IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-10 E-ISSN: 2347-2693

Providing RC5 Security for Messages in Android Based Mobile Devices for Achieving Confidentiality

Shahebaz Ahmed Khan[1*], P. Padmanabham[2] and K V Naganjaneyulu[3]

[1,2,3] Department of Computer Science and Engineering

Bharat Institute of Engineering and Technology

Mangalpally (Vill), Ranga Reddy (Dist.), Telangana (State), Pin – 501 510, India

www.ijcseonline.org

Received: Sep/17/2015 Revised: Oct/01/2015 Accepted: Oct /16/2015 Published: Oct /31/ 2015

***Abstract*:-**The idea of this paper is to study the symmetric key algorithms like DES, RC5, AES, Triple DES, BLOWFISH etc. so that the better algorithm can be picked to import its functionality in the Android based mobile devices. Here, we analyse their performance mainly this beats, end memory requirements and speed are studied to pick suitable algorithms to be implemented on the mobile and handheld devices. The above algorithms will be first implemented in C, C++ or JAVA and their performance will be analysed. The proposal extends as when an encrypted message is sent from one mobile phone to the other, a standard and essential key is provided which is symmetric in nature. If any of the two or more parties want to open the message that is sent to them, they have to utilize the secret code in the provided key without leaving a single digit. The message will be decrypted only after the full key version is matched with the given symmetry of the key .This makes the data or any information more secure even in the mobile devices for the common users by non-repudiation. This ensures the use of cryptography and its advantages by the end users of mobile phones for confidentiality.

***Keywords*— Non-repudiation, symmetric algorithms, RC5,DES, AES, 3DES, full key, cryptography.**

I. INTRODUCTION

Do we really enjoy the fruits of the security in the mobile? Though there are a number of ways that are provided by internet to build all the possible ways to make sure security in the mobile devices but, are these practically dealing from a person to person. When we deal with the present day commerce and business it comes to a point of necessity to provide security to the information even in mobile phones.

There are many aspects to security and many applications like passwords authentication etc. A secure communication and simple security logic is only possible by Cryptography. This paper discusses two aspects in terms of Cryptography [1]. The first is to define some of the terms and analyse the concepts behind basic cryptographic methods, offer a way to compare the myriad cryptographic algorithms in use today. The second is to import the best suitable algorithm in the mobile phones for the symmetric message encryption. Non-repudiation is successfully achieved in this along with confidentiality. Generally among all three cryptographic schemes present here in our paper we use symmetric algorithmic approach for encryption and decryption process of message text.

Later, the selected algorithm is imported in Android based mobile devices. Android is an Operating System that supports a large number of applications in Smart Phones. These applications are advanced for the users. Hardware of Android is mainly based on ARM architect Android applications are written in java programming language. For software development, Android has a development kit called Android SDK (Software development kit).

II.METHODOLOGY

II a) Data Encryption Standard (DES)

DES is most common secret key cryptography scheme used today, DES is a block-cipher which employs a 56-bit key that operates on 64-bit blocks. The set of rules and transformations are complex. To yield fast hardware implementations and slow software implementations. Later a 112 –bit key was proposed but, rejected due to some technical reasons. The 56-bit key is divided into eight 7-bit blocks and to each block 8th odd parity bit is added We use these parity bits for some error detection, Although the DES has 56 bits which are random its key is 64 bits in length. DES functions as:

1. Input
2. Initial permutation
3. Rounds
4. Reverse Initial permutation
5. Output.

DES Algorithm Breaking

DES is easily gets affected by the Brute Force attacks and is also more vulnerable to it as it uses encrypt words, which means the entropy of the 64-bit block is reduced effectively[3]. About ¼ bit combinations are likely to occur in a given byte. The possible values of a given byte are 256 or 2^8 when we are encrypting these streams of bits .Because of its vulnerability to simple brute force attacks DES has been deprecated and is replaced by the Advanced Encryption Standard. The security implications of DES can be known from RFC 4772.Due to its simplicity many

software developers and designers continue to deploy DES in their new applications.

When the DES algorithm was written by us and tested the time to decrypt the encrypted text of 12 characters it took a time of 0.14 milliseconds for us. The source code was tested in the C programming language as it is a fact that the results are same irrespective of the programming platform. The algorithm was designed for 64 bits block size and 56 bits key length. The possible keys were 2^{56} values. The result of the DES key decryption is given in the figure 1 is as follows:

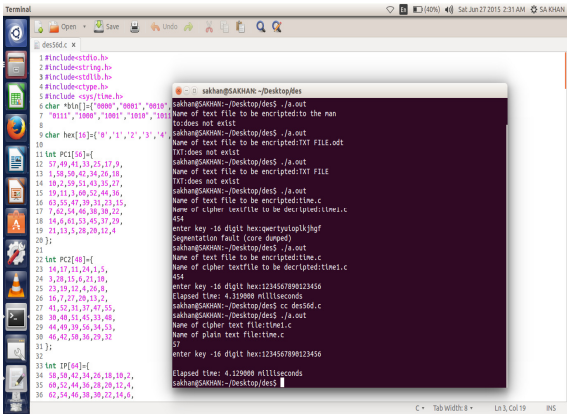


Figure: - 1 DES Test Analysis Results

II b).Advanced Encryption Standard (AES)

AES[7]. is secret key cryptography scheme used for more security when compared to DES More over AES is a replacement for DES and 3 DES. AES is a block-cipher which employs a 128 or 192 or 256 -bit key that operates on the same 128,192,256 -bit blocks. Though it has a possible keys to the power of the bit sizes and considered secured.It has 10 or 12 or 14 rounds with some different set of rules and transformations that are complex. The AES has 3 stages in which the algorithm shows and completes its functionality and operations. The operational stages are as follows;-

Stage:-1

- AddRound Key transformation

Stage:-2

- **Nr**-1 Rounds comprises:
  - SubBytes transformation
  - ShiftRows transformation
  - MixColumns transformation
  - AddRoundKey transformation

Stage:-3

- A final Round comprises:
  - SubBytes transformation
  - ShiftRows transformation
  - AddRoundKey transformation

The AES Cipher Key can be 128, 192, or 256 bits in length. During each round of encryption operation a cipher key is used to derive another different key and this derived key is applied to the round of encryption operation. The expanded key[8]. size is formed with original cipher key of length 32 bits and this expanded key later produces the new key material of which *AddRoundKey()*, *SubBytes()*, *ShiftRows()*, and *MixColumns()* are functions .

When the AES algorithm was written by us and tested the time to decrypt the encrypted text of 12 characters it took a time of 0.12 milliseconds for us. Even here for this algorithm the source code was tested in the C programming language as it is a fact that the results are same irrespective of the programming platform. The algorithm was designed for 64 bits block size and 128 bits key length. The possible keys were 2^{128} values. The result of the AES key decryption is given in the figure 2 is as follows:

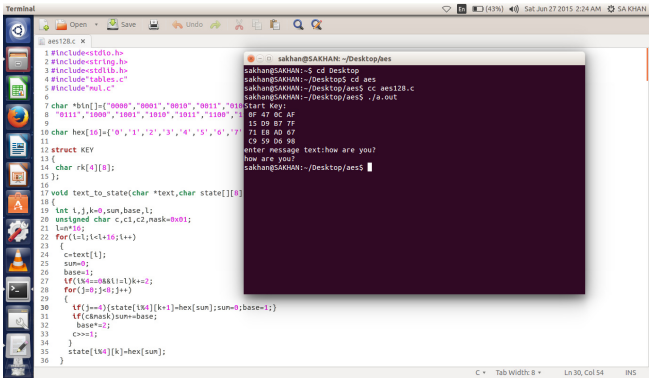


Figure:-2 AES Test Analysis Results

II C). Rivest Cipher (RC5)

RC5, Rivest Cipher 5, is a symmetric block cipher that is designed simple and for fast. It uses a Fiestel like structure in manipulating plaintext into cipher text. RC5 uses various block sizes of 32/64/128 bits, various key sizes ranging from 0to2048bits, and various round lengths from 0-255. RC5 stands for its strength due to its 'data dependent' rotations[3]. The RC5 algorithm uses three basic schemes to operate its functionality:-

1) Key expansion algorithm
2) An encryption algorithm
3) Decryption algorithm.

Key expansion[9] is an important algorithm within the cipher. A secret key is supplied by the user and this secret key is expanded to a key array. The values of key array are applied sequentially over the rounds in increasing order for encryption or decreasing order for decryption. The process is as follows:

1. Define magic constantsRC5 uses two magic constants Pw and Qw[4].

2. Convert the secret key K from bytes into words
3. Mix in K over arrays S and L.

The secret key K is now integrated into the key arrays S and L.

The Exclusive OR (XOR) Function

Exclusive OR (XOR) is a fundamental mathematical operations used in many applications, especially in cryptography[2]. It uses a group of logical operations with more than one or equal to one inputs with a single output as a result and the input and output are either TRUE or FALSE. The most elemental Boolean operations are: NOT,AND, OR and XOR.

In this RC5 we use only XOR truth table to implement the Boolean logic.Fig:3 shows the XOR logic.

XOR		Input 1	
		0	**1**
Input 2	**0**	**0**	**1**
	1	**1**	**0**

Figure:- 3 XOR Operations

When the RC5 algorithm was written by us and tested the time to decrypt the encrypted text of 12 characters it took a time of 0.9 milliseconds for us. The source code was tested in the JAVA programming language as well as in C programming as it is a fact that the results are same irrespective of the programming platform. The algorithm was designed for 64 bits block size and 128 bits key length. The possible keys were 2^{128} values. The result of the RC5 key decryption is given in the figure 4 and 5 is as follows:-

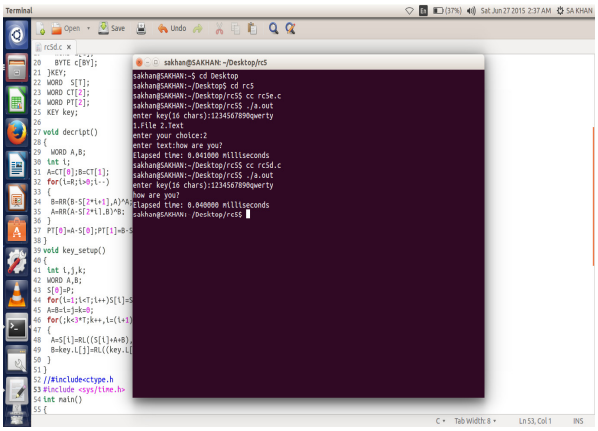


Figure:- 4 RC5 Test Analysis Result in C.

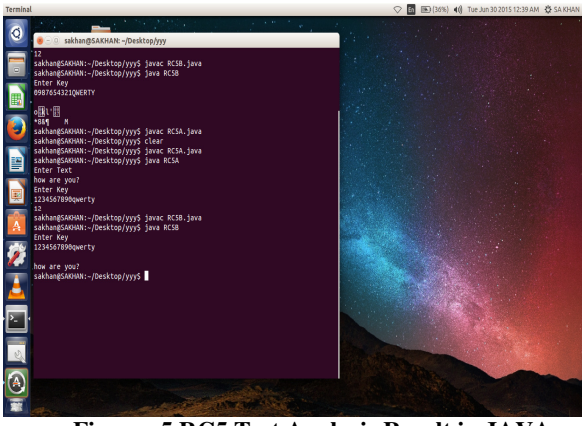


Figure:-5 RC5 Test Analysis Result in JAVA.

Comparison of RC5 with AES and DES

A comparative analysis of time and memory of RC5, AES & DES is performed to provide some measurements on the encryption and decryption. Results and impacts of several parameters like number of rounds, block size and the length of secret key on the performance evaluation criteria are analysed and known. This is shown in below table:1

Factors	DES	AES	RC5
Key length	56	128	0-2048
Ciphertype	Symm	Symm	Symm
Block size	64	128	64
Security	Inadequate	Vulnerable	Differential
Possiblekeys	2^{56}	2^{128}	2^{128}
Time	400	$5*10^{21}$	$10*10^{256}$
Rounds	16	10	16

Symm= Symmetric.

Table 1:-Comparison of Algorithms

In the above analysis of algorithms, we come to a note that RC5 is best suitable in terms of time and memory requirements. So it can be chosen to import in the Android mobile phones in order to build an message encryption application.

III. Android Operating Environment and Tools

Background theory in this work serves as for developing an application. This allows us to understand compatibly principals and technologies of Android development [4] so that we can develop the project application. Android has a complete software package for a mobile device. The tools and its framework make this easier to develop an application. Android applications even manage low memory requirements and work fast.

Eclipse (software) IDE

Eclipse software is an integrated_development environment (IDE). A base workspace and an extensible plug-in system is present in the environment IDE[5] of

Eclipse for customizing it.This Eclipse Ide is written in java programming for developing applications. Eclipse supports other languages for building an application.

Eclipse Android Development Tools (ADT) is a plugin for the Eclipse IDE that is designed to provide an integrated environment in which to build Android applications. It is a free download and open source. To debug the applications it uses Android SDK tools from Android Studio[10]. After you download the Eclipse, to open it, double-click on the .exe file by name 'eclipse.exe'. Then the Eclipse system prompts you for a *workspace[5]*. This is a location in the file system where the eclipse resources are stored. The projects developed are stored in this *workspace* is the location.

All the javadoc files of the source code can be opened in a separate editor called javadoc editor. Three important files of code are created in order to build any Android application. These three files are MainActivity[6], SmsBroadcastActivity[6]. and Manifest file. Rests are the java source code files.

The following figures fig:6 and fig:7 show the original and emulator images of the application for the message encryption and decryption by using symmetric key implementing RC5 algorithm based on its time and memory feasibilities. The designed application is as follows:-

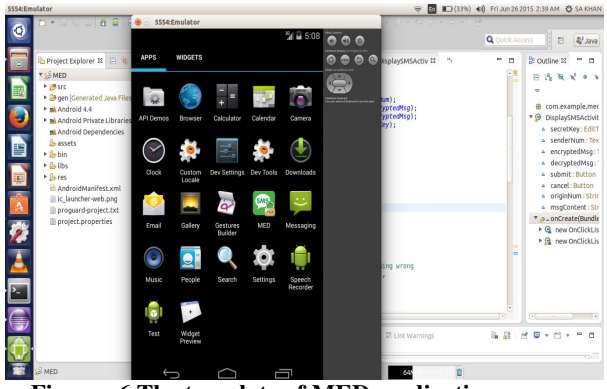


Figure:-6 The template of MED application

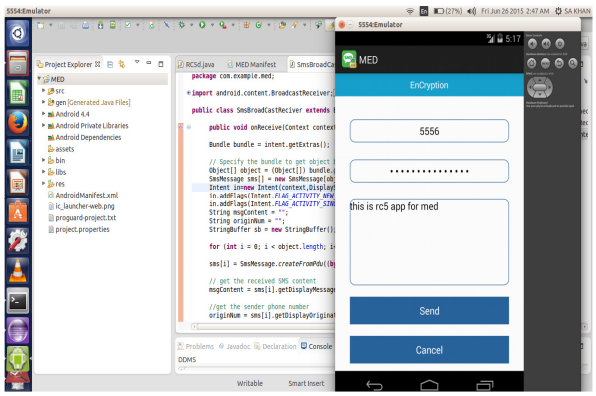


Figure:-7 The look of MED application in Emulator

When this MED is installed in mobile devices that work on Android operating system,it gives the below look as shown in fig:8.

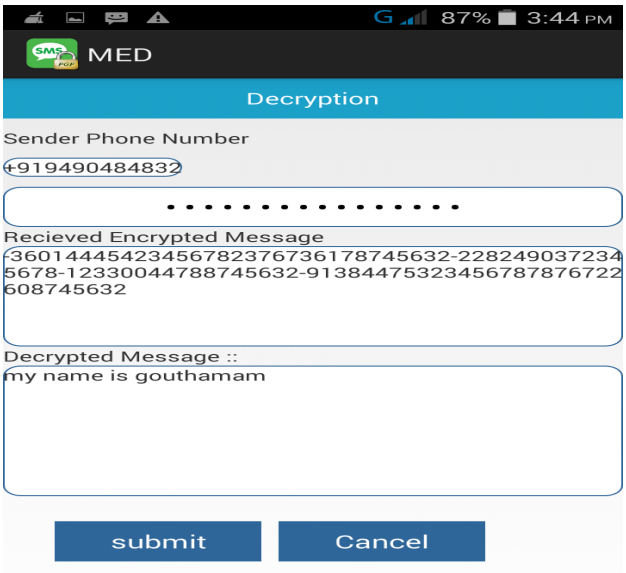


Figure:- 8 The Sample Look of MED

IV.CONCLUSION

In this criteria, RC5, AES and DES block cipher algorithms were compared by using C and JAVA programs Linux terminal. Performance of these three algorithms were measured on a 4 GB of RAM running Ubuntu 12.2 Version 2014-15, Comparative analysis of RC5, AES and DES have been done with a set of input files and evaluated the encryption & decryption time as mentioned in figures 1,2,4 and 5.Thus the RC5 is selected to import for its functionality in the mobile phones. Future enhancement can be achieved even by capturing the suitable code with the needed modifications to import the same algorithm in the i-phones. The same idea can be successfully implemented as a part of the further progress in the project in the mobile devices that works with i-OS and even other handheld devices used for communication.

This application can be used by any android mobile phone uses for any secure and private message transfer. This can be a good application for the government and defence services.

References:-

[1.] Atul Kahate "Cryptography and Network Security", Tata McGraw-Hill Companies, 2008.

[2.] William Stallings "Network Security Essentials (Applications and Standards)", Pearson Education, 2004

[3] Ronald L. Rivest, "RC5 Encryption Algorithm", Dr Dobbs Journal, Vol. 226, PP. 146-148, Jan 1995

[4] Ronald L. Rivest, The RC5 Encryption Algorithm, MIT Laboratory for Computer Science 545 Technology Square, Cambridge, Mass.02139 (Revised March 20, 1997).

[5]Khawlah A. AI-Rayes, Aise Zulal Sevkli, Hebah F. AI-Moaiqel, Haifa M. AI-Ajlan, Khawlah M. AI-Salem, Norah I. AI-Fantoukh "A Mobile Tourist Guide for Trip Planning" IEEE MULTIDISCIPLINARY ENGINEERING EDUCATION MAGAZINE, VOL. 6, NO. 4, DECEMBER 2011

[6]MIDP_Mobile_Media_API_Developers_Guide_v2_en

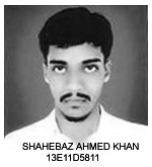
[7] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[8.] R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978.

[9] Ronald L. Rivest, The RC5 Encryption Algorithm, MIT Laboratory for Computer Science 545 Technology Square, Cambridge, Mass.02139 (Revised March 20, 1997). Available at: httu://theory.lcs.mit.cdu/-rivest/Rivest-rc5rev.pd

[10]"Detecting passive content leaks and pollution in android applications," in Proceedings of the Network and Distributed System Security Symposium , 2013.

AUTHORS' PROFILE



Shahebaz Ahmed Khan is a M.Tech research scholar at Bharat Insitute of Engineering and Technology and has Published 2 research papers in conferences and in an international journal. His areas of interest include data mining, network security, operating systems and automata.

Professor P Padmanabham has completed his phd in computer science and is also double masters degree holder is currently working as the director of academics at BIET and he was the former director of SIT, JNTUH. He has 47 years of experience in Technical Education in the areas of Teaching, Administration, Research and Consultancy and published more than 30 papers in national and international journals and conferences. His areas of interest include programming, network security, operating systems and networks.

KVN is presently working as associate professor at BIET and he has over14 byears of experience in teaching .He published more than 12 research papers in national and international journals. His areas of interest are software testing, computer organization and networks.