Authenticated and Secure End-To-End Communication Channel Using SMS Messages

Abdullah A. Abdullah
Lect. Assistance

Computer Science Department
College of computer and Mathematic Sciences
University of Mosul
aaamoa@gmail.com

استخدام الرسائل النصية القصيرة لتوفير قناة اتصال موثوقة وامنة بين طرفين

الملخص

يعد تأسيس وتطبيق قناة امنة للاتصال ونقل البيانات بين طرفين عبر بيئة اتصال غير امنة ابتداءا من المسائل المهمة في علم التشفير الحديث. ان خدمة الرسائل النصية عبر الهاتف النقال تعد واسعة الانتشار وسهلة الاستخدام من قبل المستخدمين حيث يتم ارسال تقارير لمعلومات حساسة ومهمة وخاصة في مجال الاعمال التجارية وارسال كلمات المرور وغير ذلك. وعادة يتم ارسال هذه الرسائل على شكل نص صريح عبر شبكات الهاتف المحمول وعبر الجو وربما من خلال شبكة الانترنت بصياغة مفهومة. هذا يمكن اي شخص متصنت وقادر على الولوج الى الشبكة وربما عبر الجو ايضا من قراءة او تغيير محتوى الرسالة.

في هذا البحث تم تقديم طريقة لتوفير السرية وتتكون من خطوتين، الاولى هي استخدام طريقة الدالة الهاشية الامنيةSHA-1 لتوليد شفرة توثيق للرسالة حيث تضاف الى شفرة توثيق الرسالة السابقة ومفتاح سري مشترك لتكوين المفتاح الاولي. وفي الخطوة الثانية ستستخدم قيم هذا المفتاح كمدخلات الى معادلة رياضية بصيغة (اسبقية العملية) مشتقة من مجموعة عمليات ودوال متوفرة من قبل البيئة البرمجية المستخدمة ومستخرجة من جدول خاص بها. ان القيم المخرجة من هذه المعادلة تمثل مفتاح التشفير النهائي الذي سيستخدم في التشفير وهو من نوع مفتاح الوقت الواحد. اخيرا سيتم ارسال الرسالة المشفرة ثم يعقبها عملية بعثرة لجدول الدوال لزيادة السرية. ان طرق مفتاح الوقت الواحد تعتبر من اكفأ طرق التشفير. لذا فالرسالة المشفرة ستنتقل بامان بين الهاتف المحمول والشبكة ومن خلالها ايضا.

ABSTRACT

One of the key issues of modern cryptography is the problem of establishing a secure end-to-end communication over an insecure communication channel. Short Message Service (SMS) is a hugely popular and easily adopted communications technology for mobile devices. Users conduct business, disclose passwords and receive sensitive notification reports from systems using this communication technology. SMSs by default are sent in clear text form within the serving GSM (Global System for Mobile communications) network, Over The Air (OTA), and potentially over the public Internet in a predictable format. This allows anyone accessing the GSM system to read, and or modify the SMS content even on the fly.

In this paper, we present an approach mainly consists of two steps, first, SHA-1 authentication is used to generate a message digest that is combined with previous message digest and a shared secret key to form an initial key stream. Secondly, this key will be used as input to a mathematical equation derived in prefix notation from randomly selected set of operators and functions supported by the software platform extracted from special table. The final key stream is the output of this equation which is a one time pad to encrypt the original message text. Lastly, encrypted SMS message will be sent and a randomized operation will be then applied to that table. A one-time pad, considered to be the only perfectly secure cryptosystem, secures an SMS message for transport over any medium between a mobile device and the serving GSM network and through it too.

Keywords: SMS encryption, SMS authentication, SHA-1**.**

I. INTRODUCTION

The Global System for Mobile communications (GSM) is a popular digital circuit switched network [10]. GSM is a common telecommunications standard originally issued by the European Telecommunications Standards Institute (ETSI) [19]. GSM provides recommendations, not requirements. The GSM specifications define the functions and interface requirements in detail but do not address the hardware. The reason for this is to limit the designers as little as possible but still to make it possible for the operators to buy equipment from different suppliers.

The initial Short Message Service (SMS) standard was first discussed in the early 1980s but the world's first commercial SMS service was not introduced until 1992. SMS was created as part of Phase I of the GSM standard. SMS is widely adopted with approximately 1 billion SMS messages sent every day worldwide [18]. The SMS message, as specified by the ETSI organization in documents GSM 03.40 [19] and GSM 03.38 [4], can be up to 160 characters long, where each character is 7 bits according to the 7-bit default alphabet. Eight-bit messages (max 140 characters) are usually not viewable by the phones as text messages; instead they are used for data in e.g. smart messaging (images and ringing tones) and Over The Air (OTA) provisioning of Wireless Application Protocol (WAP) settings . 16-bit messages (max 70 characters) are used for Unicode (UCS2) text messages, viewable by most phones. A 16-bit text message will on some phones appear as a Flash SMS (aka blinking SMS or alert SMS). The Short Message Peer-To-Peer Protocol (SMPP) [20], is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities such as short message service centers (SMSCs).

SMS makes use of the Mobile Application Part (MAP) [6], which defines methods and mechanisms of communication in wireless networks between peer entities. However, MAP is an unencrypted protocol allowing anyone with access to the signaling system the ability to read and or modify SMS messages. With an increase of SMS messages being used to communicate sensitive information, such as banking information, and now also being used in search queries [9], the need arises to find a solution to ensure these SMS messages are secure and the content remains private.

A one-time pad [6] is a very simple yet completely unbreakable symmetric cipher where the same key is used for encryption and decryption of a message. To use a one-time pad, you need two copies of a "pad" or key which is a block of truly random data.

To encrypt a message each bit of each letter in the plaintext is combined with the corresponding letter's bit in the pad in sequence using a transformation called the bitwise exclusive or (XOR). If the key is truly random, an XOR-based one-time pad is perfectly secure against cipher text cryptanalysis. A pad is only used once and discarded, hence the name one-time pad.

In this paper we provide a solution to the SMS security problem. Our approach is to secure an SMS message using mixture of shared secret information and a couple of authenticated message digests of current and previous messages sent over the channel between both parties.

II. BACKGROUND

A. GSM Architecture

The GSM system has two major components: the fixed installed infrastructure (network) and the Mobile Station (MS) [5] [21]. Mobile users make use of the serving GSM network's services by communicating over a radio interface. Figure 1 illustrates GSM architecture.

The Mobile Station (MS) is the mobile phone or GSM compliant device. The Base Transceiver Station (BTS) is a radio tower or pico (single) cell with which the Mobile Station communicates. The Base Station Controller (BSC) acts as a common node between multiple BTSs and the network's backbone. The Mobile Switching Centre (MSC) performs the switching functions of the network. The MSC has an interface to one or more BSCs and to external networks. Several databases are available for control and network management.

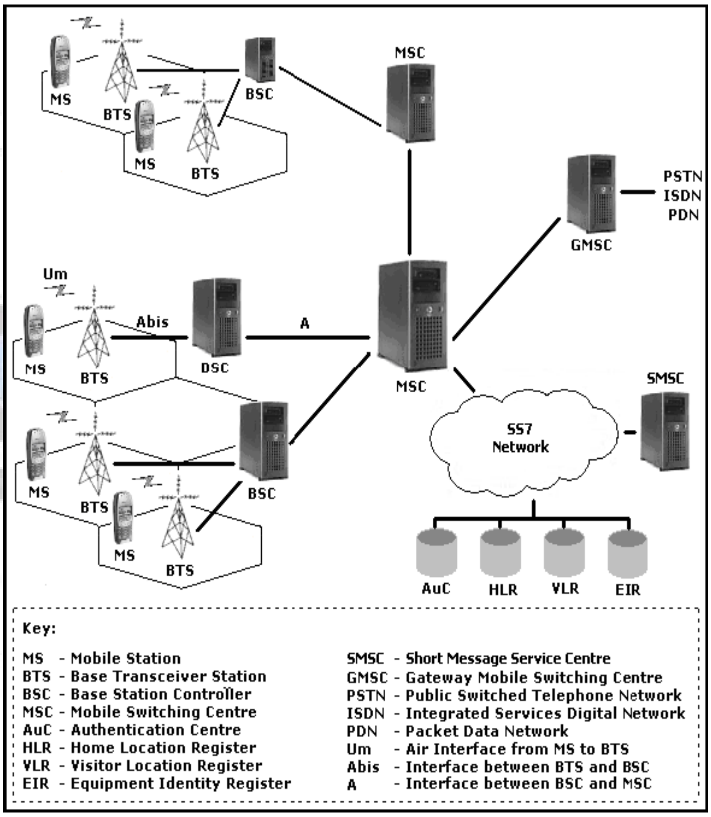
MS
BTS
BSC
MS
BTS
MSC
PSTN
ISDN
PDN
GMSC
Um
Abis
A
MS
BTS
DSC
MSC
SMSC
SS7 Network
MS
BTS
BSC
MS
BTS
AuC
HLR
VLR
EIR
Key:
MS - Mobile Station
BTS - Base Transceiver Station
BSC - Base Station Controller
MSC - Mobile Switching Centre
AuC - Authentication Centre
HLR - Home Location Register
VLR - Visitor Location Register
EIR - Equipment Identity Register
SMSC - Short Message Service Centre
GMSC - Gateway Mobile Switching Centre
PSTN - Public Switched Telephone Network
ISDN - Integrated Services Digital Network
PDN - Packet Data Network
Um - Air Interface from MS to BTS
Abis - Interface between BTS and BSC
A - Interface between BSC and MSC

Figure. 1. GSM Architecture (adapted from [12])

B. SHORT MESSAGE SERVICE

Short Message Service (SMS), is characterized by an out-of-band packet delivery and low-bandwidth message transfer, which results in a highly efficient means for transmitting short bursts of data. SMS works on a store-and-forward basis and when received, is stored on the SIM card or on the MS's internal store. An SMS is transferred in a connectionless packet mode over the signaling channel of the serving GSM network. Once a message is sent, it is received by a SMSC (refer to Figure 1), which must then get it to the appropriate recipient mobile device via the MSC [9].

SMS messages travel between several network nodes before being delivered. We now describe the process flow when an SMS message is sent from one sender MS to a recipient MS.

1) The SMS message is submitted from the sender MS to the SMSC
2) After the message is processed at the SMSC, it sends a request to the HLR and receives routing information for the recipient MS
3) The SMSC sends the SMS to the MSC
4) The MSC retrieves the recipient's information from the VLR. This may include an authentication operation between the MSC and VLR
5) The MSC forwards the message to the recipient MS
6) If delivered successfully, the SMS is stored on the recipient MS's SIM card under USER-DATA
7) The MSC returns to the SMSC the outcome of the SMS delivery status
8) If requested by the sending MS, the SMSC reports delivery status of the SMS back to the sender

III. Security of SMS communication

A. Network vulnerabilities identification and analysis

SMS messages are delivered in a best effort manner to other cellular telephone users asynchronously through the cellular network. These networks operate separately from the internet and are sometimes considered to be more secure, accessible and less open to misuse (such as spam). However the GSM network does not provide important security services such as mutual authentication, end-to-end security, non-repudiation or user anonymity [16].

Many users are used to SMS messaging so much that they prefer it to voice calls. It is important to realize the fact that SMS messaging – though attractive – introduces security problems for both parties of communication, especially if it is used for exchange of sensitive information, which should not be available to third parties. In this section we present the vulnerabilities identified in [11] that occurs within a mobile environment. Let us review some of the risks.

1. *Easy interception of SMS messages:*

   SMS messages can be intercepted (wiretapped) very easily. Costs of wiretaps are lower than in voice communication. For an operator, it is easy to scan all SMS going through their network for keywords, which is often really done. Also wiretap devices can be bought on black market from many corporations and private detectives.

2. *Capturing and Modifying of data during OTA transmission*

   SMS messages are sent across the air interface between the MS and BSS. In most GSM networks all traffic (digitized voice and data) and signaling data sent across this air interface is encrypted optionally, using one of two GSM-specific algorithms known as A5/1 or A5/2. The A5 algorithm is a symmetric cipher. Biryukov, Shamir and Wagner [1] demonstrated that the secret key could be cracked in minutes, rendering A5/1 only to counter casual eavesdropper and A5/2 completely insecure.

3. *Compromise of text due to users' error:*

   SMS is more persistent than a call. So, if you forget to delete an incoming or outgoing SMS, it will be present in your phone until you delete it finally. Now, if you leave your phone for a few minutes, anyone can look into your SMS list and read the secrets. This, of course, also concerns situations when your phone is stolen.

4. *Long lifetime*

   SMS are very small in size, and therefore can be stored easily. Currently, when a gigabyte of storage capacity costs less than $1, the possibility of long-term archivation is clear. So, some people could have access to a long history of your SMS communication.

5. *Danger of message modification*

   SMS message, going through operator's network in plaintext, can be not only intercepted, but also modified. For example, identity of the sender can be altered, or the text changed. One can never be sure, whether a normal SMS has been received in the same form as it has been sent, and who is the real author. The network acts as a black-box to both parties of communication.

6. *SMS Spoofing to the MS or AS*

   The possibility exists that an attacker manages to inject SMS messages into the messaging network with a ‘spoofed’ originator IDs. The attack can be applied in both ways by impersonating the AS for a legitimate MS or impersonating the MS for a legitimate AS. With the former case, the possibility of spoofing is very high as it is possible to send SMS message from the internet with the correct headers, without the recipient being able to detect that it comes from the internet. Also the mobile service provider is able to change the originator ID.

In the latter case, the possibility of spoofing is also high; however the attacker is required to know the authenticating information of the user. This depends on how the SMS service is implemented. If the attacker can manage to spoof an SMS message, fraudulent transactions can be conducted.

B. Features of real SMS protection: must fulfill the following requirement [8]:

1. Security against eavesdropping

Messages between two users are encrypted and a key derived from a hybrid security information. An adversary which monitors the communication seems only a senseless sequence of binary data, and is unable to decrypt them without knowledge of having previous message and the secret password. Also, the keys (passwords) can be changed very easily, when the two sides agree upon new ones.

2. Protection of integrity of messages

Any encrypted message exchanged between two end users includes a special security code (MD) based on SHA-1 standard. This code prevents anyone in the network from altering contents of the message. If a single bit is changed, the message's code will not match anymore and the receiving user will be notified about decryption failure.

3. Prevention of impersonation attacks

Successful decryption of a received message is also a proof of the fact that the sending person has the correct key. Without knowledge of the key, the adversary is unable to generate a message which would decrypt into correct text on the receiving side. Therefore, the fact that a message has been really sent by its author, is ensured.

4. Protection of saved messages from reading

All received and sent messages of our proposed system, which are saved into the phone, are protected by encryption, with use of SHA-1 and our MOF encryption method. At each start, the system asks for the, main application password. Without it, it cannot decrypt the data correctly. Any adversary which gets access to your saved data will need to guess the correct password as well. In case of a good password, checking of all possibilities will takes long time.

IV. CRYPTOSYSTEMS: Secure Hash Function And One-Time Pad

A cryptosystem is a mechanism that allows two or more users to communicate in a secure manner, that is nobody but these users must be able to learn the content of the communication message. Every message, denoted by *m*, is subject to an encryption operation, denoted by *E*. The encrypted message is often referred to as cipher text. In order to recover the original message from a given cipher text a decryption operation, denoted by *D* is performed [13].

A hash function *H* is a transformation that maps an arbitrary length message M to a fixed length message digest (MD), often referred to as the hash value or *MD* = *H*(*M*). The basic properties of a hash function are:

- The description of *H( )* is publicly known with no hidden information
- *H*(*M*) is relatively easy to compute for any given *x*
- *H*(*M*) is one-way meaning its difficult to invert such that given MD, it is hard to find a message M where H(M) = MD, and given M and H(M), it is hard to find a message M' (≠M) such that H(M') = H(M)

SHA-1 [14] algorithm is a popular algorithm for generating cryptographic hash functions. SHA-1, considered the successor to MD5 [17], produces 160-bit output while MD5 produces 128-bit output.

A perfect, or unconditionally secure cryptosystem, is an encryption technique that can not be broken even if unlimited time and computational power were present. A common example of a perfect cryptosystem is the Vernam cipher, often referred to as one-time pad. At a character-level, all the bits in the first letter of the message *m* are XORed with all the bits in the first letter of the key *k*. This produces a binary pattern of the encrypted letter [15]. The one-time pad has the following requirements, namely:

- Each key *k* is used only once
- The key *k* used to encrypt a message *m* is at least as long as *m*,
  that is $length(k) \geq length(m)$

- Each key *k* is random and unpredictable

If these requirements are satisfied, the one-time pad is an unconditionally secure cryptosystem. However, the one-time pad has some associated difficulties in its practical implementation. These include the fact that a new truly random secret key must be issued prior to every communication and must be significantly long for large messages. Again, once a key is generated it must be distributed between the communicating parties. This aspect is commonly referred to as the key distribution problem, as the key *k* used in the encrypting and decrypting of messages *m* must only be shared between the communicating parties.

V. PRACTICAL

The main goal of this work is to create a safe communication channel between two parties through unauthenticated and insecure environment (i.e. SMS messages), which can then be sent over mobile networks. Due to the limited capabilities of the mobile phone in processing speed, memory size and SMS small size (140 byte), so the proposed algorithm should be suitable to these mentioned constraints.

A. SHA authenticates SMS message:

SHA-1 hash algorithm from variable length input produces 160-bit output. The idea of using SHA-1 algorithm to authenticate SMS messages is really simple, the message plain text which is entered from user will be considered as input to SHA-1 algorithm in order to produce 160-bit message digest which we call CMD (Current Message Digest). This message digest then will be stored in front of message text (i.e. resides in first 20 bytes of the message). After that the user should select an integer value that indicates the complexity of ciphering equation which we call OFTD (Operators and Functions Tree Depth) explained later, this means that the first 21 bytes is allocated to message header.

Current Message Digest CMD	operators and functions tree depth OFTD	Plain text
20 byte (160 bit)	1 byte (8 bit)	n bytes

SMS Message proposed structure

From section I, we recall that an SMS User Data (the message) is 140 bytes long. The message body thus contains 1120 bits (140 x 8) of data which exists in clear text form. For example if message body was full (i.e. 140 byte) in length, then 119 bytes will be only specialized for actual plain text storage.

An important thing to notice, that is where CMD is the output of the SHA-1 hash for input M. The CMD is insufficient for a strong cryptosystem, so with addition of PMD (Previous Message Digest) and SSK (Shared Secret Key) which is only known by the two parties; the probability of an interception from an eavesdropper is minimal.

B. Encryption using Mathematical Prefix Equation (MPEQ):

A perfect, or unconditionally secure cryptosystem, is an encryption technique that can not be broken even if unlimited time and computational power were present. So our proposed encryption will depend on using a mixture of symmetric cipher features (i.e.

SSK) and employing message authentication process with a time-differ message digests (i.e. PMD and CMD). Finally cipher key is generated by a mathematical equation derived in a randomized style as follows.

Cipher Key Generation

For the simple reason that one time pads require the key *k* used to encrypt a message *m* to be at least as long as *m*, we propose a two step process of generating the cipher key satisfying this condition in order to be finally XORed with original message text:

1. *Initialize Key Stream (IKS)*: which consist of multiples of 400 bit or 50 byte repeated stream consist of previous message digest (160 bit), current message digest (160 bit) and shared secret key (80 bit) such that:

   IKS = (k_1, k_2, k_3, …, k_i) where k_1= k_2 = k_3 …

   The count of ki depends on the length of original message text as illustrated below

PMD	CMD	SSK	PMD	CMD	SSK	…
160 bit	160 bit	80 bit	160 bit	160 bit	80 bit	…

Initialize Key Stream (IKS)

2. *Final Key Stream (FKS):* This process involves applying a set of mathematical operators and functions that supported by software platform which applied in, this set is to be selected in random fashion to ensure the one time aspect for the final cipher key as follows:

   a. The first n bytes of IKS is considered as indices in a Mathematical Operators and Functions Table (MOFT) to select the corresponding set of operators and functions as in Figure 2, our table size was 16 record so each byte value must be a module to base 16 in order to prepare right indices values. The value of n is equal to the value of the first byte before the original message text portion started which we call operators and functions tree depth OFTD (i.e. byte no. 21) which is selected by sender.

Byte no.	1	2	3	4	5	6	7	8	…
Values	4	3	15	0	2	3	0	10	

a. Beginning bytes of IKS stream

Index	Operator or Function	Binary or Unary
0	cos	1
1	*	0
2	%	1
3	log	1
4	sin	0
5	exp	0
…	…	…
15	+	

b. MOFT table state

Figure. 2. Using IKS to Select set of operators and functions

b. The selected set of mathematical operators and functions is then used to form a mathematical equation represented in prefix expression notation and all the needed arguments will be inserted for expression completeness. Then the input x is equaled to IKS stream to generate the final key stream FKS which is then XORed with the original text to produce the cipher text message.
For example if OFTD = 5 then set of equations is {% , cos , + , log , sin}
Figure 3, shows the complete mathematical encryption equation in prefix notation after inserting the needed arguments with consideration of binary or unary types, so the final equation will be as follows:

$$Y(x) = \%(\cos(+\,(\log(\sin(\,x\,)),\,x)),\,x) \quad \text{, where } x = \text{IKS.}$$

This means that every byte value of IKS will be applied to five operations in order to generate the corresponding encryption key value that is used to encrypt the corresponding original message byte value.

Now we can summarize our proposed encryption process as in the following notation:

CMD = SHA-1 (M)
IKS = {PMD || CMD || SSK}^{n}
FKS = MOF_equation (IKS)
C = E (FKS, M)

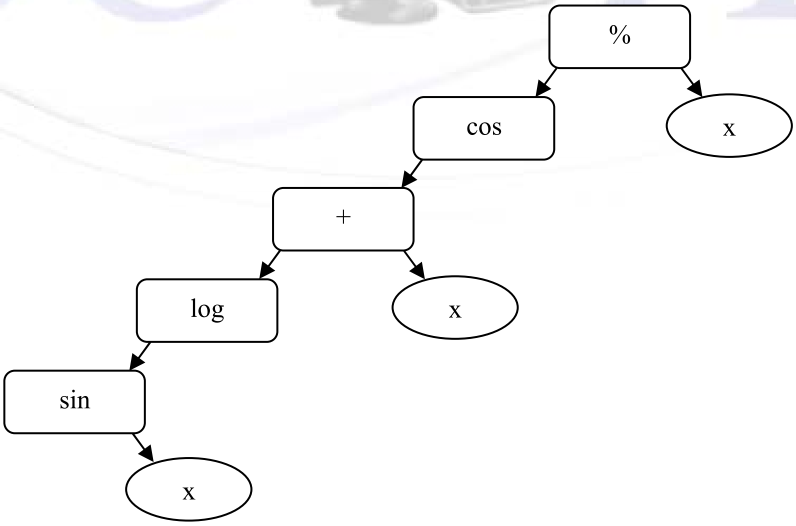

Figure. 3. Prefix mathematical equation with inserted arguments

C. Re-indexing MOFT:

In order to support one time pad feature, the last step of our proposed algorithm is to re-index the mathematical operators and functions table to prepare it to next message ciphering process. The re-indexing schema is to be applied using shifting technique by considering the OFTD value as index of the new first record in this table as in Figure 4.

This step participates in randomizing the cipher key stream which will be used in the encryption process for the next SMS message, and ensuring that next encryption parameters will defer even if same SMS message was sent again, therefore security level will increase.

Index	Operator or Function	Binary or Unary
0	cos	1
1	*	0
2	%	1
3	Log	1
4	Sin	0
5	exp	0
…	…	…
15	+	

a. Before re-indexing

Index	Operator or Function	Binary or Unary
5	exp	0
6	-	1
7	tan	0
8	/	1
9	acos	0
10	pow	1
…		
4	sin	0

b. After re-indexing

Figure. 4. MOFT table re-indexing with OFTD = 5

D. Proposed Sending algorithm

The algorithm as in Figure 5 begins by reading the user SMS message that is entered by the user. The byte stream of message plain text then used as an input to the SHA-1 method in order to obtain a message digest (CMD ,160 bit or 20 byte), after that the initial cipher key will be formed from three parts: previous message digest, current message digest and shared secrete key.

Our proposed encryption method depends on a cipher key stream generated as output of randomly-formed mathematical equation to be XORed with the original plain text stream producing the final cipher text message. So, before the encryption process started, a mathematical equation should be produced. This process is performed as follows, firstly OFTD value is used to specify the indices from IKS beginning stream to select the mathematical operators and functions in order to form a mathematical prefix equation. After that needed operands are inserted to form a true prefix style equation, secondly, IKS is sent as input to this equation and the output is the final cipher key stream which will be XORed with the original plain text of SMS message to produce the ciphered SMS message to send it.

In order to strength the security and to support the one-time property of the cipher key stream which will be used in the encryption process for the next SMS message, so the final step is re-indexing MOFT table using OFTD value as a transposition key in order to randomize this table. This process ensures that next encryption parameters will defer even if same SM message was sent again.

E. Proposed receiving algorithm:

1. Extract CMD, OFTD and ciphered text stream from received message
2. Create IKS = PMD || CMD || SSK with repetition if needed
3. Extract selected operators and functions from MOFT according to OFTD value
4. Build the mathematical prefix equation
5. Producing FKS by applying MPEQ to IKS
6. Decrypting message text by XORing with FKS

7. Apply SHA-1 to produce MD and compare it with CMD extracted from received message to satisfy message authentication and display the original plain text
8. Re-indexing MOFT by shifting depending on OFTD value
9. Store CMD to be used as PMD for next message ciphering process

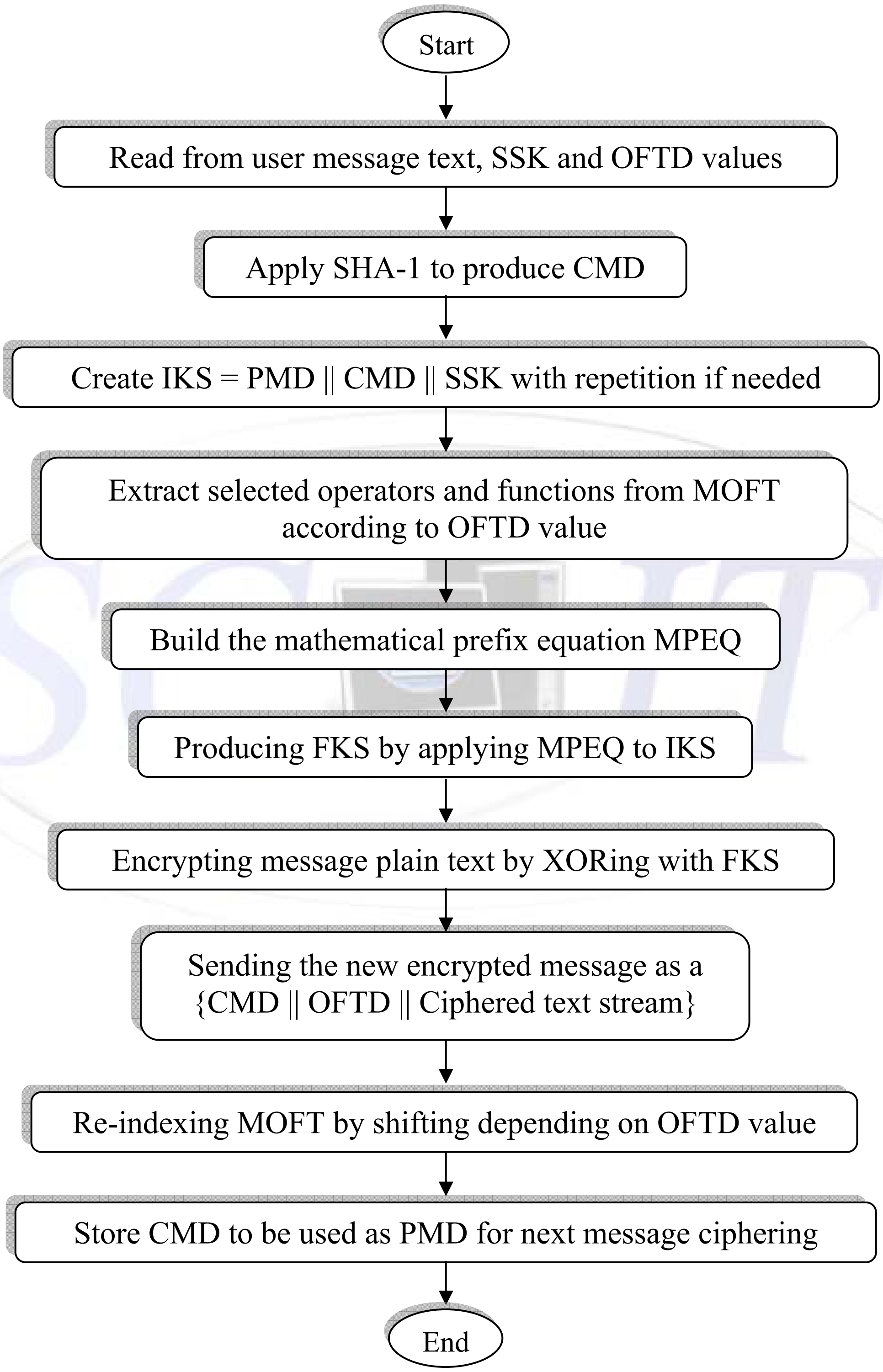
Start
Read from user message text, SSK and OFTD values
Apply SHA-1 to produce CMD
Create IKS = PMD || CMD || SSK with repetition if needed
Extract selected operators and functions from MOFT according to OFTD value
Build the mathematical prefix equation MPEQ
Producing FKS by applying MPEQ to IKS
Encrypting message plain text by XORing with FKS
Sending the new encrypted message as a {CMD || OFTD || Ciphered text stream}
Re-indexing MOFT by shifting depending on OFTD value
Store CMD to be used as PMD for next message ciphering
End

Figure. 5. Flow chart of proposed sending algorithm

SCIT

VI. CONCLUSION AND FUTURE WORKS

In this paper we have presented a proposed algorithm to securing SMS messages, which at present are inherently insecure. We began by providing a description of GSM architecture and SMS messages, how they are composed and sent. Afterward, we gave a detailed description of current SMS messages security features and vulnerabilities followed by a real protection software requirements.

Our devised approach mainly consists of two steps, authentication and encryption. Firstly, SHA-1 authentication is used to generate a message digest that is combined with previous message digest and a shared secret key to form an initial key stream. Secondly, this key will be used as input to a mathematical equation derived in prefix notation from randomly selected set of operators and functions supported by the software platform from special table. The final key stream is the output of this equation which is a one time pad to encrypt the original message text. Finally, encrypted SMS message will be sent and a randomized operation applied to that table.

With this, one-time pad considered an unbreakable symmetric cipher, and the complete-key distribution problem eliminated, our approach allows for secure messaging at an acceptable level while not physically altering the underlying GSM network.

Future work includes investigating the speed and computational complexity for a Mobile Station in generating one-time pad with increasing the number of used mathematical functions in order to boost the security level and also the addition of a computational time indicator to every operator and function to notify the user about expected time needs and help the user to select a suitable set of functions.

VII. REFERENCES

[1] A Biryukov, A Shamir, and D Wagner, 2000. Real Time Cryptanalysis of A5/1 on a PC. [Online]. Available: http://cryptome.org/a51-bsw.htm.

[2] Digital cellular telecommunications system (Phase 2+), 1998, Technical realization of the Short Message Service (SMS); Point to Point (PP)(GSM 03.40 version 6.0.0), European telecommunications Standard Institute, ETSI.

[3] B. Schneier, 1996, *Applied Cryptography: Protocols, Alorithms and Source Code in C*. Wiley Computer Publishing, John Wiley and Sons, Inc.

[4] Digital cellular telecommunications system (Phase 2+), 1998, Alphabets and language-specific information (GSM 03.38 version 7.0.0 Release 1998), European telecommunications Standard Institute, ETSI.

[5] E. T. 929, 1999, “Digital cellular telecommunications system (Phase 2); Security related network functions,” European Telecommunications Standards Institute.

[6] GSM Recommendation 09.02, “Mobile Application Part (MAP) Specification,” European Telecommunications Standards Institute.

[7] K. R. R. Schusteritsch, S. Rao, 2005, “Mobile Search with Text Messages: Designing the User Experience for Google SMS,” in *Technology, Safety, Comminity (CHI)*, Conference on Human Computer Interaction. Portland, Oregon, USA: ACM, pp. 1777–1780.

[8] Lo JL, Bishop J and Eloff JHP 2008, 'SMSSec : an end-to-end protocol for secure SMS', Computers & Security, vol. 27, no. 5-6, pp. 154-167.

[9] M. Rahnema, 1993, “Overview of GSM system and protocol architectures,” *IEEE Communications magazine*.

[10] M. Rahnema, 1993, “Overview of the gsm system and protocol architecture,” IEEE Communications Magazine, vol. 31, no. 4, pp. 92–100.

[11] Mobile Payment Forum 2003. Risks and Threats Analysis and Security Best Practices for Mobile 2-Way Messaging Systems. [Online]. Available: http://www.mobilepaymentforum.org/pdfs/MPF_Security_Best_Practices.pdf.

[12] N. Croft, 2003, “Secure Interoperations of Wireless Technologies,” Masters Dissertation, University of Pretoria, School of Computer Science.

[13] N. Ferguson and B. Schneier, 2003. *Practical Cryptography.* Indianapolis, Indiana: Wiley Publishing, 75-82, 89-91, 233, 350-352.

[14] National Institute of Standards and Technology, 1995, NIST FIPS PUB 180-1, “The Secure Hash Algorithm (SHA-1),” US Department of Commerce, Tech. Rep.

[15] NJ Croft and MS Olivier, 2005, "Using an approximated One-Time Pad to Secure Short Messaging Service (SMS)," *Southern African Telecommunication Networks and Applications Conference 2005 (SATNAC 2005) Proceedings*, Vol 1, 71-76, Champagne Castle, South Africa.

[16] O. Kolsi and T. Virtanen, 2004. MIDP 2.0 Security Enhancements. In *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii, 287 - 294.

[17] R. Rivest, 1992, “The MD5 Message-Digest Algorithm,” Internet Engineering Task Force, RFC 1321.

[18] R.Safavi-Naini, W.Susilo, G. 2001. Towards securing 3G mobile phones (extended abstract). In Networks. In Proceedings Ninth IEEE International Conference, 222–227.

[19] Recommendation GSM 02.09, 1993, Security related network functions, European telecommunications Standard Institute, ETSI, tech. Rep.

[20] Short Message Peer to Peer Protocol Specification v5.0, 2003, The SMS Forum.

[21] V. K. Garg, 1999, Principles and applications of GSM. Prentice Hall PTR.