Triple layered Security on Android based SMS transaction

Tamal Biswas

*[1]Department of Computer Science and Engineering, National Institute of Technology,
Agartala 799046, India.*

---***---

Abstract— *In this paper, the authors have proposed a triple layer encryption technique for Short Message Service (SMS), which is secure, fast, and data is encrypted strongly. SMS is a very popular way for mobile phone and portable device users to send and receive simple text messages. Unfortunately, SMS does not offer a secure environment for confidential data during transmission. The proposed more secured and advanced SMS encryption technique on android application has some stages. In first stage, SMS or any image is converted to byte and then it is converted to hexadecimal number and some bit manipulation is done. In the second step, a mapping table is used to convert each hex digit to alphabet using a predefined conversion table and then hill cipher is applied. Finally, AES encryption is used to ensure the algorithm is secure and non-vulnerable. The proposed algorithm primarily designed for android SMS transaction can be used for image or message containing any alphanumeric or special characters.*

Keyword **— Advance Encryption Techniques, hill cipher, android application, SMS.**

1. Introduction:

In present day scenario, data security is the major issue for sending data from one end to another. There are lots of method to use the data to make it more secure but still all these are vulnerable. For this reason, it is very essential that the data cannot be intercepted or misused by any means. For example, we can assume a situation where an investigation agency is sending some important data to another agency, then they should need to make the data more secure that no one else can be able to break the encrypted data in the open network or we can also assume a situation where a military person wants to send some important message to another higher authority. In this situation if any intruder attacks it then it can be highly devastating and can cause much more destruction. Different encryption methods are used by different organization and different government institutes.

The basic cryptography is classified into two types:

1. Symmetric key
2. Asymmetric key

Symmetric key cryptography uses only one key for encryption as well as decryption purpose. It is easy to deal with symmetric key system as there we need only a single key but here too many keys will be required for decryption which is a tough job. On the other hand, public key crypto system is also very popular and secure where for encryption it needs the receiver's public key which is known to all and for decryption it needs the receiver's private key which is kept secured.

In our proposed method, we combined two different algorithm in an advanced way and it is more secured and robust since we used advanced hill cipher technique, as we know hill cipher is a polygraphed substitution based on linear algebra where letter is represented by number mod 26. For encryption of message, each block of n letter is multiplied by an invertible n*n key matrix and then mod 26 is applied. To decrypt the message, each block is multiplied by the inverse of the key matrix. Another technique we used in our algorithm is AES method. AES is advance encryption standard for the encryption of electronic data. It is based on substitution and permutation method where it combines both substitution and permutation and the message is divided into fixed block of 128 bit and key size is of 128,192 or 256 bit. In our method, both data and image can be encrypted using bit manipulation in a more robust way.

2. Related work

The different encryption modules which made up the Image Encryption System cryptographic methods are as follows:

Modified Bits Rotation and Reversal Technique: In this technique, a password is supplied along with an input image. Equivalent eight bit binary number is obtained by converting the value of each pixel of input image. Then the ASCII Value of each byte of the password is added and a number is generated from the password which is used for the Bits Rotation and Reversal technique. Finally, this generated number is modular operated by 7 to generate the effective number (NR), according to which the bits will be rotated and reversed. Since, the value of each pixel denotes its color; change that takes place in the value of each pixel of input image due to modified Bits Rotation & Reversal produces the encrypted image.

Extended Hill Cipher Technique: An involutory matrix is generated using the algorithm presented in [3]. The algorithm is a involutory matrix of dimensions m x m built using the password supplied as input. Index value of each row of input image is converted into x-bit binary number, where x is number of bits present in binary equivalent of index value of last row of input image. The resultant x-bit binary number is rearranged in reverse order. This reversed-x-bit binary number is converted into its equivalent decimal number. Therefore value of index value of each row changes and hence position of all rows of input image changes. i.e., Positions of all the rows of input image are rearranged in Bits-Reversed-Order. Similarly, positions of all columns of input image are also rearranged in Bits-Reversed-Order. Final encrypted image is obtained by applying Hill Cipher technique on the Positional Manipulated image generated from Step 2.

3. General Approach of Triple Layered Encryption

The Triple Layered Encryption is a process to encrypt the data multiple times using the same algorithm or different algorithms. This technique is widely used due to its feature of enhanced security for data communication over the vulnerable wireless network as the Internet. The concept of multiple encryptions can be described as a technique to provide multilayer and multi-level security over unreliable wireless network. This technique can be understood through a real life example, where we are keeping our precious item within a box and this box is kept in another box and finally we kept in a locker and lock it with a key. Here, we are protecting our precious item through multilayer and multilevel security. If anyone wants to achieve this precious item he/she has to cross all boundaries. First, he has to unlock the locker with the key, and then he has to open the box to get the inner one. In the same manner, lots of time and efforts are required to achieve the original message if it is encrypted by multiple encryptions.

3.1. Working Criteria of Multiple Encryption

In modern cryptography, by encrypting the data and information thrice, with different algorithms, we would anticipate the resultant encryption to be stronger in all but some special conditions with better level of security.

The encryption operation of triple layered encryption can be described as:

Cipher text = {(Encrypt_with AES (Encrypt_with HILL Cipher (Bit Manipulation)))}

Plain text = {(Decrypt_with AES (Decrypt_with HILL Cipher (Bit Manipulation)))}

3.2. Proposed algorithm

Algorithm-1: User interface for sending and receiving SMS

Encryption	Decryption
1) Write SMS	1) Get SMS.
2) Provide the SMS recipient number	2) Authenticating using 16 bit secret key.
3) Give the 16 bit secret number	3) If(key=true)
4) Encrypt the message AES	4) Decrypt the message
5) Send the SMS	

3.3. Algorithm-2: internal structure of triple layered security on android based SMS transaction.

Encryption	Decryption
1. Take plain text/image as SMS.	1. Receive the cipher text.
2. Calculate the length of SMS ->L	2. Enter the 16 digit key
3. If L>Max. length of SMS	3. If(key=true)
4. Divide SMS	4. Decrypt the message with AES
5. Take each part of the message and convert into binary digits.	5. Decrypt the message using hill cipher
6. Apply bit manipulation i.e. bit rotation and shifting technique.	6. Convert the alphabet into hexadecimal using substitution table.
7. Convert the digits into hexadecimal.	7.Convert it into binary digits
8. Convert the hexadecimal using substitution table.	8.Apply bit manipulation i.e. bit rotation and shifting technique
9. Apply hill cipher.	9.Finally receive the plain text
10. Finally apply AES.	10.Else
11. Enter16 bit secret key.	11.Re-enter the key.
11. Send the cipher text	

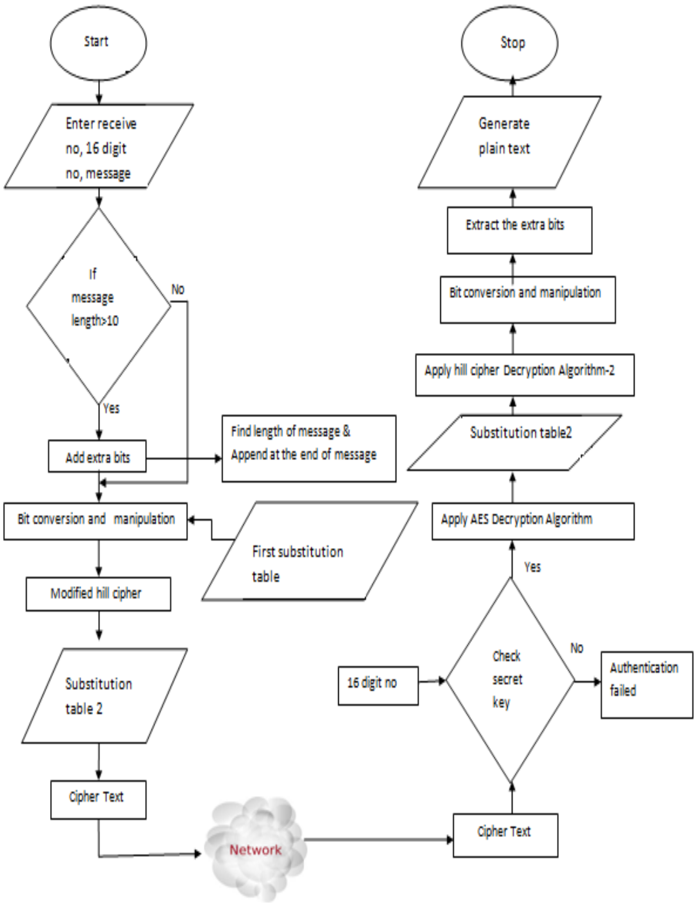
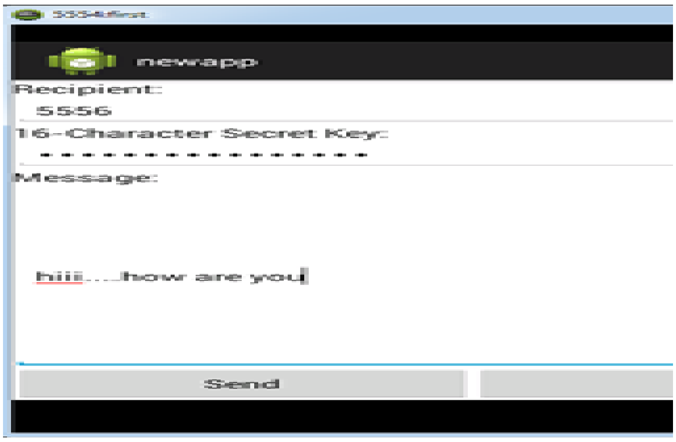
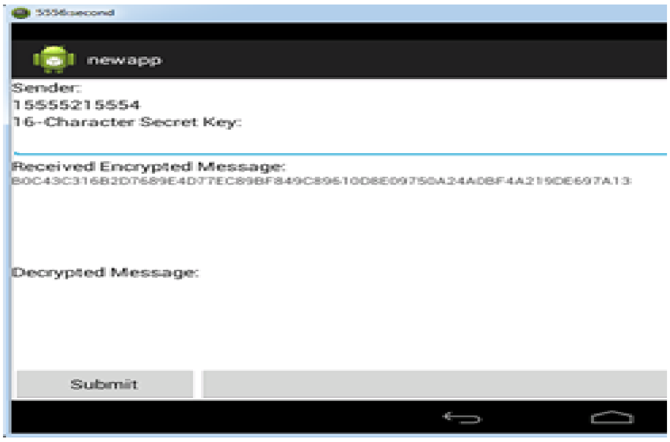


Fig : Process Flowchart

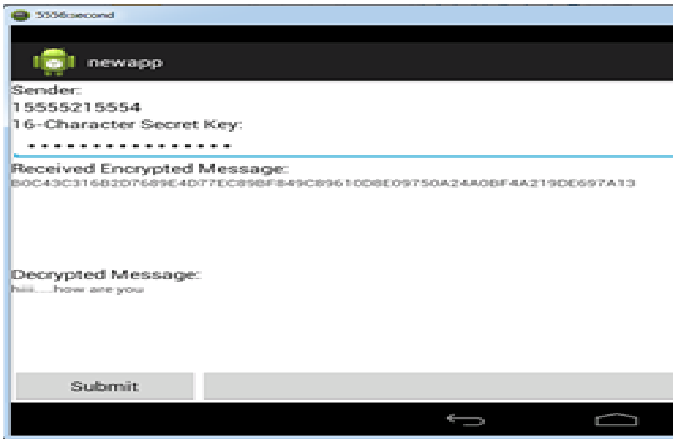
The flowchart shows when a sender wants to send the SMS using triple layered security application, he/she needs to provide a 16 bit symmetric code and receiver's number; the SMS is then sent in encrypted format. Also the SMS is stored in encrypted form at both the sender and receiver ends. When the receiver first receives the SMS, he/she needs to authenticate himself/herself using 16 bit secret code, then only he/she can decrypt the SMS.


5554:first
newapp
Recipient:
5556
16-Character Secret Key:
················
Message:
hiii....how are you

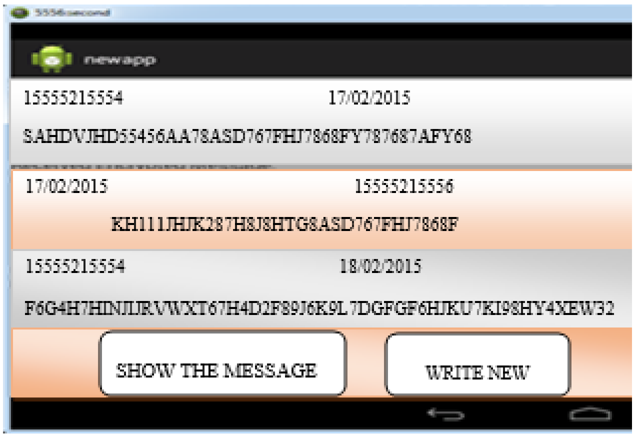
(a)


5556:second
newapp
Sender:
15555215554
16-Character Secret Key:
Received Encrypted Message:
B0C43C316B2D7689E4D77EC89BF849C89610D8E09750A24A0BF4A219DE697A13
Decrypted Message:

(b)


5556:second
newapp
Sender:
15555215554
16-Character Secret Key:
················
Received Encrypted Message:
B0C43C316B2D7689E4D77EC89BF849C89610D8E09750A24A0BF4A219DE697A13
Decrypted Message:
hiii....how are you

(c)


5556:second
newapp
15555215554 17/02/2015
SAHDVJHD55456AA78ASD767FHJ7868FY787687AFY68
17/02/2015 15555215556
KH111JHJK287H8J8HTG8ASD767FHJ7868F
15555215554 18/02/2015
F6G4H7HINJLRVWXT67H4D2F89J6K9L7DGFGF6HJKU7KI98HY4XEW32

(d)

Fig: screenshots of Triple layered Security; (a) sending the encrypted SMS ; (b)) Receiving the encrypted SMS (c) Decryption of the SMS using by authenticating 16 bit key; (d) Display of messages in encrypted form.

The screen shots shown above are taken from the application. The length of the SMS should be less than 32 bits. As the encrypted SMS generated is of 140 bit, so message greater than 140 bit cannot be send at once.

4. Conclusions and Future Research Directions:

In this paper, we are proposing unique idea which is suitable for the IT environment from the customer point of view. Due to flexibility, application provides quality of service "Anytime", "Anywhere", "And Anyplace". This application is made to improve data security by encrypting the text, by merging encryption methods such as bit manipulation, Hill Cipher and AES Cipher has further strengthened data security.

5. REFERENCES

[1] 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.

[2] R.K. Balan, N. Ramasubbum, K. Prakobphol, N. Christin, and J. Hong, "mFerio: The Design and Evaluation of a Peer-to-Peer Mobile PaymentSystem", MobiSys '09, 2009.

[3] ashpal Mote, Paritosh Nehete, Shekhar Gaikwad, "Superior Security Data Encryption Algorithm (NTRU)", International Journal of Engineering Sciences ISSN: 2229-6913 Issue July 2012, Vol. 6.

[4] Prof. Avinash Wadhe, Miss Namrata A.Sable,"Mobile SMS Banking Security Using Elliptic Curve Cryptosystem In Binary Field",International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 3, May-Jun 2013.

[5] Tarek M. Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed," Hybrid Compression Encryption Technique for Secur-ing SMS", IJCSS), Volume (3): Issue (6).

[6] Vishal Pachori, Gunjan Ansari, Neha Chaudhary- "Improved Performance of Advance Encryption Standard using Parallel Computing" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.967-971

[7] Tehrani M.A., Amidian AS., Muhammadi 1., and Rabiee H.R., "A survey of system platforms for mobile payment", The 4th international conference on data management on E-commerce and E-Government (ICMECG),2010.

[8] Gandharba Swain1 and Saroj Kumar Lenka2, "LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits", Springer-Verlag Berlin Heidelberg , Part II, CCIS 270, pp, 479–488, 2012.

[9] Tzung-Her Chen and Chang-Sian Wu, "Efficient multi-secret image sharing based on Boolean operations". Signal Processing 91(2011) 90-97.

[10] Li B., He, J. Huang, J.She, Y.Q,"A Survey on Image Steganography and Steganalysis" Journal of Information hiding and Multimedia Signal Processing 2(2), pp,142–172 2011.

[11] Bibhudendra Acharya et al. "Image Encryption Using Advanced Hill Cipher Algorithm". International Journal of Recent Trends in Engineering, Vol.1, No.1, May 2009, pp.663-667.

[12] Bibhudendra Acharya et al. "Involutory, Permuted and Reiterative key Matrix generation Methods for Hill Cipher System". International Journal of Recent Trends in Engineering, Vol.1, No.4, May 2009, pp.106-108.

[13] Amanpreet Kaur, Renu Dhir, and Geeta Sikka , "A New Image Steganography Based On First Component Alteration Technique", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3,pp,53-56 ,2009.

[14] Debnath, D. ; Deb, S. ; Kar, N., "An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher &amp; RGB Image Steganography" ,Computational Intelligence and Networks (CINE), 2015

[15] Panduranga, H.T. ; Sharath Kumar, H.S. ; Naveen Kumar, S.K., "Hybrid approach for dual image encryption using nibble exchange and Hill-cipher ", Machine Vision and Image Processing (MVIP), 2012 .

[16] Gupta, S. ; Sengupta, S. ; Bhattacharyya, M. ; Chattrejee, S. ; Sharma, B.S., "Cellular phone based web authentication system using 3-D encryption technique under stochastic framework" ,Internet, 2009. AH-ICI