Volume 4, Issue 2, February 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Design of New Cryptosystem Using Menezes Vanstone Cryptosystem

Vincy.J , Gowtham.K
PG Scholar ,
Kumaraguru College of Technology,
Coimbatore-641049, Tamil Nadu, India

Krithika.S
Assistant Professor,
Kumaraguru college of Technology,
Coimbatore-641049, Tamil Nadu, India

Balaparamesh.V
PG Scholar
Karpagam college of Engineering,
Coimbatore-641049, Tamil Nadu, India

ABSTRACT- This paper proposes a new approach to encrypt data with new modified cryptosystem based on elliptic curve. This new version utilizes the original Menezes Vanstone cryptosystem. But it has some additional features to cryptosystem's encryption method. According to the encryption method, first the message is divided into blocks that contain only one character, and then each character is converted to hexadecimal value. A hexadecimal value of each character has two digits. These two digits allow us to express the message as a point in curve. The knowledge of each character's point need not be sent to the recipient. The paper explains the implementation of encrypting data with new modified cryptosystem based on elliptic curve using VHDL.

KEY WORDS: Cryptography, Menezes Vanstone cryptosystem, Elliptic curve cryptography, Symmetric key.

I. INTRODUCTION

Internet provides an essential communication between tens of millions of people in the world. And it is being increasingly used as a tool for commerce hence security becomes tremendously important. Message authentication plays a prominent role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the sensor energy. Many authentication schemes have been developed to provide message authenticity and integrity verification for wireless sensor networks.

Message authentication plays a prominent role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the sensor energy. Many authentication schemes have been developed to provide message authenticity and integrity verification for wireless sensor networks.

The symmetric-key based approach requires complex key management and lacks of scalability. It is not resilient to large numbers of node compromise attacks since the message sender and the receiver have to share a secret key. The shared key (letter or symbol) is used by the sender to generate a message authentication code for each transmitted message.

In network communication there are a lot of security and safety approaches being used. Security is required to keep the data safe from unauthorized person. But this confidential data or information in transit becomes vulnerable to the unauthorized attacks by hackers. There are many aspects for security and many applications, ranging from secure commerce and payments to private communications and protecting passwords which are called as cryptography and steganography.

Cryptography is used to convert the secured message into undecipherable format during the transmission of data. Cryptography is a tool for protecting information (message) in computer systems and networks. To send the message from source to destination there is a chance of data theft and access by third persons in network. In computer networking there is need of cryptography to secure information from third person.

Cryptography is the most secure techniques which uses mathematical calculations and variable values known as a 'key'. The selected key is acting as an input on encryption and is integral to the changing of the data [3]. In cryptography plain text is converted into unreadable cipher text using key, this process is called encryption of message [4].

Data communication takes place over an unsecured channel, as is the case when the Internet provides the pathways for the flow of data [1]. In this case the cryptographic protocols would enable secured communications by addressing the following,

- **Confidentiality**: private data remains as private.
- **Authentication:** identification of all parties attempting access.
- **Authorization:** identification of permissions.
- **Data Integrity:** an object is not altered by third person.

II. BOOLEAN ALGEBRA BASED EFFECTIVE AND EFFICIENT ASYMMETRIC KEY CRYPTOGRAPHY ALGORITHM: BAC ALGORITHM

This Algorithm is used to convert plaintext to cipher text (i.e. Encryption) and cipher text to plain text (i.e.Decryption). The algorithm uses ASCII value for conversion. This algorithm takes corresponding ASCII values of each character, number and symbol [2].

After implementing this algorithm on various characters, numbers and symbol in messages, it is found that the cipher text will be totally secured and unreadable. In these method ASCII values of characters, numbers and symbols are manipulated. The ASCII values are converted into binary numbers that takes 32 bits. Other algorithms use 128 bit encrypting and decrypting techniques, which require more space in transferring data. 1's and 2's complement method and XOR operations of data are used to encrypt data in this algorithm. Same Public and Private Keys are used in encryption as well as decryption process [2]. In the decryption process, if the resultant ASCII value is 1B, the corresponding character is ESC key which makes the cipher text as meaningless. So this algorithm is inefficient.

III. ELLIPTIC CURVE CRYPTOGRAPHY

Koblitz and Miller introduced the use of elliptic curves in public key cryptography which is called as Elliptic curve Cryptography (ECC). The main operation of elliptic curves is multiplying a point by a scalar in order to get a second point. The complexity arises from the fact that, given the initial point and the final point, the scalar could not be deduced It leads to a very difficult problem of reversibility, or cryptanalysis, called as elliptic curve discrete logarithm problem [1].

The ECC algorithms with their small key sizes are the best challenge for cryptanalysis problems compared to RSA or AES, thus ECC will lead to smaller area hardware, less bandwidth use, and more secure transactions.

An elliptic curve E takes the general form as:

$$E: l = x3 + ax + b\ [p] \quad \rightarrow (1)$$

Where a, b are in the appropriate set (rational numbers, real numbers, integers mod p) and x, y are elements of the finite field GF (p), satisfying $4a^3 + 27b^2 \neq 0 \pmod{p}$ and p is known as modular prime integer making the elliptic curve finite field. There are two basic group operations on elliptic curve.

It is given by

- Point addition
- Point doubling

A. *Point Addition*

Addition means that given two points on E and their coordinates are P = $(X_1\ Y_1)$ and Q = $(X_2\ Y_2)$, E (GF (p)), we have to compute the coordinates of a third point R such that,

$$P + Q = R \quad \rightarrow (2)$$

$$(X_1, Y_1) + (X_2, Y_2) = (X_3, Y_3) \quad \rightarrow (3)$$

This is the case, we need to compute R = P +Q and P ≠ Q. Point R's coordinates (X_3, Y_3) also E (GF (p)).

$$\lambda = (Yp\text{-}Yq) / (Xp\text{-}Xq) \quad \rightarrow (4)$$

$$Xr = [\lambda^2\text{-}Xp\text{-}Xq] \bmod p \quad \rightarrow (5)$$

$$Yr = [\text{-}Yp+\lambda\ (Xp\text{-}Xr)] \bmod p \quad \rightarrow (6)$$

B. *Point Doubling*

Point doubling is the addition of a point P on E to obtain another point R. This is the case where we need to compute P + Q but P = Q. Hence R = P + P = 2P.

$$\lambda = (3X^2p+\alpha)/2Yp \quad \rightarrow (7)$$

$$Xr = [\lambda^2\text{-}2Xp] \bmod p \quad \rightarrow (8)$$

$$Yr = [\text{-}Yp+\ \lambda\ (Xp\text{-}Xr)] \bmod p \quad \rightarrow (9)$$

IV. MODIFIED CRYPTOSYSTEM

In the modified cryptosystem, we can encrypt not only point but also message according to request of sender. If sender wants to encrypt the message, the plaintext dimension d is calculated and then plaintext is divided into blocks as the size of plaintext and each block is encrypted by an identical key set K' = {(E', α', a', β'): β' = a' . α'} that has exactly the same characteristic of the original Menezes Vanstone ECC cryptosystem. Every block has only one character. After that the character's equivalent of hexadecimal (base-16) number system is calculated. Every character's equivalent of hexadecimal value is given below,

HEX. CHAR DEC	HEX. CHAR DEC	HEX. CHAR DEC	HEX. CHAR DEC	HEX. CHAR DEC	HEX. CHAR DEC	HEX. CHAR DEC	HEX. CHAR DEC
00 nul	01 soh	02 stx	03	04	05 enq	06 ack	07 bel

			etx	eot			
08 bs	09 ht	0A nl	0B vt	0C np	0D cr	0E so	0F si
10 dle	11 dc1	12 dc2	13 dc3	14 dc4	15 nak	16 syn	17 etb
18 can	19 em	1A sub	1B esc	1C fs	1D gs	1E rs	1F us
20 sp	21 !	22 “	23 #	24 $	25 %	26 &	27 ‘
28 (	29)	2A *	2B +	2C ,	2D -	2E .	2F /
30 0	31 1	32 2	33 3	34 4	35 5	36 6	37 7
38 8	39 9	3A :	3B ;	3C <	3D =	3E >	3F ?
40 @	41 A	42 B	43 C	44 D	45 E	46 F	47 G
48 H	49 I	4A J	4B K	4C L	4D M	4E N	4F O
50 P	51 Q	52 R	53 S	54 T	55 U	56 V	57 W
58 X	59 Y	5A Z	5B [	5C \	5D]	5E ^	5F _
60 `	61 a	62 b	63 c	64 d	65 e	66 f	67 g
68 h	69 i	6A j	6B k	6C l	6D m	6E n	6F o
70 p	71 q	72 r	73 s	74 t	75 u	76 v	77 w
78 x	79 y	7A z	7B {	7C |	7D }	7E ~	7F del

Tab.1 Hexadecimal values of each character

According to Tab.1, each character's hexadecimal value, is located to the left of character's in Tab.1, has two digits whose units digit indicates X_{2i} and tens digit indicates X_{li} for that reason the character represented as a point (X_{li}, X_{2i}), subscript i symbolizes block number, it is an integer and $1 \leq\ i \leq d$. X_{2i} can be one of these letters A, B, C, D, E, and F, in this case hexadecimal value is converted to decimal. These are A →10,B→11 C→12,D→13,E→14,and F→15 Etc. Encryption and decryption of this algorithm is based on elliptic curve cryptography. But it uses the point as hexadecimal values of each character.

A. Flowchart

The steps to be followed during encryption and decryption are given in the flowchart. In our implementation, encryption and decryption processes are the same with Menezes Vanstone ECC algorithms while sending only point.

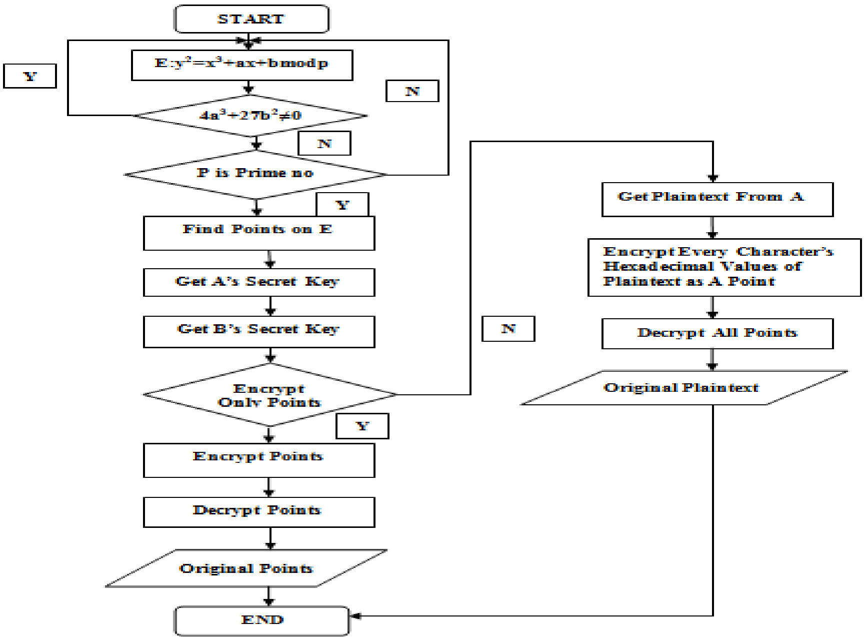


Fig.1 Flow chart

This algorithm has three blocks. That is given by

- Key generation
- Encryption
- Decryption

B. KEY GENERATION

Recipient B selects a random number a' =[1, n'-1] and it is public key, α' is the generator point and n' is the order of α', computes β' private key as follows:

$$\beta' = a' \cdot \alpha'$$

Recipient B selects a random number a' = [1, n'-1] and it is the public key, α' is the generator point and n' is the order of α', computes β' private key as follows:

$$\beta' = a' \cdot \alpha' \quad \rightarrow (10)$$

C. ENCRYPTION

Sender A gets B's public key β', selects a random number k' = [1, n'-1], selects the plaintext x'. Then x' is sent to the Convert to Point function. The steps for converting to point function is given by

Steps Pseudo Code of Convert to Point Function

```
1    d = sizeof (plaintext) // Calculate d, d is dimension of plaintext
2    for i =1 to d
3    key→ A[i]
4    e[i] = int (key)
5    b[i] = e[i]/16 // X2i
6    if b[i] is a letter A→ 10, B→11, C→ 12, D→ 13, E→ 14, and F→15
7    o[i] = e[i]%16 // Xli
8    A[i] = (b[i], o[i])
```

This function converts to plaintext's value as X' = (X_{li}, X_{2i}) then computes,

$$Y'_0 = k' \cdot \alpha' \quad \rightarrow (11)$$

$$(C'_l, C'_2) = k'. \beta' \quad \rightarrow (12)$$

$$Y'_{1i} = C'_1 \cdot X_{li} \bmod p \quad \rightarrow (13)$$

$$Y'_{2i} = C'_2 \,.\, X_{2i} \bmod p \rightarrow (14)$$

After calculating these equations, every character of the plaintext as a point (Y'_0, Y'_{li}, Y'_{2i}) is transmitted n' times.

D. DECRYPTION

Recipient B uses whose secret key a' calculating:

$$(C'_l , C'_2) = a' \cdot Y'_0 \rightarrow (15)$$

$$Xi = (Y'_{li} \,.\, C_l^{-1} \bmod p, Y'_{2i} \,.\, C_2^{-1} \bmod p) \quad \rightarrow (16)$$

Using this equation ($X_i = X_{li} \cdot 16 + X_{2i}$) that represents plaintext x' = {(X_{1} ,$X_{2,}$ ... , X_n) and i = 1, 2, 3... n}.

V. IMPLEMETATION

A. KEY GENERATION

This random number is act as public key. The block diagram to generate private key is given by

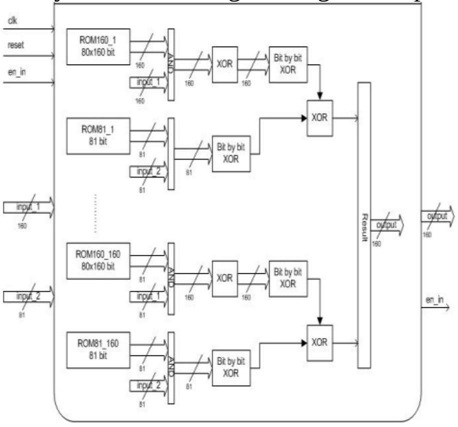


Fig.2 Block of key generation

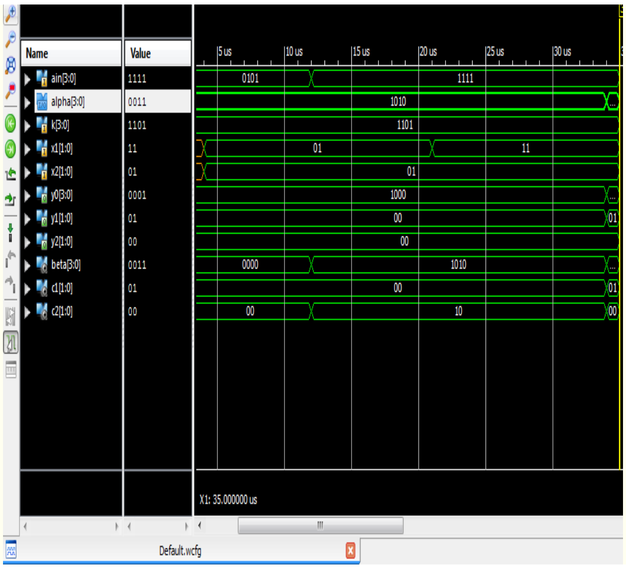


Fig.3 Result of key generation

This fig shows the simulated result of key generation part of the cryptosystem. It shows the private key generation of the user.

B. *ENCRYPTION*

The encryption block is given by

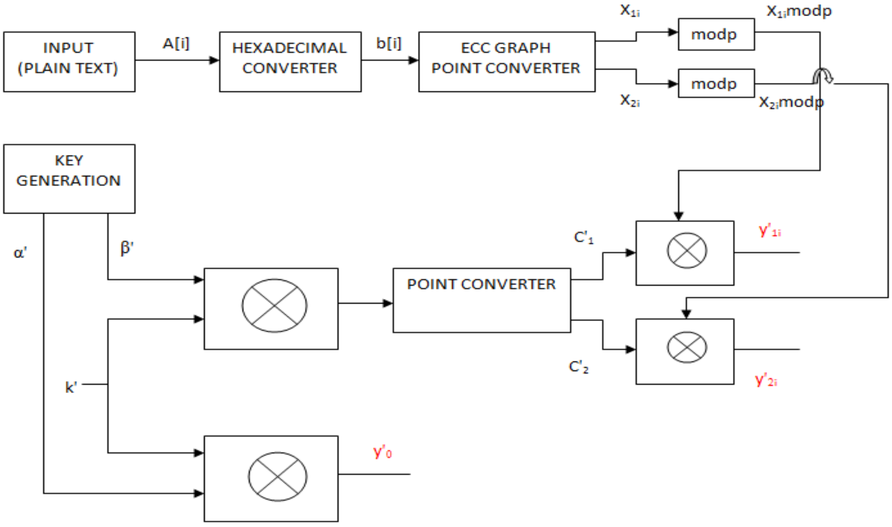


Fig.4 Encryption block

Simulation result for encryption is given by

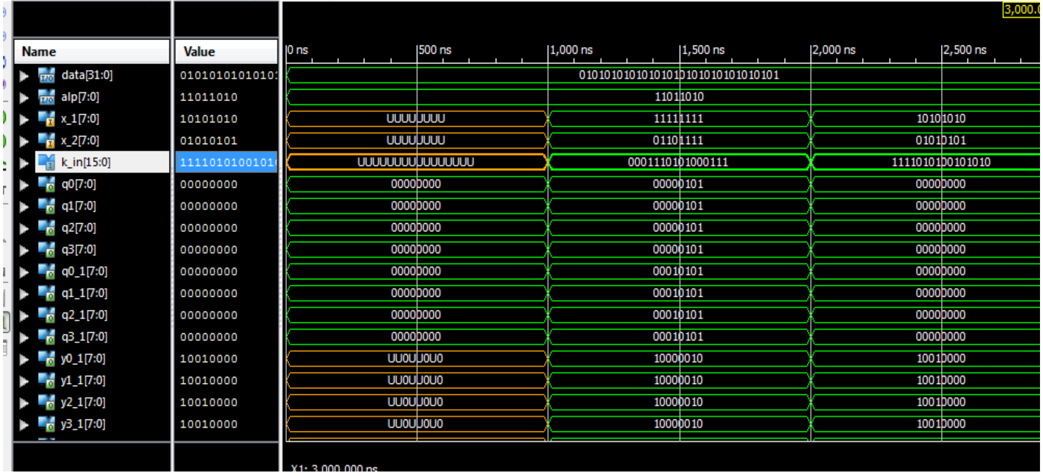
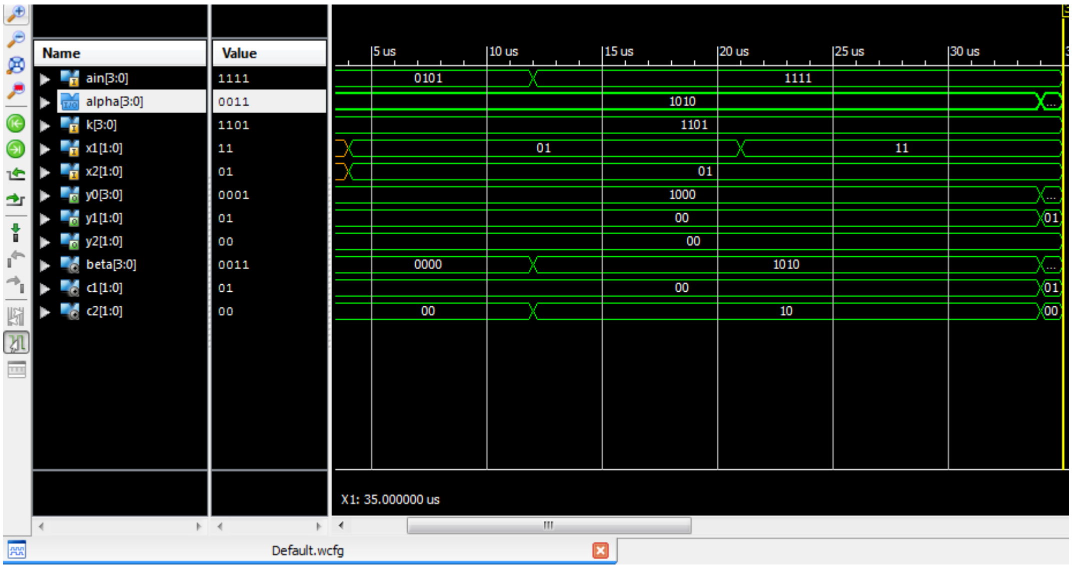


Fig.5 Simulation result for encryption

C. DECRYPTION

Simulation result for decryption is given by



Name	Value
ain[3:0]	1111
alpha[3:0]	0011
k[3:0]	1101
x1[1:0]	11
x2[1:0]	01
y0[3:0]	0001
y1[1:0]	01
y2[1:0]	00
beta[3:0]	0011
c1[1:0]	01
c2[1:0]	00

X1: 35.000000 us

Default.wcfg

Fig.5 Simulation result for decryption

VI. CONCLUSION

This algorithm provides an efficient cryptosystem compare to other cryptosystems. It gives how to encrypt characters with their hexadecimal values that provides security communication media without the necessity of code table which is agreed by communication parties based on elliptic curve. This algorithm affords efficient implementation of wireless security features, such as secure electronic mail and Web browsing. In hardware implementation, this algorithm requires less storage, less power, less memory, and less bandwidth than other systems.

REFERENCE

[1] MeltemKURT, Tank YERLiKAYA “A New Modified Cryptosystem Based on Menezes Vanstone Elliptic Curve Cryptography Algorithm that Uses Characters' Hexadecimal Values” , ISBN: 978-1-4673-5613-8©2013 IEEE.

[2] Niraj Kumar , Pankaj Gupta , Monika Sahu ,Dr. M A Rizvi, Boolean Algebra based Effective and Efficient Asymmetric Key Cryptography Algorithm: BAC Algorithm, 978-1-4673-5090-7/13/$31.00 ©2013 IEEE

[3] F. Amounas, E. H. El Kinani, "Cryptography with elliptic curve using Tifinagh characters", Journal of Mathematics and System Science 2, pp. 139-144,2012.

[4] An Integrated Symmetric key Cryptography Algorithm using Generalised modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm Debanjan Das, Megholova Mukharjee, Neha Choudhary, 978-1-4673-0126-8/2011 IEEE

[5] A new symmetric key cryptography algorithm using extended MSA method: DJSA symmetric key algorithm, dripto chatterjee, Joyshree Nath, suvadeep Dasgupta, Ashok nath, 978-0-7695-4437-3 2011 IEEE.

[6] Block Encryption standard for transfer of data Akhil Kaushik, Manoj Barnela, Anant Kumar 978-1-4244-7578-0, 2010 IEEE

[7] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, “Attacking cryptographic schemes based on ”perturbation polynomials”,” Cryptology ePrint Archive, Report 2009/098, 2009

[8] L. Ertaul, W. Lu, "ECC based threshold cryptography for secure data forwarding and secure key exchange in MANEr',IFIP, NETWORKING 2005,LNCS 3462,pp. 102-113,2005