Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

A Location Based Cryptosystem For Mobile Devices Using Improved Rabin Algorithm

Ms.Smruti. P. Patil[1],Mrs.Darshana Tambe[2],Mrs. Prerna Solanke[3]
[1,2,3]Information Technology Dept,
Padmabhushan Vasantdada Patil College of Engg, Mumbai.

Abstract: As per the recent studies, the volatile growth has been seen in the use of mobile devices as the supporting technology for accessing Internet based services, as well as for personal communication needs in networking. Various studies indicate that it is impossible to utilize strong cryptographic functions for implementing security protocols on mobile devices. Our research negates this. Explicitly, a performance analysis focused on the most commonly used cryptographic protocols based on the location address (latitude & longitude) of the user for mobile applications and projected provably secure authentication protocol that is more efficient than any of the prevailing authentication protocol is being used by the network security methods. Understanding the use of public key cryptography which makes potential use of discrete logarithms problem. The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm. To provide secure communication for mobile devices, authenticated protocol is an important primitive for establishing trusted connection. In this paper, it has been shown that the location based system using improved Rabin Algorithm provides a better security and acquires much less energy consumption than the existing authentication protocols.

Keywords- elliptic curve cryptography, location based cryptography, and authentication, Rabin Public Key Cryptosystem,J2ME.

I. Introduction

The mobile devices (cell phone, tabs etc.) are being widely used by the people and mobile applications for accessing the wireless networks. In an increasingly interconnected world, the communication among the devices and the people is increasing rapidly. Accessing the internet has become essential in many of the professions and also in the corporate sectors in today's competitive world.

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

Appreciating global roaming services became possible with the use of portable communication systems, and hence the system is available for the conversations over wireless networks. In wireless network, mobile users send and receive data packets wirelessly through the internet. Hence, portable communication is very much vulnerable to security than wired networks [1] - [7].

The security features needed to provide security to roaming services are authentication, integrity, user-privacy and non- repudiation. For achieving the goal of security, the cryptographic algorithms are being used such as pubic key and private key algorithms. Among the existing

protocols, major parts of the protocols have been proposed on the secret key algorithms because mobile devices have limited memory. However secret-keys algorithms do not support non-repudiation. [6]

Privacy in location based services has become a topic of interest for research. There is an increasing number of devices with geo-positioning system and data communication capabilities. Many places have enabled a use of wireless LAN in recent years. Not only universities, colleges, homes but stations, airports, amusement parks and shopping malls have set up wireless LANs. For this type of networks location privacy issue is of great importance. [5]

II. Background and Related Work

This section discusses the results obtained from the previous researches. It is stated in [9] that this paper instigate the fast developing cryptographic researchers and to increase the security development in the field of information and security Elliptic Curve Cryptography (ECC) is a technique which uses smallest keys to provide high security and high speed in low bandwidth.
S.Prasanna [9] has given the features of ECC as the security and efficiency. It has been examined that they also provides the basis for why the ECC is most suitable for constrained environments. This paper also explores its performance in wireless systems. ECC can be implemented in software and in hardware . ECC follows generic procedure like parties agrees on publicly-known data items and each user generates their public and private keys [11]. Many devices are constrained devices that have small and restricted storage and can be applied. ECC can be functional. For wireless communication devices like PDA's, multimedia cellular phones .It can be used for security of Smart cards , wireless sensor networks, wireless mesh networks and web servers that need to handle many encryption sessions.

S.Prasanna [10] also shows that the existing authentication protocols based on RSA asymmetric cryptography are not suitable for devices which consumes more computing power, memory capacity, key sizes and cryptographic support. For this reason only, an efficient protocol must be designed for resource constrained platforms to attain high level of security similar to the protocols which are being designed and implemented today. It has been studied that the performance of the Elliptic Curve Cryptography is good over the performance of RSA algorithm [10].

The existing authentication protocol highlighted in [10], which have the basis of RSA algorithm are not feasible for such devices having low battery power, key sizes and cryptographic support. Due to these reasons it was possible to implement Hyper elliptic Curve Cryptography (HECC) in resource constrained mobile devices with improved performance as compared to RSA. Protocols related to HECC systems can be directly used in mobile devices. The performance of this algorithm is better than RSA and somewhat low than Rabin Cryptosystem.

The paper [12] deals with the performance of various encryption techniques that have been measured for the betterment of the security services. Active server pages (ASP) has been selected and five different encryption algorithm have been studied. The different algorithms are Blowfish, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Tiny Encryption Algorithm and Towfish. These algorithms are known to be able to support 132-bit size.

The [13] paper deals with the conclusion of an efficient algorithm scheme suitable for the mobile devices. For mobile station authentication it uses Elliptic Curve Cryptosystem; this scheme provides both the communication efficiency and computational efficiency as compared to other authentication schemes. 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.

With the rapid rise in GSM and smart phones, location services in China achieved a rapid growth in the year 2009. At present, networks of domestic telecom operators are upgraded to Cell-ID, and it allows any mobile phone user to locate with a mobile base station, and as of now, most mobile phone users take this method to locate. A new approach of location service system- Mobile New Concept which applies LL-TOA method based on base station for positioning the mobile phone, thus combine mobile positioning and mobile instant messaging organically providing a brand new experience of location services and communication with friends.[16]

III. Preliminaries

In this section, we provide a brief outline 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.

Basic Security Terminologies

A message present in a clear form, which can be understood by any casual observer, is known as the plaintext. In paper [1] 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 keys 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:

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.

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.

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.

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 accomplish 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:

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.

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.

IV. Proposed Authentication Algorithm

Rabin Cryptosystem is asymmetric cryptographic
technique, whose security, like that of RSA, is related to the difficulty of factorization. Similarly in turn Improved Rabin Cryptosystem is also an asymmetric cryptosystem technique whose security, like that of Rabin is related to factorization's difficulty. The difference between the basic Rabin and the improved Rabin algorithm is the key generation on the basis of location (longitude and latitude) of the user in the later one.

Our Scheme has three phases

Key Generation Phase
The system S creates a Key pair, by the following steps
Step 1: The Latitude and Longitude position of the user is tracked with the help of the GPS system.
Step 2: 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 3: Compute n=pq
Step 4: S's public key is n and S 's private key is (p, q)

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= m2 mod n.
Step 3: Generated cipher text sends to the remote
system.

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 ml, m2,m3 and m4 are calculated.

Step 3: Check the received C value for presence of anyone of ml, 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 {O, ... ,n - I}):
Step 6: One of these square roots is the original plaintext.

V. Rabin Cryptosystem (Improved)

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 isimportant 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 improved Rabin public-key cryptosystem which authenticate the user with its recent location.

Evaluation of the algorithm

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.

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 and the location of the user. Here the efficiency is comparable to RSA and basic Rabin Algorithm .

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 and tracking the location of the user. 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 possibility today of breaking the code.

VI. 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.

Mobile **Server**

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 he 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.

VII. 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 download-able 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.

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

Table 1 Performance measurement of RSA Algorithm

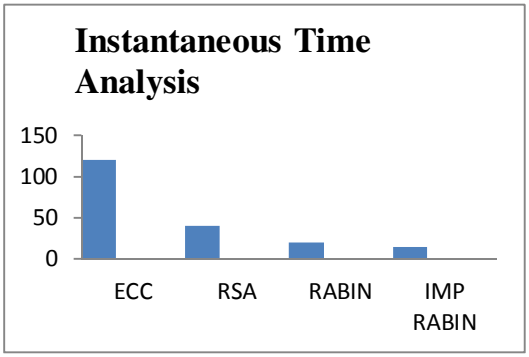
Table 2 shows the performance measurement of Elliptic Curve Cryptographic algorithm for different Key size on command prompt execution. Figure 2 shows the comparative analysis of execution time of Elliptic Curve Cryptographic algorithm for various Key sizes.

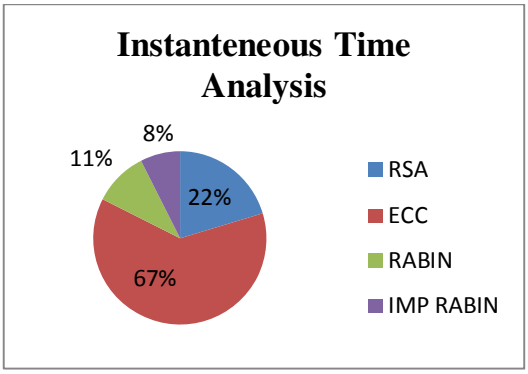
Algorithms	ECC	RSA	RABIN	Improved Rabin
Time (ms)	120	40	20	14

Table 2 Performance measurement of Elliptic curve cryptographic algorithm

ECC Key Size	Time in milliseconds
128	141
160	203
256	219
512	657
1024	4306

Table 3 . Comparison of results





Following fig 2. 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.

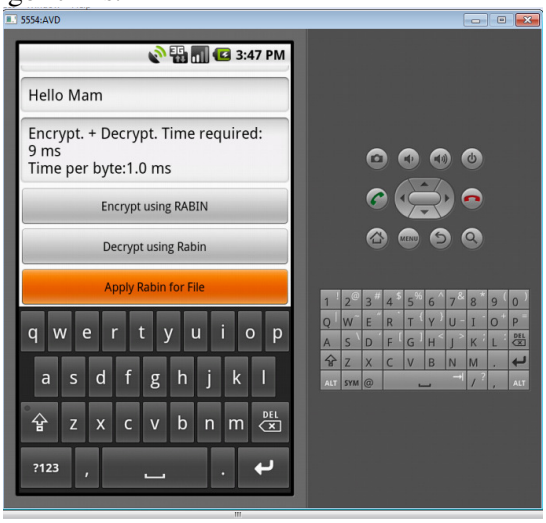


Fig-2

VIII. Conclusion

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:

l.. Our results show that proposed authentication protocol provides a better security assurance and gains 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 Improved Rabin Cryptosystem.

REFERENCES

[1] K.Saravana selvi\ T.Vaishnavi2 I.Assistant Professor ,Bharath Niketan Enginering college, Tamil Nadu "Rabin PublicKey Cryptosystem for Mobile Authentication" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

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

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

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9].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.

[10]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.

[11]. S. U. Nimbhorkar, L.G.Mallik, "A Survey On Elliptic Curve Cryptography" International Journal Of Advanced Studies In Computers Science And Engineering, survey ECC_June12.

[12]. Syed Zulkarnain Syed Idrus1, Syed Alwee Aljunid2, Salina Mohd Asi3, Suhizaz Sudin4, and R. Badlishah Performance Analysis of Encryption Algorithms' Text Length Size on Web Browsers. Ahmad5 IJCSNS International Journal of Computer Science 20 and Network Security, VOL.8 No.1, January 2008Manuscript received January 5, 2008. Manuscript revised January 20, 2008

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

[14] Binomial-Mix-based Location Anonymizer System with Global Dummy Generation to Preserve User Location Privacy in Location-Based Services. 2010 International Conference on Availability, Reliability and Security

[15] Seyed Hossein Siadat, Ali Selamat" Location-Based System for Mobile Devices Using RFID" Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, 2008 IEEE DOI 10.1109/AMS.2008.44

[16]. Xiufeng Liu1, Longguang Zhang2, Xiuju Zhan1, Pingping Chen1." Location-based Mobile Instant Messaging System" Information Technology College, Guangzhou University of Chinese Medicine, Guangzhou, China .©2012 IEEE.

