International Journal of Electrical and Computer Engineering (IJECE)
Vol. 7, No. 1, February 2017, pp. 285~288
ISSN: 2088-8708, DOI: 10.11591/ijece.v7i1.pp285-288

Symmetric Key based Encryption and Decryption using Lissajous Curve Equations

Santhosh Kumar B.J., Kruthika Vijay
Department of Computer Science, Amrita school of Arts and Sciences, Amrita Vishwa Vidyapeetham,
Amrita University Mysuru Campus, Karnataka, India

Article Info

Article history:

Received Oct 12, 2016
Revised Jan 15, 2017
Accepted Jan 30, 2017

Keyword:

ASCII: American standard code for information interchange
Decryption
Encryption
Key exchange

ABSTRACT

Sender and receiver both uses two large similar prime numbers and uses parametric equations for swapping values of kx and by product of kx and ky is the common secret key. Generated secret key is used for encryption and decryption using ASCII key matrix of order 16X16. Applying playfair rules for encryption and decryption. Playfair is a digraph substitution cipher. Playfair makes use of pairs of letters for encryption and decryption. This application makes use of all ASCII characters which makes brute force attack impossible.

Corresponding Author:

Kruthika Vijay
Department of Computer Science,
Amrita school of Arts and sciences,
Amrita Vishwa Vidyapeetham, Amrita University,
Mysuru Campus, Karnataka, India.
Email: kruthikavijay92@gmail.com

1. INTRODUCTION

Symmetric key makes use of same key for encryption and decryption. Symmtric key is confidential for encrypting a plaintext and decryption of plaintext.This application makes use of lissajous cuve equations for key. Plaintext is combined with key for encryption using 16 x 16 square matrix. Applying playfair [4] rules for encryption and inverse rules for decryption with same square matrix. Symmetric key playfair cipher is an alphabetic cipher. This application makes use of alphanumeric and special characters for encryption and decryption.

2. RESEARCH METHOD

The methodology used in this application is:

a. Key exchange mechanism.
b. Encryption and decryption

In this application parametric equations are used for secure exchange of keys. Lissajous curves equation can be represented ascan be used for two users need to exchange private keys a and b be two large prime numbers' can take values from trigonometric table values and t=1. This is a prerequisite be followed by a sender and recipient.

4. User A KEY generation:
a=35761

b=35761
k_x=30 (in radians)
t=1
k_y=120
secret key = 38502543

dy/dx=(-b*cos(k_y*t) * k_y)/(a*sin(k_x*t) * kx) substituting above values into the equation.

User B KEY generation:
a=34551
b=34551
k_x=30 (in radians)
t=1
k_y=120

dy/dx=(-b*cos(k_y*t) * k_y)/(a*sin(k_x*t) * kx) substituting above values into the equation.

$$\frac{dy}{dx} = 1$$

Exchange the values of user A's kx value to user B and User B's ky value to user A.When substituted the value of kx and ky common secret key is generated. Both users arrive at a common number. This common secret key can be further used for encryption and decryption.

Key	3	8	5	0	2	5	4	3	3	8	5
Plain text	e	n	e	m	y	k	i	l	l	e	d

Figure 1 shows ASCII Key Matrix

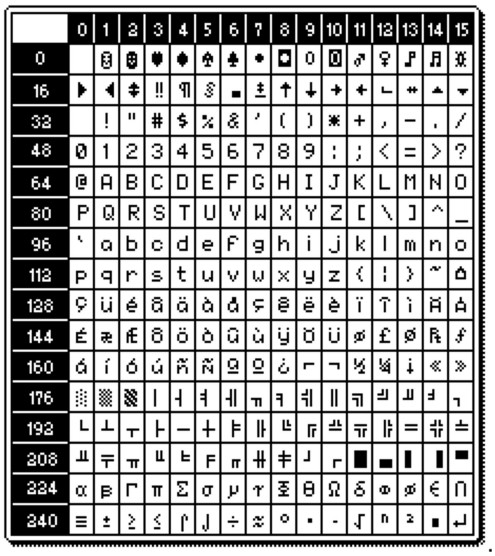

Figure 1. ASCII Key Matrix

Encryption.
Encryption process makes use of ASCII key table or square matrix without repetition and characters are arranged in a 16X16 grid.

Rules:
1. Plaintext letter pair repeated in row are separated with a filler letter, such as x to lx,lo so on.
2. Pick element to right of each letter and left wrap if required. For example, CD is encrypted as DE.
3. Pick element to below each letter and top wrap if required. For example, mu is encrypted as CM.
4. Otherwise, pick same rows opposite corners. The element forms corners of a rectangle. For example BRbecomes Rb.
Decryption is reverse (opposite) of the last rules.

Encrypting a message: “enemy killed”

Key	3	8	5	0	2	5	4	3	3	8	5
Plain text	e	n	e	m	y	k	i	l	l	e	d
Cipher text	5c	>h	Eu	M’	9r	;e	9d	Lc	Lc	5h	4e

Decryption:
Decryption is reverse of encryption.
Considering the ASCII key matrix for decryption. “5c” lies in the corners of the rectangle. The order is important – the first character of the encrypted pair is the one that lies on the same row as the first character of the cipher text pair. So “5c” can be decrypted as “3e” and so on. You will be getting the key with plain text.

Cipher text	5c	>h	Eu	M’	9r	;e	9d	Lc	Lc	5h	4e
Key	3	8	5	0	2	5	4	3	3	8	5
Plain text	e	n	e	m	y	k	i	l	l	e	d

3. RESULTS AND ANALYSIS

In this section, it is explained the results of research and at the same time is given the comprehensive discussion. Results can be presented in figures, graphs, tables and others that make the reader understand easily [2], [5]. The discussion can be made in several sub-chapters.

4. CONCLUSION

In this application**,** new requirement of symmetric key exchange with lissajous curve equations. This application also makes of exchanging secret key between two users using symmetric scheme. Using secret key generated can be used for encryption and decryption. This application makes use of novel method and high security cryptography technique using lissajous curve equations. To provide integrity of any message, message authentication scheme can be applied. It helps to ensure the information secure. Many researches are yet to be identified in future. To provide a better mechanism using asymmetric key exchange lile RSA or DHKE.

REFERENCES

[1] Ragheb Toemeh and Subbanagounder Arumugam, J., “Applying Genetic Algorithms for Searching Key-Space of Polyalphabetic Substitution Ciphers”, Vol. 5, No. 1, January 2008. The International Arab Journal of Information Technology.
[2] Omolara, A.I. Oludare and S.E. Abdulahi, “Developing a Modified Hybrid Caesar Cipher and Vigenere Cipher for Secure Data Communication”, O.E. Computer Engineering and Intelligent Systems, Vol.5, No.5, 2014.
[3] Ayman Al-ahwal, Sameh Farid. “The Effect Of Varying Key Length On A Vigenère Cipher”, *IOSR-JCE, Volume 17, Issue 2, Ver. VI (Mar – Apr. 2015)*.
[4] Safwat Hamad, “A Novel Implementation of an Extended 8x8 Playfair Cipher Using Interweaving on DNA-encoded Data”, Vol. 4, No. 1, Feburary 2014.

Text books:

1] Cryptography and Network security principles and practices.fifth edition by William stallings.
[2] Cryptography and Network security by Atul Kahate

BIOGRAPHIES OF AUTHORS

Santhosh Kumar B J has completed his M.Tech (I.T) from Karnataka State Open University (KSOU), Mysuru, Karnataka, M.Sc (SIS) from Bharathiar University, Coimbathore, Tamil Nadu, B.Sc (PMC) from Mysore University, Karnataka. Now he is working as Assistant Professor, Department of Computer Science, Amrita Vishwa Vidyapeetham University, Mysuru Campus.

Kruthika Vijay has completed M.Sc in Mathematics and 1Years of teaching experience and area of interest in discreet mathematics. Currently working as a lecturer, Assistant Professor, Department of Computer Science, Amrita Vishwa Vidyapeetham University, Mysuru Campus