IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-2 E-ISSN: 2347-2693

# Efficient and Secure SMS Encryption Technique using Elliptic Curve Cryptography

Anirban Bhowmick

*Department of Computer Science Engineering, Manipal Institute of Technology, Manipal University, Manipal*
*anirban.bhowmick1993@gmail.com*

www.ijcaonline.org

Received: Jan /09/2014 Revised: Feb/08/2014 Accepted: Feb/04/2014 Published: Feb/28/ 2014

***Abstract*—** Data security over the cellular network is critical. Mobile phones have provided operators with immense facilities at the cost of data privacy. Without ensuring data concealment, communication should be avoided. This makes cryptography an evolving research area. In this paper, the authors propose an asymmetric encryption system which maintains data confidentiality and integrity of the text message throughout the mobile network.

In the proposed system, the text message is encrypted before being transmitted over the network. Most of the traditional encryption techniques are computationally intensive. Accordingly, elliptic curve cryptography has been employed to encrypt the text message as it permits efficient use of mobile's limited resources like memory and processor. One of the key flaws in Short Message Service (SMS) is that it does not provide end-to-end security. The original text is revealed to the utility provider for a short duration of time which can be a reason for misuse. The system proposed offers this much needed data privacy.

***Keywords*—**Encryption, Cryptography, Elliptic Curves, Elliptic Curve Cryptography, SMS

## I. INTRODUCTION

Communication between two entities needs to be confidential. Altering the data to some unintelligible form can defend it from intruders. Cryptography is perhaps the most significant aspect of communication security and is becoming a basic building unit for computer security. To deny intruders from discovering the private data, the data needs to be encrypted at the sender's end. This encrypted data can be decrypted at the receiver's end to acquire the secretive information.

This era is controlled by paperless communications in business, private or government offices by means of use of email messages, SMS and phone calls. Most of the confidential specifics are delivered to the receiver through such methods. Privacy of the messages sent over wireless communication media is essential which can be achieved by encryption.

Encryption is of two types [1]

- Asymmetric Encryption or to Public key cryptography
- Symmetric Encryption or to Private key cryptography

Elliptic Curve Cryptography (ECC) [2] [3] [4] is an approach to public key cryptography grounded on the algebraic structure of elliptic curves [5] [6] over finite fields. In public key cryptography, communication between two entities involves a private key and public key. Private key is known only to the legitimate entity but public key is distributed to all entities participating in the communication process. Further, there are domain parameters used in ECC that are known to all entities. An elliptic curve over a finite field is defined by the equation

$$y^2 = x^3 + ax + b \quad (1)$$

where $4a^3 + 27b^2 \neq 0$

Each value of $a$ and $b$ gives a different equation of the curve. All points (x, y) which satisfy the equation for given $a$ and $b$ along with a point at infinity (O) lie on the elliptic curve. Further, the public key is a point on the curve and the private key is a randomly generated number. The public key is the product of the private key and the generator point $G$ on the curve. The generator point $G$ and the curve parameters $a$ and $b$ creates the domain parameter of ECC.

The rest of the paper is divided into the following sections. Section 2 contains research work done in the field of Elliptic Curve Cryptography (ECC). Section 3 provides the readers a detailed understanding of ECC. In section 4, the authors attempt to focus on the working of the Short Message Service (SMS). In section 5, the authors present the proposed algorithm. Section 6 concludes the paper.

## II. RELATED WORK

Authors in [7] propose a system in which confidential data is transmitted over the cellular network once it is subjected to encryption followed by steganography. Data encryption is implemented using elliptic curve cryptography. Further, this encrypted text is concealed in an MMS. The MMS is transmitted and the vital data is extracted and decrypted at the receiver's end.

In [8], authors suggest a Signcryption system which is based on Elliptic Curve Cryptography. It uses elliptic curve for both encryption and signature generation. Message transmission is in the form of a point P (m) embedded in elliptic curve and encrypted by point addition. Further, a novel signature generation technique has been presented that involves less time as compared to signature generated

 

by hashing scheme. The signature can be verified without decryption of the message.

The proposed algorithm in [9] uses ECC in conjunction with data encoding using DNA. The initial level of security in this suggested system is attained by mapping the plaintext with DNA Nucleotide. The next level of security is achieved by encrypting the encoded plaintext using ECC encryption.

Authors in [10] proposed a system for text encryption using elliptic curve cryptography for safe transmission of text and combining the Huffman data compression technique for effective use of channel bandwidth and improving the security. Every character of text message is transformed into the elliptic curve points, these elliptic curve points are converted into cipher text.

## III. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is a branch of public key cryptography which makes use of a private key and a public key.

### A. Key Exchange

Exchanging keys [11] in elliptic curves can be performed in the following way. Pick an integer $q$, which is a prime number or an integer of the form $2^m$, and the curve parameters $a$ and $b$. Substitute the values of $a$ and $b$ in Equation (1) to obtain the equation of the curve. Further, pick a base point, $G$ lying on the curve.

Assume the two users communicating are $A$ and $B$. Key exchange between users $A$ and $B$ can be achieved through the following steps [12].

1. $A$ picks an integer $n_A$ which is $A$'s private key. $A$ generates a public key $P_A = n_A \times G$; the public key is a point in $E_q(a,b)$. $E_q(a,b)$ are the set of points consisting of all the points $(x,y)$ that satisfy the elliptic curve equation obtained after substituting $a$ and $b$ values in Equation (1).
2. Similarly B selects a private key $n_B$ and generates a public key $P_B$.
3. $A$ generates the secret key $K = n_A \times P_B$. $B$ generates the secret key $K = n_B \times P_A$.

The two calculations in step 3 produce the same result because

$$n_A \times P_B = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P_A \quad (2)$$

***Consider the example***

$q = 211$
$E_q(0,-4)$
Curve Equation: $y^2 = x^3 - 4$
$G = (2, 2)$
$n_A = 121$
$P_A = 121(2, 2) = (115, 48)$
$n_B = 203$
$P_B = 203(2, 2) = (130, 203)$
The shared secret key $K = n_A \times P_B = n_B \times P_A$
$121(130, 203) = 203(115, 48) = (161, 69)$

The secret key obtained is a pair of numbers. We could use the x-coordinate or a simple function of x-coordinate.

### B. Encryption And Decryption

In this section, the authors have presented the simplest text encryption and decryption technique using elliptic curves (EC) [12] [13]. The plain text $m$ that is to be transmitted needs to be encoded as an x-y point ($P_m$). $P_m$ will be then encrypted as a cipher text and later decrypted. Further, the message cannot be directly encoded as the x or y coordinate of the point as the coordinates that will be generated might not be included in $E_q(a,b)$.

Similar to the key exchange technique, encryption and decryption requires a base point $G$ and an elliptic group $E_q(a,b)$ as parameters. $A$ selects a private key $n_A$ and generates a public key $P_A = n_A \times G$. Further, $A$ picks a random positive integer $k$ and generates a cipher text consisting of a pair of points.

$$C_m = \{kG, P_m + kP_B\} \quad (3)$$

To decrypt the cipher text, $B$ multiplies the first point in the pair by $B$'s secret key and subtracts the result from the second point. The equation is given below.

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m \quad (4)$$

***Consider the example***

$q = 751$
$E_q(-1, 188)$
Curve Equation: $y^2 = x^3 - x + 188$
$G = (0, 376)$

$P_m = (562, 201)$
$k = 386$
$P_B = (201, 5)$

Substituting the required values in Equation (3)
$C_m = \{386(0, 376), (562, 201) + 386(201, 5)\}$
$C_m = \{(676, 558), (385, 328)\}$

### C. Advantages of ECC

- It provides high security for a given key size.
- It provides effective and compact implementations for cryptographic operations requiring smaller chips.
- Due to smaller chips less heat generation and less power consumption.
- It is mostly suitable for machines having low bandwidth, low computing power, less memory.

- It has easier hardware implementations.

## IV. SHORT MESSAGE SERVICE (SMS)

Short Message Service (SMS) has become a common way for mobile phone users to send and receive short text messages using mobile phones and portable devices. SMS provides a convenient means for people to communicate with each other using text messages via mobile devices or Internet connected computers. Each message can cover at most 140 bytes (1120 bits) of data, which is equivalent of up to 160 English characters, or 70 Chinese characters. SMS was the most widely used data application, with an estimated 3.5 billion active users, or about 80% of all mobile phone subscribers at the end of 2010.

### A. *Working of The SMS Service*

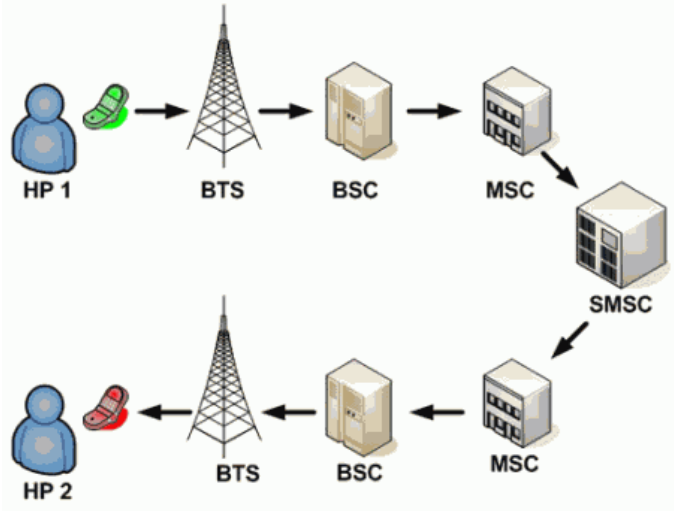


Figure 1: Transmission of SMS

Figure 1 provides a thorough idea about the transmission of the short text messages from one entity to another. The different equipments shown in the figure are-

- Base Transceiver Station (BTS) permits wireless communication between the user equipment and a network.
- The Base Station Controller (BSC) is responsible for handling traffic and processing signals.
- Mobile Switching Center (MSC) is the key service delivery node for GSM/CDMA. It routes voice calls and SMS.
- When the message is transmitted, it will be received by mobile carrier's SMS Center (SMSC). Destination routes are structured and then send it to destination devices.
- The BTS and BSC are collectively called Base Service Subsystem (BSS) [15].

### B. *Lack of Security over the Network*

Data security has at least three important requirements to meet- Confidentiality, Integrity and Authenticity [16]. The security service not delivered by SMS is end-to-end security. With end-to-end encryption security applied, data that is transmitted is encrypted from the instant it leaves the sender, and is decrypted only when it is received by the other entity (receiver). However, as such a facility is absent; the message is encrypted during over-the-air transfer and will be decrypted as soon as it enters the network after arriving at the BSS and encrypted again when it leaves the network through the BSS that delivers the message to the sender, thus temporarily revealing the original text. Thus, the data confidentiality [17] and data integrity is not assured. It is also possible for the provider to modify the messages without the receiver knowing.

## V. PROPOSED TECHNIQUE

In this paper, the author puts forward an approach to enhance the privacy of the text messages transmitted over the mobile network. To attain end-to-end security and maintain the confidentiality and integrity of the messages, the messages ought to be encrypted at the user device itself. Consequently, the message delivered to the network will be an intermediary cipher text ($C_1$). The encryption initiated by the network will add to the security of the encrypted text message ($C_1$) generating the final cipher text ($C_2$). The encryption at the initial stage will ensure that the original text is not revealed to the service provider before the over-the-air encryption.

The author proposes the use of elliptic curve cryptography for encryption of the original text message due to the following reasons-

- Short but strong keys
- Low memory consumption
- Low CPU consumption

This will allow efficient use of mobile's limited resources like memory and processing power.

In this system, the original message is encrypted through the ECC technique (as discussed in Section 3) just when the mobile operator decides to direct a message. This encrypted message ($C_1$) is then sent over the network. The intermediary cipher text ($C_1$) is further subjected to encryption employed by the SMS service provider over-the-air producing the final cipher text ($C_2$). This method helps conserving the confidentiality and integrity of the original text message. The original text is not exposed to the service provider. Subsequently, the cipher text ($C_2$) is decrypted by the SMS utility provider before reaching the receiver generating the intermediary cipher text ($C_1$) which is further decrypted by the ECC technique (as discussed in Section 3)

at the receiver's end to obtain the original plain text message.

## VI. CONCLUSION AND FUTURE WORK

Mobile communication should be secure and the vital data should remain encrypted throughout its journey from sender to receiver. The technique proposed in the paper attempts to implement the same. Mobile devices have constrained environment. So ECC can be efficiently used as it takes less memory and less power with small key sizes. It permits efficient usage of mobile's resources to attain mobile data confidentiality. With this system put into practice, the SMS utility providers will be denied inspecting the original text message.

As a part of future work, the authors suggest a number of encryption stages to enhance the security of the text messages over the mobile network. Encryption techniques with higher efficiency can also be employed.

## REFERENCES


[1]. Ayushi, "A Symmetric Key Cryptographic Algorithm", 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15

[2]. Vivek Katiyar, Kamlesh Dutta, Syona Gupta, "A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment", International Journal of Computer Applications (0975 –8887) Volume 11– No.10, December 2010

[3]. Atul Kahate, "Cryptography and Network Security"

[4]. N Harini, C K Shyamala, T R Padmanabhan, "Cryptography and Security"

[5]. Joseph H. Silverman,John T. Tate, "Rational Points on Elliptic Curves"

[6]. J.S. Milne, "Elliptic Curves", www.jmilne.org/math/Books/ectext5.pdf

[7]. N. Jagdale, R.K.Bedi, Sharmishta Desai, "Securing MMS with High Performance Elliptic Curve Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 8– No.7, October 2010

[8]. Ramratan Ahirwal, Anjali Jain, Y. K. Jain, "Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation", International Journal of Computer Applications (0975 – 8887) Volume 62– No.9, January 2013

[9]. P.Vijayakumar, V.Vijayalakshmi, G.Zayaraz, "DNA Computing based Elliptic Curve Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 36– No.4, December 2011

[10]. O.Srinivasa Rao, S. Pallam Setty, "Huffman Compression Technique in the Context of ECC for Enhancing the Security and Effective Utilization of Channel Bandwidth for Large Text", IJCA Special Issue on "Network Security and Cryptography" NSC, 2011

[11]. CH. Suneetha, D. Sravana Kumar, A. Chandrasekhar, "Secure Key Transport in Symmetric Cryptographic Protocols using some Elliptic Curves over finite fields", International Journal of Computer Applications (0975 – 8887) Volume 36– No.1, December 2011

[12]. William Stallings, "Cryptography and Network Security", 3rd Edition

[13]. N.Koblitz, "Elliptic Curve Cryptosystems, Mathematics of Computation", volA8, 1987, pp.203 - 209.

[14]. Aqeel Khalique Kuldip Singh Sandeep Sood, "Implementation of Elliptic Curve Digital Signature Algorithm", International Journal of Computer Applications (0975 – 8887)Volume 2 – No.2, May 2010

[15]. Ajay R Mishra, "Fundamentals of Cellular Network Planning and Optimisation"

[16]. Neetesh Saxena, Narendra S. Chaudhari, "A Secure Digital Signature Approach for SMS Security", IP Multimedia Communications A Special Issue from IJCA

[17]. Behrouz A. Forouzan, "Cryptography and Network Security" special Indian Edition 2007, Tata McGraw-Hill Publishing Company Limited, New Delhi