Zain Publications
Company Registration No: UAN TS02E0015729
(Govt. of India, Ministry of Micro, Small & Medium Enterprises)
Contact Person: Dr. Mohd Zainuddin
Address: #12-1-898, North Lalaguda, Secunderabad, Telangana, India

Dr. Saad Abdual Azize, International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017, Pg: 105-110
ISSN (Online): 2001-5569
UGC Approved Journal

One Time Pad Key Generation Using Elliptic Curve Key Exchange

Dr. Saad Abdual Azize
saadabdualazize@yahoo.com
Al mamoon University Collage, Iraq, Baghdad

Abstract: ***Due to the massive improvements in data communication and networks, security became one of the most important fields. Securing transmitted data in any available method implied a great variety of techniques to shelled important data from unauthorized access. Encryption is one of these techniques which depend on keys for encryption and decryption. The problem is who to transmit these keys secretly and change them frequently. In this research a new method is proposed for key generation and exchange using the powered elliptic curve, Beaufort cipher, and Porta table to produce many one-time-pad keys.***

Keyword: Authentication, elliptic curve, exchange key, Beaufort cipher, Porta Table

Introduction

Cryptography is used for securing data by developing methods that allow information to be sent in a secure form in such a way that the only the receiver can retrieve the information.
Message authentication code (MAC), sometimes known as a tag, is a short part of information or message used to authenticate message.

Message authentication code consists of three algorithms:

- A key generation algorithm selects a key.
- A signing algorithm: to returns a tag given the key and the message.
- A verifying algorithm: to verifies the authenticity of the message given the key and the tag., return accepted when the message and tag are same , otherwise return rejected[1].

Zain Publications
Company Registration No: UAN TS02E0015729
(Govt. of India, Ministry of Micro, Small & Medium Enterprises)
Contact Person: Dr. Mohd Zainuddin
Address: #12-1-898, North Lalaguda, Secunderabad, Telangana, India
Dr. Saad Abdual Azize, International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017, Pg: 105-110
ISSN (Online): 2001-5569
UGC Approved Journal

Elliptic curve

Each elliptic curve is an equation in two variables, with two coefficients. For cryptography, the variables and coefficients are limited to elements in a finite field.

Elliptic curves over Zp

$$Y^2=(X^3 +aX + b) \bmod p \qquad (1)$$

$E_P(a,b)$ consisting of all p, for all of integers (x,y) that satisfy Equation (1), There are many parameters have to be defined that are necessary to do meaningful operations. They called "domain parameters":

1. p: prime number , defines the field for the curve operates Fp. All point are taken modulo p.
2. a, b Two coefficients Integer number which satisfy Equation.
3. G(x,y): base point of the curve which belonged to the curve .
4. n: The order of the curve basic point G. [2][3].

Beaufort cipher

The Beaufort cipher is a polyalphabetic substitution cipher can be pronounced algebraically. using an encrypting of the letters A–Z as the numbers 0–25 and using addition modulo 26, let Message M ={M1….. Mn} characters of the plain text ,let C={C1...Cn} be the characters of the cipher text ,let K ={K1....Kn} the characters of the key, repeated if necessary. Then Beaufort

$C = Ek(p) = k-p \bmod 26$

$P = Dk(c) = c-p \bmod 26$

Zain Publications
Company Registration No: UAN TS02E0015729
(Govt. of India, Ministry of Micro, Small & Medium Enterprises)
Contact Person: Dr. Mohd Zainuddin
Address: #12-1-898, North Lalaguda, Secunderabad, Telangana, India
Dr. Saad Abdual Azize, International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017, Pg: 105-110
ISSN (Online): 2001-5569
UGC Approved Journal

Table 1: Characters, weights, and codes

Char	weight	Code
A	0	00000
B	1	00001
C	2	00010
D	3	00011
E	4	00100
F	5	00101
G	6	00110
H	7	00111
I	8	01000
J	9	01001
K	10	01010
L	11	01011
M	12	01100

char	weight	Code
N	13	01101
O	14	01110
P	15	01111
Q	16	10000
R	17	10001
S	18	10010
T	19	10011
Y	20	10100
V	21	10101
W	22	10110
X	23	10111
Y	24	11000
Z	25	11001

Porta Table

Giovanni Baptista della Porta developed the Porta Table is used to substitutions(exchange) two character to one character and the table below .

Table 2: Porta table

AB	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
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
GH	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
KL	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
MN	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
OP	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
QR	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
ST	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q

Zain Publications
Company Registration No: UAN TS02E0015729
(Govt. of India, Ministry of Micro, Small & Medium Enterprises)
Contact Person: Dr. Mohd Zainuddin
Address: #12-1-898, North Lalaguda, Secunderabad, Telangana, India
Dr. Saad Abdual Azize, International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017, Pg: 105-110
ISSN (Online): 2001-5569
UGC Approved Journal

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

Let d = length of message (number of character)
Let L the location of point p(x,y) in the sequence of point of carve.
Choose Ep(a,b)
Choose G ∈ Ep

User A (sender)
Choose na ∈ [2,p-2] as private key
Calculate Pa = na G as public key
Compute k=naPb
User B (receiver)
Choose nb ∈ [2,p-2] as private key
Calculate Pb = nb G as public key
Compute k=naPa

Generate key

1-Add the k to first five number of points:

2- Each point k contain x,y value ,convert each value to character using table 1.

3- K(char1 ,char2),choose d/3+1 point to be the key for encryption.

4- The intersection between char1 and char2 giver on character using table2.

5- Convert each character to number using table 1.

6- Choose the message authentication start at location d.

7- Convert the message authentication to its weight using table 1.

8- Encrypted using Beaufort cipher.

Zain Publications
Company Registration No: UAN TS02E0015729
(Govt. of India, Ministry of Micro, Small & Medium Enterprises)
Contact Person: Dr. Mohd Zainuddin
Address: #12-1-898, North Lalaguda, Secunderabad, Telangana, India
Dr. Saad Abdual Azize, International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017, Pg: 105-110
ISSN (Online): 2001-5569
UGC Approved Journal

Implementation

Consider the curve E29(1,1) y2 = x3 + x + 1 mod 29 , with a = 1 ,b = 1 and p = 29 .
With E29(1,1) , The points in E29 are the following:
{(0,1),(0,28),(6,7),(6,22),(8,17),(8,12),(10,24),(10,5),(11,26),(11,3), (12,24),(10,5),(11,26),(11,3),(12,28),(12,1),(13,23),(13,6),(14,27),(14,20), (16,16),(16,13),(17,28),(17,1),(18,15),(18,14),(19,21),(19,8),(22,17), (22,12),(24,25),(24,4),(25,22),(25,17),(27,22),(27,7),(28,17),(28,12), (29,1), (29,28) }

Sender (A)

1-Let na = 3∈ [2,P-2] G=(0,1) P=29

2-Pa=naG =3(0,1) =(14,2)

3-K=naPb=3(16,16)=(14,27)

Receiver (B)

1-Let nb = 5 [2,P-2] G=(0,1) P=29

2-Pa=nbG =5(0,1)= (16,16)

3-K=naPb=3(16,16)=(14,27)

Generate key

1-Add K to first five points in carve:

K1=K+p1 =(14,27)+(0,1) = (22,12)

K2=K+p2 =(14,27)+(0,28) = (19,21)

K3=K+p3 =(14,27)+(6,7) = (18,17)

K4=K+p4 =(14,27)+(6,22) = (18,14)

Zain Publications
Company Registration No: UAN TS02E0015729
(Govt. of India, Ministry of Micro, Small & Medium Enterprises)
Contact Person: Dr. Mohd Zainuddin
Address: #12-1-898, North Lalaguda, Secunderabad, Telangana, India
Dr. Saad Abdual Azize, International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017, Pg: 105-110
ISSN (Online): 2001-5569
UGC Approved Journal

2- From above contain 10 points:

P1=(14,27)=(O,A)=T=19

P2=(0,1)=(A,B)=O=14

P3=(22,12)=(W,M)=O=14

P3=(0,28)=(0,1)=(A,B)=O=14

P4=(19,21)=(T,V)=E=4

P5=(6,7)=(G,H)=R=17

P6=(18,17)=(S,R)=A=0

P7=(6,22)=(G,W)=M=12

P8=(18,14)=(S,O)=K=10

P9=(8,17)=(I,R)=I=8

P10=(13,23)=(N,X)=D=3

3-Convert the message to code

M	A	L	M	A	M	O	O	N
M	0	11	12	0	12	14	14	13
K	19	14	14	14	4	19	14	14
cipher	19	3	2	14	-8	5	0	1
					18			
Code	10011	00011	00010	01110		00101	00000	00001

The decryption process is the reverse of the encryption process.

Zain Publications
Company Registration No: UAN TS02E0015729
(Govt. of India, Ministry of Micro, Small & Medium Enterprises)
Contact Person: Dr. Mohd Zainuddin
Address: #12-1-898, North Lalaguda, Secunderabad, Telangana, India
Dr. Saad Abdual Azize, International Journal of Research in Information Technology, Volume 1, Issue 2, Dec 2017, Pg: 105-110
ISSN (Online): 2001-5569
UGC Approved Journal

Conclusions

In this research the powered elliptic curve was used to exchange symmetric key. From this key many other one-time-pad keys were generated by producing other points on the curve. The proposed method was able to produce more than ten keys from one exchanged point. Using Beaufort and Porta table increase the security of the proposed encryption method.

References

[1] William Stallings, Prentice Hall, "Cryptography and Network Security Principles and Practice Fifth Edition". FIFTH EDITION 2011.
[2] N. Koblitz,“ Elliptic curve cryptosystem,” matematics of computer, vol.48, pp.203-209, 1987.
[3] V.Miller,“ Uses of elliptic curves in cryptography,” Advance in Cryptology (CRYPTO), LNCS vol.218, pp. 417–428, 1985
[3] Kuldeep Singh “Implementation of Elliptic Curve Digital Signature Algorithm” International Journal of Computer Applications, volume2 No.2, May 2010.
[4] F.Amounas, E.H. El Kinani and A. Chillali, An application of discrete algorithms in asymmetric cryptography, International Mathematical Forum, Vol. 6, no. 49, pp.2409 - 2418, 2011
[5] R. Rajaram Ramasamy, M. Amutha Prabakar, M. Indra Devi, and M.Suguna, Knapsack based ECC Encryption and Decryption, International Journal of Network Security, vol. 9, no. 3, pp. 218-226, Nov. 2009.
[6] F.Amounas and E.H. El Kinani, An Elliptic Curve Cryptography Based on Matrix Scrambling Method, Proceedings of the JNS2, pp 31-35, 2012.
[7] Dr.K.Thamodaran, Security Scheme for Data Authentication Based on Elliptic Curve Cryptography, International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 7 No. 04 Apr 2016
[8] **DOI:** 10.1109/TCSII.2006.889459