ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 3, pp: (99-103), Month: July - September 2017, Available at: www.researchpublish.com

Secure SMS Using Elliptic Curve Algorithm and its Implementation

[1]Mohammed Rajhi, [2]Hatim Madkali

[1, 2] Jazan University, Teacher Assistance, Dept. of Computer Science and Information System, Jazan, Saudi Arabia

Abstract: **Short message services (SMS) are built up as a broadly utilized and across the board approach for content information in present day's enormously versatile dependent world. SMS today has turned into a usual hotspot for imparting classified or restrictive data. Under such circumstances, the essential component is "Security." One of the consistently used techniques for security is known as encryption. Its significance increases many folds when characterized information is working in the framework by filling in as a security network for the extraordinary rough data avoiding interference. There are different standards, and symmetric encryption calculations present to ensure the safety, each having its specific level of protection. The most significant aspect to be kept in mind while utilizing coded message or cryptography to give short message service protection is the limit and consideration of the properties of the cell phone. Considering all perspectives, this paper puts forth a methodology for giving great confirmation. Additionally, protection to communication transfer that can be capably used as a piece of little contraptions, such as phones.**

Keywords: **elliptic curve cryptography, encryption, decryption, RSA, security, SMS.**

1. PROPOSAL

The proposed structure uses the above-portrayed thought of elliptic curve cryptography to encode the message and send it over a regular channel. The sender forms a message and gives the recipient's number when he sends the message the calculation is enacted upon both the contraptions. The keys have made and shared amongst the devices, and the encryption occurs at the sender's end. After encryption, the message has sent to a beneficiary; likewise, he unscrambles it utilizing his key to scrutinize it. The Encryption and Decryption techniques in ECC are wanted to encode and disentangle a point on the bend and not the entire message. In the middle of encryption, all character in a message ought to be changed over toward bytes then the bytes into motivations behind the edge (x, y) and a short time. Next, the concentrations must encode by mapping each of them with each point on the elliptic bend, and a while later the entire encoded shows should be changed over back to bytes and after that, to strings, as SMS can pass on simple string values. Once the message accomplishes the recipient, in the midpoint of the technique of disengaging, the string must be changed over to bytes. These bytes should be decoded to concentrates again using the mapping methodology and after that the concentrations to bytes in conclusion to characters that causing the message and at exactly that point the decoded plain content can be seen by the collector.

2. INTRODUCTION

Among the most recent couple of years, the use of phones has been extending exponentially. SMS (Short Message Services) is a bit of the administration of the GSM, and another cell arranges that give an instrument to transmit short messages to, and from adaptable devices. The incomprehensible base of mobile phones and the SMS affirmation have propelled its employment for many unconventional applications as opposed to sending short and brief discussion. SMS is remarkably simple; a final message's length is 160 characters. SMS utilizes just an arrangement of characters as information sort. It requires low information transmission, and it is a simplicity benefit took a gander at with others which make it fitting for brisk correspondence. Regardless its flexibility, SMS has a couple of limitations that would be basic for some whimsical applications. For a couple of utilizations, like trades, portions, and checking, it is helpful to solidify many administrations that can give order, reliability, affirmation and non-repudiation administrations that are standard for framework security.

The assumption of using Elliptic Curves in Cryptography was presented by Victor Miller and N. Koblitz as a different option to build up open key frameworks, for example, DSA and RSA. The Elliptic Curve Discrete Log Problem makes it hard to break an ECC when contrasted with other traditional crypto systems where the issues of factorization or the discrete legitimize can be settled in sub-exponential time. Here implies little parameters essentially can be utilized as a part of ECC than in other focused frameworks. Therefore, it means in having small key size subsequently speedier calculations and therefore demonstrates productive in little gadgets like cell phones. This paper relies on upon the end to end secure transmission of SMS using cryptography. The calculation relies on upon the blend of Elliptic Curve Cryptography which gives high approval with minimal key size and small handling time.

3. LITERATURE REVIEW

O Shoewu and Segun, in their paper, talk on encryption, decryption, the transmission module, and demodulation in a remote domain to secure messages sent on GSM. This article focuses on the utilization of Elliptic Curve Cryptography (ECC) for encryption and decoding of instant messages keeping in mind the end aim to protect the quality, trustworthiness, and security of instant messages. The study depends on enhancing the consistent quality of SMS sent in remote systems, and it is gone for the utilization of ECC encryption and decoding algorithms to distinguish/check its utilization as a solid strategy based on the main contemplations (speed, key length, quality).

Ruchika and Gurvinder discuss in their paper how counteracting unapproved access to corporate data frameworks is fundamental for some associations. Security communication is one of the real zones of intrigue. The information utilized as a part of communication is exceptionally touchy and should be shielded and made conceptual from interlopers of a framework. The late offshoot of Network security is Cryptography utilizing Elliptic Curve Architectures which depends on the number-crunching of elliptic curves and discrete logarithmic issues. ECC plans are public key based systems that give encryption, excellent marks, and key trade algorithms.

Laiprakhpam et al in their paper introduces a method in their paper where the high strategy of mapping the characters to relative focuses in the elliptic curve has been evacuated. The relating ASCII estimations of the plain content are combined up. The combined qualities fill in as the contribution for the Elliptic curve cryptography. This new system maintains a strategic distance from the expensive operation of mapping and the need to share the common query table between the sender and the beneficiary. The algorithm is planned in a manner that it can be utilized to scramble or decode any script with characterized ASCII values.

4. METHODOLOGY

The approach for this paper is analytical. The resources for this research are gathered from online databases which include scholarly articles and books. These databases provided with various approaches and methods for Cryptography. Considering all viewpoints, this paper proposes a method for giving high confirmation, what's more, protection to those messages shared which can proficiently utilize as a part of little gadgets like cell phones.

5. ANALYSIS AND DISCUSSION

The need of offering security to SMS has been essential for a long time, and various calculations and techniques have been completed in various stages to endeavor and offer security to the messages. At today, there are numerous calculations in light of symmetric cryptography that offers security to the messages traded in light of a common Secret key. The rule insult of a symmetric-key cryptosystem is relevant to the exchange of keys. There exists the issue of key apportionment in them. Private-key systems need to use centers that are on any occasion the length of the message to be encoded. Symmetric encryption requires that a secured channel be utilized to exchange the key, which diminishes the estimation of this sort of encryption structure when we talk regarding SMS.

In this way, the use of conventional crypto systems is considered in this paper. One such conventional cryptosystem specifically being used is the RSA. The RSA is a Public key cryptography in light of significant factorizing numbers. In the RSA calculation, the key period relies on upon two distinct prime numbers. The greatest drawback of the RSA calculation is that anyone having an open key can find distinctive ways to deal with translate the message. The assaults against RSA can be normal the picking of slight plain substance, frail parameters decision, or inappropriate utilization. There are distinctive attacks plausible on RSA few of them are:

1. Chosen-Cipher Attack
2. Factorization Attack
3. Broadcast Attack

Another than the assaults on RSA there are numerous different issues identified with utilizing this algorithm for SMS protection. SMSs are created from cell phones which for the most part have low handling limits also, besides low memory and battery restrict. Calculations like RSA are customary calculations with tremendous key sizes which require higher memory points of confinement and high get ready forces. In light of these deductions the use of RSA for giving SMS security will diminish the execution of the contraption and moreover, the taking care of time will be high. The proposed arrange relies on upon Elliptic Curve Cryptography which is a more gainful routine cryptosystem. The bit measure of ECC is less appeared differently about that of RSA and moreover because of the discrete logarithmic issue it is greatly difficult to unscramble the messages by just knowing the open key. ECC wears down less key size and now planning power in this way can be exceptionally beneficial in little contraptions like mobiles.

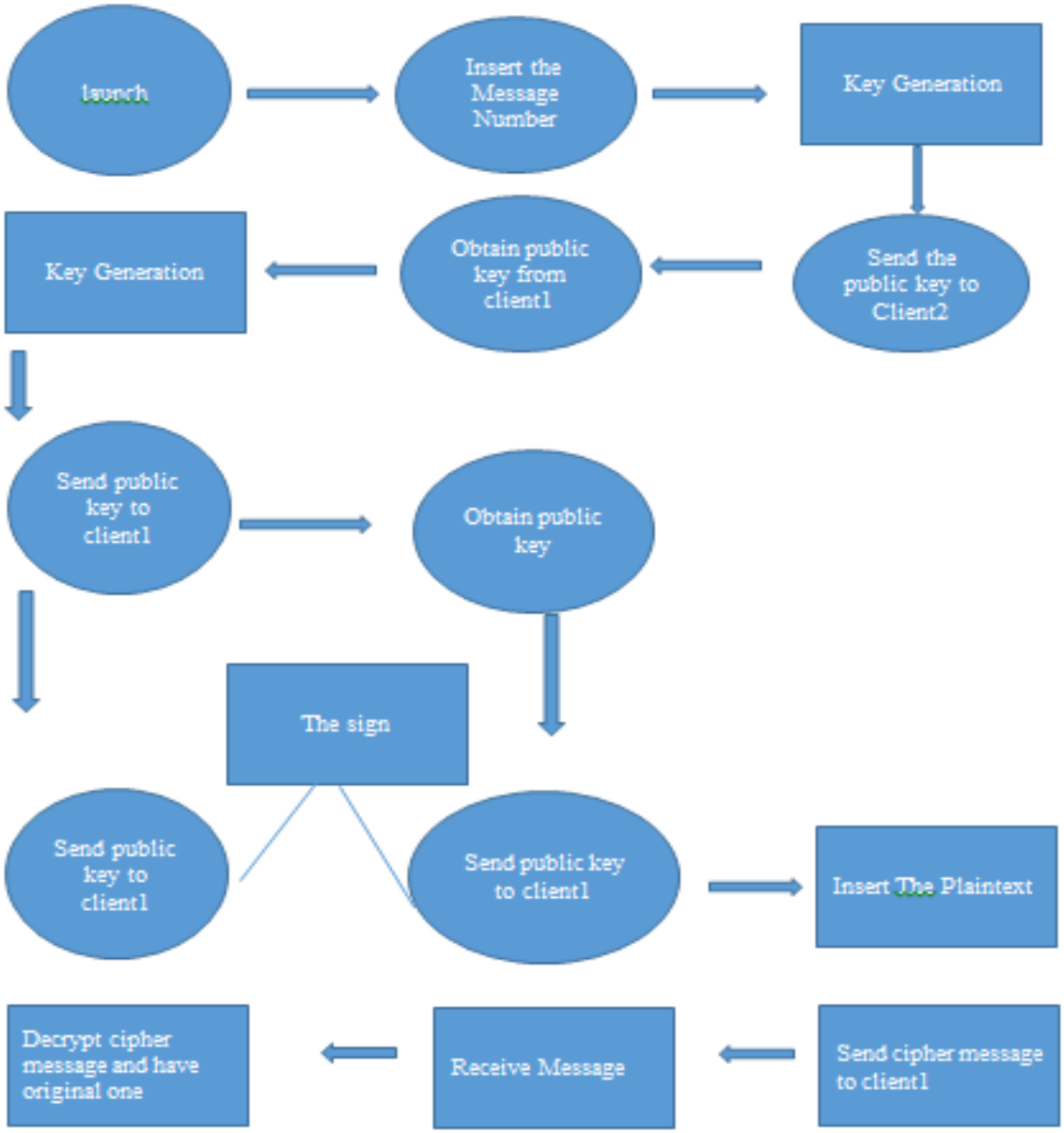
Elliptic Curve Cryptography:

ECC is an adequate method to public-key cryptography based on the algebraic structure of elliptic curves beyond finite fields. One of the main benefits in rapprochement with non-ECC cryptography is the equivalent level of security provided by keys of lower size. Elliptic curves are appropriate for encryption, digital signatures, pseudorandom generators and another process. Likewise, they are utilized in various integer factorization methods that have applications in cryptography, such as Lenstra elliptic curve factorization.

Implementation:

The client1 connects with the client2 within any conventional means for the protected communication to be followed. Once both the client1 and client2 are outfitted with their application, the sender sorts in the recipient's number and the body of the message and clicks send. On this instruction, the ECC algorithm triggered at the client1 side, and the keys are generated. The client1's public key is then sent to the client2. The user2 confirms this by clicking the Read button in which the obtained key is read by the recipient application and the ECC algorithm has triggered at client2's end. The client2's secret key is created, and its public key is sent to the sender. On receiving the public key from the client2, client1's secret key is generated at the client1 side, and the message is encrypted applying ECC algorithm and sent to the client2. The client2 receives the message and decrypts it utilizing his secret key by the ECC the algorithm to retrieve the original message.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 3, pp: (99-103), Month: July - September 2017, Available at: www.researchpublish.com



6. CONCLUSION

As phones have minimum storage or limited battery, ECC is an efficient tool to protect data on mobiles. Symmetric key algorithms can be used. However, it does not ensure message authentication. A secure channel is needed for the transfer of messages alongside the missing key. Otherwise, the chance of intrusions and attacks becomes high. For the conventional RSA cryptosystem, the key size and the speed becomes a major problem. To encrypt messages using this system, smaller keys are used. However, the encryption becomes weaker under this system. ECC is useful, not simply in resource obliged environment related to mobiles, pagers or sharp card devices which have confined memory, limited protection of limit, and compelled support on successful PCs since it gives strong security smaller key sizes. Because of its service of end-to-end secure data transfer, ECC also offers authentication of the messages.

The most important reason for using this technique for secure correspondence is that both the transmitter and the beneficiary should use a comparable technology, and should be changing meanwhile. This assures full check and the way the SMS can be decoded exactly when it is transferred and consequently protected from other people who attempt to decode it at a later point. By this way, ECC can be efficiently utilized as a part of securing and confirming the correspondence between the two parties. SMS can be sent starting with one cell phone then onto the next without interruption. Above all, the messages containing sensitive data are put away safely and stay secure even when mobile go

in wrong hands. A message can be decoded by the beneficiary when it is received and never again can be decoded. High confidentiality should be kept, and along these lines shield the message data from abuse. Therefore, it confirms the secure end-to-end exchange of information without the corruption of data.

REFERENCES

[1] Burguera, I., Nadjm-Tehrani, S., & Zurutuza, U. (2011). Crowdroid: behavior-based malware detection system for Android. *SPSM@CCS*.

[2] Chaudhari, N.S., & Saxena, N. (2012). A secure approach for SMS in GSM network. *CUBE*.

[3] Eberle, H., Gura, N., Patel, A., Shantz, S.C., & Wander, A. (2004). Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. *CHES*.

[4] Hankerson, D., Menezes, A., & Vanstone, S. (2004).Guide to Elliptic Curve Cryptography.

[5] Jadhav, M.A., & Kolhekar, M.M. (2011). Implementation of Elliptic Curve Cryptography on Text and Image.

[6] Koblitz, N. (2010). Elliptic Curve Cryptosystems.

[7] Laiphrakpam Dolendrosingh Khumanthem Manglem Singh. Implementation of Text Encryption using Elliptic Curve Cryptography http://www.sciencedirect.com/science/article/pii/S1877050915013332

[8] Miller, V.S. (1985). Use of Elliptic Curves in Cryptography. *CRYPTO*. O.Shoewu and Segun O. Olainwo."Securing Text Messages using Elliptic Curve Cryptology and Orthogonl Frequency Division Multiplexing" http://www.academia.edu/5383818/Securing_Text_Messages_using_Elliptic_Curve_Cryptography_and_Orthogonal_Frequency_Division_Multiplexing

[9] Rao, O.S. (2011). Comparative study of Arithmetic and Huffman Compression Techniques for Enhancing Security and Effective Bandwidth Utilization in the Context of ECC for Text.

[10] SMS Encryption for Mobile Communication, IEEE 2008 International Conference of Security Technology.

[11] SMS Encryption using AES Algorithm on Android, International Journal of Computer Applications (0975 – 8887) Volume 50– No.19, July 2012.