EMBEDDED CRYPTOSYSTEM IN ANALYTICAL GEOMETRY

S Ramachandran[1], Dr Sindhu J Kumaar[2] and Dr C V Jayakumar[3]

[1] B S Abdur Rahman Crescent Institute of Science & Technology, Tamil Nadu, India.
[2] B S Abdur Rahman Crescent Institute of Science & Technology, Tamil Nadu, India.
[3] Agni College of Technology, Tamil Nadu, India.

Abstract: The stored information in any form is Data, Data security is regarded as to prevent from unauthorized access. Cryptography provides functionality to encrypt the data and authenticate other users in secure manner. At present several cryptographic techniques are available. This paper propose a new cryptographic technique based on analytical geometry. Encoding and decoding are influenced by focal length and rotation. This work provides cipher key associated with given key to encrypt the plain text and decrypt cipher text. We include four essential characters "spaces" , "comma" ," semicolon" and "full stop" in addition to alphabets. This work provides high security from harmful attacks and brute force hacking. The cipher system can be used in wide range like Information security, Random number and one time password generation.

Keywords: **Encryption, Decryption, Vital points, Cipherkey, Focal length.**

1. INTRODUCTION

The data transmission in secured manner is a major issue in communication system. The reliable communication system means that the one which provides superior level security in data transmission, personal information or important documents are interchanged. Every second a significant amount of data is exchanged through unsecured channels in internet and multimedia. Therefore, it is essential to prevent the data from harmful attacks and brute full hackers. While exchanging personal information or important document, security and authentication should be provided [1]. In this case cryptography can be used to secure data.

Nowadays cryptography has vital role in preventing private data from being hacked and stolen. Cryptosystem having two stages encryption (encoding), decryption (decoding). Encryption is the process of converting plaintext into cipher text which is performed in sender's end and decryption is reversal of encryption which is performed in receiver's end [4]. The vital objective of this work is to provide a new cryptosystem based on analytical geometry. Encoding and Decoding process will be done in both sender's and receiver's ends by new key, called *cipherkey* which is generated from original key.

2. Cipher key and Base value

The keyword which is geometrically generated to encrypt plain text and decrypt cipher text from the original communicated keyword in secrete called cipherkey. The base value of alphabets A - Z as 0 – 25 and special characters **spaces, comma, semicolon** and **full stop** respectively as 26 ,27, 28, and 29, which is in table (1).

Table 1. Alphabet, Characters and Base Value

Alphabets	A	B	C	D	E	F	G	H	I	J	K	L	M
Base value	0	1	2	3	4	5	6	7	8	9	10	11	12
Alphabets	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Base value	13	14	15	16	17	18	19	20	21	22	23	24	25

characters	/	:	,	.
Base value	26	27	28	29

Let us point the space as the character " / " for the visibility of the place where the space located in encrypted date because of that there is chance to encrypt space at the start or end of encrypted data.

3. Proposed Cryptosystem

Suppose that there are m letters in the key the corresponding base values are b_k, $k = 1,2, \ldots, m$. Summed up the base value of key is $\Omega = \sum_{k=1}^{m} b_k$. Constructing an ellipse whose major and minor axes of length $2a$ and $2b$ such that $\Omega = 2a$ and $2b = a$. Foci of the ellipse are $F\ (ae, 0)$ & $G\ (-ae, 0)$ and an arbitrary point $P(a\cos\theta, b\sin\theta)$, the eccentricity

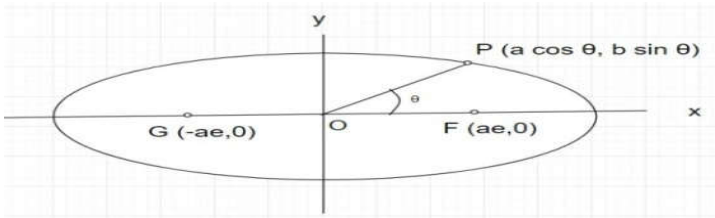

Figure 1. Ellipse E_1

$$e = \sqrt{\frac{a^2 - b^2}{a^2}} = \frac{\sqrt{3}}{2} \tag{1}$$

By rotating the ellipse E_1 in counter clock with an angle α about origin, which forms new ellipse E_2, where angle α is obtain as below

$$\alpha = \frac{\Omega}{m} = \frac{sum\ of\ base\ value\ of\ key}{no.\ of\ letters\ in\ key} \tag{2}$$

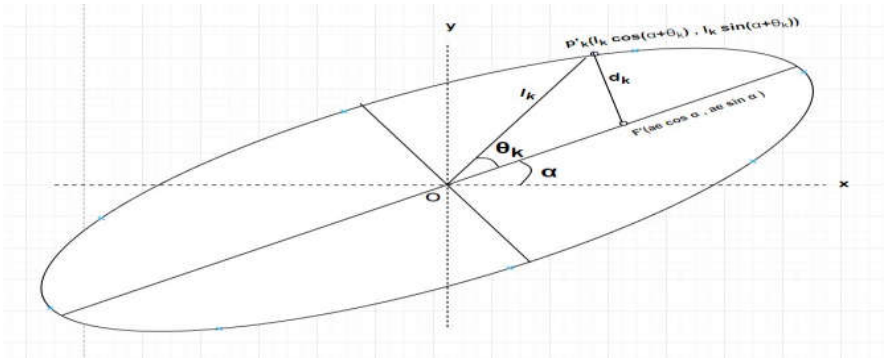

Figure 1. Ellipse E_2

The focus of the ellipse is $F'(ae\cos\alpha, ae\sin\alpha)$ and any point on the ellipse E_2 is $P_k'(l_k\cos(\varphi_k), l_k\sin(\varphi_k))$, where $\varphi_k = \alpha + \theta_k$, $k = 1,2, \ldots . m$. and l_k is the radial length of the point P_k' from origin O and θ_k is the angle of radial vector P_k' with major axis. Where $l_k = (a^2\cos^2\theta_k + b^2\sin^2\theta_k)^{\frac{1}{2}}$

$$l_k = \frac{a}{2}(3cos^2\theta_k + 1)^{\frac{1}{2}}, \quad k = 1,2, \ldots . m. \tag{3}$$

Let

$$\emptyset = \frac{180}{m} \tag{4}$$

$$\theta_k = k\emptyset, \quad k = 1,2, \ldots \ldots \ldots \ldots m. \tag{5}$$

The focal distance d_k of point $P_k^{'}(l_k cos(\ \varphi_k)\ , l_k sin(\ \varphi_k)$ from focus $F^{'}(ae\cos\alpha\ , ae\ sin\ \alpha)$ and the sum s_k of the coordinates of vital point $P_k^{'}$ are

$$d_k = \sqrt{(l_k cos(\ \varphi_k) - ae\cos\alpha)^2 + (l_k sin(\ \varphi_k) - ae\ sin\ \alpha)^2} \tag{6}$$

and

$$s_k = l_k cos(\ \varphi_k) + l_k \sin(\ \varphi_k), \quad k = 1,2, \ldots m. \tag{7}$$

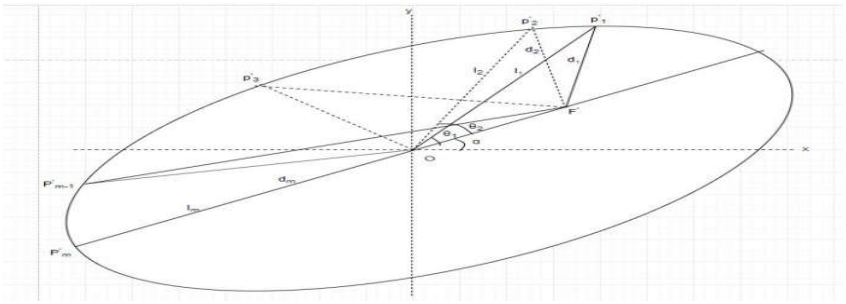

Figure 1. Ellipse E_3

Let n_k be the integral part of ten times of $(d_k + s_k)$

$$n_k = \text{ integral part of } 10\ (d_k + s_k)\ , \ k = 1,2, \ldots m. \tag{8}$$

Adding respectively n_k to base value b_k and addition is performed modulo 30, which generates the base value c_k of cipher*key*. that is

$$\boldsymbol{c_k = (n_k + b_k)\ modulo\ 30}, \quad \boldsymbol{k = 1,2, \ldots, m}. \tag{9}$$

The base value of characters in *Cipherkey* are $\boldsymbol{c_1, c_2, c_3, \ldots \ldots, c_m}$, using cipher key in any cryptographic technique with key, encoding plain text into cipher text can be made and decoding procedure is vice versa.

4. Example

An illustrative example for the proposed cryptosystem in two different cryptographic techniques, namely *Transposition cipher* and *Vigener's cipher*. Consider the plain text ***SUPER CIPHER*** to encrypt with keyword ***HERO.*** The procedure of *cipherkey generation* , *encoding* and *decoding* as below

4.1. Cipherkey Generation

Key word: *HERO*

H	*E*	*R*	*O*
7	4	17	14
Sum of base value of key $\Omega = 42$			

Number of letters in key $m = 4$

Refer to "(2)" the rotation angle $\alpha = \frac{\Omega}{m} = \frac{42}{4} = 10.5$ Major and minor axis of ellipse E respectively $2a = 42$ and $2b = a = 21$

Constant eccentricity fron "(1)" we have $e = \frac{\sqrt{3}}{2}$ and focu $F(ae, 0) = F\left(\frac{21\sqrt{3}}{2}, 0\right)$

By "(4)"&"(5)" we have $\emptyset = \frac{180}{4} = 45$ and $\theta_k = k\emptyset$ $.k = 1,2,3,4$

θ_1	θ_2	θ_3	θ_4
45	90	135	180

Having radial length l_k, by" (3)", $l_k = \frac{a}{2}(3cos^2\theta_k + 1)^{\frac{1}{2}}$, $k = 1,2,3,4.$

l_1	l_2	l_3	l_4
16.60	10.50	16.60	21.00

The focal distance d_k values from "(6)"
$d_k = \sqrt{(l_k cos(\ \varphi_k) - ae\cos\alpha)^2 + (l_k s\,in(\ \varphi_k) - ae\ sin\ \alpha)^2}$ we have

d_1	d_2	d_3	d_4
13.39	21	32.14	39.19

By "(7)", $s_k = l_k cos(\ \varphi_k) + l_k \sin(\ \varphi_k)$, $k = 1,2, \ldots m.$ we have

s_1	s_2	s_3	s_4
23	8.41	-4.28	-24.48

By "(8)", $n_k =$ *the integral part of* $10\,(d_k + s_k)$, *we have* n_k values

n_1	n_2	n_3	n_4
363	294	278	147

Cipherkey generation ,from "(9)", $c_k = (n_k + b_k)$ ***modulo 30*** we have

Key	*H*	*E*	*R*	*O*
Base value of key b_k	*7*	*4*	*17*	*4*
n_k*value*	363	294	278	147
Sum	370	298	295	151
c_k *value*	10	28	25	1
Cipherkey	K	,	Z	B

The generated *cipherkey* with proposed cryptosystem is **K,ZB**

4.2. Transposition chipher

We use the base value of Cipherkey ***K,ZB*** *to encrypt the plain text SUPER CIPHER*

S	*U*	*P*	*E*	*R*	/	*C*	*I*	*P*	*H*	*E*	*R*
18	*20*	*15*	*4*	*17*	*26*	*2*	*8*	*1*	*7*	*4*	*17*

$$\text{No. of rows} = \frac{\text{No. of letters in plain text}}{\text{No. of letters in key}} = \frac{12}{4} = 3$$

$No.\ of\ column = No.\ of\ letters\ in\ key = 4$

Base value of Key word			
K	,	Z	B
10	28	25	1
S	U	P	E
	/	C	I
P	H	E	R

The cipher text is ***EIRSRPPCEU / H***.

We now decrypt the cipher text ***EIRSRPPCEU / H***. using cipherkey ***K,ZB***

$$\text{No. of rows} = \frac{\text{No. of letters in plain text}}{\text{No. of letters in key}} = \frac{12}{4} = 3$$

$$No.\ of\ column = No.\ of\ letters\ in\ key = 4$$

Base value of Key word			
K	,	Z	B
10	28	25	1
S	U	P	E
R	/	C	I
P	H	E	R

The plain text is ***SUPER CIPHER***

4.3. Vigenere's chipher

The encryption of plain text SUPER CIPHER using cipherkey ***K,ZB***

The cipher text is ***,SKF;Y;JZF.S***

(i) Plain text:	S	U	P	E	R	/	C	I	P	H	E	R
(ii) Base value of plain text	18	20	15	4	17	26	2	8	15	7	4	17
(iii) Cipher key	K	,	Z	B	K	,	Z	B	K	,	Z	B
(iv) Base value of cipher key	10	28	25	1	10	28	25	1	10	28	25	1
(v) Sum of (ii) &(iv)	28	48	40	5	27	54	27	9	25	35	29	18
(v) modulo 30	28	18	10	5	27	24	27	9	25	5	29	18
(vi) Cipher text	,	**S**	**K**	**F**	;	**Y**	;	**J**	**Z**	**F**	.	**S**

Decryption of cipher text ***,SKF;Y;JZF.S*** using cipherkey ***K,ZB***

(i) Cipher text	,	**S**	**K**	**F**	;	**Y**	;	**J**	**Z**	**F**	.	**S**
(ii) Base value of Cipher text	28	18	10	5	27	24	27	9	25	5	29	18
(iii) Cipher key	K	,	Z	B	K	,	Z	B	K	,	Z	B
(iv) Base value of cipher key	10	28	25	1	10	28	25	1	10	28	25	1
(v) Difference (ii)-(iv)	18	-10	-15	4	17	-4	2	8	15	-23	4	17
(v) modulo 30	18	20	15	4	17	26	2	8	15	7	4	17
(vi) Plain text:	S	U	P	E	R		C	I	P	H	E	R

The plain text is ***SUPER CIPHER***

Conclusion

Cryptosystem based on analytical geometry is a new technique. Use of cipherkey in encoding plain text and decoding cipher text provides more security in communication system, data security and multimedia since encryption made under multi security stages. Also cipherkey is entirely different from the key in communication between sender's and receiver's end. One can in security concern use cipherkey which is generated by the same procedure in N evolutions.

Acknowledgements

The author is deeply indebted to the Management, Sri Ganesh college of Engineering and Technology, Pondicherry for allowing to do research work in the field of Mathematics. Author is very much grateful to Assistant Professor S Ravichandran , HOD, Department of mathematics , Manakula Vinayagar Institute of Technology, Pondicherry for triggering ideas in Cryptography. Author is also takes this opportunity to express sincere thanks to R. Dhanalakshmi , Manager, Agriculture market committee, Cuddalore for the financial support and valuable suggestions.

REFERENCES

[1] Atul Kahate, "Cryptography and Network Security" Mc Graw Hill Education (India) Private Limited, 2013.

[2] Cunsheng ding and Arto salomaa. "*On co-operatively distributed ciphering and hashing*", Turku centre for computer science, May 1996.

[3] Davis R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16,Nov 1978.

[4] Ramachandran S, Dr.Sindhu J Kumaar and Dr. Jayakumar C V. "Application of Cryptosystem Using NSPPL", Bulletin Monumental Journal, Vol 21, Issue 08, pp 31-36, 2020.

[5] Sindhu J Kumaar, P. J Abisha, D. G. Thomas, Nor Haniza Sarmin and K. G. Subramaniam. "Languages defined by pure patterns", International journal of applied mathematics and computer intelligence , vol. 2, pp.195-203, 2013.

[6] Salomaa A. and Yu S. "*On a public-key cryptosystem based on iterated morphisms and Substitutions*", Theoretical computer science. Vol 48, pp 283-296, 1986.