Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.1 No.1, 2012, pp.37-42

DOI: https://doi.org/10.51983/ajcst-2012.1.1.1675

An Efficient Mobile Authentication Protocol for Wireless Communications Using Rabin PublicKey Cryptosystem

Karthiyayini and Karthikeyan
Sethu Institute of Technology, Virudhunager, Tamil Nadu, India
E-mail: bublykarthi@gmail.com

***Abstract* - The past few years have witnessed an explosive growth in the use of mobile devices as the enabling technology for accessing Internet based services, as well as for personal communication needs in networking environments. Most studies indicate that it is impossible to utilize strong cryptographic functions for implementing security protocols on mobile devices. Our work refutes this. Specifically, we present a performance analysis focused on the most commonly used cryptographic protocols for mobile applications and we proposed provably secure authentication protocol that is more efficient than any of the existing authentication protocol in the literature.**

The increasing progress in wireless mobile communication has attracted an important amount of attention on the security issue. To provide secure communication for mobile devices, authenticated protocol is an important primitive for establishing trusted connection. In this work, we focus on an important constraint of such devices – battery life – and examine how it is impacted by the use of security protocols. We believe such investigations to be an important first step toward addressing the challenges of energy-efficient security for battery-constrained systems. Our result shows that proposed authentication protocol provides a better security guarantee and incurs much less energy consumption than the existing authentication protocols. Finally, performance analysis will show that compared with existing authentication protocols, our proposed scheme is to be more simple, secure and efficient.

***Keywords*—Security, Cryptographic algorithms, RSA, Elliptic Curve Cryptography, Rabin Public-key Cryptosystem, J2ME**

1. Introduction

Nowadays, handheld devices (i.e., cellular phones and PDAs) are popularly and widely used by people and many mobile applications, such as wireless internet services, mobile access services and mobile e-commerce. In an increasingly interconnected world, the interactions among mobile devices, systems, and people are growing rapidly. Accessing the internet has become mandatory in many professions. Now mobile phone is also replacing the laptop by enabling internet access through the mobile phone. This has given way to service providers to provide various internet services. Mobile banking and stocks updates have become a common affair for the mobile phone user.

Secure and fast transmission of sensitive digital information over wireless channels has become increasingly very important. The use of public key cryptography consumes a significant portion of the overall system resource. The computation complexity of asymmetric key based operations is negligible, but the key management for asymmetric key based system is complicated, and is always subject to attacks by adversaries.

Portable communication system permits mobile users to enjoy global roaming services, and so the system is useful for the conversations conducted over wireless networks [1], [6]. In wireless networks, mobile users send and receive packets by wireless, and thus it is easy for anyone to eavesdrop on communicating messages transmitted over wireless networks. Hence, portable communication systems have more security vulnerabilities than wired systems. For securing the systems, several protocols have been proposed [1], [2], [3], [4], [5], [6], [7], [8].

For secure roaming services, we need many security features such as the secrecy, authenticity, integrity, user privacy and non-repudiation. To achieve the goals, we use cryptographic algorithms such as secret-key systems and public-key systems. Among existing protocols, the great parts of them have been proposed based on secret-key systems since mobile devices have limited capacity. However, secret-key systems cannot provide the non-repudiation.

Hence, we should use public-key systems when the property is inevitably required. When we use public-key systems, the cost of underlying mathematical operations is one of difficulties. However, in these days, mobile devices have more computing power than before, and so it is possible to implement public-key systems on mobile devices. For critical commercial and military applications we propose a secure authentication scheme which incurs high level of security and less time consumption by using Rabin Public-key Cryptosystem.

II. Related Work

To give more prospective about the performance of the compared algorithms, this section discusses the results obtained from other resources.

A study in [9] is conducted and observed that this paper instigate the fast developing cryptography researchers and to increase the security development in the field of information security. ECC's uses with smaller keys to provide high security, high speed in a low bandwidth. The security level which is given by RSA, can be provided even by smaller keys of ECC.

In [10], ECC is a promising candidate for the next generation public key cryptosystem. Although ECC's security has

not been completely evaluated, it is expected to come into widespread use in various fields because of its compactness and high performance when it is hardware-implemented. ECC has been proven to involve much less overheads when compared to RSA.

A study in [11] is conducted and observed that the existing authentication protocols, based on RSA asymmetric cryptography are not suitable for such devices due to their confines in computing power, memory capacity, key sizes and cryptographic support. For that reason, an efficient protocol for resource constrained platforms that attain a level of security similar to the one achieved by the protocols in use today is designed and implemented. Elliptic curve asymmetric cryptography and the results demonstrate that the performance achieved is good in contrast to RSA.

In [12], The use of mobile devices demands to accommodate limitations on power and bandwidth, and to provide an adequate level of Security. The ECC used for such constrained environment. Its security comes from the elliptic curve logarithm, which is the DLP in a group defined by points on an elliptic curve over a finite field. This results in a dramatic decrease in key size needed to achieve the same level of security.

In [13] , it highlights that the existing authentication protocols, based on RSA asymmetric cryptography, are not appropriate for such devices due to their limitations in computing power, memory capacity, key sizes and cryptographic support. This work shows that it is possible to implement the authentication protocol using HECC in resource constrained mobile devices with reasonable performance compared to RSA. Protocols based on this HECC asymmetric cryptography can be directly used in such devices. This paper addressed the design of a protocol based on HECC asymmetric cryptography. Furthermore, an implementation for J2ME Wireless Tool Kit 2.5.1 is also described.

A study in [14] is conducted for different popular secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [15].

In [16] a study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of measuring the performances of encryption process at the programming language's script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption Performance Evaluation of Symmetric Encryption Algorithms versus Web browser.

It was concluded in [17] that an efficient authentication scheme, which is suitable for mobile devices. It uses an elliptic-curve-cryptosystem for mobile station authentication; this scheme enjoyed both computation efficiency and communication efficiency as compared to known mobile authentication schemes. In this paper, a novel and efficient mobile authentication scheme is proposed, and its security property has been analyzed. The scheme requires one scalar point multiplication operation and two short messages on mobile stations for each session establishment after the initial one-time delegation key verification. It is well suited for low-power mobile devices in wireless networks.

III. Preliminaries

In this section, we provide a brief overview of commonly employed security concepts and terminology. We begin by defining the widely used terms in the fields of cryptography and network security, and follow it by describing different kinds of protection measures, referred to as security objectives, desired in practical applications with a need for security. The concern for security in practice is addressed by choosing a security protocol, which achieves all the required security objectives. Security protocols realize the security objectives through the use of appropriate cryptographic algorithms.

A. Basic Security Terminologies

A message present in a clear form, which can be understood by any casual observer, is known as the plaintext. The encryption process converts the plaintext to a form that hides the meaning of the message from everyone except the valid communicating parties, and the result is known as the cipher text. Decryption is the inverse of encryption, i.e., the cipher text is mapped back to its corresponding plaintext. The processes of encryption and decryption are parameterized on a quantity known as the key, which is ideally known only to the legitimate communicating parties. Since the strength of a security scheme depends on the secrecy of the key(s) used, it is highly imperative that the communicating parties take utmost precaution to safeguard the keys belonging to them.

A security protocol formally specifies a set of steps to be followed by two or more communicating parties, so that the mutually desired security objectives are satisfied. It is assumed that the parties involved have the means to execute the various steps of the security protocol. The term security an objective is often used to denote the security services or functionality required in a system or network to protect sensitive data and/or identity. The four main security objectives include:

1) Confidentiality : This is the most popular requirement of security protocols, and it means that the secrecy of the data

being exchanged by the communicating parties is maintained, i.e., no one other than the legitimate parties should know the content of the data being exchanged.

2) Authentication : It should be possible for the receiver of a message to ascertain its origin, i.e., to ensure that the sender of the message is who he claims to be, and the message was sent by him. This prevents a malicious entity from masquerading as someone else.

3) Integrity : It provides a means for the receiver of a message to verify that the message was not altered in transit. This is necessary to prevent a malicious entity from substituting a false message in the place of a legitimate one or to tamper with the original message.

4) Non-repudiation : The sender of a message should not be able to falsely deny later that he sent the message, and this fact should be verifiable independently by an independent third-party without knowing too much about the content of the disputed message(s). This feature has important applications in the E-commerce domain, where it is common for users to send online messages authorizing the intended recipients of the messages to perform important actions on their behalf.

Security objectives thus provide trust, analogous to that present in face-to-face meetings, to the "faceless" interactions on the Web (or any data network). They are realized through the use of cryptographic algorithms (also referred to as cryptographic primitives), which are divided into three categories depending on their characteristics. These categories are:

5) Symmetric algorithms : These algorithms use the same key for encryption and decryption. They rely on the concepts of "confusion and diffusion" to realize their cryptographic properties and are used mainly for confidentiality purposes.

6) Asymmetric algorithms : These algorithms use different keys, known as the public key and the private key, for encryption and decryption, respectively. They are constructed from the mathematical abstractions known as "trapdoor one-way functions," which are based on computationally intractable number-theoretic problems like integer factorization, discrete logarithm, etc.. They are primarily used for authentication and non-repudiation.

B. Rivest, Shamir and Adleman (RSA)

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. The RSA algorithm involves three steps: key generation, encryption and decryption. Depending on the security objectives needed by a transaction among various parties and the constraints imposed by them, a security protocol is devised by composing a formal sequence of steps and deciding which algorithms should be used for carrying out each step.

RSA Algorithm (Rivest, Shamir & Adleman)

Step 1 : Select two large primes - p, q

Step 2 : Compute their system modulus N=p.q where ø(N)=(p-1)(q-1)

Step 3 : public encryption key: KU={e,N} where $1<e<ø(N)$, gcd(e,ø(N))=1

Step 4 : private decryption key: KR={d,p,q} where e.d=1 mod ø(N) and $0\leq d\leq N$

Step 5 : Encrypt a Message M, $C=M^e \bmod N$

Step 6 : Decrypt the cipher text C, $M=C^d \bmod N$

C. Elliptic Curve Cryptography (ECC)

In ECC Algorithm (Elliptic Curve Cryptography)

An elliptic curve is a plane curve defined by an equation of the form $Y^2=x^3+ax+b$

Both parties agree to some publicly-known data items

Step 1 : select a suitable curve Ep(a,b)

Step 2 : select base point $G=(x_1,y_1)$ with large order n where nG=O(point of infinity)

Step 3 : A & B select private keys $n_A<n$, $n_B<n$

Step 4 : compute public keys: $P_A=n_AG$, $P_B=n_BG$

Step 5 : compute shared key: $K=n_AP_B$, $K=n_BP_A$

D. Encode and Decode

Step 1 : Encode any message M as a point on the elliptic curve Pm

Step 2 : Encrypt the message P_m : $C_m=\{kG, P_m+kP_B\}$, k random int number $1<k<p-1$

Step 3 : To decrypt, computes the product of the first point from Pm and his private key, n $n_B * (kG)$

Step 4 : Takes this product and subtracts it from the second point from P_m

$(P_m + kP_B) – [n_B(kG)] = P_m + k(n_BG) – n_B(kG)= P_m$

E. Proposed Authentication Algorithms

Rabin Cryptosystem is asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. Our Scheme has three phases

1) Key Generation Phase

The system S creates a Key pair, by the following steps

Step 1: Choose two large distinct primes *p* and *q*. One may choose p=q=3(mod 4) to simplify the computation of square

roots modulo p and q.

Step 2: Compute n=*pq*

Step 3: S 's public key is *n* and S 's private key is (*p*, *q*)

2) Encryption Phase

The system S creates cipher text by the following steps

Step 1 : Receives the key pair from key generation phase.

Step 2 : Calculate cipher text C= m^2 mod n.

Step 3 : Generated cipher text sends to the remote system.

3) Authentication Phase

Step 1: Receives the request C and checks the validity.

Step 2: with the help of Chinese remainder theorem, the four square roots m1, m2,m3 and m4 are calculated.

Step 3: Check the received C value for presence of anyone of m1, m2, m3 and m4. If the value of C is equal to any of the square root value, then accept the login request.

Step 4: Otherwise reject the request.

Step 5: The four square roots are in the set {0,...,n − 1}):

Step 6: One of these square roots is the original plaintext.

F. Rabin Cryptosystem - Advantages

The Rabin cryptosystem is an asymmetric cryptographic technique, whose security, like that of RSA, is related to the difficulty of factorization. However the Rabin cryptosystem has the advantage that the problem on which it relies has been proved to be as hard as integer factorization, which is not currently known to be true of the RSA problem. The Rabin cryptosystem was the first asymmetric cryptosystem where recovering the entire plaintext from the cipher text could be proven to be as hard as factoring.

Accessing and checking the authentication of a user is important for any types of network–based applications. Recently, more number of schemes is proposed. Still we do not have a scheme, which provides a high security. In this paper we propose a new authentication scheme using Rabin public–key cryptosystem.

G. Evaluation of the algorithm

1) Effectiveness

If the plaintext is intended to represent a text message, guessing is not difficult. However, if the plaintext is intended to represent a numerical value, this issue becomes a problem that must be resolved by some kind of disambiguation scheme.

2) Efficiency

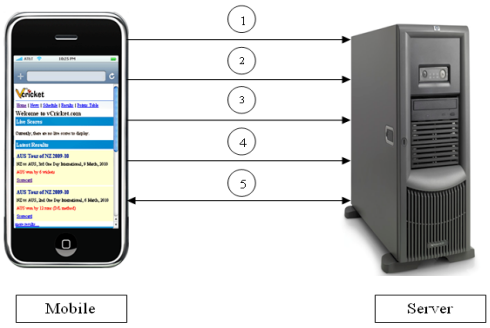
For encryption, a square modulo n must be calculated. This is more efficient than RSA, which requires the calculation of at least a cube. For decryption, the Chinese remainder theorem is applied, along with two modular exponentiations. Here the efficiency is comparable to RSA.

3) Security

The great advantage of the Rabin cryptosystem is that a random plaintext can be recovered entirely from the cipher text only if the code breaker is capable of efficiently factoring the public key n.It has been proven that decoding the Rabin cryptosystem is equivalent to the integer factorization problem, which is rather different than for RSA. Thus the Rabin system is 'more secure' in this sense than is RSA, and will remain so until a general solution for the factorization problem is discovered, or until the RSA problem is discovered to be equivalent to factorization Without such an advance, an attacker would have no chance today of breaking the code.

IV. Architecture

The authentication protocol must be able to create a secure channel between two principals on top of an insecure network, like the internet. The protocol must ensure the mutual authentication of both parties and the confidentiality and integrity of all the data transmitted through it before data get transmitted.



The idea behind this protocol is simple: in step 1, the mobile starts the protocol by sending its ID (e.g. Serial Number) to the server. In step 2, the server stores the mobile's ID for authentication purpose and generates mobile's private key and public key using the Rabin Public-key Cryptosystem. These keys (private and public key of the mobile) along with the public key of the server are sent to the mobile. Notice that the keys travel from the server into the mobile through a secure channel. To send the key to the respective destination, one can even adopt Diffie-Hellman key exchange algorithm.

In step 3, the mobile generates a challenge and sends it along with its ID to the server, encrypted with a combination of the server's public key and the mobile's private key. The server decrypts the message with mobile's public key and its private key and verifies if this ID matches the ID sent in step 1. This authenticates the client.

In step 4, the server sends the challenge received in the previous step plus one and a randomly generated session key and encrypted with a combination of mobile's public key and server's private key. The mobile then decrypts this message with server's public key and its private key and verifies the challenge. If it matches the one that was sent in step 3,

then the mobile can trust that it's indeed talking to the right server. Both encryption and decryption process, specified in step 3 and 4 are done using Rabin Public-key Cryptosystem technique. From now on, in step 5, a secure channel has been created and all data is encrypted with a session key. Notice that a new key is setup for each message to prevent replay attacks.

V. Implementation And Results

Emulator Setup : Java Platform, Micro Edition, or Java ME, is a Java platform designed for mobile devices and embedded systems. Target devices range from industrial controls to mobile phones and set-top boxes. Java ME was formerly known as Java 2 Platform, Micro Edition (J2ME).Java ME was designed by Sun Microsystems, now a subsidiary of Oracle Corporation; the platform replaced a similar technology, Personal Java. Originally developed under the Java Community Process as JSR 68, the different flavors of Java ME have evolved in separate JSR. Sun provides a reference implementation of the specification, but has tended not to provide free binary implementations of its Java ME runtime environment for mobile devices, rather relying on third parties to provide their own. Java ME devices implement a profile.

The most common of these are the Mobile Information Device Profile aimed at mobile devices, such as cell phones, and the Personal Profile aimed at consumer products and embedded devices like set-top boxes and PDA's. Profiles are subsets of configurations, of which there are currently two: the Connected Limited Device Configuration (CLDC) and the Connected Device Configuration (CDC).Designed for mobile phones, the Mobile Information Device Profile includes a GUI API, and MIDP 2.0 includes a basic 2D gaming API. Applications written for this profile are called MIDLETS. Almost all new cell phones come with a MIDP implementation, and it is now the de facto standard for downloadable cell phone games. However, many cell phones can run only those MIDLETS that have been approved by the carrier.

Table 1 shows the performance measurement of RSA algorithm for different Key size on command prompt execution. Figure 1 shows the comparative analysis of execution time of RSA algorithm for various Key sizes.

Table 1 Performance measurement of RSA Algorithm

RSA Key Size	Time in milliseconds
128	141
256	219
512	657
1024	4306

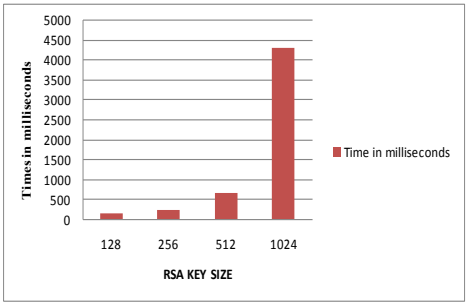


Fig.1 Comparative analysis of execution time of RSA algorithm

Table 2 shows the performance measurement of Elliptic Curve Cryptographic algorithm for different Key size on command prompt execution. Figure 2 shows the comparative analysis of execution time of Elliptic Curve Cryptographic algorithm for various Key sizes.

Table II Performance measurement of Elliptic curve cryptographic algorithm

ECC KEY SIZE	Time in milliseconds
128	172
160	203
256	282
512	843
1024	5391

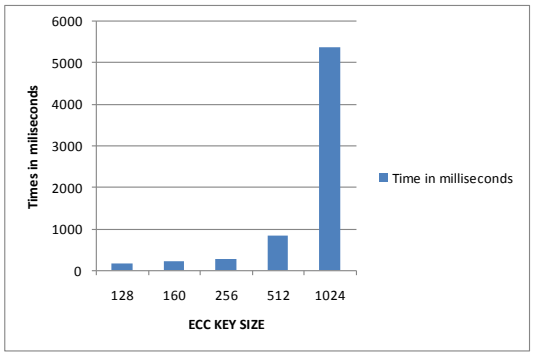


Fig. 2 Comparative analysis of execution time of Elliptic curve cryptographic algorithm in command prompt

Table III . Comparison of results

Algorithm(s)	ECC	RSA	RABIN
Time(ms)	120	40	20

Fig 4 & Fig 5 illustrates the instantaneous time taken to run those algorithms with J2ME emulator. From the figures, we observe that the proposed authentication algorithm takes minimum time than the existing authentication algorithms. From Fig. 6 & Fig.7, We observe that the energy consumption comparison of several of authentication algorithm in Java 2 Micro Edition (J2ME) emulator.

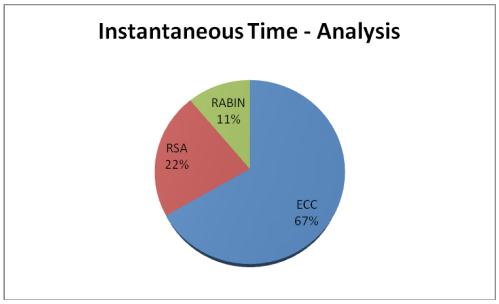


Fig 4

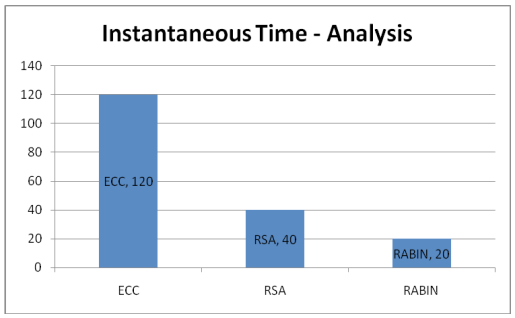


Fig 5

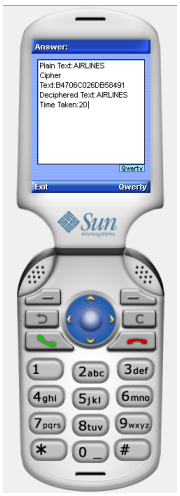


Fig 6

Fig 7

VI. Conclusions

Mobile handheld devices have strict constraints on the resources, such as memory space and time efficiency. How to minimize time consumption while maintaining a desirable level of security is very challenging. In this paper we proposed an authentication protocol and calculated the time efficiency to run on mobile handheld devices.

From experimental results, we have the following conclusions:

1. Our results show that proposed authentication protocol provides a better security guarantee and incurs much less time consumption than the existing authentication protocols. Finally, performance analysis shows that compared with existing authentication protocols, our proposed scheme is more simple, secure and efficient
2. We believe that such investigations to be an important first step toward addressing the challenges of time efficiency using Rabin Cryptosystem.

References

[1] M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," *IEEE J. Sel. Areas Commun.,* vol. 11, pp. 821-829, 1993.

[2] C. C. Lo and Y. J. Chen, "Secure communication mechanisms for GSM networks," *IEEE Trans. Consum. Electron.,* vol. 45, pp. 1074-1080, 1999.

[3] T.-F. Lee, C.-C. Chang, and T. Hwang, "Private authentication techniques for the global mobility network," Wireless Personal Commun., vol. 35, no. 4, pp. 329-336, 2005.

[4] T.-F. Lee, S.-H. Chang, T. Hwang, and S.-K. Chong, "Enhanced Delegation-Based Authentication Protocol for PCSs," *IEEE Trans. Wireless Commun.,* vol. 8, no. 5, pp. 2166-2171, 2009.

[5] H.-Y. Lin and L. Harn, "Authentication protocols with non-repudiation services in personnel communication systems," *IEEE Commun. Lett.,* vol. 3, no. 8, pp. 236-238, 1999.

[6] H.-Y. Lin, "Security and authentication in PCS," Comput. Elect. Eng., vol. 25, no. 4, pp. 225-248, 1999.

[7] W.-B. Lee and C.-K. Yeh, "A new delegation-based authentication protocol for use in portable communication systems," *IEEE Trans. Wireless Commun.,* vol. 4, no. 1, pp. 57-64, 2005.

[8] M. Rahnema, "Overview of the GSM system and protocol architecture,"*IEEE Commun. Mag.,* pp. 92-100, 1993.

[9] Dr.R.Shanmugalakshmi(2009),"Research Issues on Elliptic Curve Cryptography and Its applications - IJCSNS *International Journal of Computer Science and Network Security,* VOL.9 No.6, June 2009, Pg.No :19 – 22.

[10] Marisa W. Paryasto (2009), "Issues in Elliptic Curve Cryptography Implementation "- *Internetworking Indonesia Journal,* Volume 1/No. 1(2009), Pg.No 29-33.

[11] S. Prasanna Ganesan, Dr. GRD College of Science, "An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography" 978-1-4244-5848-6/10/$26.00 © 2010 IEEE, Pg.No 107-109.

[12] Wendy Chou,Dr. Lawrence Washington,"Elliptic Curve Cryptography and Its Applications to Mobile Devices." Department of Mathematics University of Maryland, College Park.

[13] S. Prasanna Ganesan, Dr. GRD College of Science, "An Authentication Protocol For Mobile Devices Using Hyperelliptic Curve Cryptography" *International Journal of Recent Trends in Engineering and Technology,* Vol. 3, No. 2, May 2010.

[14] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84- 89.

[15] Results of comparing tens of encryption algorithms using different settings- Crypto++ benchmark- . etrieved October 1, 2008, from: http://www.eskimo.com/~weidai/benchmarks.html

[16] S.Z.S. Idrus,S.A.Aljunid,S.M.Asi, ''Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers,'' IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008 ,Pg 20-25.

[17] Caimu Tang, Member, IEEE, and Dapeng Oliver Wu, Senior Member, IEEE" -An Efficient Mobile Authentication Scheme for wireless networks" *IEEE transactions on wireless communications,* vol. 7, NO. 4, APRIL 2008.

[18] Anoop MS, " Elliptic curve Cryptography", available at http://security.ittoolbox.com/research/elliptic-curvecryptography,5 Jan 2007

[19] J. Lopez, R. Dahab (2000), "An overview of elliptic curve cryptography", Technical report, IC-00-10, May 22. Available at <http://www.dcc.unicamp.br/ic-main/public-cation - e.html>.

[20] Standard Specifications for Public Key Cryptography, IEEE Standard 1363, 2000.