ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

An Android Application to Secure Text Messages: A Survey

Dr. Vishwanath Y[1], Aishwarya M[2], Kavya Bhat[3], Anusha T.G[4]

Assistant Professor, Department of ISE, New Horizon College of Engineering, Bangalore, India[1]

Student, Department of ISE, New Horizon College of Engineering, Bangalore, India. [2]

Student, Department of ISE, New Horizon College of Engineering, Bangalore, India. [3]

Student, Department of ISE, New Horizon College of Engineering, Bangalore, India. [4]

ABSTRACT: Nowadays, short message service (SMS) is being used in many daily life applications, including healthcare monitoring, mobile banking, mobile commerce, and so on. But when we send an SMS from one mobile phone to another, the information contained in the SMS transmit as plain text. Sometimes this information may be confidential like account numbers, passwords, license numbers, and so on, and it is a major drawback to send such information through SMS while the traditional SMS service does not provide encryption to the information before its transmission. In this paper, we propose an efficient and secure android application to secure SMS, The application is well featured and provides encryption and decryption that can protect message from unauthorised access and disclosure over networks. With compared to other messaging systems, the proposed secure messaging system can be used for chat in both web and android application.

KEYWORDS**:** Securemessaging; Encryption; Decryption; AES; Android Application

I. Introduction

Secure messaging is a server based approach to protect sensitive data from unauthorised access over Internet. It is confidential and authenticated exchange by any internet user worldwide. Secure messages provide non-repudiation as the recepients are personally identified and transactions are logged by the secure email platform[3]. Cryptography is a technique that makes data or network secure by providing security. It is the science of devising methods that allow information to be sent in a secure form in such a way that the only intended recipient can retrieve the information. Network security is highly based on cryptography. Basically, Cryptography is an art of hiding information by encrypting the message[1].

In cryptography original message is basically encoded in some non readable format. This process is called encryption. The only person who knows how to decode the message can get the original message. This process is called Decryption. On the basis of key used encryption algorithms as asymmetric key algorithms and symmetric key algorithms. Asymmetric key algorithms are those in which encryption and decryption is done by two different keys and symmetric key algorithms are those in which same key is used for both encryption and decryption.In this paper we have focused on symmetric key algorithms[2].

II. Related work

Short message services[6] is a very popular and easy to use communication medium for mobilephone users. Using SMS mobile users send some confidential information such as password, account number, banking information in the form of text messages from one mobile to another mobile. The information sent is in plaintext format the hacker easily can read this information and privacy can't be maintained. Short message service[7] has to protected hence a protocol called secured SMS which make use of the symmetric key shared between the end users this providing secure and safe communication between two users. The analysis of this protocol shows that it is highly secure as it is able to prevent the information content from various attacks.

III. Comparison of Symmetric Key Algorithms

Following methods are based on Symmetric encryption methods-

DES- Data Encryption Standard (DES) is a symmetric key block cipher. The key length is 56 bits and block size is 64 bit length. It is vulnerable to key attack when a weak key is used. DES was found in 1972 by IBM using the data encryption algorithm. The government of USA as standard encryption algorithm adopted it. It began with a 64 bit key. The NSA put a restriction to use of DES with a 56 bit key length; hence, DES discards 8 bits of the 64 bit key. Then it uses the compressed 56 bit key derived from 64 bit key to encrypt data in block size of 64 bits. DES can operate in different modes such as CBC, ECB, CFB and OFB, making it flexible[3].

Triple-DES- In cryptography, Triple DES is a block cipher. Triple data encryption standard was first published in a 1998,which gets its name so because it applies DES 3 times to each block of data, encryption, Decryption, and Encryption using DES.

AES- AES was developed by Vincent Rijmen and Joan Daeman. Because of the small key length the DES is no longer considered as safe for today's application. AES come up with key length 128bit using the symmetric block cipher. AES algorithm is not only for security but also for great speed. The encryption steps are as follows.
1.The set of round keys from the cipher key.
2.Initialize state array and add the initial round key to the starting state array.
3.Perform round =1 to 9 :Execute Usual Round.
4.Execute Final Round.
5.Corresponding cipher text chunk output of Final Round Step.
Each round consists of following four steps.
* Sub Bytes: The first transformation, Sub Bytes, is used at the encryption site. TO substitute a byte, we interpret the byte as two hexadecimal digits.
* Shift Rows: In the encryption, the transformation is called Shift Rows.
*Mix Columns: The Mix Columns transformation operates at the column level ;it transforms each column of the state to a new column.
* Add Round Key: Add Round key proceeds one column at a time. Add Round Key adds a round key word with each state column matrix ;the operation in Add Round Key is matrix addition.
*The last step consists of XORing the output of the previous three steps with four words from the key schedule.
*And the last round for encryption does not involve the "Mix columns "step.

Blowfish- Blowfish was first published in 1993. It is a symmetric key block cipher with key length variable from 32 to 448 bits and block size of 64 bits. Its structure is fiesta network. Blowfish is a symmetric block cipher that can be used as a informal replacement for DES or IDEA. It takes a variable length key, from 32 bits to 448 bits, making it ideal for both domestic and commercial use.

Bruce Schneier as a fast, free alternative to existing encryption algorithms designed Blowfish. From then it has been analysed considerably, and it is slowly gaining popularity as a robust encryption algorithm. Blowfish is not patented, has free license and is freely available for all uses[3].

Comparison summary

Algorithm	Created by	Key size	Block size
DES	IBM in 1975	56	64
3-DES	IBM in 1978	112 or 168	64
Blow Fish	Bruce Schneier in 1993	32-448	64
AES	Daeman in 1998	256	128

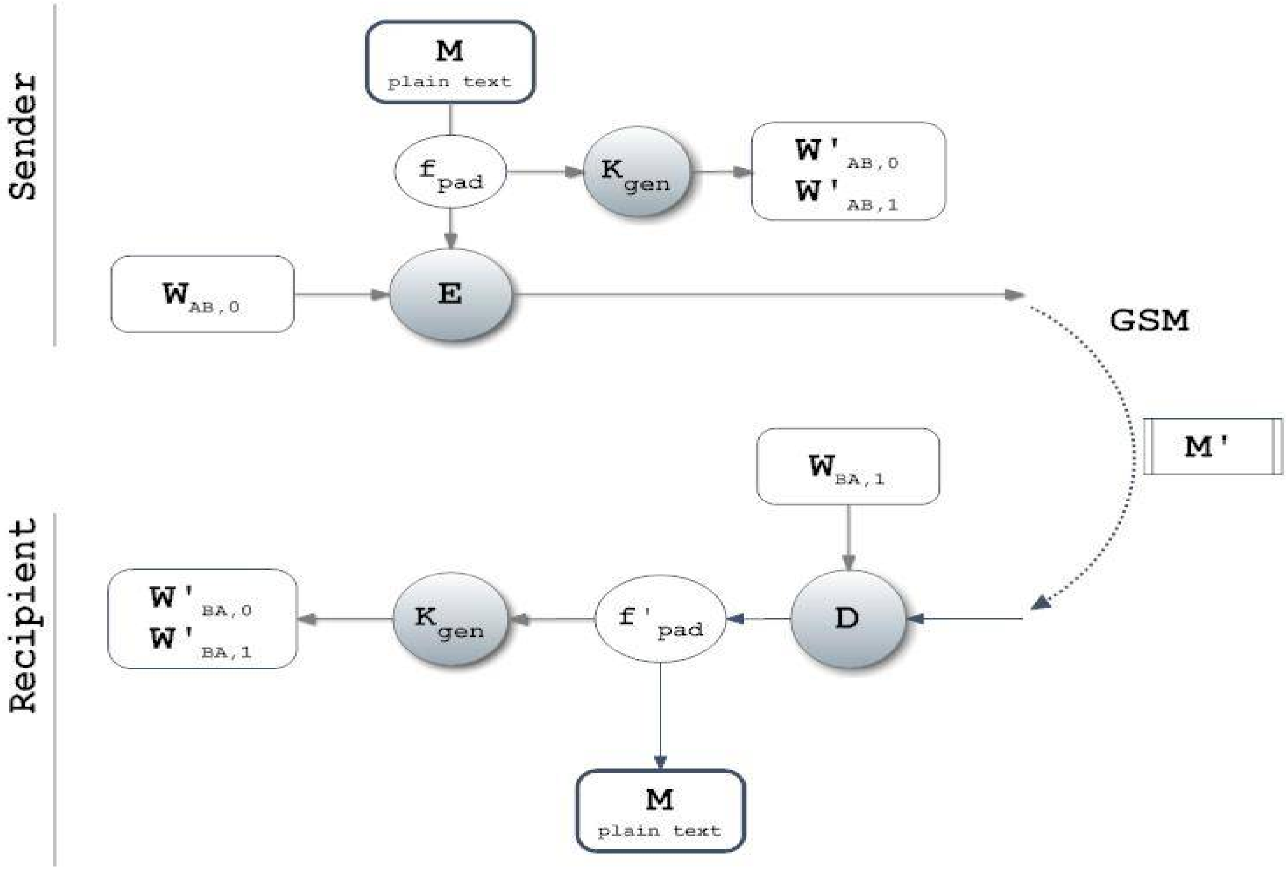

Fig1.Secure transmission and key generation

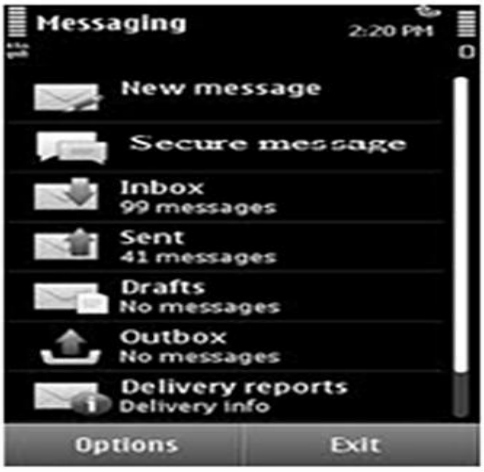

Fig 2.Secure message in menu

DOI: 10.15680/IJIRCCE.2018.0603113

IV. Encryption

Encryption is the process that converts the text message into encrypted message by using mono-alphabetic substitution algorithm, described in section 2.4.In the proposed system ,the sender selects key from key list and writes message as input. The sender end produces the encrypted message from the input message. After encryption the message stored as encrypted form is draft and sent to the receiver. The encrypted message is an apparently random stream of data, as it stands, it is unintelligible. Only authorized receiver can decrypt the decrypted messages[5].

V. Decryption

Decryption is the reverse process of encryption. It is also used mono-alphabetic substitution algorithm described in section 2.4.In this system the receiver must know both the key that was selected by the sender during encryption and encrypted message for decryption. The decryption process is very simple with the correct key; without the correct key it is impossible[5].

VI. Android Application

An android application is software application running on the android platform. Because the android platform is built for mobile devices, a typical android app is designed for a smart phone or a tablet PC running on the Android OS. Google released android which is open source mobile phone operating system with Linux based platform. It consists of the operating system, middleware, and user interface and application software.

A. Research problem

Sometimes, we send the confidential information like pass-word, pass code, banking details and private identity to our friends, family members and service providers through an SMS. But the traditional SMS service offered by various mobile operators surprisingly does not provide information security of the message being sent over the network. In order to protect such confidential information, it is strongly required to provide end-to-end secure communication between end users. SMS usage is threatened with security concerns, such as SMS disclosure, man-in-the-middle attack, replay attack and impersonation attack. There are some more issues related to the open functionality of SMS which can incapacitate all voice communications in a metropolitan area, and SMS-based mobile botnet [15] as Android botnet [16]. SMS messages are transmitted as plaintext between mobile user (MS) and the SMS center (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel.

B. Key contribution

The above requirements can be accomplished by proposing a protocol called Easy SMS which provides end-to-end security during the transmission of SMS over the network. The Easy SMS protocol prevents the SMS information from various attacks including SMS disclosure, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack. This Easy SMS sends lesser number of transmitted bits, generates less computation overhead, and reduces bandwidth consumption and message exchanged as compared to SMS Sec and PK-SIM protocols.

C. Attack model

An attack model describes different scenarios for the possibilities of various attacks where a malicious MS can access the authentic information, or misguide the legitimate MS. Since, the SMS is sent as plaintext, thus network operators can easily access the content of SMS during the transmission at SMSC. This leads to SMS disclosure attack. In traditional cellular network, the OTA interface between the MS and the Base Transceiver Station (BTS) is protected by a weak encryption algorithm (such as A5/1 or A5/2), thus an attacker can compromise these algorithms to capture the information contained in the SMS or can alter the SMS information. The attacker can also try to cryptanalyze the generated crypto-graphic keys used in the authentication protocol. The attacker may fraudulently delay the conversation between both MS and can capture or reuse the authenticated information (during the protocol execution) contain in previous messages which results in the form of replay attack.

DOI: 10.15680/IJIRCCE.2018.0603113

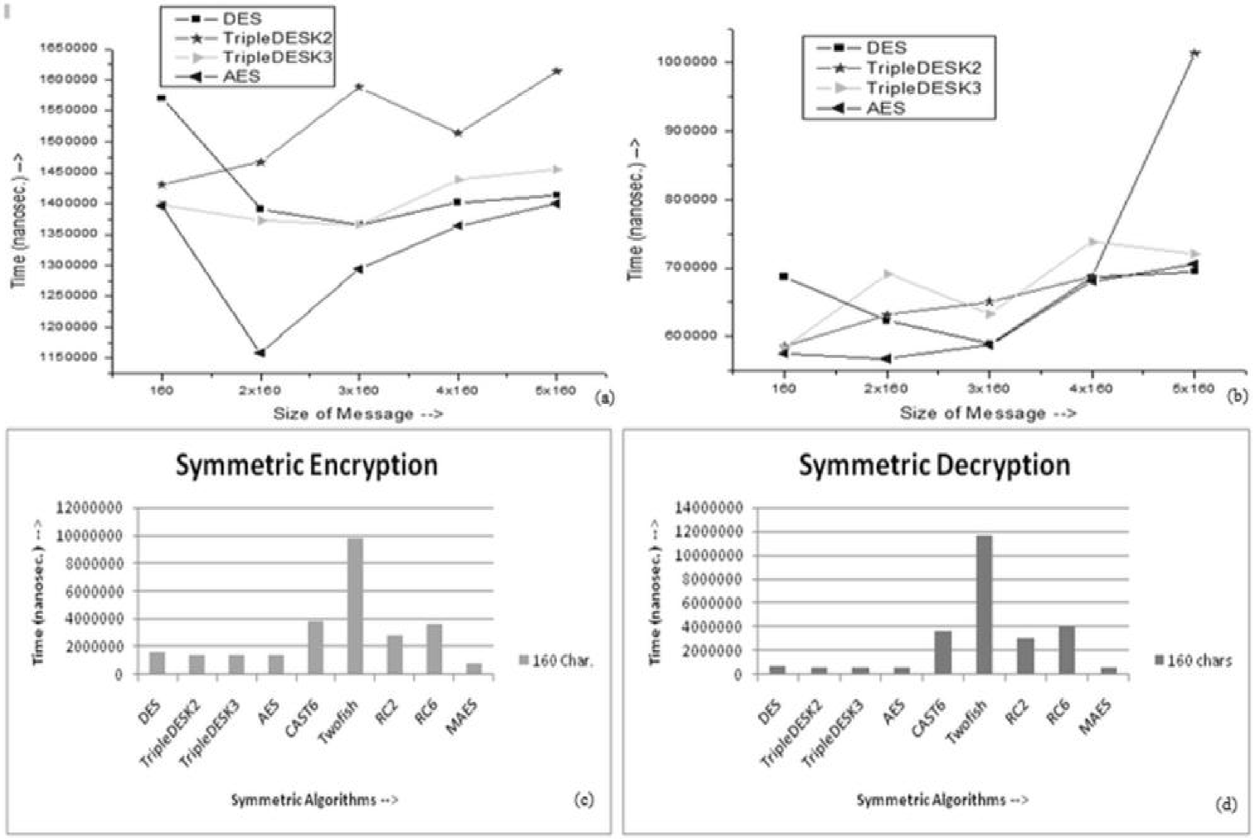

Fig 3.Encryption and decryption using different sizes

D.System and Communication model

Inorder to overcome the above stated attacks, various cipher algorithms are implemented with the proposed authentication protocol. We recommend that the cipher algorithms should be stored onto the SIM (part of MS) as well as at AS. Since providing security needs to do some extra effort which is measured in terms of cost, thus providing or adding extra security means increasing more cost. Authors propose to include one more service as Secure Message in the menu of mobile software developed by various mobile companies as shown in Fig. 1. Mobile operators can add some extra charges to send secure message by their customers over the networks. Whenever a user wants to send a secure message to other user, the proposed protocol namely EasySMS is executed which makes available the symmetric shared key between both MS and then ciphering of message takes place using a symmetric key algorithm.

E. Efficient key management

The Easy SMS protocol is able to efficiently handle the key management issue in both scenarios where the DK1 key (from the symmetric key of MS1) is securely transmitted by the AS to the MS2 (scenario-1) or by the AS2 to the MS2 through AS1 (scenario-2). Thus, this protocol successfully ciphers the message before its transmission over the network. We preferred a symmetric key algorithm because these algorithms are 1000 times faster than the asymmetric algorithms [24] and improve the efficiency of the system.

F. Resistance to attack

In this subsection, we justify that the EasySMS protocol is able to prevent the transmitted SMS from various attacks over the network. It is assumed that the cryptographic functions used in the paper are not publically available and are secret. The capturing of any secret key SK is not possible because no secret key has been transmitted in any phase of the proposed protocol and always a delegation key DK1 is being transferred in the cipher mode whenever is required. Secret keys are also not publically available and are secret.

SMS Disclosure: In the EasySMS protocol, a crypto-graphic encryption algorithm AES/MAES is maintained to provide end-to-end confidentiality to the transmitted SMS in the network. Thus, encryption approach prevents the transmit-ted SMS from SMS disclosure.

Replay Attack: The proposed protocol is free from thisattack because it sends one timestamp (like T1, T2, T3, T4 and T5) with each message during the communication over the network. These unique timestamp values prevent the system from the replay attack. This attack can be detected if later previous information is used or modified.

Man-in-the-middle Attack: In the EasySMS protocol,a symmetric algorithm AES/MAES is used for encrypting/ decrypting end-to-end communication between the MS and the AS in both scenarios. The message is end-to-end securely encrypted/decrypted with DK1 key for every subsequent authentication and since attacker does not have sufficient information to generate DK1, thus it prevents the communication from MITM attack over the network.

This paper presents the impact of context aware in ICN routing protocols. Three techniques of context aware is discussed, namely, environmental, historical and personal context aware. The three techniques show the improvement of ICN routing protocols when they are employed. The improvement of ICN routing protocol when context aware is employed is reported between 8% and 15%.

VII. Conclusion

In this paper we have proposed a android application to provide secure end-to-end communication through SMS between mobile users. The focus is mainly on the Symmetric algorithms.DES, triple DES, AES and blowfish algorithms are explained and compared to know the suitable algorithm that is required for an android application.

REFERENCES

[1] R.Ling and S.W.Campbell, "Mobile Communication: Bringing Us Together and Tearing Us Apart", Transaction Publishers, 2012.

[2] J. L.-C.Lo,J.Bishop, and J.H.P.Eloff, "SMSSec: An end -to-end protocol for secure SMS," Computer.Security,vol.27,no.5-6,pp.154-167, October 2008.

[3]M.Agoyi and D.Seral, "SMS Security: An Asymmetric Encryption Approach,"2010 Sixth International Conference on Wireless and Mobile Communication (ICWMC),Valencia, Spain, Sept.20-25,2010,pp.448-452.

[4] M. Batista, R. Das, A. Carol, " A research on software security vulnerabilities of new generation smart mobile phones", 2nd International symposium on digital forensics and security", pp.6-16, May 12-13,2014, Sam Houston State university, Houston, USA.

[5] S.Murphy,"The Advanced Encryption Standard (AES)," Information Security Technical,vol,no.4, pp,12-17,1999.

[6]R.EAndersonetal.,"ExperienceswithatransportationinformationsystemthatusesonlyGPSandSMS",inProc.IEEEICTD,no.4Dec.2010.

[7]D.RisingandM.Teofilo,"Mobiledeck:turningSMSintoarichuserexperience",inProc.6thmobisys,no.33,2009.

DOI: 10.15680/IJIRCCE.2018.0603113