ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

New Encryption Technique for Secure SMS Transmission

Paritosh S. Patil
Department of Computer Engineering, G.H.Raisoni College of Engineering and Management, Ahmednagar

Abstract: Short Message Service (SMS) is a very popular way for mobile phone and portable device users to send and receive simple text messages. Unfortunately, SMS is does not offer a secure environment for confidential data during transmission. This paper deals with an SMS encryption for mobile communication on Android message application. The transmission of an SMS in mobile communication is not secure, therefore it is desirable to secure SMS by additional encryption. In this paper, there is proposed the use of 3D-AES block cipher symmetric cryptography algorithm for SMS transfer securing. From the experiment, the 3D-AES has low encryption time when message size is more then 256 bits. It can be indicate that SMS encryption application using the 3D-AES block cipher will be proposed running after 256 bits.

Keywords: component; 3D-AES, SMS, block cipher, encryption, mobile application

I. Introduction

SMS is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. Users can used SMS to send or receive from a single person, or several persons, personal messages, email notifications, information services [1], school activity alerts, notification from teacher, job dispatches, and also stock alerts. With these usable application, SMS is now more and more common among mobile phone users. However the security issue [12] of SMS's is still an open challenging task.

SMS is now a very common communication tool. The security protection of SMS messages is not yet that sophisticated and difficult to implement in practice. The confidentiality and integrity mechanisms are only specified as optional security measures that can be made available, but they are not mandatory requirements for SMS system implementation [14]. In this paper, there proposed the use of symmetric cryptography for SMS transfer securing.

Rest of paper is organized as follows. Section II discuss related works about encryption, block cipher algorithm and current development of securing SMS transmitted message. Section III describes the 3D-AES block cipher algorithm.

2

Section IV is present the description of design and implementation of the application for mobile phones, which encrypts and signs SMS using a symmetric 3D-AS block cipher. Section V analyses the SMS Encryption and Section VI describes conclusion and future extension of the application.

II. RELATED WORK

The field of cryptography [15] can be divided into several techniques of study. There are two types of techniques in cryptography which are asymmetric key algorithm and symmetric key algorithm. Asymmetric key algorithm or sometimes called public key algorithm is usually based on complex mathematical problems. Symmetric key algorithm can be broadly grouped into block ciphers and stream ciphers [16]. Other symmetric key algorithms are cryptographic hash functions and Message Authentication Codes (MACs).

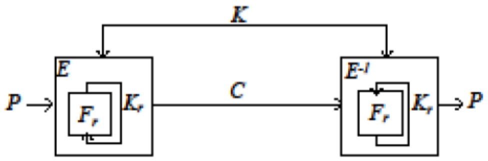

Figure 1. Diagram of symmetric block cipher

The symmetric key block cipher technique operates on the same block or fixed-length groups of bits. The algorithm is illustrated in Fig. 1. The encryption function in (1) , denoted as *E*, is a process of enciphering information called Plaintext, denoted as *P*, using some secret codes called secret Key, denoted as *K*, into an unreadable form called Ciphertext, denoted as *C*. The *P*, as it goes through each round of the cipher, is referred to as the cipher-state, denoted as *F*.

Decryption function in (2) is the inverse process of encryption, denoted as E^{-1}, where the ciphertext is deciphered to readable information using the same secret key. The encryption process can be described as :

$$E_K\,(P) = C \tag{1}$$

and decryption process can be describe as :

$$E_K^{-1}(C) = P \tag{2}$$

In the literature as shown in Tab. 1, many authors have used different cryptography algorithms in the SMS encryption application to provide confidentiality in sending and receiving messages. Even though there are several authors (2 out of 8) used DES, 3DES and AES block cipher algorithms in their works but most of these works are asymmetric key encryption techniques. Therefore it is advisable that can develop SMS Encryption using symmetric key encyption.

Table 1. Review on SMS Encryption

Author	Algorithm
Lisonek & Drahansky [17]	RSA
Albuja&Carrera [18]	DES, 3DES, AES and RSA
Toolani&Shirazi[19]	ECDLP
Zhao et al [20]	identity-based
Harb et al [2]	3 DES
Sonam [3]	elliptic curve
Hosain et al [4]	A5
Kuate et al [5]	SMSsec

Owning from suggestion of Garza-Saldana &DiazPerez [6] that symmetric encryption could provide confidentiality to SMS, this paper perform an evaluation of three block cipher symmetric encryption techniques. This is done in order to find the most suitable block cipher symmetric encryption technique for securing SMS transmitted messages.

III. 3D-AES BLOCK CIPHER

The 3D-AES block cipher [7] is based on the AES block cipher [8][9] which is a key-alternating block cipher, composed of rotation key function, minimum 3 iterations of round function and key mixing operations. The round function consists of non linear substitution function, permutation function and transposition function. A block diagram of the 3D-AES block cipher is given in Fig. 2 in the form of 4 x 16 bytes. The original message is called the plaintext, denoted P^i, where i= {0, 1, 2, 3}. The unreadable form is called the ciphertext, denoted by C^i, where i= {0, 1, 2, 3}. The secret master key is denoted by K. The transformation of P into C is called encryption and the reverse process is called decryption. The P, as it goes through each round of the cipher, is referred to as the cipher state, denoted as F. Note that, the output cipher state, F of the key mixing layer of round r_1 forms the input cipher state to the next round r. The 3D-AES block cipher is improved confusion performance [10] of round transformation.

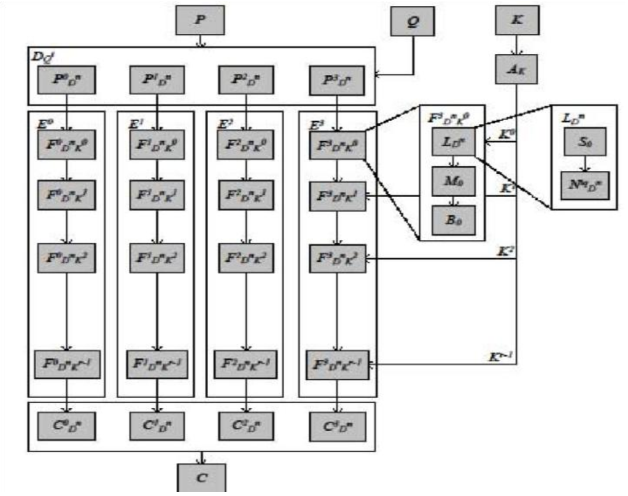

Figure 2. The structure of 3D-AES block cipher.

A detailed description of all the layers of 3D-AES block cipher follows:

$P^i_{D^n}$ is a plaintext for ith slice at nth cube.

$C^i_{D^n}$ is a ciphertext for ith slice at nth cube. is a rotation key .

D^n_Q is the output of nth cube from arranging function at rotation key Q.

E^i isa encryption function for ith slice. $F^i_{D\ \ K}$ is a output block of encryption function for ith slice at cipher state for nth cube in round r.

K^r is the sub key used in round r.

A_K is key scheduling function. $L^i_{D^n}$ is a output block of linear transformation function for ith slice at Q rotation key at nth cube.

S_i is a nonlinear transformation of the ith slice at round function .

$N^{iq}_{D^n}$ is a rotation function at arranging function of ith slice and q degree at nth cube.

M_i is a linear transformation of the ith slice at round function.

B_i is a XOR operation.

The 3D-AES block cipher identified the encryption and decryption functions. When r = 3, the output cipher state is the ciphertext. The third round of the 3D-AES block cipher operates on plaintext size of 16 x 4 bytes to produce an output ciphertext 64 bytes. The secret key size required by the 3D-AES block cipher is 16 bytes. All the operations in the 3D-AES block cipher are performed in the finite field of order 2^8, denoted by *GF(2^8).*

This immune-inspired block cipher adopted amino acid sequences model that can be rotate with a different angle [11]. However for the purpose of evaluation and testing the implementation of the 3D-AES block cipher, every *Slice* of the *Cube* module will be rotate at *3D-SliceRotate* module implementation in four types of angel and clockwise rotation only, which is denoted as N_{pn}^{iq}. The q degree is based on the rotation angel for every i^{th}*Slice* where i= {1, 2, 3, 4} and q = {0, 1, 2, 3}. There is no rotation slice for the first slice, second will be rotate in 90^0, third slice will be rotate in 180^0 and fourth slice will be rotate in 270^0.

IV. DESIGN OF SMS ENCRYPTION

A. *Programming Platforms for Mobile Phones*

The SMS Encryption was developed for evaluating two symmetric encryption techniques which is AES and 3DAES. It has been developed using a Java Programming Language, Java Micro Edition (Java ME) which is produced by Sun Microsystems. Almost all mobile phones include this programming platform. The Eclipse IDE is the essential starting point for Mobile developers, including a Java IDE, C language support, a Git client, XML Editor and Mylyn.

B. *Design flow*

In this SMS Encryption is used a standardized facility defined as part as of the Global System for Mobile Communications (GSM) series of standards [13] as shown in Fig. 3. Any message, sent via SMS, is not directly delivered to its destination, but it is stored into an SMS Center (SMSC) after passing through a Mobile Switching Center (MSC), which has the important role of message routing, according to the information provided by Home Location Register (HLR) and the Visitor Location Register (VLR)

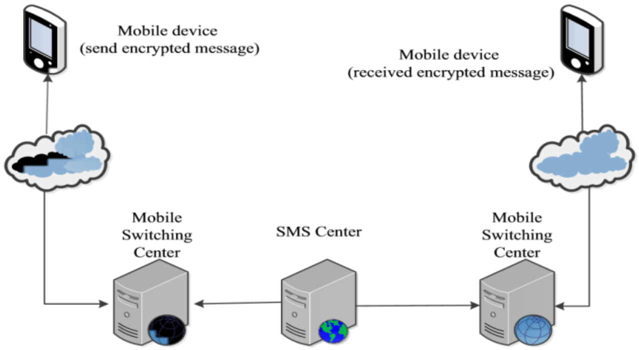

Figure 3. SMS achitecture

The SMS Encryption application works only with SMS, which is encrypted in the first step, digitally signed in the second step and sent in the last step.

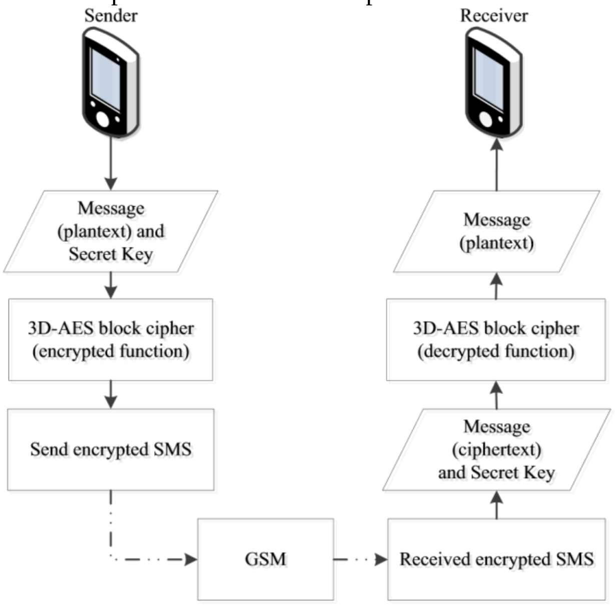

Figure 4. SMS Encryption

V. RESULT DISCUSSION

This application was tested on Android operating system, v4.1.2 (Jelly Bean), Cortex-A5 processor mobile phone running at 1 GHz speed, with 4 GB internal Memory and 786 MB RAM. The performance data were collected by applying 100 sequences of random SMS message or plaintext for each sizes on the phone to get the encryption and decryption time for both algorithms. The AES block cipher has a fixed block length of 128 bits and a key length of 128, 192, or 256 bits. It can be specified with block and key sizes in any multiple 35 of 32 bits with a minimum of 128 bits. The AES block cipher has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. The experiment only taking into consideration on 128bit-keys only as well as 3D-AES block cipher.

Encryption time is the time taken to transform the SMS plaintext into cipher text. For each key size of same algorithm, random SMS message of different bit sizes was encrypted. The average of the encryption time is calculated using the formula in (3) and the results are tabulated in Tab. 2.

$$E_t = \frac{1}{n}\sum_{i=1}^{n=100} e_i \tag{3}$$

Where n is total number of encrypted message sequences, $e_i$is the consecutive encryption time and E_t is the average encryption time.

Table 2. Encryption time in milliseconds

Plaintext size	AES	3D-AES
32	45	243
64	73	243
128	145	243
256	298	243
512	412	243
1024	872	486

Tab. 2 indicates that encryption time and the plaintext size are related. The rise in plaintext size of the AES block cipher increases the encryption time. Even though the 3DAES block cipher has a high encryption time when the plaintext size between 32 bit to 128 bits compared to the AES block cipher, the 3D-AES has low encryption time when plaintext size more then 256 bits. It can be indicate that SMS encryption using the 3D-AES block cipher will be proposed after 256 bits. The encryption time of below 512 on the 3D-AES does not change because the 3D-AES is 512 bit in block.

Decryption time is the time taken to transform the SMS cipherext into plaintext. For each key size of same algorithm, random SMS message of different bit sizes was decrypted. The average of the decryption time is calculated using the formula in (4) and the results are tabulated in Tab. 3.

$$C_t = \frac{1}{n}\sum_{i=1}^{n=100} c_i \qquad (4)$$

wheren is total number of decrypted message sequences, c_i is the consecutive decryption time and C_t is the average decryption time.

Table 3. Decryption time in milliseconds

Ciphertext size	AES	3D-AES
32	47	241
64	71	241
128	142	241
256	287	241
512	409	241
1024	821	483

Tab. 3 indicates that decryption time and the ciphertext size are related. The rise in plaintext size of the AES block cipher increases the decryption time. Even though the 3DAES block cipher has a high decryption time when the ciphertext size between 32 bit to 128 bits compared to the AES block cipher, the 3D-AES has low decryption time when plaintext size more then 256 bits. It can be indicate that SMS decryption using the 3D-AES block cipher will be proposed after 256 bits. Since the 3D-AES and AES have use a same key size to achieve high security, it can be concluded that the 3D-AES block cipher is the most cost effective algorithm for SMS encryption as compared with the AES block cipher.

VI. CONCLUSION AND FUTURE WORK

The application of SMS Encryption of 3D-AES block cipher on android application has been designed and implemented. The application is running in the mobile phone and does not require any additional encryption devices. The result showed that suitable and easy to implement in mobile device for the proposed scheme. 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.

ACKNOWLEDGMENT

This work is supported by two grant schemes. First grant scheme is from the Fundamental Research (FRGS) provided by the Ministry of Higher Education Malaysia, under the Grant Number FRGS/1/11/SG/UPM/02/4. The second grant scheme is from the Research Intensive Faculty (RIF) provided by UniversitiTeknologi MARA, under Grant Number 600-RMI/DANA 5/3/RIF (409/2012).

REFERENCES

[1] S. Doyle, “Using short message service as a marketing tool”, Journal of Database Marketing, vol. 8, no 3, 2001, pp. 273-277.

[2] H. Harb, H. Farahat, M. Ezz, “SecureSMSPay: secure SMS mobile payment model”, 2nd International Conference on Anticounterfeiting, Security and Identification, ASID. Guiyang, China, 2008, pp. 11-17.

[3] R. Soram, “Mobile sms banking security using elliptic curve cryptosystem”, International Journal of Computer Science and Network Security, vol. 9, no. 6, pp. 30-38.

[4] M. A. Hossain, S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz, “A proposal for enhancing the security system of short message services in GSM”,

2nd International Conference on Anticounterfeiting, Security and Identification, ASID, Guiyang, China, 2008, pp. 235- 240.

[5] P. H. Kuaté, J. L. Lo and J. Bishop, "Secure asynchronous communication for mobile devices", Proceedings of the Warm Up Workshop for ACM/IEEE ICSE 2010,Cape Town, South Africa, 2009, pp. 5 – 8

[6] J. J. Garza-Saldana and A. Diaz-Perez, "State of security for SMS on mobile devices", Proceedings of the Electronics, Robotics and Automotive Mechanics Conference, 2008, pp. 110 – 115

[7] S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin, "Byte Permutations in Block Cipher Based on Immune Systems", International Conference on Software Technology and Engineering, 3rd (ICSTE 2011). ASME Press, New York, NY. , 2011.

[8] NIST, "Fips197: Advanced Encryption Standard (AES)", FIPS PUB 197 Federal Information Processing Standard Publication 197, Technical report, National Institute of Standards and Technology, 2001.

[9] J. Daemen, V. Rijmen, V., "The Design of Rijndael, AES - The Advanced Encryption Standard", Springer-Verlag, 2002.

[10] S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin, "An immune system-inspired byte permutation function to improve confusion performance of round transformation in symmetric encryption scheme", Computer Science and Applications, Lecture Notes in Electrical Engineering, Springer, 2012.

[11] S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin, "Symmetric Encryption Algorithm Inspired by Randomness and Non-linearity of Immune Systems", International Journal of Natural Computing Research, IGI Global Publishing, 2012.

[12] D. Lisonek and M. Drahansky, "SMS encryption for mobile communication", International Conference on Security Technology, Hainan Island, 2008, pp 198 – 201.

[13] S. Redl, M. W. Oliphant, M. K. Weber, and M. K. Weber, "An Introduction to GSM", 1st ed. Norwood, MA, USA: Artech House, Inc., 1995.

[14] "Short Message Service Security on Febuary 2008", available http://www.infosec.gov.hk/english/technical/files/short.pdf dated on August 2013.

[15] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., New York, NY, USA, 2nd edition, 1995.

[16] W. Stallings, "Cryptography and network security", Prentice Hall, New Jersey, United State, 2006.

[17] D. Lisonek and M. Drahansky, "SMS encryption for mobile communication", International Conference on Security Technology, Hainan Island, 2008, pp 198 – 201.

[18] J. P. Albuja and E. V. Carrera, "Trusted SMS communication on mobile devices", 11th Brazilian Workshop on Real-Time and Embedded Systems, Pernambuco, Brazil, 2009, pp.165- 170.

[19] S. Zhao, A. Aggarwal and S. Liu, "Building secure user-touser messaging in mobile telecommunication networks", Proceedings of Wireless Telecommunications Symposium, Pomona, CA, 2008, pp.151-157.