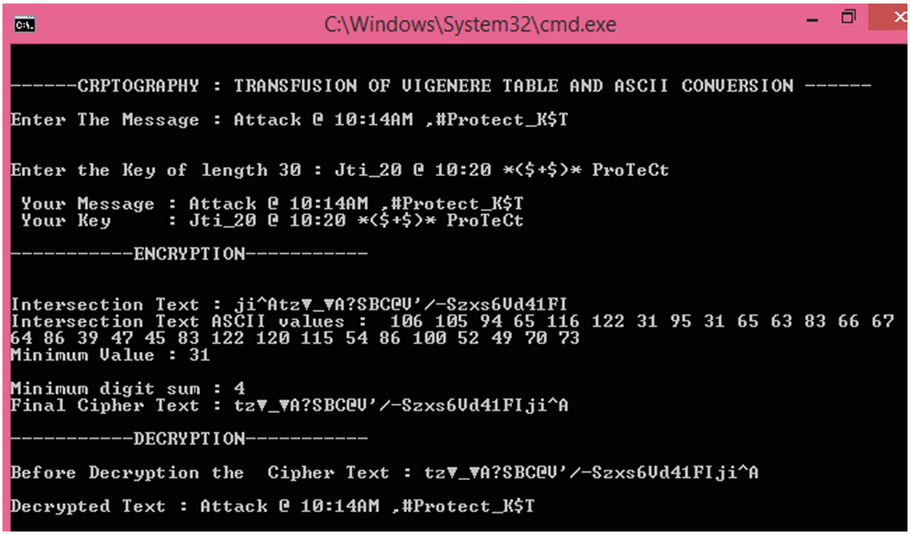
Input: Plain Text, Secret key. **Output**: Cipher Text

```
1.  Begin: Read the Plain Text.
2.  Generate a random Key equal to the length of Plain Text.
3.  Determine the Intersecting text(I.T) – each character
4.  Check the modified extended Vigenere table or
5.  Calculate using formula
        a.  I.T=Plain Input Text - 33+key
        b.  If (I.T > 126)
        c.  Then I.T = I.T - 94;
6.  Take rotate= Smallest ASCII value from all characters of the Intersection
    Text.
        a.  If (Rotate >9)
        b.  Then Rotate=sum of all digits of Rotate.
7.  Left Circular Shift the characters of Intersection text by the value of Rotate.
8.  Append the value of rotate at the beginning of Intersection Text = Intermediate Text.
9.  Final CIPHER TEXT = Intermediate Text.
10. End
```

Decryption:

```
1.  Begin: Take the cipher Text.
2.  Extract the rotate value from beginning of cipher text.
3.  Right Circular Shift the characters of the Cipher Text by the value of rotate.
4.  Find the Final Intersection Text (FIT)
    a)  FIT = Cipher Text +33 – key
    b)  If (FIT > = 126)
    c)  Then FIT = FIT -94;
    d)  If (FIT < = 33)
    e)  Then FIT = FIT+94;
5.  Convert the Final Intersection Text To Plain Text.
6.  End
```

The implementation of the above algorithm can be in any language of our choice. A sample output screen of the encryption and decryption is given below (Fig. 3).



```
------CRPTOGRAPHY : TRANSFUSION OF UIGENERE TABLE AND ASCII CONUERSION ------
Enter The Message : Attack @ 10:14AM ,#Protect_K$T

Enter the Key of length 30 : Jti_20 @ 10:20 *($+$)* ProTeCt
 Your Message : Attack @ 10:14AM ,#Protect_K$T
 Your Key     : Jti_20 @ 10:20 *($+$)* ProTeCt
-----------ENCRYPTION-----------

Intersection Text : ji^Atz▼_▼A?SBC@U'/-Szxs6Ud41FI
Intersection Text ASCII values :  106 105 94 65 116 122 31 95 31 65 63 83 66 67
64 86 39 47 45 83 122 120 115 54 86 100 52 49 70 73
Minimum Ualue : 31

Minimum digit sum : 4
Final Cipher Text : tz▼_▼A?SBC@U'/-Szxs6Ud41FIji^A
-----------DECRYPTION-----------
Before Decryption the  Cipher Text : tz▼_▼A?SBC@U'/-Szxs6Ud41FIji^A

Decrypted Text : Attack @ 10:14AM ,#Protect_K$T
```

Fig. 3. Complete execution of the proposed algorithm

5 Comparative Analysis

While comparing the various existing and proposed algorithm till now, it has been found that the proposed algorithm is greatly secured in context of, uniqueness, security and it is more efficient for every printable characters of the plain text message. The encrypted text [13] produced by this algorithm takes very less execution time which is very high in the other existing papers.

The algorithm of Saraswat takes into consideration of only alphabetical and numeric characters whereas the proposed model works for every type of characters alphanumeric and special characters. This provides a range of security for the data. The algorithm execution time of Mathur increases with the length of character exponentially, whereas in the presented algorithm the execution time never exceeds the size of the smallest ASCII value in the intersection text. The work of Gupta works efficiently for all types of characters but the number of steps taken in the encryption is high and complex, the presented algorithm makes the encryption simpler and secure. Here is a comparison between the existing algorithm and proposed algorithm based on their execution time (in milliseconds) and size of the plain text and it can be referred from the graph that the proposed algorithm works far better than the existing algorithm (Fig. 4).

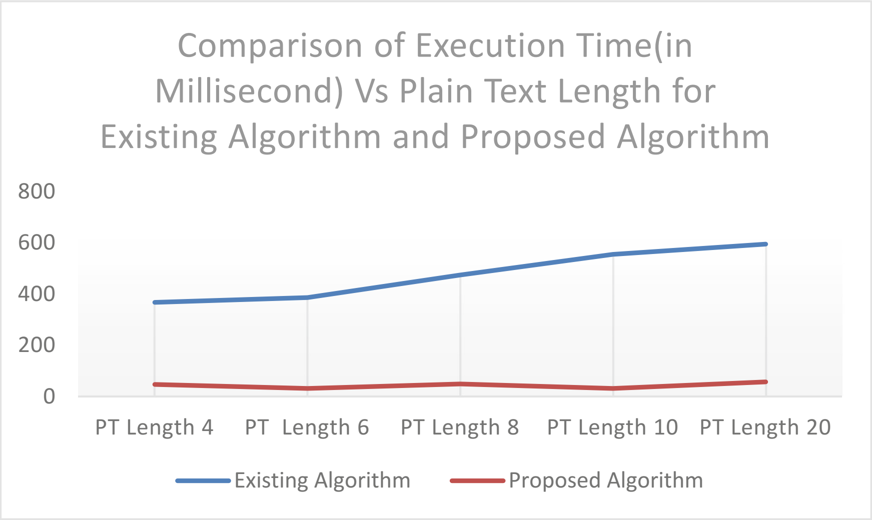


Fig. 4. Comparison graph of execution time (in Millisecond) vs plain text length for existing algorithm and proposed algorithm

6 Conclusion

In this research paper, we have introduced a more efficient and secure mechanism for the encryption of the plaint text. The algorithm addresses the major issue of security and privacy at the transmission phase of the data. The plain text throughout the process remains encrypted until the intended user provides the valid encryption key. From the previous section of the algorithm, we conclude that this new technique is robust and provides high level of security. The algorithm uses 4 steps to perform the encryption making it more secure. The range of characters that have been provided for encryption makes it tougher for cryptanalysis. Even the brute force attack will also take a large amount of time for decryption. The range of possibilities i.e. the 94 characters makes it tough to correctly reach to the plain text.

Even there are some limitations with the current system as the length of key and plain text must be same. The key security is also an issue. It's a belief that, this technique is a notable initiative towards the securing the data over network transmission. For future work our target would be to take a whole text file and then decrypt it with less time. Also to come up with more participation for data security of the cloud server such that we can secure the data storage over there.

References

1. Stallings, W.: Cryptography and Network Security Principles and Practice. Pearson Education Inc., Prentice Hall (2011)
2. Rivest, R.L.: Cryptography. In: Van Leeuwen, J. (ed.) Handbook of Theoretical Computer Science, vol. 1. Elsevier, Amsterdam (1990)
3. Justin, M.J., Manimurugan, S.: A survey on various encryption techniques. Int. J. Soft Comput. Eng. **2**(1), 429–432 (2012)
4. Shinghe, S.R., Patil, R.: An encryption algorithm based on ASCII value. Int. J. Comput. Sci. Inf. Technol. **5**(6), 7232–7234 (2014)
5. Sultana, R., Kamari, T.: An ASCII value based optimized text data encryption system. Int. J. Adv. Res. Electr. Electron. Instrum. Eng. **5**(8) (2016)
6. Sukhraliya, V., Chaudhary, S., Solanki, S.: Encryption and decryption algorithm using ASCII values with substitution array approach. Int. J. Adv. Res. Comput. Commun. Eng. **2** (8), 3094–3097 (2013)
7. Mathur, A.: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms. Int. J. Comput. Sci. Eng. **4**(9), 1650–1657 (2012)
8. Saraswat, A., Khatri, C., Sudhakar, Thakral, P., Biswas, P.: An Extended Hybridization of Vigenere and Caeser cipher techniques for secure communication. Procedia Comput. Sci. **92**, 355–360 (2016)
9. Krishna, Y.S.R.: Cryptographic algorithm based on ASCII conversions and a Radix function. Int. J. Sci. Eng. Res. **6**(11), 1191–1194 (2015)
10. Bhargava, U., Sharma, A., Chawla, R., Thakral, P.: A new algorithm combining substitution & transposition cipher techniques for secure communication. In: ICOEI Tamil Nadu, pp. 619–624 (2017)
11. Gupta, C., Thakral, P.: ASCII conversion based two keys V4S scheme for encryption and decryption-a four step approach. In: IEEE International Conference on Computing, Communication & Networking ICCCNT 2017, IIT Delhi, pp. 1–6 (2017)
12. Liwandouw, V., Wowor, A.: The existence of cryptography: a study on instant messaging. Procedia Comput. Sci. **124**, 721–727 (2017)
13. Joshi, A., Wazid, M., Goudar, R.H.: An efficient cryptographic scheme for text message protection against brute force & cryptanalytic attacks. Procedia Comput. Sci. **48**, 360–366 (2015)