MESSAGE ENCRYPTION AND DECRYPTION ON MOBILE PHONES

Murtala, Kabir[1] and Adeniyi, Abidemi[2]

Department of Computer Science, Kwara State Polytechnic, Ilorin, Nigeria

Abstract

Encryption is process of turning a plaintext to jargon or the method of changing confidential file to jargon in order prevent unauthorized persons to gain access to confidential message. Message is the transfer of information from the sender to the receiver through a particular medium. Encryption is the most effective process for achieving data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. This paper presents an Encryption/Decryption application of messages on both java and Android phones. The method of encryption of message in this paper is AES (Advance Encryption System) where the same key that is used to encrypt is used to decrypt. The Encryption key is entered into the mobile phone text field by the user. The same encryption key is also used to decrypt the encrypted binary file.

Keywords: *Encryption, Decryption, plain text, mobile phone, cipher key*

1. Introduction

Information is the glue that cements the existence of human life. Uninterrupted message can be achieved through encryption. This paper is aimed to develop message encryption and decryption on mobile phones. If we are protecting confidential information then encryption provides high level of privacy of individuals and groups. However, the main purpose of encrypting message is not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation etc. Encryption is the method that allows information to be sent in a secure form in such a way that the only receiver is able to retrieve this information with the cipher key. To make this section more meaningful, it must be related to certain phenomenon which is Mobile Phone. Mobile phones are used for a variety of purposes, including keeping in touch with family members, conducting businesses, and having access to a telephone in the event of an emergency. Some people carry more than one cell phone for different purposes, such as for business and personal uses [11].

The future of mobile computing is becoming even more exciting. Mobile devices are continually growing more capable, especially with the advent of cleverly integrated phone capabilities. With better and better wireless networks capable of transferring media in real time, entirely new breed of applications are now possible. Riding this new wave may be extremely profitable for organizations positioned to take advantage of it [7], [1].

There is a very high level of interest in software development revolving around J2ME (Java 2 Micro Edition). J2ME is a slimmed-down version of Java targeted at devices that have limited memory, display, and processing power. However, this paper is concerned with mobile phone as a useful tool in National Security Agency (NSA) Department. In cryptography, encryption is the conversion of messages (or information) in cipher text in such a way that unauthorized users cannot read it, but that authorized parties can access it [3]. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm, which usually requires a secret decryption key that adversaries do not have access to. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys [3]. As discussed by [3], there are two basic types of encryption schemes: symmetric-key and Asymmetric-key encryption. In symmetric-key schemes, the encryption and decryption keys are the same. Thus, communicating parties must agree on a secret key before they wish to communicate. In asymmetric-key schemes, the encryption key and decryption key are different. One is a public key by which a sender can encrypt messages and the other is a private key by which a recipient can decrypt the message. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages [12]. Asymmetric-key encryption is a relatively recent invention: historically, all encryption schemes have been private-key schemes [3].

2. Literature Review

The best known types of symmetric encryption are the Data Encryption Standard (DES), Triple DES (3DES), the Advanced Encryption Standard (AES), and Rivest Cipher (RC4). The former three are block ciphers while RC4 is a true stream cipher [9]. The AES was developed as a replacement for DES and 3DES. It supports key lengths of 128, 192, and 256 bits and a variable block length. AES is based on the Rijndael encryption algorithm. Rijndael is a block cipher adopted as an encryption standard by the U.S. government, developed by Joan Daemen and Vincent Rijmen. It has been analyzed extensively and is now used widely worldwide as was the case with its predecessor, DES [11], [9]. During the evaluation of candidates for the AES standard, Rijndael was analyzed by some of the world's best cryptanalysts. It has proven to be very effective against known attacks, very efficient, and simple to implement. [6], [7], [9]. Rijndael supports a larger range of block and key sizes; AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits, whereas Rijndael can be specified with key and block sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits [8]. This proposed research paper uses the AES cipher algorithm to perform data encryption and decryption. The key sharing will be secured by the implementation of the public key algorithm, RSA. The use of AES cipher algorithm allows us to store the data in a compressed encrypted form which consequently results in a small-size database. This implementation, therefore, addresses some of the common issues raised in previous sending of plain text message from one mobile phone to another.

3. Material and Method

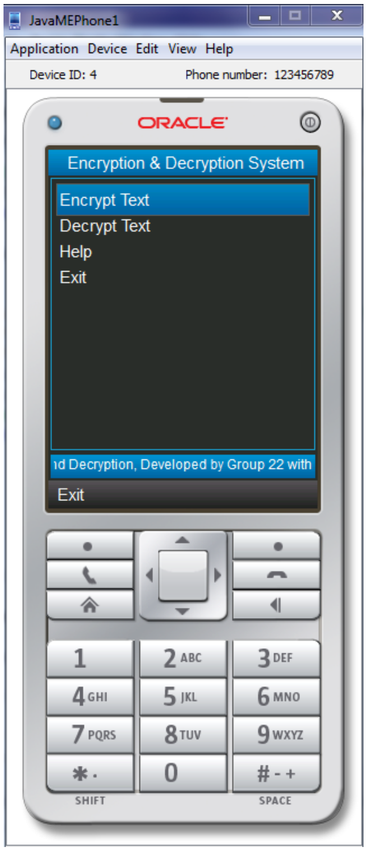
The programming language used in this paper is Java 2 Micro Edition (J2ME) being used to develop encryption and decryption of messages on mobile phone with AES (Advanced Encryption System). J2ME combines a resource constrained JVM (Java Virtual Machine) and a set of Java APIs for developing applications for mobile devices. The most popular profile and configuration that Sun provides are the Mobile Information Device Profile (MIDP) and Connected Limited Device Configuration (CLDC), respectively. As the name suggests, CLDC is for devices with limited configurations; for example, devices that have only 128 to 512KB of memory available for Java applications. Consequently, the JVM that it provides is very limited and supports only a small number of traditional Java classes. This limited JVM is actually called the *KVM*. Its counterpart, the Connected Device Configuration (CDC), is for devices with at least 2MB of memory available and supports a more feature-rich JVM (but still not a standard JVM). **Java emulator** is a tool that helps for java-based software that can be run on your computer's operating system. There are varieties of java applications usages example are; games, music, videos etc all embedded in mobile phones. Because it is a java emulator so application must have the extension Jar or Jad while for android phone will have extension of apk and the computer must be installed java platform: Java SE/*JRE* (*Java Runtime Environment*).The reason is that JRE, runs the file API of each platform java program.

4. Discussion of Results

The figures below show the output of mathematical software library that was developed for mobile phone.

Screen Shoot of Message Encryption Main Menu

Once you run the jar file on your phone, encryption, Decryption, Help and Exit will be displayed on the phone screen as shown below. The screen shoots display the options where users can select what they wish to do.



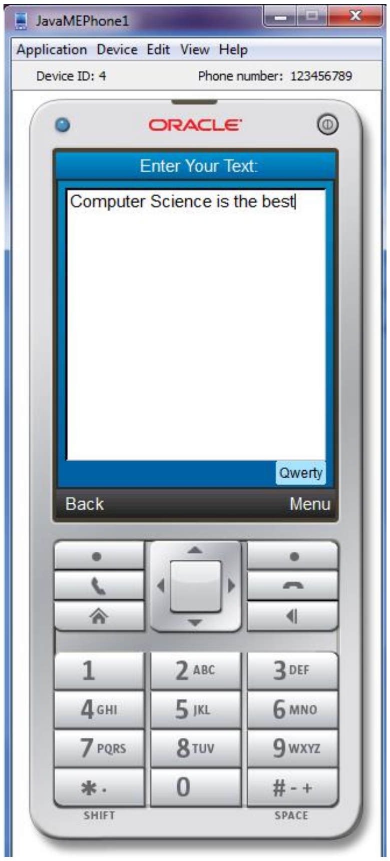
Device ID: 4 Phone number: 123456789

ıd Decryption, Developed by Group 22 with

Fig. 1: This Figure displays the Main Menu of Message Encryption and Decryption on Mobile Phone.

Plain Text before Encryption

This section displays the plain text before encrypting the message, after the message have been typed correctly, then the Menu button will be pressed in order to achieve our aim. In order to compute the result on these types of phone, you will need to select menu and then click the encrypt label, by doing so the Plain text will be turned to jargon in the text field. The type of phone used is any java phone or Android platform.

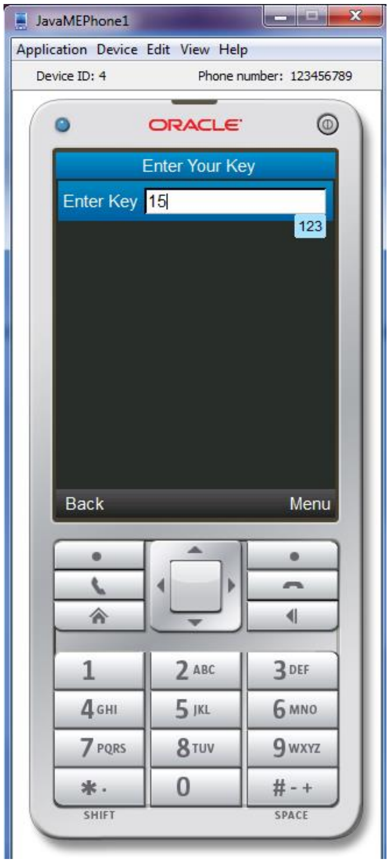


Computer Science is the best

Fig. 2: This Figure Displays the Plain text that have not yet been encrypted.

Cipher Key

The Cipher Key to encrypt the plain text is being entered into the textbox. The cipher key is numeric value. Once entered into the textbox, click the Menu Button and click on Encrypt label to turn the real plain text into jargon.



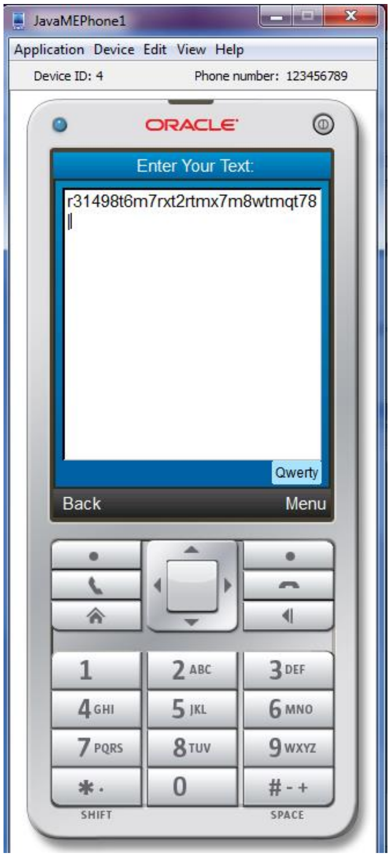
Enter Your Key

Enter Key 15

Fig. 3: The Figure above displays the Module where the user will enter the cipher key to encrypt the typed message.

Encrypted Text

In this module, the plain text has been turned to jargon with the aid of the cipher key supplied by the user. The jargon displays in the textfield below have made the message read protected from the third party. This can be turned to real text by using the former cipher key used to encrypt to decrypt.



Device ID: 4 Phone number: 123456789

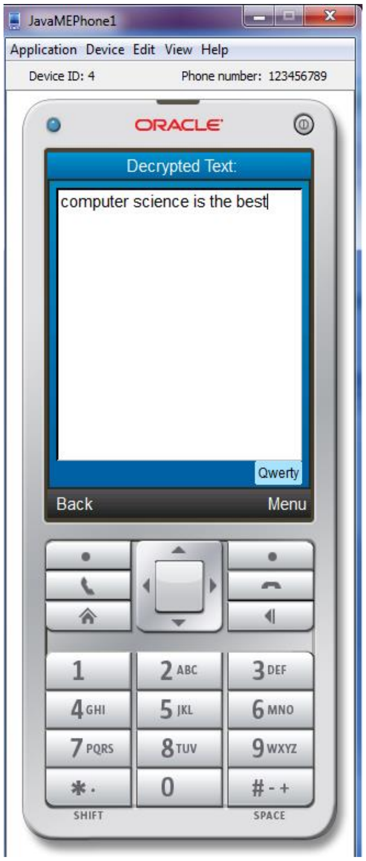
Enter Your Text:

r31498t6m7rxt2rtmx7m8wtmqt78

Fig. 4: This Figure displays the encrypted text.

Decrypted Text

In this module, the jargon has been turned to plain text with the aid of the cipher key supplied by the user. The decrypted text is displayed in the textfield below. Unathorized user can not have access to the real plain text except the cipher key has been given to recipient.



Decrypted Text:

computer science is the best

Fig. 5: This Figure Displays the Decrypted Text.

5. Conclusion

This research work has a lot of benefits to both private and public firm and even individuals to protect their confidential information on mobile phones. This research does not require SMS gateway for the message to be sent from the sender to the receiver. What you need is just to install the software on your phone and continue the process of encrypting message. Based on the study so far, we give the following recommendations:

i. The software should be used in a firm where their medium of sharing of information is mainly by text messages.

ii. Individuals should install this software on their mobile phones in order to deprive the third party from accessing the message.

iii. Those that perform transaction online through their mobile phones should install it on their phones.

This paper can be developed further by creating some application that will be useful for both the citizens and the governments of the states.

References

[1] Burnette, Ed. (2008). Hello, Android Introducing Google’s Mobile Development Platform communications”, Schweitzer Engineering Laboratories, SEL 2003 Inc. Pullman WA, USA.

[2] Heeks, R. (2008). Meet Marty Cooper – the inventor of the mobile phone, Accessed June,2013 from *htpp://news.bbc.co.uk/2/hi/programmes,* from IRKHS 2040 at International Islamic University Malaysia.

[3] Helen, F. (2009). “Cryptanalysis”, Dover, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA

[4] John, M. (1973). Advance Development of handheld mobile telephone equipment, By Chicago Sun-Times, USA.

[5] Khurana, VG; Teo, C., Kundi, M., Hardell, L., Carlberg, M.(2009). "Cell phones and brain tumors: A review including the long term epidemiologic data, US National library of medicine, national institute of health, USA.

[6] MMA,"Mobile Application", Mobile Marketing Association, Sept. 2008. 1670 Broadway, Suite 850, Denver CO, USA

[7] Murphy, L. (2009). A textbook “Beginning Android2”, published by Apress L. P. USA.

[8] Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. & Roback, E. (2000). “Report on the Development of the Advanced Encryption Standard (AES)” Computer security division information technology laboratory national institute of standards and technology administration, U.S. Department of Commerce, USA

[9] Risley, A. Roberts, J. & LaDow, J. (2003). “Electronic security of real-time protection and SCADA, Western Power Delivery Automation Conference spokane, Washington, USA

[10] Sanadhya, S. & Sarkar, P. (2009). A new hash family obtained by modifying the SHA-2 family. ACM Symposium on Information, Computer and Communications Security, ASIACCS, Sydney, Australia

[11] Saylor, M. (2012). The Mobile Wave: How Mobile Intelligence Will Change Everything. *Perseus Books/Vanguard Press*, USA

[12] Yumbul, K. & Savas, E. (2009).Efficient, secure, and isolated execution of cryptographic algorithms on a cryptographic unit. ACM Proceedings of the 2nd international conference on Security of information and networks, Pages 143-151, Famagusta, North Cyprus.