Chapter

SMS Security on Android Using RC4 Algorithm

Kaung Htet Myint

Abstract

SMS plays an important role in mobile communication systems. The sending side is acting like as a server for the receiving side that receives short message service at the receiving side. SMS does not incorporate a procedure to accord security for the text sent as data. A majority of the applications for mobile devices are designed and implemented without taking security into account. SMS messages are not normally encrypted by default. Confidentiality is the notion of making sure that data is not made accessible or exposed to unauthorized people. Encryption is the main approach to confidentiality. Both symmetric and asymmetric encryption can be employed. As confidentiality was the original purpose of cryptology, this chapter is introduced as a data confidentiality approach to SMS on Android. It encompasses SMS network architecture as well as cryptographic protocols as theory background and it also deals with design, implementation, and confidentiality assessment of RC4 stream cipher for SMS data confidentiality on mobile networks.

Keywords: SMS, security, encryption, confidentiality, cryptography

1. Introduction

Data confidentiality is the notion of making sure that data is not made accessible or exposed to unauthorized people and is approximately comparable with secrecy. Measurements approximated to confirm confidential information is intended to avoid useful data from unauthorized users' getting them, creating certain hurdles which authorized users can surmount. Access will be limited to intended persons to interpret the facts in query. The facts to be classified in accordance with the quantity and damaged type are public. This type drops into unauthorized users. Strict procedures can be fulfilled in accordance with those classifications. An encipher security system can be used for the security of data confidentiality.

A text messaging service component of most telephones, Internet, and mobile-device systems is known as short message service (SMS). Standardized communication protocols are used to permit smart phones to transfer short text messages. Short message service is also commonly referred to as a "text message." The user can conduct a message of up to 160 characters to another device with a SMS. In SMS, longer messages will automatically be fragmented into several parts. This type of text messaging is supported by most cell phones.

The formal name for text messaging is SMS. Short message service is a way to conduct short, text-only messages from one phone to another. These messages are usually conducted over a cellular data network.

The procedure for conducting SMS is launching the Messages application on the phone. Tap on the Compose Message button. Enter the phone number or name of the contact you want to text. Type your message and finally hit Send. These days, there exist a number of security issues and vulnerabilities related to SMS [1, 2].

Cryptography is related with the procedure of changing ordinary plain text into unintelligible text and vice versa [3]. SMS sent for data confidentiality over mobile networks can be protected by RC4 stream cipher [4]. The objective of this chapter is to offer data secrecy during the SMS messages transmission to prevent them from being received by illegal parties and to ensure the authenticity of the message from the genuine sender.

2. Related works

Phyo Su Khin proposed a short message service (SMS) security for mobile devices with AES algorithm, which focused on the security of short message service (SMS) based on advanced encryption standard (AES) with 128 bits which allows user to encrypt messages before it is transmitted over the network with the use of encryption to protect SMS messages. This application can run on Android devices. The sender and the receiver use the same key to encrypt and decrypt the message as per user requirement in order to improve security and to get high confidentiality.

Aye Mya MoMo proposed image encryption based on XTS-AES MODE where a secure image encryption using XTS-AES and WHIRLPOOL Hash function was implemented. This system improves integrity and confidentiality and is suitable for parallel operation.

Myo Thinzar Aung proposed a secure video streaming system using SRTP and RC4 algorithm where Ronald Rivest symmetric key algorithm (RC4) is used for data encryption and then the encrypted data is embedded into secure real-time transport protocol (SRTP) header. Data acknowledgement is generated to the sender and receiver by using secure real-time transport control protocol (SRTCP).

Yu Loon Ng proposed short message service (SMS) security solution for mobile devices, where the focus is 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.

3. Basic concepts of SMS technology

By cooperating with the cellular network, short message service transmits text messages from one phone to other phones. These devices require short messaging entities (SMEs). These are starting points (sender) and endpoints (receiver) for SMS messages. They never connect directly with each other [5]. They always connect with a short message service center (SMSC). A mobile telephone can be an SME. Computer containing a messaging software [6], which can connect directly with the SMSC of the service source, can be an SME. Two types of SMS messages conditional on the character of the device in the network are mobile-originated (MO) messages and mobile-terminated (MT) messages. The mobile phone sends MO messages to the SMSC and receives MT messages. These MO and MT messages are encrypted in a different way during conduction [7].

The Common Channel Signaling System 7 (SS7) conveys SMS messages. A worldwide standard that describes the processes and procedures for exchanging

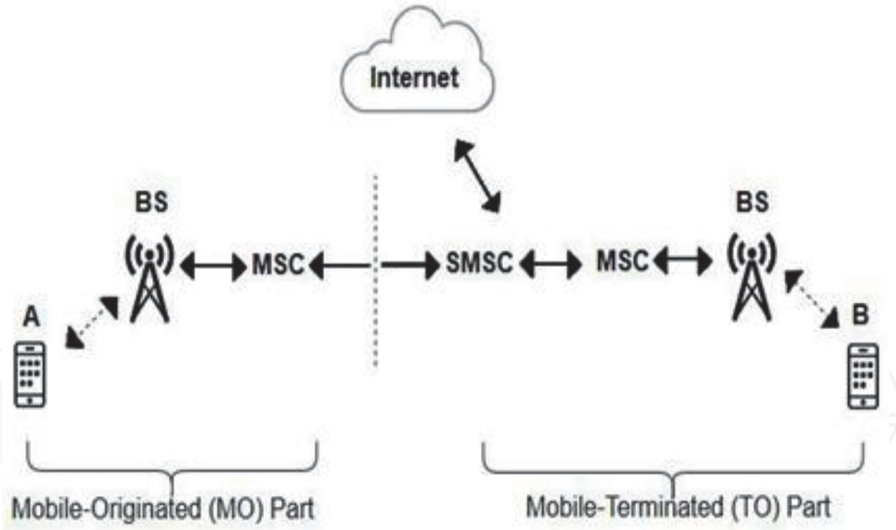

Figure 1.
Mobile network architecture.

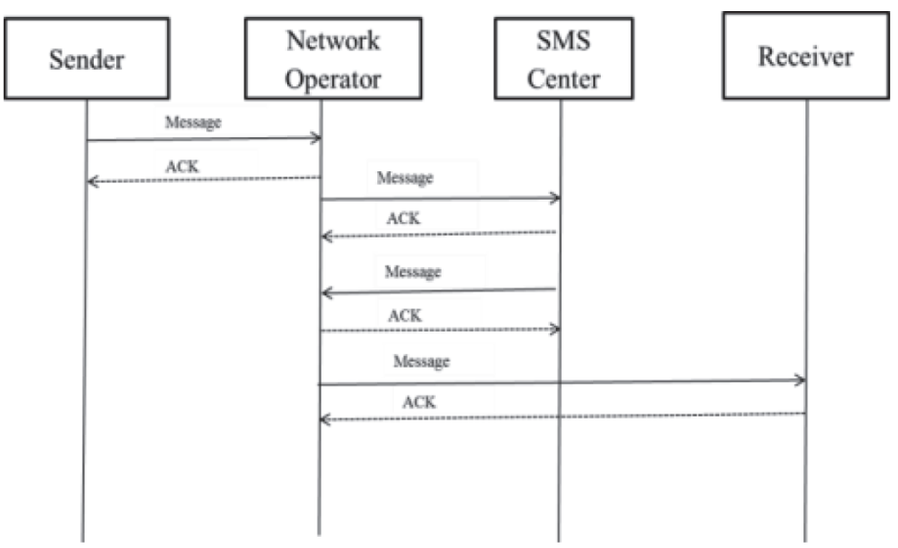

Figure 2.
Message flow of SMS network.

data among network components of wire line and wireless phone carriers is known as SS7 [5]. These components use the SS7 procedure to give-and-take control data for call system, movement control, etc. Theoretically, the common SMS mobile network architecture contains two parts known as mobile originating (MO) part and mobile terminating (MT) part (**Figure 1**). The wireless structure for network part of the sending mobile switching center changes all circulation into and out of the structure in spite of the source are known as MO. The other part contains an improper location and the termination of MSC for the phone, as well as a central stock and onward server is called SMS Centre. It is accountable for receiving information and keeping information (**Figure 2**).

4. Cryptography

Cryptographic algorithms can be separated into: symmetric key algorithms and asymmetric key algorithms. The general concept of RC4 is it uses a symmetric-keystream cipher as shown in **Figure 3**. A stream cipher stands for a symmetric key cipher where plaintext digits are merged with a keystream.

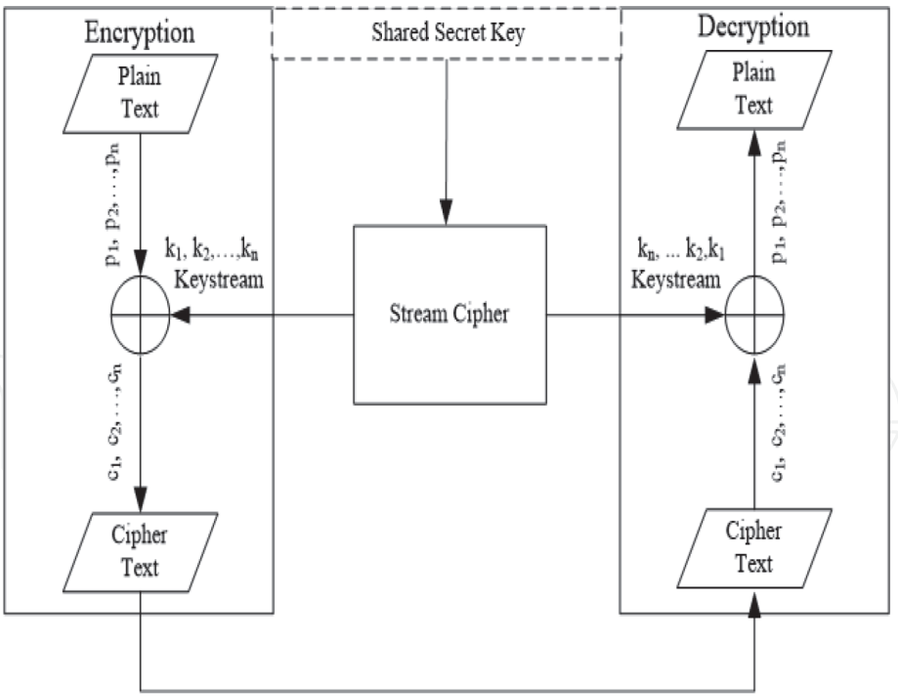

Figure 3.
Stream cipher.

5. RC4 stream cipher

Rivest Cipher 4 (RC4) is very popular because it is simple and can be very fast. It is an adjustable stream size key cipher that included bytes focused on processes. It is founded on the practice of unplanned arrangement. RC4 makes bits of a pseudo-random stream (a keystream). As with any stream cipher, these can be used for the procedure of hiding a data in disguising its material (encryption) by merging it with the message to be sent securely from the source to the intended endpoint of the message (plaintext) using bit-wise exclusive OR. A procedure to revert cipher text into plain text (decryption) is executed in the similar way. This stream cipher includes two parts.

5.1 Key-scheduling algorithm (KSA)

The key-scheduling algorithm is used to start up the arrangement in the range "S." The number of bytes in the key is called "keylength" and can be in the array $1 \leq \text{keylength} \leq 256$. It is used to start up the arrangement in the "S" box. Keylength stands for number of bytes in key and ranges from 1 to 256. The key-scheduling algorithm (KSA) [3] is as follows:

```
Begin
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
end
```

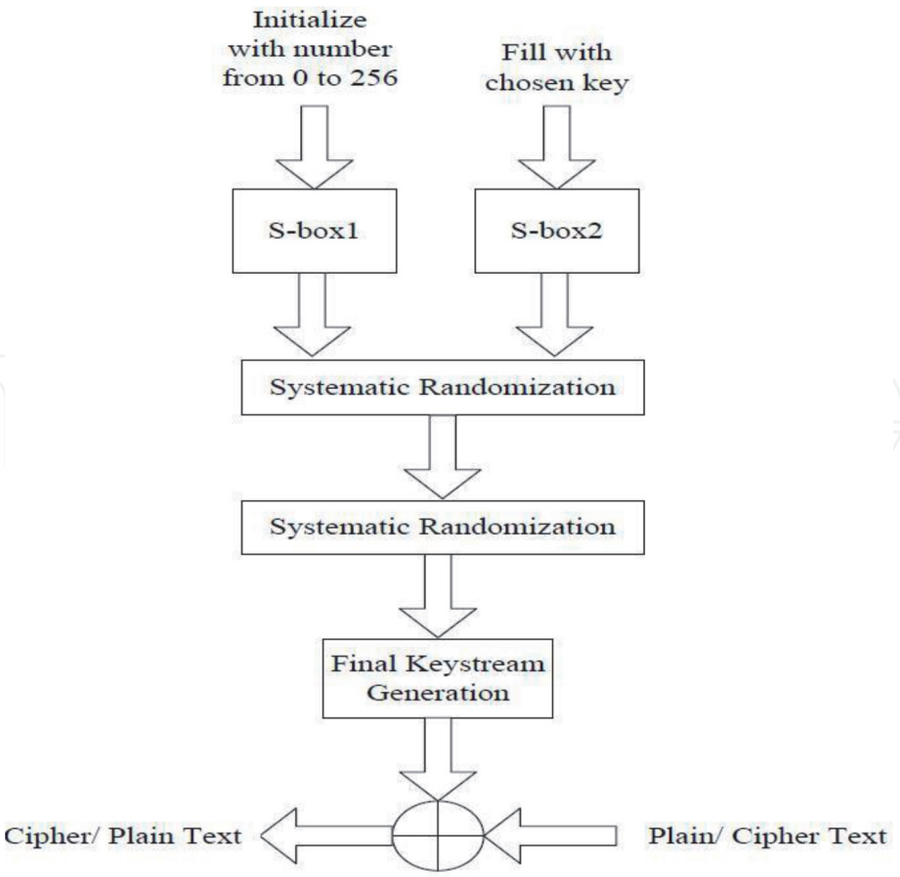

Figure 4.
General RC4 stream cipher.

5.2 Pseudorandom generation algorithm (PRGA)

The arrangement is started with a variable length key, characteristically between 40 and 2048 bits, via the key-scheduling algorithm (KSA). The stream of bits is created using the **pseudorandom generation algorithm (PRGA)**. RC4 creates a keystream. After that, the stream of bits is created by a PRGA. It amends the condition and outputs a byte of the keystream.

```
Begin
    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
end
```

First, we implement RC4 stream cipher by using key-scheduling algorithm (KSA) and pseudorandom generation algorithm (PRGA) in Java programming language (**Figure 4**).

6. Design and implementation

The SendSMS mobile application receives SMS plain text, password, and phone number of the receiver as inputs and comes out as a cipher text. The cipher text is

passed through mobile network communication channel. The ReceiveSMS mobile application receives the cipher text that is passed through the mobile network communication channel, the password, and the phone number of the sender as inputs and comes out as a SMS plain text. The implementation of two smart phone applications is displayed in **Figure 5**.

The *SendSMS* mobile application is used by the creator and the *ReceiveSMS* mobile application is used by the intended person (**Figure 6**). The creator must input the phone number of the intended person, password, and SMS message to *SendSMS* smart phone application and press *Send Message* button. The intended person must input the phone number of the creator and the same password used by the creator to *ReceiveSMS* mobile application and press *ReceiveMessage* button. Then,

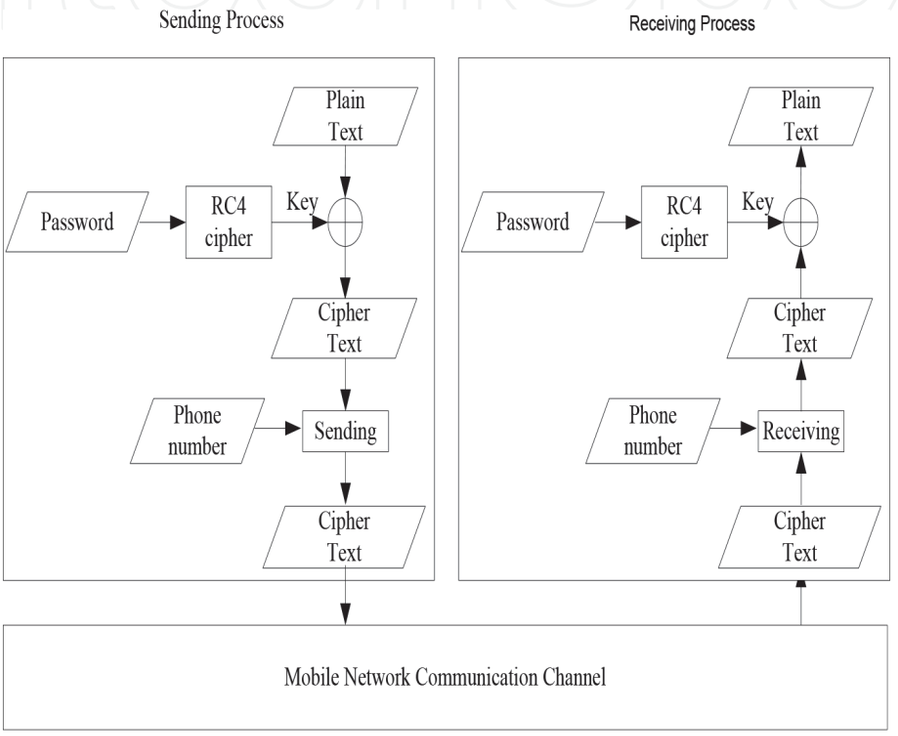

Figure 5.
Design for implementation.

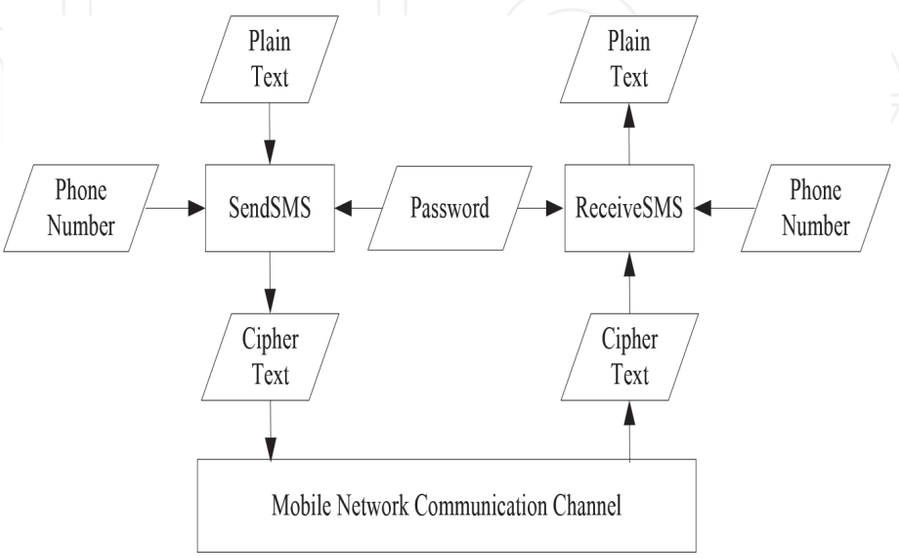

Figure 6.
Data flow diagram.

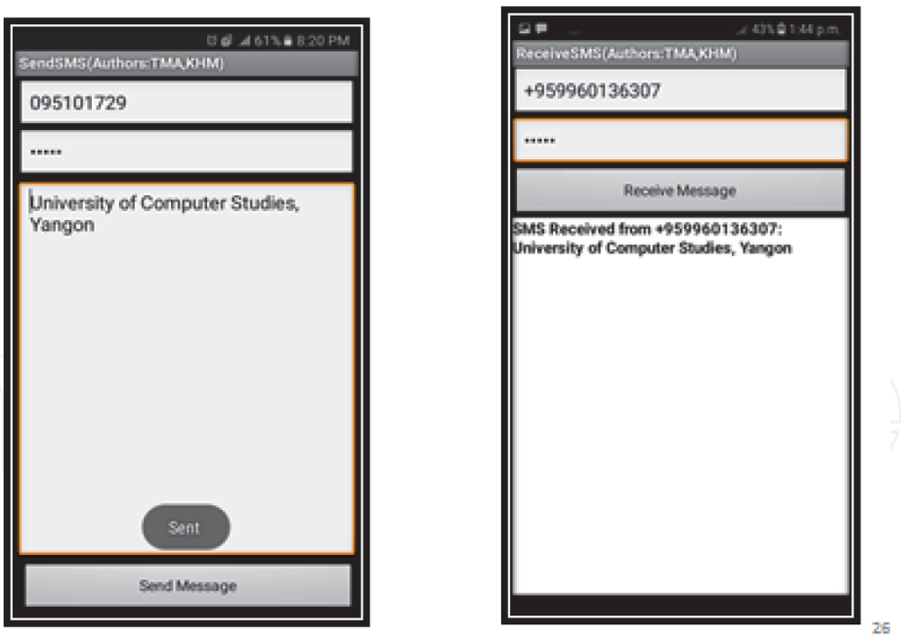

Figure 7.
System user interface.

the SMS message of the creator is shown in the window screen of the *ReceiveSMS* smart phone application (**Figure 7**).

7. Results and measurements

7.1 Implementation results of RC4

PlainText:0123456789012345678901234567889012345678901234567890123456
7890123456789012345678901234567890123456789012345678901234567890
Password:APPLE
Keystream:lvUùi+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|?I² ?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:0123456789012345678901234567889012345678901234567890123456
7890123456789012345678901234567890123456789012345678901234567890

The following statistical tests are applied to test the randomness of arbitrarily long binary sequences produced by the developed system based on RC4 pseudo-random number generators.

7.2 Frequency test

The objective of Frequency test is to decide whether the number of ones and zeros in an arrangement is just about the same as would be predictable for an actually random sequence [8].

Let the keystream 1011010101 be tested by the Frequency test. The result of Frequency test is SUCCESS because the numbers of occurrences of bits—zero and one—in the keystream are equal.

The description of the test is the tests change the sequence ε into a new sequence X, such that Xi = 2εi − 1 = ±1. The calculation of this sequence is assumed by

$$S_n = X_1 + X_2 + \ldots + X_n. \tag{1}$$

If ε = 1011010101, then n = 10 and

$$S_n = 1 + (-1) + 1 + 1 + (-1) + 1 + (-1) + 1 + (-1) + 1 = 2.$$

The test statistic for the observed sum s_{obs} is assumed by

$$s_{obs} = \frac{|s_n|}{\sqrt{n}}. \tag{2}$$

$$s_{obs} = \left(\frac{|2|}{\sqrt{10}}\right) = 0.632455532$$

The P-value is assumed by

$$P - \text{value} = \text{erfc}\left(\frac{s_{obs}}{\sqrt{2}}\right) \tag{3}$$

erfc(z) is the complementary error function

$$\text{erfc}\left(\frac{.632455532}{\sqrt{2}}\right) = 0.527089$$

7.2.1 Decision rule

The verified sequence is recognized as random if the P-value ≥ 0.01, if not it is nonrandom. P-value = 0.527089 ≥ 0.01. Therefore, the sequence is random [8].

7.3 Runs test

The objective of Runs test is to define whether the number of runs of ones and zeros of various lengths is as predictable for a random sequence. In particular, this test defines whether the oscillation between such zeros and ones is too fast or too slow [8].

Let the keystream 1011010101 be tested by Frequency test. The description of the test is to calculate the pre-test proportion π of ones in the input sequence:

$$\pi = \frac{\sum_j \varepsilon_j}{n} \tag{4}$$

If ε = 1001101011, then n = 10 and $\pi = \frac{6}{10} = \frac{3}{5}$.

Define if the prerequisite Frequency test is approved: if it can be displayed that $|\pi - \frac{1}{2}| \geq r$, then the Runs test need not be executed. If the test is not appropriate, then the P-value is set to 0.0000. For this test, $r = \frac{2}{\sqrt{n}}$ has been predefined in the

testcode. $|\pi - \frac{1}{2}| = 0.1 < r = \frac{2}{\sqrt{10}} = 0.63246$, and the test is not run. Since the observed value π is within the particular bound, the Runs test is appropriate.

Calculate the test statistic

$$V_n(\text{obs}) = \sum_{k=1}^{n-1} r(k) + 1 \tag{5}$$

r(k) = 0 if $\varepsilon_k = \varepsilon_k + 1$ and r(k) = 1 otherwise. Since ε = 1 00 11 0 1 0 11, then V10 (obs) = (1 + 0 + 1 + 0 + 1 + 1 + 1 + 1 + 0) + 1 = 7.

$$P - \text{value} = \text{erfc}\left(\frac{|v_n(obs) - 2n\pi(1-\pi)|}{2\sqrt{2n}\ \pi(1-\pi)}\right). \tag{6}$$

$$P - \text{value} = \text{erfc}\left(\frac{7 - 2 * 10 * \frac{3}{5}\left(1 - \frac{3}{5}\right)|}{2\sqrt{20}\ \frac{3}{5}\left(1 - \frac{3}{5}\right)}\right) = 0.147232$$

7.3.1 Decision rule

If the calculated P-value is <0.01, then define that the sequence is non-random. If not, define that the sequence is random. P-value = 0.147232 ≥ 0.01. The sequence is random [8].

Cryptographic algorithms of randomness testing are attacker and designer importance choice. Short sequences of at most 512-bit length are considered for block ciphers and hash functions. The National Institute of Standards and Technology guides to influence the properties of randomness of generators and sequences of statistical test suites. Some tests of this suite cannot be applied to short sequences and do not produce reliable test values. Most of the test suites are producing relatively short sequences that are not suitable for evaluation. Therefore, only the Frequency test and Runs Test approach to evaluate short sequences without tweaking the test. Apart from these tests in the test suite, other tests are not considered for short sequences that transmit SMS over mobile [9, 10].

7.4 Result of testing

Frequency test examines the numbers of occurrences of the bits in the keystream. Runs test examines the independence of the keystream bits.

Let the keystream 1011010101 be tested by Frequency test and Runs test. The result of Frequency test is SUCCESS because the numbers of occurrences of bits—zero and one—in the keystream are equal. The result of Runs test is FAILURE because the adjacent bits of the keystream are dependent.

Keystream : 1011010101
Frequency Test SUCCESS p_value = 0.527089
Runs Test FAILURE p_value = 0.005658

Let the keystream 1001101011 be tested by Frequency test and Runs test. The result of Frequency test is SUCCESS because the numbers of occurrences of bits—zero and one—in the keystream are equal. The result of runs test is SUCCESS because the adjacent bits of the keystream are independent.

Keystream : 1001101011
Frequency Test SUCCESS p_value = 0.527089
Runs Test SUCCESS p_value = 0.147232

In practical use, the following plain text is encrypted by using the following RC4 keystream. The confidentiality of the RC4 keystream is measured by using the Frequency test and Runs test. We found that their results are SUCCESS. Therefore, the confidentiality of RC4 stream cipher may be strong for SMS Security.

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):01101000011011000111011001010101011010010010101101
00010101010011001110110011000000101001000000110110111000001011
00111111010011110110000100110000010111110001110001101111001101 10
Frequency Test SUCCESS p_value = 0.763025
Runs Test SUCCESS p_value = 0.446643

8. Conclusion and future work

Nowadays, in this chapter, the pseudorandom number sequence made by RC4 stream cipher is measured by Frequency test and Runs test. The confidence of the pseudorandom number sequence is measured to be randomness with a confidence of 99% given to P-value of every single test. For that reason, it is suggested that the user should use the pseudorandom number sequence made by the RC4 steam cipher for data confidentiality of SMS message on Android.

Acknowledgements

I would like to express my gratitude to my invaluable university, University of Computer Studies, Yangon. Furthermore, I would like to thank all teachers at University of Computer Studies for giving me useful comments on my presentation.

I would like to express my gratefulness to IntechOpen Limited for suggestions, patience, and support while I wrote my paper in Myanmar.

DOI: http://dx.doi.org/10.5772/intechopen.90119

Author details

Kaung Htet Myint
University of Computer Studies, Yangon, Myanmar

*Address all correspondence to: kolynn.2013@gmail.com

References

[1] Saxena N, Payal A. Enhancing security system of short message service for M-commerce in GSM. International Journal of Computer Science & Engineering Technology (IJCSET). 2011;**2**(4). ISSN: 2229-3345

[2] Verma SK, Ojha DB. An approach to enhance the mobile SMS security. Journal of Global Research in Computer Science. 2014;**5**(5). ISSN: 2229-371X

[3] Forouzan BA. Cryptography and Network Security. International ed. McGraw Hill; 2008. ISBN: 978-007-126361-0

[4] Singh V, Shrivastawa S. RC4 stream cipher design for data security. International Journal of Advance Research in Science and Engineering. 2017;**6**(5). ISSN: 2319-8346

[5] Medani A, Gani A, Zakaria O, Zaidan AA, Bahaa B. Review of mobile short message service security issues and techniques towards the solution. Scientific Research and Essays. 2011; **6**(6). ISSN: 1992-2248

[6] Ozeki NG. SMS Gateway. Available from: http://www.ozekisms.com/

[7] Katankar VK, Thakare VM. Short message service using SMS gateway. International Journal on Computer Science and Engineering. 2010;**02**(04)

[8] Rukhin AL, Bassham LE. NIST. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. US: National Institute of Standards and Technology Special Publication 800-22; 2010

[9] Evaluation of randomness test results for short sequences. In: SETA 2010, 6th International Conference; Paris, France; September 13–17, 2010

[10] Agoyi M, Seral D. SMS security: An asymmetric encryption approach. In: IEEE 6th International Conference on Wireless and Mobile Communications (ICWMC 2010). Valencia, Spain; Sep 2010. pp. 448-452