International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.80 ISSN: 1308-5581 Vol 14, Issue 05 2022

CRYPTOGRAPHY WITH PENTAGONAL FUZZY NUMBER AND CIPHERS

S. Kavitha,
Department of Mathematics, VELS Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India.
kavithakavi.s1011@gmail.com.

K. Selvakumari
Department of Mathematics, VELS Institute of Science, Technology and Advanced Studies, Chennai, Tamilnadu, India.
Corresponding author: selvafeb6@gmail.com

Abstract: Cryptography is a more helpful to secure our data and transfer to right person. In social network it allows users to exchange messages and conversations, as well as videos, pictures, voice messages, audio and video calls, and storey updates in secure manner. This paper explores the secret conversion through pentagonal fuzzy number and ciphers.

Keyword: Cryptography, membership function, Vigenère cipher, Playfair cipher, fuzzy numbers.

1. Introduction

Lotfi A. Zadeh [1, 5, 11] publish the “Theory of fuzzy set” in the 1965. Author uses membership function [0, 1] and it applied based on human thinking and reasoning way. It has a quantitative meaning and is regarded as a set of fuzzy numbers [9]. A fuzzy number [16] is a quantity whose values are approximate rather than precise, as with a single-valued function. So far, membership functions have been introduced for fuzzy numbers such as triangular fuzzy numbers [7], trapezoidal fuzzy numbers [19], pyramid fuzzy numbers, pentagonal fuzzy numbers, etc. Non-linear equations, risk analysis, and reliability are just a few of the uses for these values. Many processes were carried out using fuzzy numbers [6]. Power engineering, chemical industry, robotics, image processing, factory automation, security, conditioners, electronics, washing machines, structures engineering, and pattern recognition are just a few of the industries where fuzzy is applied.

Everyone uses internet to send information to opponent. But the main problem occurs from the unknown person. If A and B communicate without security. Then the unknown person easily collects the information and send to B or convey a wrong message. To break this type of struggle we use cryptography to preserve our data. It encrypts the message and convert to cipher text (CT) with help of key. If key matches then the CT convert to original chat or else not. The CT uses letters, numbers, symbols or phrase. The cryptography has three types such as: [3, 15, 21, 23]

- Symmetric Key Cryptography

  It shares a message with same key for both encrypt and decrypt.

- Hash Function cryptography

  It cannot use any type of key but helps to convert a message to CT and it can't get back to normal text (NT). It takes an input of arbitrary length and outputs a fixed size value called hash value.

- Asymmetric Cryptography

  Most of the applications and software use this type for safe communication. It provides two keys for every user such as

  - Public key

    It helps to lock a sender message with the help of CT is called encrypt or encryption.

  - Private key

    It used to convert CT to NT is known as decrypt or decryption.

  If person A send message with encrypt, they lock with use of person B public key and person B decrypt with the help of person A private key. If the both public and private key matches then only the message encrypt otherwise not only shows a code of message. This is also called as end-to-end encryption or secret conversation. [13]

2. Preliminaries

2.1 Membership Function [17, 22]

Membership function (MF) is characterized by values from zero to one. Then encrypt linear membership function of $\tilde{C}$ is defined as

$$\tilde{C} = \{(x, \mu_{\tilde{C}}(x)); x \in X\}$$

and its mapping is $\tilde{C}: X \rightarrow [0,1]$ known as degree of MF of a fuzzy set where X = universe.

2.2 Fuzzy Number (FN) [1]

Let $\tilde{C}$ be a FN. Then it satisfies the below conditions:

- $\mu_{\tilde{C}}(x)$ is a piecewise condition
- Normalized fuzzy set
- It defined real number.

2.3 Pentagonal Fuzzy Number (PFN) [2]

A PFN of a fuzzy set $\tilde{C} = \{p, q, r, s, t\}$ and its membership function is

$$\mu_{\tilde{C}}(x) = \begin{cases} 0 & , \quad x < p \\ \frac{(x-p)}{(q-p)} & , \quad p \le x \le q \\ \frac{(x-q)}{(r-q)} & , \quad q \le x \le r \\ 1 & , \quad x = r \\ \frac{(s-x)}{(s-r)} & , \quad r \le x \le s \\ \frac{t-x}{(t-s)} & , \quad s \le x \le t \\ 0 & , \quad x > e \end{cases}$$

2.4 Average of PFN (APFN) [8]

Let $\tilde{C} = \{p, q, r, s, t\}$ will be PFN. Then average value is,

$$P(\tilde{C}) = \frac{p + q + r + s + t}{5}$$

2.5 Bounded Sum [9, 10]

Any two fuzzy sets $\tilde{\aleph}_1$ and $\tilde{\aleph}_2$. A *bounded sum* E = $\tilde{\aleph}_1 \oplus \tilde{\aleph}_2$ is denoted by $\mu_{\tilde{\aleph}_1 \oplus \tilde{\aleph}_2}(x)$

(i.e.) $\mu_{\tilde{\aleph}_1 \oplus \tilde{\aleph}_2}(x) = \min\{1, (\mu_{\tilde{\aleph}_1}(x) + \mu_{\tilde{\aleph}_2}(x))\}$ for all x ∈ X.

where $\mu_{\tilde{\aleph}_1}(x) + \mu_{\tilde{\aleph}_2}(x) \le 1$, $\mu_{\tilde{\aleph}_1}(x)$ = row values and $\mu_{\tilde{\aleph}_2}(x)$ = column values.

2.6 Modular Addition [13]

Let $\tilde{\aleph}$ be a fuzzy set. The fuzzy modular sum (mod) was used reduce the value of $\mu_{\tilde{\aleph}_1 \oplus \tilde{\aleph}_2}(x)$ only when the value is more than N then we divided by the value with N until it become less than N. Otherwise remains the same value.

(i.e.) $\mu_{\tilde{\aleph}}(x) = \mu_{\tilde{\aleph}_1 \oplus \tilde{\aleph}_2}(x) \bmod N$ for all x ∈ X.

where N = total number of letters.

2.7 Mobile screen keypad [12]

Every android mobile we can see the screen keypad which is visible when we touch the textbox otherwise not. So, the mobile can show full screen for other uses. In keypad buttons have many texts like small and capital alphabet letters, numbers, fractional numbers, symbols, latin letters, shift key (change lower letters and upper letters), space key (to leave space inbetween to words), enter (shift the text to next line), backspace (remove the wrong typed message) or delete or erase, go or send or done (it shows right side of text box to send a message), etc. Also, we can change the language of keypad which is comfortable to type, change the theme settings for keypad, stickers, variety of smileys (express how you feel), dictionary (help to text fast or correct words) and change font styles.

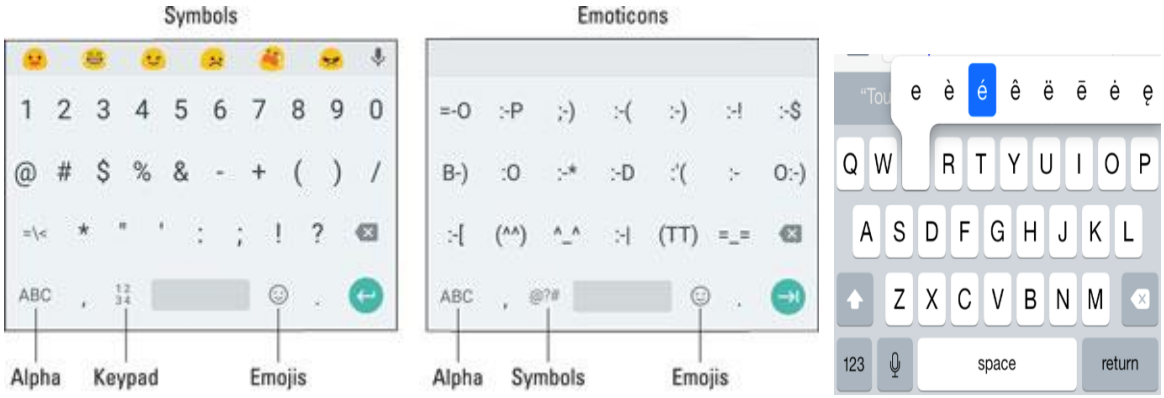

Figure 12. Onscreen Keypad

2.8 Vigenère cipher [4, 14]

It is a type of substitution cipher introduced by the French cryptographer Blaise de Vigenère at 16th century. Create a table and fix alphabetic letters for first row and column and next row we may do the little change like fix first letter to last and second letter came to first do this for complete table. Hereafter create a keyword and fix each letter to each plain text (PT) we need to send. Key is common for both encryption and decryption. Later check the encrypt letter for column and key for row then the intersection letter will be PT

For example,

Plain text : MIX

Key text : HIT

(i) We compare the compare M in column and H for row.

Then, the intersection letter is T.

(ii) I in column and row

Then, intersection letter is Q.

Similarly, we do for next finally we get decrypt is TQQ.

Then for decryption you can fix CT to key text (KT). Then, check KT row and find the CT where it can appear in the column then we get PT letter.

For example,

CT : TQQ

KT : HIT

Now we compare with table H row and find T place on row.

Then, we note the column letter straight the T is M.

Do it for other two letters.

Finally, we get normal text “MIX”.

	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

Figure 11. Vigenère cipher

2.10 Playfair Cipher [18, 20]

In 1854, Charles Wheatstone was invented the Playfair cipher. We encrypt and decrypt with pair of letters from PT or CT. Create a matrix table with equal number of row and column. First fill the KT and continue alphabet characters then neglect the repeated letters. Also, we have 26 letters in alphabet but table have only 25 cells. So, neglect a character like i/j.

Follow the below rules:

Rule 1: Divide the normal message like two characters and reject space. Suppose repeated character will be appeared continuously or last letter will be remain single. Then use X.

Rule 2: Find each character from the pair on table and take the intersection letter.

Rule 3: Suppose the pairing letters will be appear on same row or column. Then write the next letter.

For example:

Encryption:

HELLO, Key = MATH

Split: HE LX LO

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

First pair HE will be in different row and intersection letter will be FT, Next LX shows on same column. So, write the next letter on same column is RT.

PT	HE	LX	LO
CT	FT	RT	NI

Finally, CT is FTRTNI

Decryption

To get back the original text. We pair the CT and follow the above rules then get back the result.

Algorithm for Ciphers

Step 1: Our aim is to encode and decode the message by using PFN and cipher. First, we given the APFN for each character. These characters will be chosen by mobile keypad

Step 2: Develop the Vigenère cipher table by using the APFN and characters.

Step 3: If $\tilde{\aleph} < N$ then add 0.0002. Suppose $\tilde{\aleph} > N$ then divided with N. We taken equal number of rows and columns.

3. Numerical Example

We tabulate the letter by using mobile keypad and tag APFN values for each character from Definition 2.3 and 2.4.

A	B	C	D	E	F	G	H	I	J
0.0002	0.0006	0.0010	0.0014	0.0018	0.0022	0.0026	0.0030	0.0034	0.0038

K	L	M	N	O	P	Q	R	S	T
0.0042	0.0046	0.0050	0.0054	0.0058	0.0062	0.0066	0.0070	0.0074	0.0078

U	V	W	X	Y	Z	a	b	c	d
0.0082	0.0086	0.0090	0.0094	0.0098	0.0102	0.0106	0.0110	0.0114	0.0118

e	f	g	h	i	j	k	l	m	n
0.0122	0.0126	0.0130	0.0134	0.0138	0.0142	0.0146	0.0150	0.0154	0.0158

o	p	q	r	S	t	u	v	w	x
0.0162	0.0166	0.0170	0.0174	0.0178	0.0182	0.0186	0.0190	0.0194	0.0198

y	z	\	/	-	_	–	(	)	[
0.0202	0.0206	0.0210	0.0214	0.0218	0.0222	0.0226	0.0230	0.0234	0.0238

]	{	}	:	&	#	*	“	”	„
0.0242	0.0246	0.0250	0.0254	0.0258	0.0262	0.0266	0.0270	0.0274	0.0278

@	‘	’	,	!	?	;	.	+	$
0.0282	0.0286	0.0290	0.0294	0.0298	0.0302	0.0306	0.0310	0.0314	0.0318

<	>	%	⅍	⅌	℅	℆	=	≡	¿
0.0322	0.0326	0.0330	0.0334	0.0338	0.0342	0.0348	0.0350	0.0354	0.0358

~	∧	√	|	¦	§	○	●	…	₡
0.0362	0.0366	0.0370	0.0374	0.0378	0.0382	0.0386	0.0390	0.0394	0.0398

¢	¤	©	®	±	™	α	β	ɤ	Ω
0.0402	0.0406	0.0410	0.0414	0.0418	0.0422	0.0426	0.0430	0.0434	0.0438

÷	Δ	п	₹	∅	ø	Φ	0/∞	≈	≠
0.0442	0.0446	0.0450	0.0454	0.0458	0.0462	0.0466	0.0470	0.0474	0.0478

≤	≥	π	∑	×	≪	≫	♪	¶	★
0.0482	0.0486	0.0490	0.0494	0.0498	0.0502	0.0506	0.0510	0.0514	0.0518

☻	♣	♠	♦	♥	†	‡	‹	›	←
0.0522	0.0526	0.0530	0.534	0.538	0.0542	0.0546	0.0550	0.0554	0.0558

↑	↓	→	↔	↕	↨	∞	ą	å	ā
0.0562	0.0566	0.0570	0.0574	0.0578	0.0582	0.0586	0.0590	0.0594	0.0598

ä	*à*	*á*	*â*	*ã*	ç	č	ć	*ď*	đ
0.0602	0.0606	0.0610	0.0614	0.0618	0.0622	0.0626	0.0630	0.0634	0.0638

ë	ē	*é*	*è*	*ê*	į	ī	ì	ï	ł
0.0642	0.0646	0.0650	0.0654	0.0658	0.0662	0.0666	0.0670	0.0674	0.0678

ľ	Í	ń	ñ	ⁿ	ö	ō	õ	ó	ò
0.0682	0.0686	0.0690	0.0694	0.0698	0.0702	0.0706	0.0710	0.0714	0.0718

ž	ź	ż	œ	æ	€	¥	£	₦	₱
0.0722	0.0726	0.0730	0.0734	0.0738	0.0742	0.0746	0.0750	0.0754	0.0758

Æ	ß	ô	ŕ	ř	ś	š	ť	ū	ú

0.0762	0.0766	0.0770	0.0774	0.0778	0.0782	0.0786	0.0790	0.0794	0.0798

ù	û	ü	ÿ	Œ	Å	Ā	Ä	À	Â
0.0802	0.0806	0.0810	0.0814	0. 0818	0. 0822	0. 0826	0.0830	0.0834	0.0838

Á	Ã	Ą	Č	Ć	Ç	Ď	Đ	Ë	È
0.0842	0.0846	0.0850	0.0854	0.0858	0.0862	0.0866	0.0870	0.0874	0.0878

É	Ê	Ē	Ė	Ę	Í	Î	Ï	Į	Ī
0.0882	0.0886	0.0890	0.0894	0.0898	0.0902	0.0906	0.0910	0.0914	0.0918

Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö
0.0922	0.0926	0.0930	0.0934	0.0938	0.0942	0.0946	0.0950	0.0954	0.0958

Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù
0.0962	0.0966	0.0970	0.0974	0.0978	0.0982	0.0986	0.0990	0.0994	0.0998

Ú	Ü	Ÿ	Ź	Ż	Ž	0	⅔	1	¹
0.1002	0.1006	0.1010	0.1014	0.1018	0.1022	0.1026	0.1030	0.1034	0.1038

½	⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒	2
0.1042	0.1046	0.1050	0.1054	0.1058	0.1062	0.1066	0.1070	0.1074	0.1078

²	⅔	⅖	3	³	¾	⅗	⅜	4	⁴
0.1082	0.1086	0.1090	0.1094	0.1098	0.1102	0.1106	0.1110	0.1114	0.1118

⅘	5	⅚	⅝	6	7	⅞	8	9
0.1122	0.1126	0.1130	0.1134	0.1138	0.1142	0.1146	0.1150	0.1154

Table 1. Mobile keypad letters with pentagonal fuzzy numbers

Using the Definition 2.6 to fill table 1. If $\tilde{\aleph} < N$ then add 0.0002. Suppose $\tilde{\aleph} > N$ then divided with N where $N = 0.1154$. Here we taken equal number of rows and columns. Then create a Vigenère cipher table.

$\tilde{\aleph}$	A	B	C	D	E	F	G	H	I	J	K	L	….	9
A	B	C	D	E	F	G	H	I	J	K	L	M		A
B	C	D	E	F	G	H	I	J	K	L	M	N		B
C	D	E	F	G	H	I	J	K	L	M	N	O		C
D	E	F	G	H	I	J	K	L	M	N	O	P		D
E	F	G	H	I	J	K	L	M	N	O	P	Q		E
F	G	H	I	J	K	L	M	N	O	P	Q	R		F
G	H	I	J	K	L	M	N	O	P	Q	R	S		G
H	I	J	K	L	M	N	O	P	Q	R	S	T		H
I	J	K	L	M	N	O	P	Q	R	S	T	U		I
J	K	L	M	N	O	P	Q	R	S	T	U	V		J
K	L	M	N	O	P	Q	R	S	T	U	V	W		K

L	M	N	O	P	Q	R	S	T	U	V	W	X		L
M	N	O	P	Q	R	S	T	U	V	W	X	Y		M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z		N
O	P	Q	R	S	T	U	V	W	X	Y	Z	a		O
P	Q	R	S	T	U	V	W	X	Y	Z	a	b		P
Q	R	S	T	U	V	W	X	Y	Z	a	b	c		Q
R	S	T	U	V	W	X	Y	Z	a	b	c	d		R
S	T	U	V	W	X	Y	Z	a	b	c	d	e		S
T	U	V	W	X	Y	Z	a	b	c	d	e	f		T
U	V	W	X	Y	Z	a	b	c	d	e	f	g		U
V	W	X	Y	Z	a	b	c	d	e	f	g	h		V
W	X	Y	Z	a	b	c	d	e	f	g	h	i		W
X	Y	Z	a	b	c	d	e	f	g	h	i	j		X
Y	Z	a	b	c	d	e	f	g	h	i	j	k		Y
Z	a	b	c	d	e	f	g	h	i	j	k	l		Z
a	b	c	d	e	f	g	h	i	j	k	l	m		a
b	c	d	e	f	g	h	i	j	k	l	m	n		b
c	d	e	f	g	h	i	j	k	l	m	n	o		c
d	e	f	g	h	i	j	k	l	m	n	o	p		d
e	f	g	h	i	j	k	l	m	n	o	p	q		e
f	g	h	i	j	k	l	m	n	o	p	q	r		f
g	h	i	j	k	l	m	n	o	p	q	r	s		g
h	i	j	k	l	m	n	o	p	q	r	s	t		h
i	j	k	l	m	n	o	p	q	r	s	t	u		i
j	k	l	m	n	o	p	q	r	s	t	u	v		j
k	l	m	n	o	p	q	r	s	t	u	v	w		k
l	m	n	o	p	q	r	s	t	u	v	w	x		l
m	n	o	p	q	r	s	t	u	v	w	x	y		m
n	o	p	q	r	s	t	u	v	w	x	y	z		n
o	p	q	r	s	t	u	v	w	x	y	z	\		o
p	q	r	s	t	u	v	w	x	y	z	\	/		p
q	r	s	t	u	v	w	x	y	z	\	/	-		q
r	s	t	u	v	w	x	y	z	\	/	-	_		r
s	t	u	v	w	x	y	z	\	/	-	_	–		s
t	u	v	w	x	y	z	\	/	-	_	–	(		t
u	v	w	x	y	z	\	/	-	_	–	(	)		u
v	w	x	y	z	\	/	-	_	–	(	)	[		v
w	x	y	z	\	/	-	_	–	(	)	[	]		w
x	y	z	\	/	-	_	–	(	)	[	]	{		x
y	z	\	/	-	_	–	(	)	[	]	{	}		y
z	\	/	-	_	–	(	)	[	]	{	}	:		z
\	/	-	_	–	(	)	[	]	{	}	:	&		\
/	-	_	–	(	)	[	]	{	}	:	&	#		/
-	_	–	(	)	[	]	{	}	:	&	#	*		-
_	–	(	)	[	]	{	}	:	&	#	*	“		_
–	(	)	[	]	{	}	:	&	#	*	“	”		–
(	)	[	]	{	}	:	&	#	*	“	”	„		(
)	[	]	{	}	:	&	#	*	“	”	„	@		)

[	]	{	}	:	&	#	*	“	”	„	@	‘		[
]	{	}	:	&	#	*	“	”	„	@	‘	’		]
{	}	:	&	#	*	“	”	„	@	‘	’	,		{
}	:	&	#	*	“	”	„	@	‘	’	,	!		}
:	&	#	*	“	”	„	@	‘	’	,	!	?		:
&	#	*	“	”	„	@	‘	’	,	!	?	;		&
#	*	“	”	„	@	‘	’	,	!	?	;	.		#
*	“	”	„	@	‘	’	,	!	?	;	.	+		*
“	”	„	@	‘	’	,	!	?	;	.	+	$		“
”	„	@	‘	’	,	!	?	;	.	+	$	<		”
„	@	‘	’	,	!	?	;	.	+	$	<	>		„
@	‘	’	,	!	?	;	.	+	$	<	>	%		@
‘	’	,	!	?	;	.	+	$	<	>	%	⅍		‘
’	,	!	?	;	.	+	$	<	>	%	⅍	⅋		’
,	!	?	;	.	+	$	<	>	%	⅍	⅋	℅		,
!	?	;	.	+	$	<	>	%	⅍	⅋	℅	℆		!
?	;	.	+	$	<	>	%	⅍	⅋	℅	℆	=		?
;	.	+	$	<	>	%	⅍	⅋	℅	℆	=	≡		;
.	+	$	<	>	%	⅍	⅋	℅	℆	=	≡	¿		.
+	$	<	>	%	⅍	⅋	℅	℆	=	≡	¿	~		+
$	<	>	%	⅍	⅋	℅	℆	=	≡	¿	~	∧		$
<	>	%	⅍	⅋	℅	℆	=	≡	¿	~	∧	√		<
>	%	⅍	⅋	℅	℆	=	≡	¿	~	∧	√	|		>
%	⅍	⅋	℅	℆	=	≡	¿	~	∧	√	|	¦		%
⅍	⅋	℅	℆	=	≡	¿	~	∧	√	|	¦	§		⅍
⅋	℅	℆	=	≡	¿	~	∧	√	|	¦	§	○		⅋
℅	℆	=	≡	¿	~	∧	√	|	¦	§	○	●		℅
℆	=	≡	¿	~	∧	√	|	¦	§	○	●	…		℆
=	≡	¿	~	∧	√	|	¦	§	○	●	…	ℂ		=
≡	¿	~	∧	√	|	¦	§	○	●	…	ℂ	¢		≡
¿	~	∧	√	|	¦	§	○	●	…	ℂ	¢	¤		¿
~	∧	√	|	¦	§	○	●	…	ℂ	¢	¤	©		~
∧	√	|	¦	§	○	●	…	ℂ	¢	¤	©	®		∧
√	|	¦	§	○	●	…	ℂ	¢	¤	©	®	±		√
|	¦	§	○	●	…	ℂ	¢	¤	©	®	±	™		|
¦	§	○	●	…	ℂ	¢	¤	©	®	±	™	α		¦
§	○	●	…	ℂ	¢	¤	©	®	±	™	α	β		§
○	●	…	ℂ	¢	¤	©	®	±	™	α	β	ɤ		○
●	…	ℂ	¢	¤	©	®	±	™	α	β	ɤ	Ω		●
…	ℂ	¢	¤	©	®	±	™	α	β	ɤ	Ω	÷		…
ℂ	¢	¤	©	®	±	™	α	β	ɤ	Ω	÷	Δ		ℂ
¢	¤	©	®	±	™	α	β	ɤ	Ω	÷	Δ	π		¢
¤	©	®	±	™	α	β	ɤ	Ω	÷	Δ	π	₹		¤
©	®	±	™	α	β	ɤ	Ω	÷	Δ	π	₹	∅		©
®	±	™	α	β	ɤ	Ω	÷	Δ	π	₹	∅	ø		®
±	™	α	β	ɤ	Ω	÷	Δ	π	₹	∅	ø	Φ		±
™	α	β	ɤ	Ω	÷	Δ	π	₹	∅	ø	Φ	0/∞		™
α	β	ɤ	Ω	÷	Δ	π	₹	∅	ø	Φ	0/∞	≈		α

β	ɤ	Ω	÷	∆	π	₹	∅	ø	Φ	0/∞	≈	≠		β
ɤ	Ω	÷	∆	π	₹	∅	ø	Φ	0/∞	≈	≠	≤		ɤ
Ω	÷	∆	π	₹	∅	ø	Φ	0/∞	≈	≠	≤	≥		Ω
÷	∆	π	₹	∅	ø	Φ	0/∞	≈	≠	≤	≥	π		÷
∆	π	₹	∅	ø	Φ	0/∞	≈	≠	≤	≥	π	∑		∆
π	₹	∅	ø	Φ	0/∞	≈	≠	≤	≥	π	∑	×		π
₹	∅	ø	Φ	0/∞	≈	≠	≤	≥	π	∑	×	≪		₹
∅	ø	Φ	0/∞	≈	≠	≤	≥	π	∑	×	≪	≫		∅
ø	Φ	0/∞	≈	≠	≤	≥	π	∑	×	≪	≫	♪		ø
Φ	0/∞	≈	≠	≤	≥	π	∑	×	≪	≫	♪	¶		Φ
0/∞	≈	≠	≤	≥	π	∑	×	≪	≫	♪	¶	★		0/∞
≈	≠	≤	≥	π	∑	×	≪	≫	♪	¶	★	☻		≈
≠	≤	≥	π	∑	×	≪	≫	♪	¶	★	☻	♣		≠
≤	≥	π	∑	×	≪	≫	♪	¶	★	☻	♣	♠		≤
≥	π	∑	×	≪	≫	♪	¶	★	☻	♣	♠	♦		≥
π	∑	×	≪	≫	♪	¶	★	☻	♣	♠	♦	♥		π
∑	×	≪	≫	♪	¶	★	☻	♣	♠	♦	♥	†		∑
×	≪	≫	♪	¶	★	☻	♣	♠	♦	♥	†	‡		×
≪	≫	♪	¶	★	☻	♣	♠	♦	♥	†	‡	‹		≪
≫	♪	¶	★	☻	♣	♠	♦	♥	†	‡	‹	›		≫
♪	¶	★	☻	♣	♠	♦	♥	†	‡	‹	›	←		♪
¶	★	☻	♣	♠	♦	♥	†	‡	‹	›	←	↑		¶
★	☻	♣	♠	♦	♥	†	‡	‹	›	←	↑	↓		★
☻	♣	♠	♦	♥	†	‡	‹	›	←	↑	↓	→		☻
♣	♠	♦	♥	†	‡	‹	›	←	↑	↓	→	↔		♣
♠	♦	♥	†	‡	‹	›	←	↑	↓	→	↔	↕		♠
♦	♥	†	‡	‹	›	←	↑	↓	→	↔	↕	↕		♦
♥	†	‡	‹	›	←	↑	↓	→	↔	↕	↕	∞		♥
†	‡	‹	›	←	↑	↓	→	↔	↕	↕	∞	ą		†
‡	‹	›	←	↑	↓	→	↔	↕	↕	∞	ą	å		‡
‹	›	←	↑	↓	→	↔	↕	↕	∞	ą	å	ā		‹
›	←	↑	↓	→	↔	↕	↕	∞	ą	å	ā	ä		›
←	↑	↓	→	↔	↕	↕	∞	ą	å	ā	ä	à		←
↑	↓	→	↔	↕	↕	∞	ą	å	ā	ä	à	á		↑
↓	→	↔	↕	↕	∞	ą	å	ā	ä	à	á	â		↓
→	↔	↕	↕	∞	ą	å	ā	ä	à	á	â	ã		→
↔	↕	↕	∞	ą	å	ā	ä	à	á	â	ã	ç		↔
↕	↕	∞	ą	å	ā	ä	à	á	â	ã	ç	č		↕
↕	∞	ą	å	ā	ä	à	á	â	ã	ç	č	ć		↕
∞	ą	å	ā	ä	à	á	â	ã	ç	č	ć	ɗ		∞
ą	å	ā	ä	à	á	â	ã	ç	č	ć	ɗ	đ		ą
å	ā	ä	à	á	â	ã	ç	č	ć	ɗ	đ	ë		å
ā	ä	à	á	â	ã	ç	č	ć	ɗ	đ	ë	ē		ā
ä	à	á	â	ã	ç	č	ć	ɗ	đ	ë	ē	é		ä
à	á	â	ã	ç	č	ć	ɗ	đ	ë	ē	é	è		à

DOI:10.9756/INTJECSE/V14I5.80 ISSN: 1308-5581 Vol 14, Issue 05 2022

á	â	ã	ç	č	ć	ď	đ	ë	ē	é	è	ê		á
â	ã	ç	č	ć	ď	đ	ë	ē	é	è	ê	į		â
ã	ç	č	ć	ď	đ	ë	ē	é	è	ê	į	ī		ã
ç	č	ć	ď	đ	ë	ē	é	è	ê	į	ī	ì		ç
č	ć	ď	đ	ë	ē	é	è	ê	į	ī	ì	ï		č
ć	ď	đ	ë	ē	é	è	ê	į	ī	ì	ï	ł		ć
ď	đ	ë	ē	é	è	ê	į	ī	ì	ï	ł	ľ		ď
đ	ë	ē	é	è	ê	į	ī	ì	ï	ł	ľ	Í		đ
ë	ē	é	è	ê	į	ī	ì	ï	ł	ľ	Í	ń		ë
ē	é	è	ê	į	ī	ì	ï	ł	ľ	Í	ń	ñ		ē
é	è	ê	į	ī	ì	ï	ł	ľ	Í	ń	ñ	ⁿ		é
è	ê	į	ī	ì	ï	ł	ľ	Í	ń	ñ	ⁿ	ö		è
ê	į	ī	ì	ï	ł	ľ	Í	ń	ñ	ⁿ	ö	ō		ê
į	ī	ì	ï	ł	ľ	Í	ń	ñ	ⁿ	ö	ō	õ		į
ī	ì	ï	ł	ľ	Í	ń	ñ	ⁿ	ö	ō	õ	ó		ī
ì	ï	ł	ľ	Í	ń	ñ	ⁿ	ö	ō	õ	ó	ò		ì
ï	ł	ľ	Í	ń	ñ	ⁿ	ö	ō	õ	ó	ò	ô		ï
ł	ľ	Í	ń	ñ	ⁿ	ö	ō	õ	ó	ò	ô	ŕ		ł
ľ	Í	ń	ñ	ⁿ	ö	ō	õ	ó	ò	ô	ŕ	ř		ľ
Í	ń	ñ	ⁿ	ö	ō	õ	ó	ò	ô	ŕ	ř	ś		Í
ń	ñ	ⁿ	ö	ō	õ	ó	ò	ô	ŕ	ř	ś	š		ń
ñ	ⁿ	ö	ō	õ	ó	ò	ô	ŕ	ř	ś	š	ť		ñ
ⁿ	ö	ō	õ	ó	ò	ô	ŕ	ř	ś	š	ť	ū		ⁿ
ö	ō	õ	ó	ò	ô	ŕ	ř	ś	š	ť	ū	ú		ö
ō	õ	ó	ò	ô	ŕ	ř	ś	š	ť	ū	ú	ù		ō
õ	ó	ò	ô	ŕ	ř	ś	š	ť	ū	ú	ù	û		õ
ó	ò	ô	ŕ	ř	ś	š	ť	ū	ú	ù	û	ü		ó
ò	ô	ŕ	ř	ś	š	ť	ū	ú	ù	û	ü	ÿ		ò
ô	ŕ	ř	ś	š	ť	ū	ú	ù	û	ü	ÿ	ž		ô
ŕ	ř	ś	š	ť	ū	ú	ù	û	ü	ÿ	ž	ź		ŕ
ř	ś	š	ť	ū	ú	ù	û	ü	ÿ	ž	ź	ż		ř
ś	š	ť	ū	ú	ù	û	ü	ÿ	ž	ź	ż	œ		ś
š	ť	ū	ú	ù	û	ü	ÿ	ž	ź	ż	œ	æ		š
ť	ū	ú	ù	û	ü	ÿ	ž	ź	ż	œ	æ	€		ť
ū	ú	ù	û	ü	ÿ	ž	ź	ż	œ	æ	€	¥		ū
ú	ù	û	ü	ÿ	ž	ź	ż	œ	æ	€	¥	£		ú
ù	û	ü	ÿ	ž	ź	ż	œ	æ	€	¥	£	₦		ù
û	ü	ÿ	ž	ź	ż	œ	æ	€	¥	£	₦	₱		û
ü	ÿ	ž	ź	ż	œ	æ	€	¥	£	₦	₱	Æ		ü
ÿ	ž	ź	ż	œ	æ	€	¥	£	₦	₱	Æ	ß		ÿ
ž	ź	ż	œ	æ	€	¥	£	₦	₱	Æ	ß	Œ		ž
ź	ż	œ	æ	€	¥	£	₦	₱	Æ	ß	Œ	Å		ź
ż	œ	æ	€	¥	£	₦	₱	Æ	ß	Œ	Å	Ā		ż
œ	æ	€	¥	£	₦	₱	Æ	ß	Œ	Å	Ā	Ä		œ
æ	€	¥	£	₦	₱	Æ	ß	Œ	Å	Ā	Ä	À		æ
€	¥	£	₦	₱	Æ	ß	Œ	Å	Ā	Ä	À	Â		€
¥	£	₦	₱	Æ	ß	Œ	Å	Ā	Ä	À	Â	Á		¥

DOI:10.9756/INTJECSE/V14I5.80 ISSN: 1308-5581 Vol 14, Issue 05 2022

£	₦	₱	Æ	ß	Œ	Å	Ā	Ä	À	Â	Á	Ã		£
₦	₱	Æ	ß	Œ	Å	Ā	Ä	À	Â	Á	Ã	Ą		₦
₱	Æ	ß	Œ	Å	Ā	Ä	À	Â	Á	Ã	Ą	Č		₱
Æ	ß	Œ	Å	Ā	Ä	À	Â	Á	Ã	Ą	Č	Ć		Æ
ß	Œ	Å	Ā	Ä	À	Â	Á	Ã	Ą	Č	Ć	Ç		ß
Œ	Å	Ā	Ä	À	Â	Á	Ã	Ą	Č	Ć	Ç	Ď		Œ
Å	Ā	Ä	À	Â	Á	Ã	Ą	Č	Ć	Ç	Ď	Đ		Å
Ā	Ä	À	Â	Á	Ã	Ą	Č	Ć	Ç	Ď	Đ	Ë		Ā
Ä	À	Â	Á	Ã	Ą	Č	Ć	Ç	Ď	Đ	Ë	È		Ä
À	Â	Á	Ã	Ą	Č	Ć	Ç	Ď	Đ	Ë	È	É		À
Â	Á	Ã	Ą	Č	Ć	Ç	Ď	Đ	Ë	È	É	Ê		Â
Á	Ã	Ą	Č	Ć	Ç	Ď	Đ	Ë	È	É	Ê	Ē		Á
Ã	Ą	Č	Ć	Ç	Ď	Đ	Ë	È	É	Ê	Ē	Ė		Ã
Ą	Č	Ć	Ç	Ď	Đ	Ë	È	É	Ê	Ē	Ė	Ę		Ą
Č	Ć	Ç	Ď	Đ	Ë	È	É	Ê	Ē	Ė	Ę	Í		Č
Ć	Ç	Ď	Đ	Ë	È	É	Ê	Ē	Ė	Ę	Í	Î		Ć
Ç	Ď	Đ	Ë	È	É	Ê	Ē	Ė	Ę	Í	Î	Ï		Ç
Ď	Đ	Ë	È	É	Ê	Ē	Ė	Ę	Í	Î	Ï	Į		Ď
Đ	Ë	È	É	Ê	Ē	Ė	Ę	Í	Î	Ï	Į	Ī		Đ
Ë	È	É	Ê	Ē	Ė	Ę	Í	Î	Ï	Į	Ī	Ì		Ë
È	É	Ê	Ē	Ė	Ę	Í	Î	Ï	Į	Ī	Ì	Ľ		È
É	Ê	Ē	Ė	Ę	Í	Î	Ï	Į	Ī	Ì	Ľ	Ł		É
Ê	Ē	Ė	Ę	Í	Î	Ï	Į	Ī	Ì	Ľ	Ł	Ĺ		Ê
Ē	Ė	Ę	Í	Î	Ï	Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ		Ē
Ė	Ę	Í	Î	Ï	Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń		Ė
Ę	Í	Î	Ï	Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò		Ę
Í	Î	Ï	Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó		Í
Î	Ï	Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô		Î
Ï	Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö		Ï
Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö	Õ		Į
Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö	Õ	Ō		Ī
Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö	Õ	Ō	Ŕ		Ì
Ľ	Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö	Õ	Ō	Ŕ	Ř		Ľ
Ł	Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö	Õ	Ō	Ŕ	Ř	Ś		Ł
Ĺ	Ñ	Ń	Ò	Ó	Ô	Ö	Õ	Ō	Ŕ	Ř	Ś	Š		Ĺ
Ñ	Ń	Ò	Ó	Ô	Ö	Õ	Ō	Ŕ	Ř	Ś	Š	Ť		Ñ
Ń	Ò	Ó	Ô	Ö	Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū		Ń
Ò	Ó	Ô	Ö	Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û		Ò
Ó	Ô	Ö	Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù		Ó
Ô	Ö	Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù	Ú		Ô
Ö	Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù	Ú	Ü		Ö
Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù	Ú	Ü	Ÿ		Õ
Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù	Ú	Ü	Ÿ	Ź		Ō
Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù	Ú	Ü	Ÿ	Ź	Ż		Ŕ
Ř	Ś	Š	Ť	Ū	Û	Ù	Ú	Ü	Ÿ	Ź	Ż	Ž		Ř
Ś	Š	Ť	Ū	Û	Ù	Ú	Ü	Ÿ	Ź	Ż	Ž	0		Ś
Š	Ť	Ū	Û	Ù	Ú	Ü	Ÿ	Ź	Ż	Ž	0	⅔		Š

Ť	Ũ	Û	Ù	Ú	Ü	Ÿ	Ź	Ż	Ž	0	⅔	1		Ť
Ũ	Û	Ù	Ú	Ü	Ÿ	Ź	Ż	Ž	0	⅔	1	1		Ũ
Û	Ù	Ú	Ü	Ÿ	Ź	Ż	Ž	0	⅔	1	1	½		Û
Ù	Ú	Ü	Ÿ	Ź	Ż	Ž	0	⅔	1	1	½	⅓		Ù
Ú	Ü	Ÿ	Ź	Ż	Ž	0	⅔	1	1	½	⅓	¼		Ú
Ü	Ÿ	Ź	Ż	Ž	0	⅔	1	1	½	⅓	¼	⅕		Ü
Ÿ	Ź	Ż	Ž	0	⅔	1	1	½	⅓	¼	⅕	⅙		Ÿ
Ź	Ż	Ž	0	⅔	1	1	½	⅓	¼	⅕	⅙	⅐		Ź
Ż	Ž	0	⅔	1	1	½	⅓	¼	⅕	⅙	⅐	⅛		Ż
Ž	0	⅔	1	1	½	⅓	¼	⅕	⅙	⅐	⅛	⅑		Ž
0	⅔	1	1	½	⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒		0
⅔	1	1	½	⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒	2		⅔
1	1	½	⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒	2	2		1
1	½	⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒	2	2	⅔		1
½	⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒	2	2	⅔	⅖		½
⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒	2	2	⅔	⅖	3		⅓
¼	⅕	⅙	⅐	⅛	⅑	⅒	2	2	⅔	⅖	3	3		¼
⅕	⅙	⅐	⅛	⅑	⅒	2	2	⅔	⅖	3	3	¾		⅕
⅙	⅐	⅛	⅑	⅒	2	2	⅔	⅖	3	3	¾	⅗		⅙
⅐	⅛	⅑	⅒	2	2	⅔	⅖	3	3	¾	⅗	⅜		⅐
⅛	⅑	⅒	2	2	⅔	⅖	3	3	¾	⅗	⅜	4		⅛
⅑	⅒	2	2	⅔	⅖	3	3	¾	⅗	⅜	4	4		⅑
⅒	2	2	⅔	⅖	3	3	¾	⅗	⅜	4	4	⅘		⅒
2	2	⅔	⅖	3	3	¾	⅗	⅜	4	4	⅘	5		2
2	⅔	⅖	3	3	¾	⅗	⅜	4	4	⅘	5	⅚		2
⅔	⅖	3	3	¾	⅗	⅜	4	4	⅘	5	⅚	⅝		⅔
⅖	3	3	¾	⅗	⅜	4	4	⅘	5	⅚	⅝	6		⅖
3	3	¾	⅗	⅜	4	4	⅘	5	⅚	⅝	6	7		3
3	¾	⅗	⅜	4	4	⅘	5	⅚	⅝	6	7	⅞		3
¾	⅗	⅜	4	4	⅘	5	⅚	⅝	6	7	⅞	8		¾
⅗	⅜	4	4	⅘	5	⅚	⅝	6	7	⅞	8	9		⅗
⅜	4	4	⅘	5	⅚	⅝	6	7	⅞	8	9	A		⅜
4	4	⅘	5	⅚	⅝	6	7	⅞	8	9	A	B		4
4	⅘	5	⅚	⅝	6	7	⅞	8	9	A	B	C		4
⅘	5	⅚	⅝	6	7	⅞	8	9	A	B	C	D		⅘
5	⅚	⅝	6	7	⅞	8	9	A	B	C	D	E		5
⅚	⅝	6	7	⅞	8	9	A	B	C	D	E	F		⅚
⅝	6	7	⅞	8	9	A	B	C	D	E	F	G		⅝
6	7	⅞	8	9	A	B	C	D	E	F	G	H		6
7	⅞	8	9	A	B	C	D	E	F	G	H	I		7
⅞	8	9	A	B	C	D	E	F	G	H	I	J		⅞
8	9	A	B	C	D	E	F	G	H	I	J	K		8
9	A	B	C	D	E	F	G	H	I	J	K	L		9

Table 2. 289 x 289 matrix Vigenère cipher table

We did same for other rows and columns. Now I send the message to my friend via Facebook messenger. The message will be

"Everyday is a 2nd change"

We create a keyword is Miɤ*â*Ç1€.

Encryption

We may fix each letter KT to a PT and repeated KT until reached the end of message. Compare these with table 2, PT for row and key for column then take intersection letter for CT.

PT	E	v	e	r	y	d	a	y		i	s		a	
KT	M	i	ɤ	*â*	Ç	1	€	M		i	ɤ		*â*	
CT1	R	%	←	€	⅛	9	Ę	:		„	*â*		ô	

2	n	d		c	h	a	n	g	e
Ç	1	€		M	i	ɤ	*â*	Ç	1
ś	J	Ï		p	”	†	ź	Û	A

CT1:

R%←€⅛9Ę: „*â* ô śJÏ p”†źÛA

Next create a Playfair cipher table with keypad,

M	i	ɤ	*â*	Ç	1	€	A	B	C	D	E	F	G	H	I	J
K	L	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	a	b
c	d	e	f	g	h	J	k	l	m	n	o	p	q	r	s	t
u	v	w	x	y	z	\	/	-	_	–	(	)	[	]	{	}
:	&	#	*	“	”	„	@	‘	’	,	!	?	;	.	+	$
<	>	%	ª⁄c	ª⁄s	℅u	℅	=	≡	¿	~	∧	√	|	¦	§	○
●	…	ℂ	¢	¤	©	®	±	™	α	β	Ω	÷	Δ	π	₹	∅
ø	Φ	0/∞	≈	≠	≤	≥	*π*	∑	×	≪	≫	♪	¶	★	☻	♣
♠	♦	♥	†	‡	‹	›	←	↑	↓	→	↔	↕	↨	∞	ą	å
ā	*ä*	*à*	*á*	*ã*	ç	č	ć	*d́*	đ	*ë*	ē	*é*	*è*	*ê*	į	ī
ì	ï	ł	ľ	Í	ń	ñ	ⁿ	ö	ō	õ	ó	ò	ô	ŕ	ř	ś
š	ť	ū	ú	ù	û	ü	ÿ	ž	ź	ż	œ	æ	¥	£	₦	₱
Æ	ß	Œ	Å	Ā	Ä	À	Â	Á	Ã	Ą	Č	Ć	Ď	Đ	Ë	È
É	Ê	Ē	Ė	Ę	Í	Î	Ï	Į	Ī	Ì	Ľ	Ł	Ĺ	Ñ	Ń	Ò
Ó	Ô	Ö	Õ	Ō	Ŕ	Ř	Ś	Š	Ť	Ū	Û	Ù	Ú	Ü	Ÿ	Ź
Ż	Ž	0	⅔	¹	½	⅓	¼	⅕	⅙	⅐	⅛	⅑	⅒	2	²	⅔
⅖	3	³	¾	⅗	⅜	4	⁴	⅘	5	⅚	⅝	6	7	⅞	8	9

Table 3. Playfair Cipher

Now split before code like two characters,

R% ←€ ⅛9 Ę: „*â* ôś JÏ p” †ź ÛA

Follow the rule from 2.5 and intersect the characters. Finally, CT is

%NA›⅝⅔É“ €* ŕ ìÒA ?hú↓EŚ

Decryption

We may reverse the process with help of KT. Divide the CT like two characters and compare with table 3, we get CT1

R%←€⅛9Ę: „â ô śJÏ p”†źÛA

Fix a CT1 with KT. Hereafter, compare with table 2 like KT for row and analyse a CT on same row and find which column it would be appear. That column letter will be PT.

CT1	R	%	←	€	⅛	9	Ę	:		„	â		ô	
KT	M	i	ɤ	â	Ç	1	€	M		i	ɤ		â	
PT	E	v	e	r	y	d	a	y		i	s		a	

We done for all the characters then get back the original message

“Everyday is a 2nd change”

Conclusion

Everyone communicates via online chat and done work in short time. Cryptography plays a critical part in keeping our various chats safe and ensuring that we contact the proper person in a matter of seconds. In this paper, we use fuzzy modulo for secure communication with the help of Vigenère and Playfair ciphers. Other sorts of fuzzy definitions, such as bounded difference, bounded product, union, intersection, and so on, also can be used to make secret chats.

References

1. A. Kaufmann, “*Introduction to the Theory of Fuzzy Subsets*”, United Kingdom Edition, Academic Press, Inc, London, 1973.
2. A. Kumar, S. Indrni, “An Application of Pentagonal Fuzzy Number Matrix in Decision Making”, International Journal of Engineering and Management Research, vol. 7, Issue. 3, pp. 527-531.
3. A.M. Richard, “*An Introduction to Cryptography*”, CRC Taylor & Francis Group, London, New York, 2007.
4. D. Bhatia, M. Dave, “Elliptic Curve Layered: A Secure Polyalphabetic Vigenère Cryptographic Algorithm for Textual Data”, *Journal of Scientific Research,* vol. 65, no. 1, pp. 222-229, 2021.

5. D. Dubois, H. Prade, "Fuzzy numbers: an overview", *Readings in Fuzzy Sets for Intelligent Systems*, pp. 112-148, 1993.
6. D. Dubois, H. Prade, "Operations on fuzzy numbers", *International Journal of systems science*, vol. 9, no. 6, pp. 613-626, 1978.
7. D.S. Dinagar, K. Latha, "Some types of type-2 triangular fuzzy matrices", *International Journal of Pure and Applied Mathematics*, vol. *82*, no. 1, pp. 21-32, 2013.
8. G. Uthra, K. Thangavelu, B. Amutha, "An Improved Ranking for Fuzzy Transportation Problem Using Symmetric Triangular Fuzzy Number", *Advances in Fuzzy Mathematics*, vol. 12, no. 3, pp. 629-638
9. H.J. Zimmermann, "*Fuzzy Set Theory and its applications*", 3rd edition, Kluwer Academic Publishers, London, 1996.
10. I. Silambarasan, S. Sriram, "Bounded Sum and Bounded Product of Fuzzy Matrices", *Annals of Pure and Applied Mathematics*, vol. 14, no. 3, pp. 513-523, 2007.
11. J.G. Klir, Y. Bo, "*Fuzzy Sets and Fuzzy Logic: Theory and Applications*", Prentice Hall P T R, New Jersey, 1996.
12. J. Gong, P. Tarasewich, "Alphabetically constrained keypad designs for text entry on mobile devices", *In Proceedings of the SIGCHI conference on Human factors in computing systems*, 211-220, 2005.
13. J. Holden, "*The Mathematics of Secrets*", Princeton University Press, 2017.
14. K. Nahar, P. Chakraborty, "A Modified Version of Vigenère Cipher using 95× 95 Table", International *Journal of Engineering and Advanced Technology (IJEAT)*, vol. 9, no. 5, pp. 1144-1148, 2020.
15. K. Ruohonen, "*Mathematical cryptology*", Lecture Notes, vol. 1, no. 1, pp. 1-138, 2014.
16. M. Hanss, "*Applied fuzzy arithmetic*", Springer-Verlag Berlin Heidelberg, 2005.
17. M.A. Raharja, I.D.M.B.A. Darmawan, D.P.E. Nilakusumawati, I.W. Supriana, "Analysis of membership function (ANFIS) method for inflation prediction", *In Journal of Physics Conference Series, IOP publishing*, vol. 1722, no. 1, pp. 012005, 2021.
18. P. Murali, G. Senthilkumar, "Modified Version of Playfair Cipher Using Linear Feedback Shift Register", *International Journal of Computer Science and Network Security*, vol. 8, no. 12, pp. 26-29, 2008.

19. R. Parvathi, C. Malathi, “Arithmetic operations on symmetric trapezoidal intuitionistic fuzzy numbers”, International Journal of Soft Computing and Engineering, vol. 1, issue 2, pp. 268-273, 2012.
20. S.A. Khan, “Design and Analysis of Playfair Ciphers with Different Matrix Sizes”, *International Journal of Computing and Network Technology*, vol. 3, no. 3, pp. 117-122, 2015.
21. S.D. Galbraith, “*Mathematics of public key cryptography”*, Cambridge University Press, 2012.
22. S. Saati, N. Nayebi, “An Algorithm for Determining Common Weights by Concept of Membership Function”, *Journal of Linear and Topological Algebra*, vol. 4, no. 3, pp. 165-172, 2015.
23. W. Diffie, M. Hellman, “New Directions in Cryptography”, *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644-654, 1976.