SMS Security with RC4 Algorithm on Android OS

Kaung Htet Myint, Tun Myat Aung
University of Computer Studies, Yangon
kolynn.2013@gmail.com, tma.mephi@gmail.com

Abstract

Short Message Service (SMS) is a text messaging service component of mobile communication systems. It uses standardized communications protocols to exchange short text between mobile devices. SMS does not have any built-in procedure to offer security for the text transmitted as data. Most of the applications for mobile devices are designed and developed without taking security into consideration. In practical use, SMS messages are not encrypted by default during transmission. Confidentiality is the concept of ensuring that data is not made available or disclosed to unauthorized people. Confidentially is achieved through encryption. Both symmetric and asymmetric encryption can be used. Confidentiality was the original purpose of cryptography. Therefore, SMS Security on Android will be developed in the paper. It includes SMS network architecture and cryptographic protocols as theory background.

Keywords: SMS, security, encryption, confidentiality, cryptography.

1. Introduction

Data confidentiality is a protection of data from unauthorized disclosure. It is the most common aspect of information security. It not only applies to the storage of information, also applies to the transmission of information. We need to protect our sensitive information from malicious actions during transmission of SMS. Nowadays, there are many security issues and vulnerabilities related to SMS [4][7]. For data confidentiality security service, an decipherment security mechanism can be used.

Short Message Service (SMS) is a mechanism of delivery of short messages over the mobile networks. It is a store and forward way of transmitting messages to and from mobiles. The message (text only) from the sending mobile is stored in a central short message center (SMS) which then forwards it to the destination mobile. GSM (Global System for Mobiles), CDMA (Code Division Multiple Access) and TDMA (Time-Division Multiple Access) are supporting SMS.

Cryptography is the science of information and communication security [1]. Cryptographic system transforms a plaintext into a cipher text, using most of the time a key. Cryptography has two types of cypher. (1)Stream Cipher-In a stream cipher, encryption and decryption are done one symbol (a bit or byte) at a time. (2) Block Cipher - In a block cipher, a group of plaintext symbols of size are encrypted together creating a group of cipher text of the same size. RC4 is a stream cipher that is used to protect internet traffic as part of the Secure Socket Layer (SSL) [8].A data confidentiality approach to SMS on Android will be developed in the paper. It includes SMS network architecture and cryptographic protocols as theory background and it also includes design, implementation and confidentiality measurement of RC4 stream cipher for SMS data confidentiality on mobile networks.

The purpose of this paper is to provide data confidentiality during SMS message transmission period in order to prevent the SMS message from being illegally intercepted by illegal sources and to ensure the origin of the message from the legitimate sender. The structure of this paper is as follows. The section 2 includes Related Work. The section 3 includes basic concepts of SMS technology, SMS mobile network communication system, introduction to cryptography and RC4 cipher. In section 4, we discuss design and implementation of mobile applications that are used to protect data confidentiality of SMS message transmitted on mobile networks. The section 5 describes how statistical tests suite is used to measure data confidentiality. Finally, in section 6 we conclude our discussion by describing data confidentiality level of pseudorandom number sequence generated by RC4 cipher and by suggesting RC4 cipher should be used for data confidentiality of SMS message transmitted on mobile network communication system.

2. Related Work

Yu Loon Ng proposed Short Message Service (SMS) Security Solution for Mobile devices, where focused on the security of Short Message Service (SMS) and the Global System for Mobile communication (GSM) network and the use of encryption to protect SMS messages and encryption schemes was conducted to understand the properties of different encryption schemes and their applicability to SMS messages. The selected scheme was implemented in the form of a Secure SMS Chat application to validate the viability of the selected encryption scheme.

Aye Mya Mo Mo proposed Image Encryption Based On XTS-AES MODE where implemented secure image encryption using XTS-AES and WHIRLPOOL Hash function. This system improve integrity, confidentiality and suitable for parallel operation.

Myo Thinzar Aung proposed Secure Video Streaming System using SRTP and RC4 Algorithm where Ronald Rivest symmetirc key algorithm (RC4) uses for data encryption and then encrypted data is embedded into SRTP (Secure Real-Time Transport Protocol) header. The SRTCP (Secure Real-Time Transport Control Protocol), sender and receiver are generated for data acknowledgement.

3. Background Theory

3.1 Basic Concepts of SMS Technology

SMS messages are created by mobile phones or other devices (e.g.: personal computers). These devices can send and receive SMS messages by communicating with the GSM network. All of these devices have at least one MSISDN number. They are called Short Messaging Entities. The SMEs are the starting points (the source) and the end points (the receiver) for SMS messages. They always communicate with a Short Message Service Center (SMSC) and never communicate directly with each other[3]. An SME can be a computer equipped with a messaging software such as Ozeki NG - SMS Gateway[6]. Depending on the role of the mobile phone in the communication, there are two kinds of SMS messages: Mobile-originated (MO) messages and Mobile-terminated (MT) messages. MO messages are sent by the mobile phone to the SMSC. Mobile-terminated messages are received by the mobile phone. The two messages are encoded differently during transmission[9].

3.2 General SMS Architecture

SMS messages are transmitted over the Common Channel Signaling System 7 (SS7). SS7 is a global standard that defines the procedures and protocols for exchanging information among network elements of wire line and wireless telephone carriers [3]. These network elements use the SS7 standard to exchange control information for call setup, routing, mobility management, etc. Figure 1 shows the typical network architecture for SMS communication. Conceptually, the network architecture consists of two segments that are central to the SMS model of operation: the Mobile Originating (MO) part, which includes the mobile handset of the sender, a base station that provides the radio infrastructure for wireless communications, and the originating Mobile Switching Centre (MSC) that routes and switches all traffic into and out of the cellular system on behalf of the sender. The other segment, the Mobile Terminating (MT) part, includes a base station and the terminating MSC for the receiver, as well as a centralized store-and-forward server known as SMS Centre (SMSC). The SMSC is responsible for accepting and storing messages, retrieving account status, and forwarding messages to the intended recipients [9].

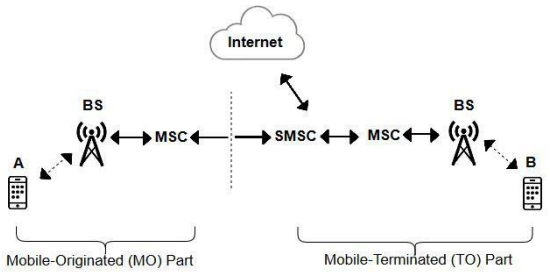

Figure 1. Mobile Network Architecture

The mobile Sender transfers the short message to the Network Operator .The Network Operator acknowledges the “Short Message” to the Sender. The Network Operator also sends the short message to the SMS Center. The SMS Center acknowledges the “Short Message” to the Network Operator. The SMS Center delivers the “Short Message” to the Network Operator. The Network Operator acknowledges the “forward Short Message” to the SMS Center. The Network Operator sends the “Short Message” to the

Receiver. The Receiver acknowledges the "Short Message" to the Network Operator.

3.3 Cryptography

Cryptography is the science of using mathematics to encrypt and decrypt data [2]. Cryptography enables you to store sensitive information or transmit it across insecure networks like the Internet so that it cannot be read by anyone except the intended recipient. Encryption is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext.

Cryptographic algorithms can be divided into:

(1) Private key/ Symmetric key algorithms

(2) Public key /Asymmetric key algorithms.

Symmetric key algorithms have the property that same keys are used for encryption and decryption. It is also called as private key encryption[1].

Asymmetric key algorithms have the property of using different keys and hence the decryption key cannot be derived from the encryption key. It is also called as public key encryption. This is a secret parameter for a specific message exchange context[1].

There are two types of symmetric-key algorithm:

- block cipher
- stream ciphers

(1) Stream Cipher - In a stream cipher, encryption and decryption operate on the basis of one symbol (a bit or byte) at a time, (2) Block Cipher - In a block cipher, encryption and decryption operate on the basis of a block of symbols of particular size.

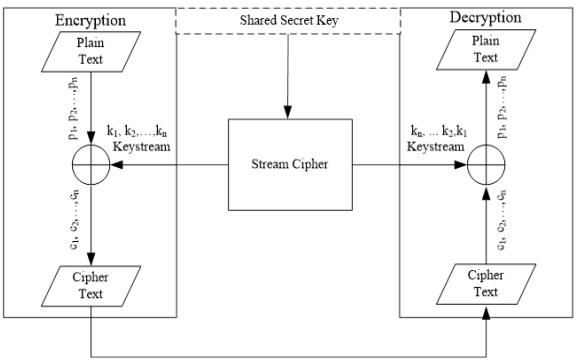

Figure 2. A Stream Cipher

3.4 RC4 Stream Cipher

RC4 is one of the most used software-based stream ciphers in the world. RC4(Rivest Cipher 4) was designed by Ron Rivest in 1987[8]. It is a standard of IEEE 802.11 within WEP (Wireless Encryption Protocol) and generates a keystream. This stream cipher consists of two parts:

(1) key-scheduling algorithm (KSA).

(2) Pseudo-random generation algorithm.

Key-scheduling algorithm (KSA) is used to initialize the permutation in the "S" box. keylength is number of bytes in key and range 1 to 256.

```
for i from 0 to 255
   S[i] :=i
endfor
j:=0
for i from 0 to 255
   j:=(j+S[i]+key[i mod keylength]) mod 256
   swap values of S[i] and S[j]
endfor
```

Pseudo-random generation algorithm (PRGA) modifies the state and outputs a byte of the keystream.

```
i :=0
 j:=0
 while GeneratingOutput:
i=(i+1) mod 256
j=(j+S[i]) mod 256
swap values of S[i] and S[j]
K:= S[(S[i]+S[j]) mod 256]
output K
endwhile
```

The RC4 algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this algorithm. During a N-bit key setup (N being your key length), the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing

operations. These mixing operations consist of swapping bytes, modulo operations, and other formulas. Once the encrypting variable is produced from the key setup, it enters the ciphering phase, where it is XORed with the plain text message to create an encrypted message. Once the receiver gets the encrypted message, he decrypts it by XORing the encrypted message with the same encrypting variable.

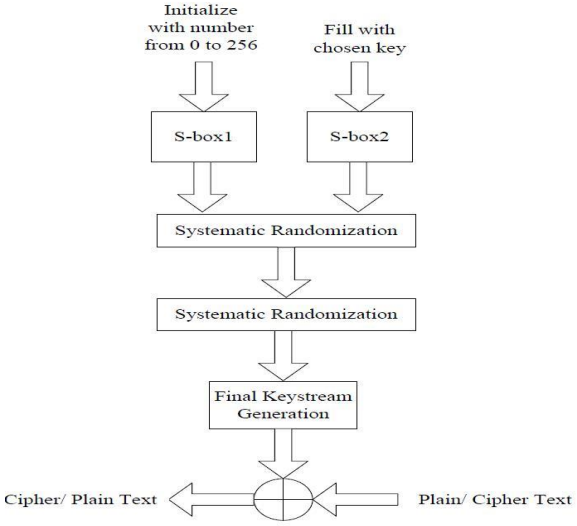

Figure 3. General RC4 Stream Cipher

4. Design and Implementation

The design for implementation of two android mobile applications, *SendSMS* and *ReceieveSMS*, is shown in Figure (4). For *SendSMS* mobile application, at first password is used in RC4 cipher to generate keystream and it is XORed with SMS plain text to output cipher text. The *Sending* process sends the cipher text to the phone number accepted by this application. Correspondingly, in *ReceieveSMS* mobile application the *Receving* process receives the cipher text from the phone number accepted by this application. Then the cipher text is XORed with the keystream generated by RC4 cipher that uses the same password to output original SMS plain text.

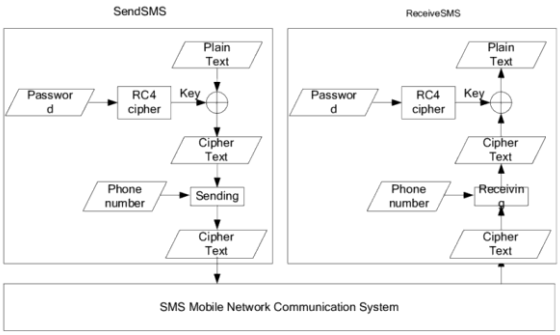

Figure 4. Design for Implementation

The general data flow diagram of these two mobile applications is shown in Figure (5). *SendSMS* mobile application accepts SMS plain text, password and phone number of the receiver as inputs and outputs cipher text. The cipher text is passed through mobile network communication system. *ReceieveSMS* \mobile application accepts cipher text that passed through mobile network communication system, password and phone number of the sender as inputs and outputs SMS plain text.

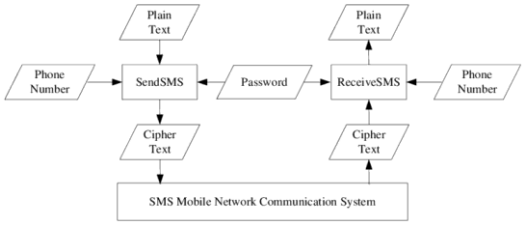

Figure 5. General Data Flow Diagram

The system user interfaces for *SendSMS* and *ReceieveSMS* mobile applications is shown in Figure (6). *SendSMS* mobile application is used at the side of the sender and *ReceieveSMS* mobile application is used at the side of the receiver. The sender must input phone number of the receiver, password and SMS message to *SendSMS* mobile application and press *Send Message* button. The receiver must input phone number of the sender and the same password used by the sender to *ReceiveSMS* mobile application and press *Receive Message* button. Then SMS message of the sender is appeared in the display window screen of *ReceiveSMS* mobile application.

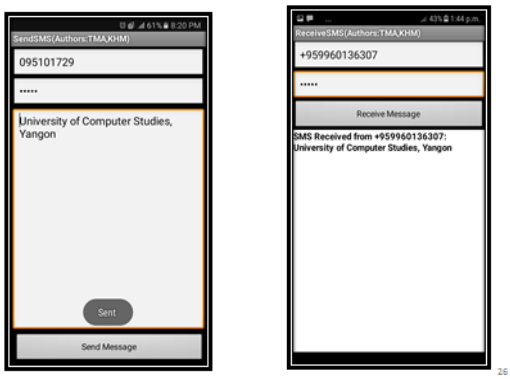

Figure 6. System User Interface

4.1. Implementation results of RC4

- PlainText:012345678901234567890123456788901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890
- Password:APPLE
- Keystream: hlvUùi+ESÑ;?é½þ0???Äã¥?)ß©Ñn??¸´O¹ÿa0_o?é6Ø?ao¬búG¢¦?)µÎEL?/p6µÅ((*c:mÿÌ7íJÞO9«Ù[?¥¯Ï8U·?oJ½q??°slr@0)?VãG?W¿o»ª
- CipherText:X]DfÍ\rkè¢Û?Ê«¢«ýÓ?¦ë?5æV¦2??|?ÊWg%_«Ûì¡WX?[Ê8u??£?ö||$´47F?üPXÉûÔzï}
  ?ìm©??ÿg?¬Z|?l² ?A_Fu6>¥gÑ's·a?W??

- Password:APPLE
- Keystream: hlvUùi+ESÑ;?é½þ0???Äã¥?)ß©Ñn??¸´O¹ÿa0_o?é6Ø?ao¬búG¢¦?)µÎEL?/p6µÅ((*c:mÿÌ7íJÞO9«Ù[?¥¯Ï8U·?oJ½q??°slr@0)?VãG?W¿o»ª
- PlainText:012345678901234567890123456788901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890

5. Measurement of RC4-Key stream

RC 4 stream cipher generates keystream that is pseudorandom number sequence. The pseudorandom number sequence can be used for data confidentiality mechanism during data transmission. The quality of this data confidentiality mechanism depends on the randomness of pseudorandom number sequence generated by RC4 stream cipher. The randomness of pseudorandom number sequence can be measured by using following statistical tests recommend by NIST, National Institute of Standards and Technology. These tests focus on a variety of different types of non-randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests.The following statistical tests are applied to test the randomness of arbitrarily long binary sequences produced by our developed system based on RC4 pseudo random number generators.

1. Frequency Test
2. Runs Test

Frequency Test is used to determine whether the number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence.

Runs Test is used to determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such zeros and ones is too fast or too slow.

- Plain Text:University of Computer Studies, Yangon (UCSY)
- Password:APPLE
- Keystream:hlvUùi+ESÑ;?é½þ0???Äã¥?)ß©Ñn??¸´O¹ÿa0_o?é6
- CipherText:=#?X,"¨ü??½_ðåæ°?×´z«Üg¸í'áÕ!Þ?wI,É°
- Password:APPLE
- Keystream:hlvUùi+ESÑ;?é½þ0???Äã¥?)ß©Ñn??¸´O¹ÿa0_o?é6
- Plain Text:University of Computer Studies, Yangon (UCSY)
- RC4 Keystream(byte) : hlvUùi+ESÑ;?é½þ0???Äã¥?)ß©Ñn??¸´O¹ÿa0_o?é6
- RC4Keystream(bit):0110100001101100011101100101010110100100101011010001010101001100111011001100000001010010000001101101110000001011001111110100111110110000100110000010111110000111000011011110011011 0
- Frequency Test SUCCESS p_value = 0.763025
- Runs Test SUCCESS p_value = 0.446643

6. Conclusion

SMS is now a very common communication tool. Security protection of SMS messages is not yet

that sophisticated and difficult to implement in practice. With the increasing use of SMS for communication and information exchange, care should be taken when sensitive information is transmitted using SMS. Users should be aware that SMS messages might be subject to interception. Solutions such as encrypted SMS should be considered if there is a need to send sensitive information via SMS.

The pseudorandom number sequence generated by RC4 stream cipher is measured by the statistical test suite developed by NIST. According to P-value of each test, the pseudorandom number sequence may be considered to be random with a confidence of 99%. Moreover, RC4 stream cipher possesses better performance among stream ciphers. Therefore, we suggest that the pseudorandom number sequence generated by RC4 stream cipher should be used for data confidentiality of SMS message transmitted on mobile network communication system.

References

[1] BehrouzA. Forouzan, "Cryptography and Network Security", International Edition, McGrawHill, ISBN:978-007-126361-0, 2008.

[2] Mary Agoyi and Devrim Seral, "SMS Security : An Asymmetric Encryption Approach", IEEE 6th International Conference on Wireless and Mobile Communications, 2010.

[3] Medani1, A. Gani1, O. Zakaria, A. A. Zaidan and B. B. Zaidan, "Review of mobile short message service security issues and techniques towards the solution" , Scientific Research and Essays Vol. 6(6), Academic Journals, ISSN 1992-2248, March, 2011.

[4] Neetesh Saxena and Ashish Payal, "Enhancing Security System of Short Message Service for M-Commerce in GSM", Vol 2, No (4), International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345, 2011.

[5] NIST, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology Special Publication 800-22, 2010.

[6] Ozeki NG - SMS Gateway, http://www.ozekisms.com/

[7] Sharad Kumar Verma and D.B. Ojha, "An Approach to Enchance the Mobile SMS Security", Volume 5, No. 5, Journal of Global Research in Computer Science ISSN 2229-371X, May 2014.

[8] Vaishali Singh and Shriddha Shrivastawa, "RC4 Stream Cipher Design for Data Security", International Journal of Advance Research in Science and Engineering ISSN 2319-8346, Vol 6, Issue 5, 2017.

[9] Veena K.Katankar and V.M.Thakare, "Short Message Service using SMS Gateway", Vol. 02, No. 04, International Journal on Computer Science and Engineering, 2010.