International Journal of Scientific Research in Computer Science and Engineering
Vol.5, Issue.4, pp.22-24, August (2017)

Research Paper

E-ISSN: 2320-7639

Secure SMS Communication Using Quasigroup Algorithm

[1*]Abhishek Shetty, [2]Haroon Antapur, [3]Mit Chauhan, [4]Nita Patil

[1]Dept. of Computer Engineering, Datta Meghe College of Engineering, Airoli, India
[2]Dept. of Computer Engineering, Datta Meghe College of Engineering, Airoli, India
[3]Dept. of Computer Engineering, Datta Meghe College of Engineering, Airoli, India
[4]Dept. of Computer Engineering, Datta Meghe College of Engineering, Airoli, India

**Corresponding Author: abhi20695@gmail.com*
Available online at: www.isroset.org

Received 10th Jun 2017, Revised 16th Jul 2017, Accepted 12th Aug 2017, Online 30th Aug 2017

***Abstract*---**This paper is on Secure SMS Communication Using Quasigroups Algorithm. We have developed an intermediate application between the bank and the user that would encrypt the data in the SMS sent by the user. Using this SMS banking service, the user can check balance or even transfer funds to someone else's account provided both accounts are of the same banks. This will be easier to use as the account holder without a smart phone can also get fruitful results out of this. This will enable the account holder to avail banking facilities via SMS. The mobile operator is the service provider to our user. Also, the confidential information will be encrypted such that the mobile operator will not have access to the contents of the SMS.

Keywords*—*cipher, encryption, decryption, quasigroup matrix, SMS banking.

I. INTRODUCTION

Short Messaging Service (SMS) is a communication service, originally developed as a part of the Global System for Mobile Communications (GSM). Today it is one of the most widely used mobile services, with million messages exchanged on a daily basis. Banks worldwide are using SMS to conduct some of their banking services. Transmission of the short messages between SMSC and phone is via the Signaling System Number 7 (SS7) within the unencrypted protocol allowing the cellular provider's network to eavesdrop or modify SMS messages. To protect our privacy, as well as to protect our confidential data, we propose a protocol that SMS messages from source to destination will be sent encrypted. In our protocol, a secure channel is established between two network-connectable mobile devices, using SMS as the transmission medium. To ensure that the SMS remains confidential, a symmetric-based cipher is used to encrypt the message's content. The encryption is defined by using Quasigroup transformations of the messages. The communication is establishing online, provided that the users have installed the needed components of our protocol.

II. LITERATURE SURVEY

In this protocol, a secure channel is established between two networks- connectable mobile devices, using SMS as the transmission medium. To ensure that the SMS remains confidential, a symmetric-based cipher is used to encrypt the message's content. The encryption is defined by using quasigroup transformations of the messages [1].

Cryptology is a science that consists of two parts: cryptography and cryptanalysis. Cryptography is a science on methods of transformation (ciphering) of information with the purpose of this information protection from an unlawful user. Cryptanalysis is a science on methods and ways of breaking down the ciphers [2].

III. BACKGROUND ON QUASIGROUPS

Quasigroups share a history with the popular game Sudoku and the long lived Latin squares. The core of a Quasigroup is defined in the same manner as a Latin square. These consist of an $n2$ set of ordered triples having the form $(ri , c\ j , vi\ j)$; $ri , c\ j , vi\ j \in$ Integers, with the additional stipulation that for each $(ri , vi\ j)$ and $(c\ j , vi\ j), vi\ j$ is unique. This relation can be represented as a $n \times n$ square matrix with ri and $c\ j$ being the row and column indices and $vi\ j$ is the value in the rith row and $c\ j$th column. The difference between a Quasigroup and a Latin square is the definition of an operator "·" on a Quasigroup [3].

One may view quasigroup transformation as a substitution and permutation operation. These operations form the basis of numerous encryption systems especially in speech encryption [4, 5]. Further, public key systems such as NTRU [7] and elliptic curve cryptosystems [6] have lower power consumptions compared to RSA however compared to secret key systems they are much more computationally expensive. Moreover, the algorithms proposed in this paper do not require any computations to be performed but only table look up operations for encryption and decryption.

IV. PROPOSED METHODOLOGY

SMS messages are sometimes used for the interchange of confidential data such as social security number, bank account number, password etc. A typing error in selecting

a number when sending such a message can have severe consequences if the message is readable to any receiver. Most mobile operators encrypt all mobile communication data, including SMS messages but sometimes even when encrypted, the data is readable for the operator. Among others these needs give rise for the need to develop additional encryption for SMS messages, so that only accredited parties are able to engage communication.

In this application for sending encrypted SMS messages using cryptographic methods based on theory of Quasigroups is proposed. The encryption algorithm is characterized by a secret key.

Our approach to this problem is to develop an application that can be used in mobile devices to encrypt messages that are about to be sent. Naturally decryption for encrypted messages is also provided. The encryption and decryption are characterized by a secret key that all legal parties have to posses.

In addition to cryptographic strength, things to consider when developing this type of an application for mobile devices are limitations in memory and processing capacity. Quasigroups are well suited for encryption of this type of data. The cryptographic strength of Quasigroup based encryption has been examined.

V. PROJECT ARCHITECTURE

Architecture of Secure SMS Banking using Quasigroups consists of following blocks:

- User 1
- User Interface
- Mobile Operator
- Bank
- Verification Agency
- User 2

The Secure SMS Banking is intended to help the user to avail banking facilities via the SMS. Application that takes as input as SMS having details of user's account number ,password and money to transfer and transfers the money to receiver. All above mentioned blocks are connected to each other in a systematic way to fulfill the purpose of application. Explanation of different blocks in this architecture is as follows:

1. User: Any person who is an authenticated account holder of the bank. There are mainly two types of user that interact with the system: user that just uses this application to get transfer money and the bank that verifies the details and permits the transaction.

User Class-1:

These users will input account number, password to avail banking services.

User Class-2:

The bank will decrypt the SMS and verify the user and then permit the transaction.

2. User Interface: It is an interface provided to user for interacting with application. The user will be presented with the application view that asks a user to input its details. On successfully inputting the SMS will be encrypted using quasigroups algorithm.

3. Mobile operator: The mobile operator will forward the SMS to the bank. While confirming, it will forward the SMS to the user.

4. Bank: The bank will decrypt the SMS and verify the user and permit the transaction.

5. Database: This is a security-centric product and it needs to store the data for the bank to verify. For that, a database is used. The System application will communicate with the database. Care is taken to make this communication secure. Verification Agency of the bank maintains the data integrity.

6. Output: The receiver will be notified and the sender will receive a SMS regarding the successful transaction.

VI. ALGORITHM

Example 1: Table 1 presents a quasigroup of order 6. The left most column and the top most row are index numbers. An initial seed element is chosen, say $s = 3$, and let the input data stream be represented by $\{m1, m2, m3, m4, m5, m6, m7, m8\} = \{1, 5, 4, 2, 6, 4, 5, 3\}$. Then the encryption process produces an encrypted output stream $\{c1, c2, c3, c4, c5, c6, c7, c8\}$ as follows:

Quasigroup encryption:

1. Let qGroup[][] represent the quasigroup matrix
2. To encrypt m_i s do,
   Set c_1 = qGroup[s][m_1]
   For $i > 1$, repeat until all m_i s are encrypted
   c_i = qGroup[c_{i-1}][m_i]

Table I: A QUASIGROUP OF ORDER 6

.	1	2	3	4	5	6
1	1	3	2	6	4	5
2	2	6	4	5	1	3
3	3	2	6	4	5	1
4	4	5	1	3	2	6
5	5	1	3	2	6	4
6	6	4	5	1	3	2

Table 1: INVERSE FOR THE QUASIGROUP IN TABLE I

.	1	2	3	4	5	6
1	1	3	2	5	6	4
2	5	1	6	3	4	2
3	6	2	1	4	5	3
4	3	5	4	1	2	6
5	2	4	3	6	1	5
6	4	6	5	3	2	1

Execution of the encryption operation for the given input stream is shown below:

$$c1 = s \,.\, m1 = 3 \,.\, 1 = 3$$
$$c2 = c1 \,.\, m2 = 3 \,.\, 5 = 5$$
$$c3 = c2 \,.\, m3 = 5 \,.\, 4 = 2$$
$$c4 = c3 \,.\, m4 = 2 \,.\, 2 = 6$$
$$c5 = c4 \,.\, m5 = 6 \,.\, 6 = 2$$
$$c6 = c5 \,.\, m6 = 2 \,.\, 4 = 5$$
$$c7 = c6 \,.\, m7 = 5 \,.\, 5 = 6$$

$$c8 = c7 \,.\, m8 = 6 \,.\, 3 = 5$$

The above encryption operation is a table look up operation over Table 1.

For the decryption operation, inverse quasigroup matrix is constructed (Table 2). To construct the invQGroup matrix, do the following: in the j^{th} column of the i^{th} row in invQ-Group matrix write the column number of element j from the i^{th} row in qGroup matrix.

To decrypt do the following:

1. m_1 = invQGroup[s][c_1]
2. For $i > 1$, do until all c_i s are decrypted

$$m_i = \text{invQGroup}[c_{i-1}][c_i]$$

In general, the direct application of the above encryption algorithm is very effective in randomizing the input data stream. However, given an input data stream and its corresponding output data stream a known plain text attack can be launched because qGroup[c_{i-1}][m_i] = c_i [3].

VII. Implementation Details

Fig.1

VIII. Conclusion

With this implementation of quasigroup transformation for encrypt and decrypt SMS messages, we happen to implement a protocol of secure mobile communication. The SMS communication is widely used and it is a service that can be used in a combination with other services. Services like mobile payment, identity checks, digital signatures, one-time passwords, etc. can be implemented using SMS services in combination with this protocol.

We have implemented a real application that used this protocol for exchanging SMS messages. An application using this protocol is working in real time on standard mobile devices. It can be easily upgraded to become a protocol that can offer other mobile services based on SMS messages.

This protocol is resistant to the main kinds of the attacks to secure mobile communications.

References

[1] Smile Markovski and Aleksandra Kuzmanovska : Secure SMS Communication Based on Quasigroup Transformations , 2009.
[2] V.A. Shcherbacov : Quasigroups in Cryptology, 2009.
[3] Matthew Battey, Abhishek Parakh : An Efficient Quasigroup Block Cipher, Springer Science+Business Media New York 2012.
[4] Borujeni, S. (2000). Speech encryption based on fast fourier transform permutation. In *The 7th IEEE international conference on electronics, circuits and systems, 2000 (ICECS 2000)* (Vol. 1, pp. 290–293).
[5] Mosa, E., Messiha, N., & Zahran, O. (2009). Chaotic encryption of speech signals in transform domains. In *International conference on computer engineering systems, 2009 (ICCES 2009)* (pp. 300–305).
[6] Ian, G. S., Blake, F., & Smart, N. P. (2005). *Advances in elliptic curve cryptography*. Cambridge University Press.
[7] Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). Ntru: A ring-based public key cryptosystem. In *Lecture Notes in Computer Science* (pp. 267–288). Springer: Berlin.

