INTERNATIONAL JOURNAL OF CURRENT MULTIDISCIPLINARY STUDIES
Available Online at http://www.journalijcms.com
VOL. 3, ISSUE,06, PP.766-772, JUNE, 2017
IJCMS

RESEARCH ARTICLE

SECURITY ISSUES OF BLUETOOTH BASED ON DIGITAL SIGNATURE USING ELLIPTIC CURVE CRYPTOGRAPHY(SBECDSA)

Ahmad Hweishel A. Alfarjat[1]., Sheshadri H.S[2] and Hanumanthappa.J[3]

[1]Department of E&CE PESCE, Mandya-571401.University of Mysore
[2]Department of E&CE PESCE Mandya-571401
[3]Department of E&CE Dept of Studies in CS Manasagangothri, Mysuru-6

ARTICLE INFO

Received 20th March, 2017
Received in revised form 16th April, 2017
Accepted 5th May, 2017
Published online 28th June, 2017

Keywords:

Bluetooth, Cryptography,Digital Signature(DS),ECC,ECDSA.

ABSTRACT

Elliptic Curve Cryptography(ECC) has been a latest innovative area in the field of Cryptography. In this research manuscript we have proposed Digital Signature based security issues of Bluetooth using Elliptic Curve Cryptography (SBECDSA). The main theme of our research work also proposed how to compute security issues of elliptic curve cryptography based on Digital Signature. The Digital Signature Standard is based on the Digital Signature Algorithm (DSA). The original version of Digital Signature used multiplicative groups of finite fields. Elliptic curves have a rich and a beautiful history, having been studied by Mathematicians for over a hundred years. Elliptic curves are mainly used to solve a diverse set of problems.

The Digital Signature Algorithm(DSA) was proposed in 1991by the U.S.National Institute of Standards and Tech (NIST) and was specified in a U.S.Government Federal Information Processing Standard (FIPS 186) called Digital Signature Standard (DSS). The Elliptic Curve Cryptography (ECC) is mainly considered based on Functionality, Security, Performance[14]. My research work also explores the Digital Signature based security issues of Bluetooth based on Elliptic Curve Cryptography (SBECDSA).We have implemented security issues of Bluetooth based on Message Authentication, Integrity, Non-Repudiation using Elliptic Key Cryptography(SBECDSA) and Matlab simulator.

INTRODUCTION

Cryptography is a Latin word[15]. As we know that the etymology of the Greek word Cryptography which specifies the Secret Writing[15]. The study of Secret Writing is called Cryptology. The elliptic curve cryptography was discovered in 1985 by Neal Koblitz and Victor Miller[14]. The elliptic curve cryptosystems are Public key mechanisms which provide the same functionality in RSA Schemes. The DSA and RSA algorithms security is based on the hardness of a different problem, namely elliptic curve discrete logarithm problem (ecdlp) [14]. Presently the best algorithms known to solve the ecdlp have fully exponential running time,in contrast to the sub exponential-time algorithms known for the integer factorization problem. As we know that ECC (Elliptic Curve Cryptography) is mainly used to solve a diverse set of problems [14]. One such problem is the congruent number problem which asks for a classification of the positive integers occurring as the area of some right angled triangle, whose sides are rational numbers [14]. The another example of Elliptic Key Cryptography is proving of Fermat's last theorem which specifies that the equation $x^n+y^n=z^n$ does not contain non-zero integer solutions for x,y and z when the integer n is greater *than 2[2][3][14]*. The Elliptic Curve Cryptography is used to implement the Mathematical modeling of Bucket Brigade attack (Man in the Middle attack) (Woman in the Middle attack) [1][2].

Introduction to Bluetooth Technology

Bluetooth is a methodology for short range Wireless data and real time two way voice transfer cooperating data rates up to 3 Mb/s.Bluetooth is a technology defined by Bluetooth Special Interest Group(BSIG). Bluetooth is a radio frequency mechanism which operates in the unlicensed 2.4GHz ISM Band. It was designed by Ericsson as a substitute for the RS-232 data cable and is meant for short distance data exchange usually 10 meters. But there are variants for a small 1 meter range and for 100 meter range. Bluetooth is specified by Bluetooth special

*✉ *Corresponding author:* **Ahmad Hweishel A. Alfarjat**
Department of Human Physiology, Gregory University, Uturu, Abia State, Nigeria

interest group A Group created by a companies such as Intel, Nokia, Microsoft, Motorola, Ericsson, Toshiba and Lenovo. Bluetooth chip costs a few costlier and are very popular in an instruments over the world. There are 3 different kinds of Bluetooth radios. Basic Rate radio(BR/EDR) which is the most widely used radio in Bluetooth technology. Low energy radio(Ler) is also a latest added radio technology into a Bluetooth. The protocol is divided into a controller part and a Host Part.

Bluetooth Security Architecture

Security in Bluetooth can be considered as a mechanism of defense against willful acts of smart adversaries people. The word security either implicitly or explicitly protection to some extent. The word protection is defined as the defense against random events such as accidents and failures. We also took an opportunity to swap safety and protection in our research and thesis work. The security design mainly involves defining a sequence of procedures for the cooperation of algorithms, protocols and their usage. As discussed above one more important aspect of security development specifically in Bluetooth is to design an efficient implementation of opted procedures consisting of their basic elements and interaction. There are so many similarities between WLAN and WPAN therefore they can merge into an individual technology known as WLANs. This section clearly explores how security issues have been considered in present public Bluetooth specifications such as blu01,blu03,blu04a,blu07a,1blu99a,blu99b etc. The fundamental Bluetooth specifications are genuinely implemented by the user who resolves how a Bluetooth instrument it's connect ability and discoverability preferences. The various categories of connect ability and discoverability strengths can be chunked into three different parts such as

1. *Silent Preference*: In Silent preference the instrument will never accepts any connections. The Bluetooth simply oversees the traffic.
2. *Private Preference*: In this phase the instrument cannot determines non-determinable instrument connections are only accepted when the Bluetooth Instrument Address(BI_ADDR) of the device is known to the perspective Master. To the best of our knowledge BI_ADDR is a 48 bit address which globally and uniquely specifies a Bluetooth instrument.
3. *Public Preference*: In a Public preference the instruments can be ascertained and connected to therefore it also called an ascertained apparatus.

The Bluetooth equipment at a time broadly implements the following four different categories of security preferences such as Non-Secure, Service-level enforced security preference, Link level enforced security preference, service level enforced security preference. We have also taken an opportunity to explore all the four different preferences as follows.

1. *Non-Secure Phase*: As we Know in this type of phase Bluetooth does not initiate any security measures.
2. *Service level enforced security Phase*: In this phase two different instruments can authenticate a non secure ACL(Asynchronous Connection less) link. The various security principles such as Integrity, Non repudiation, Authentication, Authorization, Encryption and Decryption are initiated when a L2CAP CO(Logical Link Control and Adaptation Protocol Connected Oriented) or an L2CAP CL channel request is made.
3. *Link level enforced security mode*: Security procedures are really initiated when an ACL link was constructed.
4. *Service level enforced security Phase*: This phase is exactly similar to Phase-2 except that only Bluetooth devices utilizing SSP can use it. i.e only Bluetooth 2.1+EDR instruments can use this security phase

Related Works

For the last twenty five years,many researcher's, scientists and authors have been actively engaged in proposing, exploiting and developing a new flexible security issues of Bluetooth using Elliptic Curve Cryptography. So Many authors also have exploited the strength of Elliptic Curve Cryptography and came up with implementation details of Public key cryptography such as authentication, digital signature, Key agreement, Encryption and Decryption. Public Key Cryptography was conceived in 1976 by whitefield Diffie and Martin Hellman. The first practical realization followed in 1977 when Ron Rivest, Adi Shamir, and Len Adleman(RSA) proposed their well known RSA Cryptosystem in which security is based on the intractability of the integer factorization problem. Elliptic Curve Cryptography was invented by Neal Koblitz and Victor Miller in 1985. El Gamal first described how this problem may be utilized in Public Key Encryption and digital signature schemes[7]. Koyama *et al* have proposed elliptic curve analogues of the RSA cryptosystem [20]. Kurosawa, Okada *et al* subsequently showed that these elliptic curve analogues do not have any significant advantages over their RSA counterparts [19]. Charlap and Robbins showed elementary self-contained proofs for some of the basic theory. Hermelin.M., Nyberg.K.(1999) theoretically proved that Bluetooth stream cipher with 128 bit key can be wrecked in $O(2^{64})$ steps. Canniere *et al* (2001) had proved that E0 stream cipher of Bluetooth has some security imperfections. Jakobsson.M. and Wetzel.S.(2001) [17] for the first time formulated MITM attack on Bluetooth for version 1.0B[17]. Victor S.Miller explain the use of elliptic curve cryptography in a Cryptographic methodology. Neal Koblitz, Alfred Menezes and Scott Vanstone extended the technique of discrete logarithmic problem used in Public Key Cryptography of Diffie Hellman to elliptic curve group. Darrel hankerson, Alfred menezes and scott Vanstone also explained in detail about elliptic curve arithmetic, kinds of cryptographic protocols and implementation issues. Jorko Teeriaho also implemented ECC-DH key swapping algorithm, ECC encryption, Elliptic Curve Digital Signature using mathematica. Min-Shiang Hwang, Cheng Chi Lee, Ji Zhe Lee have proposed the security issues of Bluetooth Piconets using elliptic curve cryptography. They have proposed two requirements such as Authentication and a Privacy for the security issues of Bluetooth using Elliptic Curve Cryptography. Hanumanthappa.J. and Ahmed Hweishel A.Alfarjat have proposed investigated security features of Bluetooth using Elliptic Curve Cryptography(ECC). We have also proposed Bucket Brigade Attack on Bluetooth security using Elliptic Curve Cryptography(ECC). We have computed the various Performance metrics such as Throughput, End-to-End Delay

(EED) and Packet Loss Rate (PLR) using ECC. Our research work also concentrates on algorithms for wireless LAN for secured transmission using Elliptic Curve Cryptography.

Proposed Methodology

Bluetooth and Digital Signature Based Elliptic Curve Cryptography

As we know that Cryptography is the conversion of Plain Text Message to Cipher Text Message and Vice Versa. Cryptography also secures Plain Text Message and Cipher Text Message and immune from intruders and Crackers. The Public key Cryptography is one which is playing a crucial role in forwarding information via an Internet and an E-Commerce. The Bluetooth system used in Frequency Hopping Spread Spectrum technique and split the band into several hop channels. The Bluetooth devices are connected with each other in a point to point manner or in multi-points.

The Elliptic Curve Digital Signature Algorithm(ECDSA) is the elliptic curve analogue of Digital Signature Algorithm (DSA)[17][19]. It was accepted as an American National Standard Institute standard in the year 1999 and was also accepted in 1998 as an Standard of Inter National Organizations of Standard(ISO)[17]. Elliptic Curve based Digital Signature was first proposed in 1992 by Scott Vanstone in response to National Institute of Standards and Technology(NIST) request for public comments on their first proposal for DSS[19][20]. The elliptic curve based Digital Signature was also accepted by IEEE in the year 2000 [18][19][20]. Elliptic Curve Cryptosystems are invented by Neal Koblitz [21] and Victor Miller [22] in 1985. The elliptic curve cryptography can be seen as an elliptic curve analogues of the Older Discrete Logarithm(ODL) cryptosystems in which the subgroup of Z_p^* is substituted by the sequence of points on an elliptic curve over a finite field.The mathematical foundation to the elliptic curve cryptography is computational intractability of elliptic curve discrete logarithm problem(ECDLP).

Elliptic Curve Cryptography is a relative of Discrete Logarithm Cryptography(DLC).The E over Z_p is specified in Cartesian Coordinate System by using an equation of the type such as:$y^2=x^3+ax+b$ ---------(i)

where a,b ε Z_p and $4a^3+27b^2 \neq 0 \pmod p$ with a special point such as o(the point at an infinity).The equation (i) can be also called as Weirstrass equation.

The set E(Z_p) which consists of all points(x,y),xε Z_p ,yεZ_p which satisfies the criteria of equation (i) with O. Each value of a and b specifies the different an elliptic curve. The public key is a point on the curve and private key is a random number. The value which belongs to public key can be taken by multiplying the private key with a generator point G in the curve. Elliptic Curve Digital Signature Authentication (ECDSA) are stronger and ideal for constrained environments like smart cards due to smaller bit size whereby reducing processing overhead. In general the present day Digital Signature Schemes are broadly classified into two types such as RSA based Digital Signature Scheme(RSADSS) and Discrete Logarithm Based Schemes(DLBS). Digital Signature Techniques can be used to provide the following basic cryptographic services such as

Non-Repudiation: The Process of preventing an entity from denying previous actions or commitments[26].

Data-Integrity: Ensuring that data has not been updated by an unauthorized means **B** should be able to detect when data sent by **A** has been changed by E[26].

Data Authentication: The mechanism of Corroborating the identity of an entity-**B** should be convinced of the identity of other communicating entity[26].

Data origin Authentication:The technique of corroborating the source of data -B should be able to verify that data purportedly sent by A indeed originated with A [26].

Discrete Logarithms

Discrete logarithms are ordinary logarithms involving group theory. An ordinary logarithm $\log_a(b)$ is a solution of the equation $a^x=b$ over complex or real numbers. Similarly if g and h are components of a finite cyclic group G then a solution x of the equation $g^x=h$ is called discrete logarithm to the base g of h in the group G i.e $\log_g(h)$. A group with an operation * is defined on pair of elements of G[26].

Finite Field in ECC

A finite field in ECC consists of a finite set of elements with two binary operations called addition and Multiplication. It satisfies certain arithmetic properties [26]. The order of a finite field is the total number of elements lies in a field [26]. There exists a finite field of order q if and only if q is said to be prime power. When q acts like a prime power then there is essentially only one finite field of order q which is already specified by F_q.let us consider an equation.

$q=p^m$ -------(ii) where p is a prime and m is a positive integer then p is specified as salient feature of F_q and m is called an extension degree of F_q[26].

Operations of Security issues of Bluetooth using Digital Signature and ECC in a Finite Field.
One of the crucial operation in Point Multiplication is secured by two important ECC operations such as

Point Sum(Addition):Point sum is a mechanism of summing two different points H and J to get another point K.
therefore K=H+J------(iii)(which requires 1 inversion and 3 multiplication operations).

Point Doubling*:Point doubling is the process of adding a point H to itself. i.e K=2H*----(iv*) which requires 1 inversion and 4 multiplication operations.*

Implementation of Security issues of Bluetooth and Digital Signature Based Elliptic Curve Cryptography.

The implementation details of security issues of Bluetooth and Digital Signature based ECC has the following group of operations such as Key Creation, Signature Creation and Signature Verification. The security issues of Bluetooth and Digital Signature Authentication based ECC is implemented over elliptic curve P-192 as mandated by ANSI X.962 in NS2. As we know that DSA was proposed in August, 1991 by US

National Institute of Standards and Technology (NIST) and was specified in a U.S.Government Federal Information Processing Standard such as Digital Signature Standard (DSS). The Elliptic Curve Digital Signature Algorithm (ECDSA) is an elliptic curve analogue of DSA. ECDSA is a standard and one of the most widely used standard scheme in FIPS-186-2, IEEE 1363-2000, ANSI X.962 and ISO/IEC15946-2 standard.

Algorithm-1:*ECDSA Key Creation Algorithm*

Input Domain Parameters H:(q,FR,S,a,b,P,n,h),d is a Private Key and m is a message.
Output:Signature(r,s)

1. Choose $k\varepsilon_R[1,n-1]$
2. Calculate kP=(x1,y1) and translate x1 to an integer x1.
3. Compute r=x1mod n. if r=0 then go to step-1
4. Calculate e=H(m)
5. Calculate $s=k^{-1}$ (e + dr) mod n. if s=0 go to step-1.
6. return(r,s)
   Algorithm-2:*ECDSA Signature Verification*

Input:Domain Parameters D=(q,FR,S,a,b,P,n,h),Q=Public Key,message=m,Signature(r,s).

Output:Accept or Reject the Signature.

1. Let us verify that r and s are integers in the interval[1,n-1] .if any verification fails then return("Reject the Signature").
2. Calculate e=H(m)
3. Compute $w=s^{-1}$ mod n
4. Calculate u1=ew mod n and u2=rw mod n
5. Calculate X=u1 P + u2 Q
6. if $X=\infty$ then return the ("Reject Signature")
7. Convert the x- coordinate x1 of X to an integer x1;calculate v=x1 mod n .
8. if v=r then return("Accept the Signature") else return("Reject Signature").

Security issues of Bluetooth using Digital Signature and Elliptic Curve Cryptography(SBECDSA).

In this paper we have conducted an experiment to calculate Security issues of Bluetooth using Digital Signature Technique and an Elliptic Curve Cryptography. The Fig-1 Illustrates Signature Creation and Verification in Security issues of Bluetooth using Digital Signature and an Elliptic Curve Cryptography.

We are using three different types of algorithms such as Digital Signature Authentication (DSA), RSA (Rivest, Shamir, Adleman), Elliptic Curve Digital Signature Authentication (ECDSA) in Digital Signal Certificates. All the three different algorithms such as DSA, RSA and ECDSA are used for simulation purpose using ns2 simulator. RSA, DSA and ECDSA are used with SHA-1,MD-5,ECIES and RSA. As we know that ECIES and RSA algorithms are used for Public Key Encryption which supports for Asymmetric Key Cryptography and SHA-1 and MD-5 are mainly used to produce hash of a message. A general kind of Hash algorithm is used is SHA-1. In order to verify a signature s for message m the signature first be encrypted using the author's public key(e,n). The hash function(h) is took from the equation such as $h=s^e$ mod n-(v).

Simulation Results and Discussions of SBECDSA

In order to implement the security issues of Bluetooth and Digital Signature Authentication (DSA) using Elliptic Curve Cryptography is simulated by the wired/wireless based simulator such as ns2. The wireless application feature of security issues of Digital Signature and Bluetooth based ECC(SBECDSA) is implemented by the **ISO/OSI** reference model bottom most layer such as Physical layer and MAC layer are added in wireless extension of ns2. The maximum speed of the mobile host is 40m/s(milli seconds) and a pause time of 1000s. The connection oriented protocol such as **TCP** and Connection less protocol like **UDP** are mainly used with constant bit rate traffic with a different size packets such as 32,64,128,256,512,768 and 1024 Bytes etc.

Calculation of Throughput for security issues of Bluetooth and Digital Signature Authentication(DSA) using Elliptic Curve Cryptography using Fixed Size Text and Variable Size Text.

In our research paper simulation is conducted by Matlab Version 12 on Acer Laptop with system configuration of i8 processor @2.20 GHz and 10GB Ram using 512 bit key length Department of Electronics and Communication Engineering, PESCE, Mandya recommended Elliptic Curve Parameter[16]. The input parameters for our encryption process are as follows.

The Input text is hanums and the key size is 1. Whenever key size is 1 we will get an equivalent cipher text such as ibmvnt. The Process of converting plain text to cipher text is called encryption.

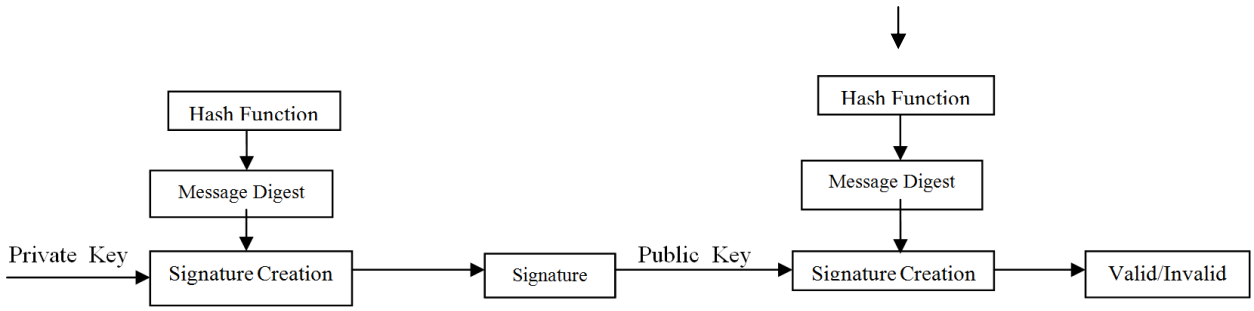

Fig.1 Signature Creation and Verification by using Elliptic Curve and Digital Signature based Bluetooth Security issues.

Table1 Encryption and Decryption with Encryption time, Decryption time, Mapping and Look table requirement (For Fixed Size Text).

Sl.No	Plain text content	Cipher text content	Key Size	Encryption time	Decryption time	Mapping Necessary	Lookup table necessary
1	hanums	ibmvnt	1	0.1ms	0.1 ms	Not required	Not required
2	hanums	jcpwou	2	0.2 ms	0.2 ms	Not required	Not required
3	hanums	kdqxpv	3	0.3 ms	0.3 ms	Not necessary	Not necessary
4	adarsh	ehevwl	4	0.4 ms	0.5ms	Not necessary	Not necessary
5	123456	67891011	5	0.5ms	0.75ms	Not necessary	Not necessary
6	abcdef(Based on ASCII value).	979899100101102	1	0.75ms	0.80ms	Not necessary	Not necessary

The encryption and Decryption process with variable length characters using an appropriate encryption time and Decryption time is explained very beautifully in Table- 2.

Table 2 Encryption time and Decryption time using variable length character

Sl.No	Plain text content	Cipher text content	Key Size	Encryption time	Decryption time	Mapping Necessary	Lookup table necessary
1	hanums	ibmvnt	1	0.1ms	0.1 ms	Not required	Not required
2	computer	enorwvgt	2	0.25 ms	0.28 ms	Not required	Not required
3	Abraham lincon	desdkdp klqfrq	3	0.48 ms	0.56 ms	Not necessary	Not necessary
4	adarsha	ehevwle	4	0.78 ms	0.65ms	Not necessary	Not necessary
5	1234567	6789101112	5	0.5ms	0.75ms	Not necessary	Not necessary
6	abcdefghijk(Based on ASCII value).	9798991001011021 03104105106107	1	0.98ms	0.94ms	Not necessary	Not necessary

The Graph-1 shows the encryption and Decryption time when we are using Fixed Size Character with different Key Sizes(Refer Table-1)in Bar Chart Format.

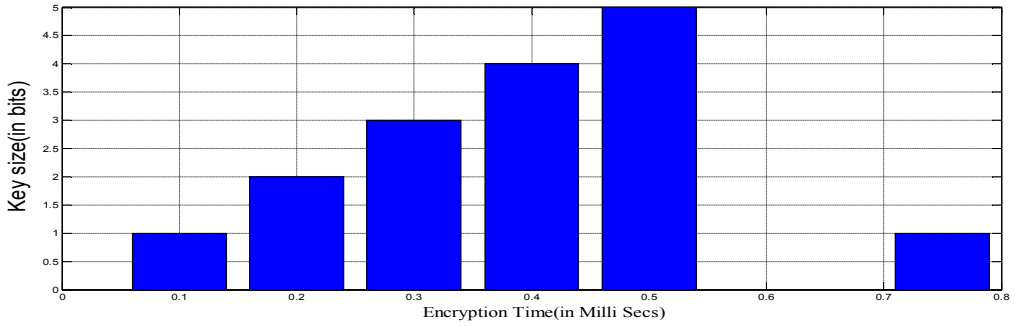

Fig.1 The value of Encryption time with respect to Key Size using Bluetooth based ECC(Fized Size Char).

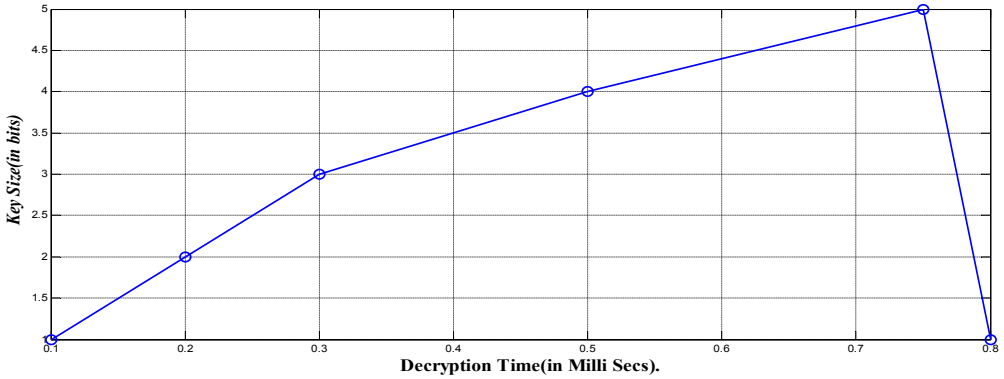

Fig 2 Comparison and Contrast between Decryption time wrt to Key Size in Bluetooth based ECC(Fized Size Char).

The various types of parameters required for encryption algorithm are i)Plain text ii)Key value iii)Encryption algorithm.The input parameters necessary for the Decryption Process are i)Cipher text ii)Key value iii)Decryption algorithm. The Table-1 which indicates the corresponding Cipher text (Modified Text) with an appropriate Plain Text (Original Text).

CONCLUSIONS

In this research article we have presented security issues of Bluetooth using Digital Signature based Elliptic Curve Cryptography(SBECDSA). In addition we have also proposed how to improve the security issues of Bluetooth using Digital Signature and an Elliptic Curve Cryptography(ECC). As we know that the security of ECC algorithm is based on Elliptic

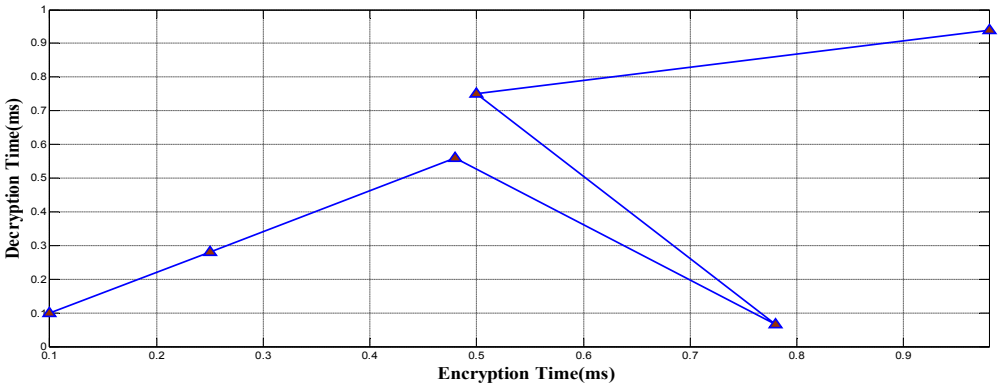

Fig.3 Comparison and Contrast between Encryption time and Decryption time in Bluetooth based ECC(Variable Length Char).

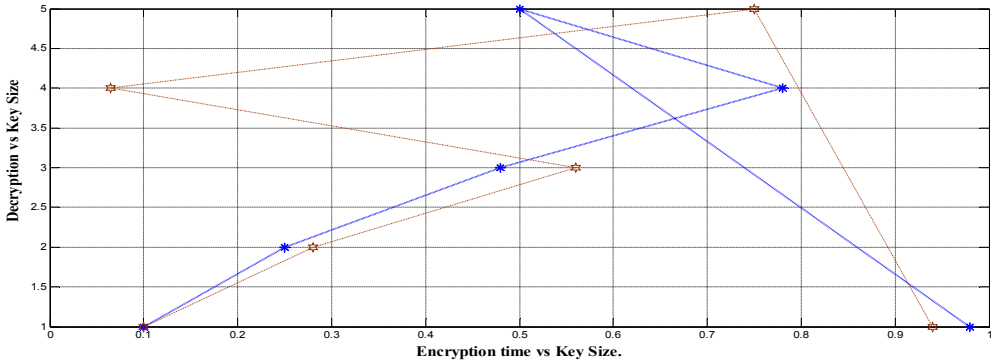

Fig 4 Comparison and Contrast between Encryption wrt Key size and Decryption time wrt Key Size using Variable Character in Bluetooth based ECC.

Curve Discrete Logarithm Problem(ECDLP) rather than integer factorization problem. Security issues of Bluetooth and Digital Signature Based Elliptic Curve Cryptography are totally simulated using Matlab.Our Matlab simulation results shows that Encryption Process(time) wrt Key Size take lesser time as compared to Decryption time wrt Key Size. The Time complexity of Bluetooth based Elliptic Curve Cryptography using $o(n^4)$ using Miller Rabin Primality technique.Broker and Stevenhagen also created an algorithm to compute time complexity and overall time complexity is $o(n^3)$. Finally we can conclude that encryption is a beautiful process to send a text message from one source location to another destination location using Digital Signature based Bluetooth and ECC.

References

1. Hanumanthappa.J., Ahmed Hweishel A.Alfarjat, Prof.H.S.Sheshadri, ”A Mathematical model to the Security issues of Bluetooth using Elliptic Curve Cryptography, *International Journal of Computer Applications*(*IJCA)*(0975-8887),Vol.161 No.8,March.2017.
2. Hanumanthappa.J.,Ahmed Hweishel A.Alfarjat,”A Survey over the Security Issues of Bluetooth Using Elliptic Curve Cryptography”, *IJCA* (0975-8887),Vol.150,No.8.,Sept-2016.
3. Andrew S.Tanenbaum, "Computer Networks", Pearson Education Inc, FourthEdition, 2003.
4. D.Abramovich. Formal Finiteness and the torsion conjecture on elliptic curves. A Foot note to a paper:”Rational torsion of prime order in elliptic curves over number fields.
5. T.M.Apostol.Introduction to analytic number theory. Springer-Verlag, Newyork, 1976, Undergraduate Text in Mathematics.
6. A.O.L.Atkin and F.Morain.Elliptic curves and Primality proving. *Math Comp*.,61(203):29-68, 1993.
7. D.Bernstein and T.Lange. Faster addition and doubling on elliptic curves. In Advances in Cryptology, ASIACRYPT, 2007, vol 4833 of Lecture notes in Comput.Sci.,pages 29-50.Springer Berlin, 2007.
8. F.Brezing and A.Weng. Elliptic curves suitable for pairing based cryptography. Des codes Cryptogr., 37(1):133-141, 2005.
9. J.W.S.Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc*.,41:193-291,1966.
10. A.Wiles. Modular Elliptic Curves and Fermat’s Last Theorem. *Ann of Math*.(2),141(3):443-551,1995.
11. W.Trappe and L. Washington, Introduction to Cryptography with coding theory,(2nd ed.). Prentice Hall, Upper Saddle River, NJ, 2006.
12. N.P.Smart. The Discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology*,12(3):193-196,1999.
13. J.H.Silverman and J.Suzuki, Elliptic Curve Discrete logarithms and the index calculus. In Advances in Cryptology-ASIACRYPT’98,vol,1514 of Lecture notes

in Comput. Sci, pages 110-125, Springer-Verlag, Berlin,1998.
14. Darrel Hankerson, Alfred Menezes, Scott Vanstone,"A Guide to Elliptic Curve Cryptography",Springer.
15. Behrouz Forouzan, TCP/IP Protocol Suite, Tata Macgrawhill Publications.
16. Joseph.H.Silvermann, The Arithmetic of Elliptic Curves,Second Edition, Springer.
17. Johnson D.B., Menezes A.J.,2007, Elliptic Curve DSA(ECDSA): An Enhanced DSA. Scientific Commons.
18. G.V.S.Raju, R.Akbani, 2003, Elliptic Curve Cryptosytem and its application. in Proceedings of the 2003 IEEE International Conference on Systems Man and Cybernetics (IEEE-SMC),1540-1543.
19. J.J.Botes,W.T.Penzhorn,1994,An Implementation of Elliptic Curve Cryptosytem Communications and Signal Processing,COMSIG-94,in Proceedings of the 1994 IEEE South African Symposium.
20. Vanstone S.A,1992.Responses to NIST's proposal communications of the ACM,35,50-52.
21. N.Koblitz, 1987, Elliptic Curve Crypto systems, Mathematics of Computation, 48,203-209.
22. Miller.V.,1985, Use of Elliptic Curve in Cryptography CRYPTO 85.
23. G.Nils, Arun.P. "Comparing an elliptic curve cryptography and RSA on 8-bit CPU's", in proceedings of 6th intl workshop,USA,pp.119-132,2004.
24. T.ElGamal, A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms, IEEE Transactions Information Theory IT-31(1985 July) 469-472.
25. W.J.Caelli, E.P.Dawson, S.A.Rea, Pki, an elliptic Curve Cryptography and Digital Signatures Computers and Security 18(1),1999,47-66.
26. Darrel Hankerson, Alfred Menezes, Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer, 2003.
27. Nils.G. ArunP, Arvinder Pal.W., Hans.E., Sheueling.S., "Comparing elliptic curve cryptography and RSA on 8 bit CPU's, in Proceedings of the 6th International Workshop, Cambridge, USA, pp.119-132, 2004.

****