A New Mobile Application for Encrypting SMS / Multimedia Messages on Android

Hazem M. El bakry, Ali E. Taki_El_Deen, Ahmed Hussein Ali El tengy

Abstract— Mobile communication devices have become popular tools for communicating among people. This paper is a launcher for sending/receiving secured SMS/Multimedia files using Blowfish algorithm. A smart mobile application on android platform is introduced as an application that helps the user to encrypt the message (SMS/Multimedia files) before it is transmitted over the mobile network. The new idea of the program is to transmit encrypted messages and multimedia files or any other type of files via mobile networks or the internet as an alternative mean. Utilizing the internet takes place through a secured hosting website with a user name and password integrated in the program. To maintain intensive security, a private key encrypts the files and another private key encrypts file name. The transferring media is maintained online in the absence of mobile network coverage.

Index Terms— Mobile Communication Devices, Secure SMS, Cryptography, SMS Encryption, MMS Encryption, File Encryption, Blowfish.

1 Introduction

Mobile communication devices [1] have become commonplace during the past few years, integrating multiple wireless networking technologies to support additional functionality and services. One of the most important developments that have emerged from communications technology is SMS [2]. They are designed as part of Global System for Mobile communications (GSM) [3]. Banks worldwide are using SMS to conduct some of their banking services [4]. For example, clients are able to query their bank balances via SMS or conduct mobile payments. In addition, people sometimes exchange confidential information such as passwords or sensitive data amongst each other [5]. SMS technology suffers from some risks such as vulnerabilities, eavesdroppers and unauthorized access [6].Therefore, we need to secure SMS messages and keep their contents private, without increasing their size. This paper provides a solution to this SMS security problem. Our approach is to secure the SMS/Multimedia message using an encryption (Blowfish) system [7]. The proposed technique encrypts SMS with 16-round Feistel cipher and uses large key-dependent S-boxes.

Section 2 Gives an overview of Short Message Service (SMS)
Section 3 Provides some details of Blowfish algorithm
Section 4 Simulation of program screens
Section 5 Conclusion.

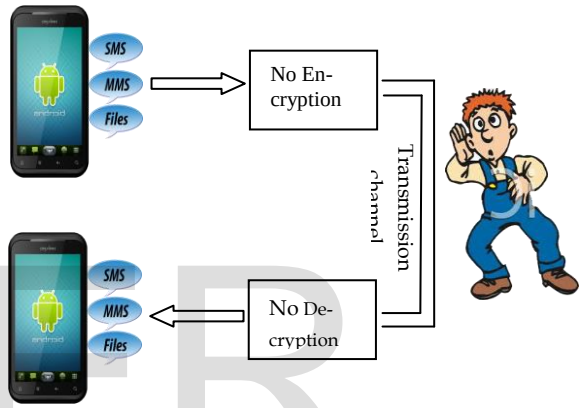

Fig.1 Send SMS/MMS/Files via network normally

Figure (1) shows the normal way to send text messages or multimedia files over mobile phone networks, which exposes them to eavesdropping operations and overhearing of information.

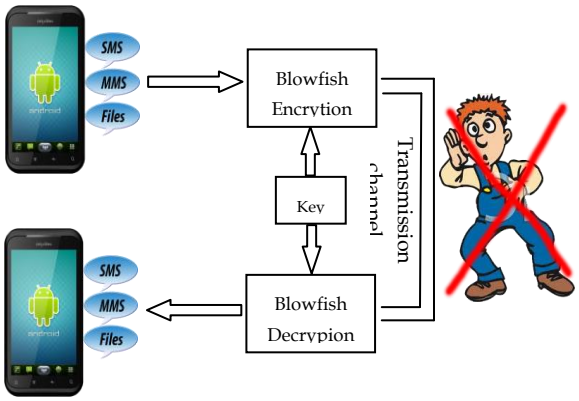

Fig.2 Send SMS/MMS/Files via network with Encryption

Figure (2) the method proposed here is to encrypt the data before sending it over the mobile phone networks, whenever is the encrypted data among the transmission channel is vulnerable. Hence, the receiver can attain authenticated data after decrypting it.

- *Hazem M. El bakry is currently pursuing Mansoura University, Egypt, E-mail: Helbakry5@yahoo.com*
- *Ali E. Taki_El_Deen is currently pursuing Alexanderia University, Egypt, E-mail: A_takieldeen@yahoo.com*
- *Ahmed Hussein Ali El tengy is currently pursuing masters degree program in electric Comunicating engineering in Alexanderia University, Egypt, E-mail: tengy_fox@yahoo.com*

International Journal of Scientific & Engineering Research Volume 4, Issue 11, November-2013
ISSN 2229-5518

2 SHORT MESSAGE SERVICE (SMS)

SMS is a communication service standardized in the GSM mobile communication systems [8]. It can be sent and received simultaneously with GSM voice, data and fax calls. This is possible because whereas voice, data and fax calls take over a dedicated radio channel for the duration of the call, short messages travel over and above the radio channel using the signalling path [9].
SMS contains some meta-data [10]:

- Information about the senders (Service center number, sender number).
- Protocol information (Protocol identifier, Data coding scheme).
- Timestamp.

3 SOME DETAILS OF BLOWFISH ALGORITHM

3.1 Introduction

An encryption algorithm [11] plays an important role in securing the data while storing or transferring it. The encryption algorithms are categorized into Symmetric (secret) and Asymmetric (public) keys encryption [12].

3.1.1 In Symmetric key encryption or private key encryption, only one key is used for both encryption and decryption of data. For example Data encryption standard (DES), Triple DES, Advanced Encryption Standard (AES) and Blowfish Encryption Algorithm [13].

3.1.2 In asymmetric key encryption or public key encryption uses two keys, one for encryption and another for decryption. For example RSA [14].

3.2 Blowfish Encryption Algorithm

Blowfish [15] is a 64-bit cipher and its key length extended from 32 bits to 448 bits, it has 16 rounds and uses large key-dependent S-boxes.

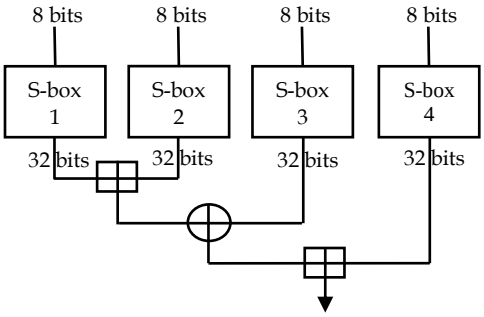

Fig.3 Substitution box of Blowfish

The diagram [16] in figure (3) shows a Function that uses four arrays S_1,..., S_4 derived from the encryption key. Each array contains 32-bit words. The arrays act as substitution boxes or S-boxes [17], replacing an 8-bit input with a 32-bit output. F splits its 32-bit input into four 8-bit bytes. It replaces each byte by the contents of an S-box, and combines the results as follows [18]:

Letting $\boxplus$ signify addition modulo 2^{32}:

$$F(a, b, c, d) = ((S_1[a] \boxplus S_2[b]) \oplus S_3[c]) \boxplus S_4[d]$$

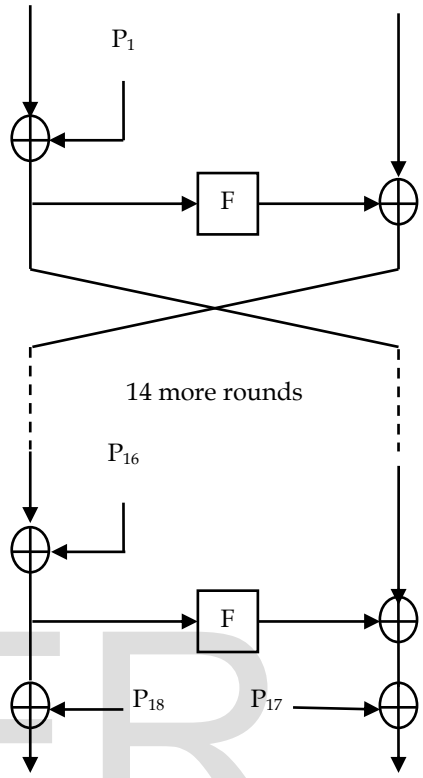

Fig.4 F-function Blowfish

The diagram [19] in figure (4) shows Blowfish's F-function. It follows the Feistel network .This algorithm is divided into two parts.

3.2.1 Key-expansion [20]:

Key is converted from 448 bits to several sub-key arrays totaling 4168 bytes. The keys are generated before data encryption or decryption.
The p-array consists of 18, 32-bit sub-keys:

$P_1, P_2, \ldots\ldots\ldots\ldots\ldots P_{18}$

Four 32-bit S-Boxes consist of 256 entries each:

$S_1, 0, S_1, 1, \ldots\ldots\ldots S_1, 255$
$S2, 0, S_2, 1, \ldots\ldots\ldots S_2, 255$
$S3, 0, S_3, 1, \ldots\ldots\ldots S_3, 255$
$S_4, 0, S_4, 1, \ldots\ldots\ldots S_4, 255$

In total, 521 iterations are required to generate all required sub-keys [21].

3.2.2 Data Encryption [22]:

In this function, there are 16 rounds. Each round consists of a key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookup tables for each round [23].

International Journal of Scientific & Engineering Research Volume 4, Issue 11, November-2013
ISSN 2229-5518

4 Simulation of Results and Interface

Fig.5 First screen of Blowfish program

Figure (5) shows the first screen in the application which has three buttons, the first button is used for encrypting and decrypting text messages, the second one is for encrypting and decrypting all files types on the mobile, the third is used for uploading or download files via Internet.

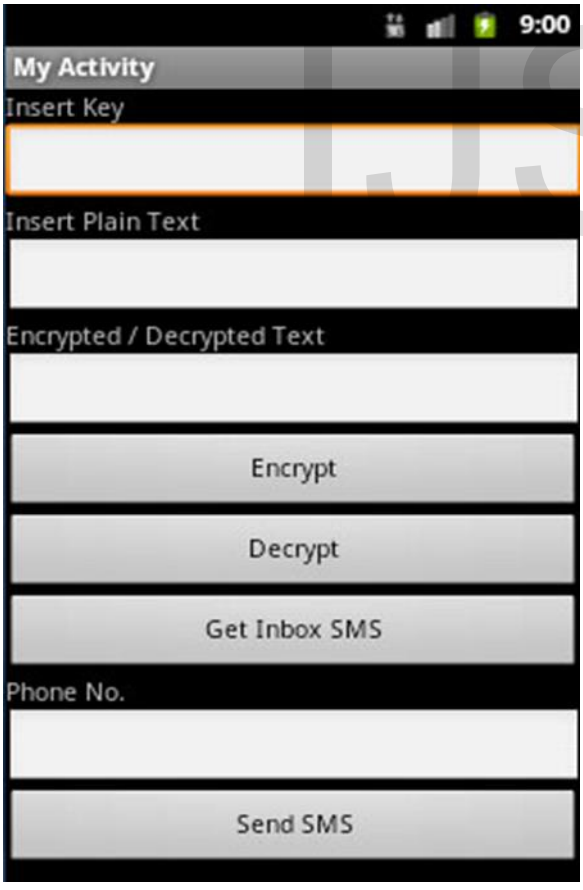

Fig.6 Main screen of encrypt/decrypt SMS

Figure (6) shows how to encrypt or decrypt text messages.

Encrypting text by inserting private key into first textbox then the message inserted to second textbox, when pressing the "Encrypt" button, the result cipher text displayed in third textbox.

Decryption cipher text by inserting private key into first textbox, when pressing "Get Inbox SMS" button then the program opens the SMS inbox of the smart phone and picking out the income cipher message, it returns in the second textbox, when pressing the "Decrypt" button the result decrypted text message displayed in the third textbox.

Fig.7 Main screen of encrypt/decrypt File

Figure (7) shows how to encrypt or decrypt multimedia or any type of files.

Encrypting files by inserting private key in the first textbox then when pressing the "Get Files" button, the program explores the mobile phone files and picks the file, its name and path returns in the second textbox, when pressing the "Encrypt" button, the encryption process starts, then the encrypted file name and path will be displayed in the third textbox.

Decrypting files by inserting private key into first textbox then when pressing the "Get Files" button, the program explore the mobile phone files and picks the encrypted file, its name and path returns in the second textbox, when pressing the "Decrypt" button, the decryption process starts, then the decrypted file name and path will be displayed in the third textbox.

International Journal of Scientific & Engineering Research Volume 4, Issue 11, November-2013
ISSN 2229-5518

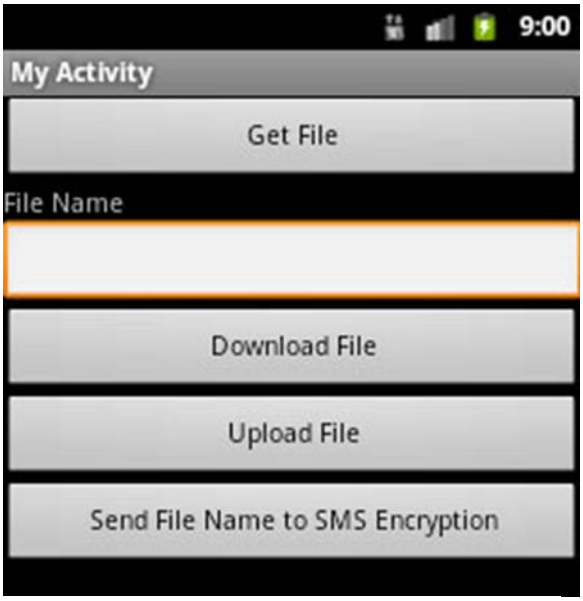

Fig.8 Alternative way to upload/download encrypted file

Figure (8) shows alternative way to upload/download files to a secured website with a username and password within the program to maintain more security so that the user has nothing to do with this information.

Uploading encrypted files: by pressing the "Get File" button, the program explores the mobile phone files and picks the file, its name and path returns in the first textbox, then when pressing the "Upload File", the program uploads the file to a secured website on the internet. When uploading completed, a notification message appears.

For high strength in the complexity of encryption, press the "Send File Name to SMS Encryption" button, as a result of that the program sends only the file name without path to the SMS encrypting screen to encrypt then send it.

Downloading encrypted files: by opening the "Main screen of encrypt/decrypt SMS" window, pressing the "Get Inbox SMS" button, choosing the message including the encrypted file name, pressing the "decrypt" button to decrypt the file name, copying this file name to the clipboard, then switching back to the "Upload/download" screen, pasting the file name in the first textbox. By pressing the "Download File" button, the program will download the file from the secured website on the internet, and then when downloading process is completed, a confirming message appears.

Sample of encrypting plain text to cipher text

Example:
Figure (9) shows input text "Encrypted SMS by Blowfish" and private key "123"

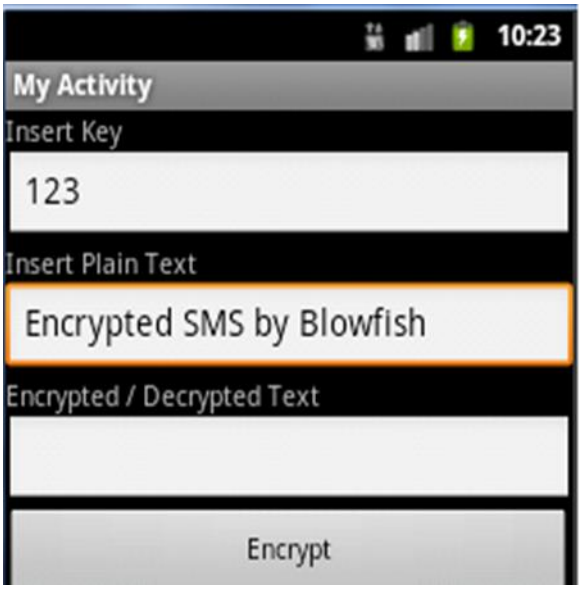

Fig.9 Input text

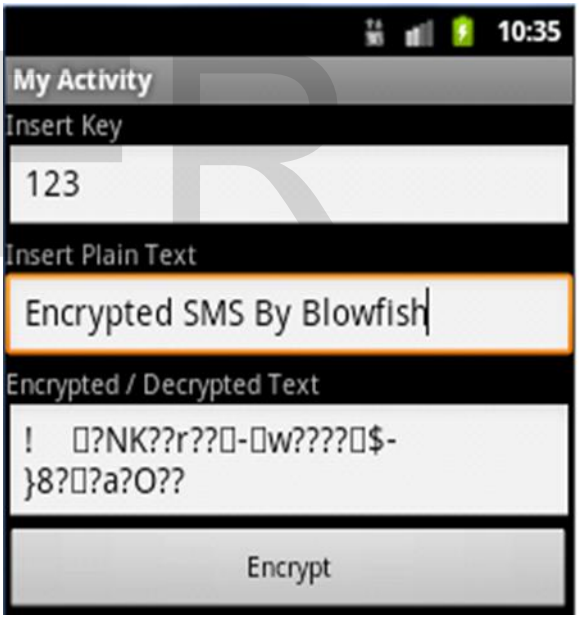

Fig.10 Output of cipher text

Figure (10) shows Cipher text as a result by pressing the "Encrypt" button, the result appears in the third text box.

5 CONCLUSION

In this paper, the importance of encrypting data in practical life is discussed, as the number of intruders, and spying attempts on private messages have recently been increased. Thus, it is mandatory to think of new ways to overcome this problem as designing a program with a simple user interface that encodes, by certain code keys, the text messages, image, voice, video files, and sends them via mobile networks. Two ways have been considered to send a message from one mo-

International Journal of Scientific & Engineering Research Volume 4, Issue 11, November-2013
ISSN 2229-5518

bile to another; the first, the program sends messages via GSM networks as text messages or multi-media ones, the second, by connecting the mobile to internet through the mobile network or a wireless internet network, where the program uploads the files to a specific file hosting site that requires a user name and a pass word already created and hidden, to maintain more security, in the program. The receiver using the same program will be able to download the files. It is clear that alternative communicating means are considered to overcome weakness or losing mobile network signals and shifting to internet connections, for instance.

6 REFERENCES

[1] Chin, E., Felt, A. P., Greenwood, K., and Wagner, D. "Analyzing Inter-Application Communication in Android". In Proc. of the Annual International Conference on Mobile Systems, Applications, and Services (2011).

[2] Marko Hassinen, "SafeSMS - End-to-End Encryption for SMS Messages", *IEEE International Conference on Telecommunications*, 2008, 359-365.

[3] S. Jahan, M. M. Hussain,M. R.Amin and S. H. Shah Newaz, "A Proposal for Enhancing the Security System of Short Message Service in GSM", *IEEE International Conference on Anti-counterfeiting Security and Identification*, 2008, 235-240.

[4] Mary Agoyi and Devrim Seral, "SMS Security: An Asymmetric Encryption Approach", *IEEE International Conference on Wireless and Mobile Communications*, 2010, 448-452.

[5] P. Traynor, W. Enck, P. McDaniel and T. La Porta. "Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks", IEEE/ACM Transactions on In Networking, 17(1):40-53, 2009.

[6] Mary Agoyi, Devrim Seral, "SMS Security: An Asymmetric Encryption Approach", Sixth International Conference on Wireless and Mobile Communications, 2010 IEEE, pp 448-452.

[7] Ferguson, N., Schneier, B. and Kohno, "Cryptography Engineering: Design Principles and Practical Applications", T. Indianapolis: Wiley Publishing, Inc. 2010.

[8] Roland Schloglhofer, "Secure and Usable Authentication on Mobile Devices", MoMM2012, 3-5 December, 2012, Bali, Indonesia. ACM 978-1-4503-1307-0/12/12 (pp 257-262).

[9] M. Toorani and A. A. Behesti, "SSMS – A Secure SMS Messaging Protocol for the M-Payment Systems", IEEE Symposium on Computers and Communications, 2012, 700-705.

[10] Marko Hassinen, "SafeSMS- End-to-End Encrption for SMS Messages", IEEE International Conference on Telecommunications, 2008, 359-365.

[11] Kuo-Tsang Huang, Jung-Hui Chiu, and Sung-Shiou Shen, "A Novel Structure with Dynamic Operation Mode for Symmetric-Key Block Ciphers". International Journal of Network Security & Its Applications (IJNSA) 5 (1): 19, (January 2013).

[12] Mary Agoyi and Devrim Seral, "SMS Security: An Asymmetric Encyrption Approach", IEEE International Conference on Wireless and Mobile Communication, 2010, 448-452.

[13] Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 1, Issue 2, December 2011)

[14] Dripto Chatterjee, Joyshree Nath, Soumitra Mondal, Suvadeep Dasgupta and Asoke Nath, " Advanced Symmetric key Cryptography using extended MSA method: DJSSA symmetric key algorithm", Jounal of Computing, Vol 3, issue-2, Page 66-71, Feb(2011).

[15] Trisha Chatterjee, Tamodeep Das, Joyshree Nath, Shayan Dey and Asoke Nath, "Symmetric key cryptosystem using combined cryptographic algorithms- generalized modified vernam cipher method, MSA method and NJJSAA method: TTJSA algorithm", Proceedings of IEEE International conference: World Congress WICT-2011 t held at Mumbai University 11-14 Dec, 2011, Page 1179-1184(2011).

[16] Somdip Dey, Asoke Nath, "Modern Encryption Standard (MES) Version-I: An Advanced Cryptographic Method", Proceedings of IEEE 2nd World Congress on Information and Communication Technologies (WICT- 2012), pp. 242-247.

[17] Dripto Chatterjee, Joyshree Nath, Sankar Das, Shalabh Agarwal and Asoke Nath, "Symmetric key Cryptography using modified DJSSA symmetric key algorithm", Proceedings of International conference Worldcomp 2011 held at LasVegas 18-21 July 2011, Page-306-311, Vol 1(2011).

[18] E. Barker and A. Roginsky, "Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes", NIST SP 800-131, 2010, Technical Report.

[19] Somdip Dey, Joyshree Nath, Asoke Nath, "An Integrated Symmetric Key Cryptographic Method - Amalgamation of TTJSA Algorithm, Advanced Caeser Cipher Algorithm, Bit Rotation and reversal Method : SJA Algorithm", International Journal of Modern Education and Computer Science (IJMECS), ISSN: 2075- 0161 (Print), ISSN: 2075-017X (Online), Vol 4, No 5, Page 1- 9, 2012.

[20] Debanjan Das, Joyshree Nath, Megholova Mukherjee, Neha Chaudhury and Asoke Nath, "An Integrated symmetric key cryptography algorithm using generalized vernam cipher method and DJSA method: DJMNA symmetric key algorithm", Proceedings of IEEE International conference: World Congress WICT-2011 to be held at Mumbai University 11-14 Dec, 2011, Page 1203-1208(2011).

[21] Jiao Wentao, "Cloud computing environments cryptographic applications", Chinese Association for Cryptologic Research, vol. 5, no. 1, pp.20-29, 2011.

[22] Satyaki Roy, Navajit Maitra, Joyshree Nath, Shalabh Agarwal and Asoke Nath, "Ultra Encryption Standard(UES) Version-I: Symmetric Key Cryptosystem using generalized modified Vernam Cipher method, Permutation method and Columnar Transposition method", Proceedings of IEEE sponsored National Conference on Recent Advances in Communication, Control and Computing Technology-RACCCT 2012, 29-30 March held at Surat, Page 81- 88(2012).

[23] Asoke Nath, Saima Ghosh, Meheboob Alam Mallik, "Symmetric Key Cryptography using Random Key generator", Proceedings of International conference on security and management (SAM'10) held at Las Vegas, USA Jull 12-15, 2010, Vol 2, Page: 239-244(2010).