International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:6, 2016

Maintaining User-Level Security in Short Message Service

T. Arudchelvam, W. W. E. N. Fernando

***Abstract*—**Mobile phone has become as an essential thing in our life. Therefore, security is the most important thing to be considered in mobile communication. Short message service is the cheapest way of communication via the mobile phones. Therefore, security is very important in the short message service as well. This paper presents a method to maintain the security at user level. Different types of encryption methods are used to implement the user level security in mobile phones. Caesar cipher, Rail Fence, Vigenere cipher and RSA are used as encryption methods in this work. Caesar cipher and the Rail Fence methods are enhanced and implemented. The beauty in this work is that the user can select the encryption method and the key. Therefore, by changing the encryption method and the key time to time, the user can ensure the security of messages. By this work, while users can safely send/receive messages, they can save their information from unauthorised and unwanted people in their own mobile phone as well.

***Keywords*—**SMS, user level security, encryption, mobile communication.

I. Introduction

MOBILE phones are being considered as an important thing in human life. Mobile phones are used for not only voice communication but also for other purposes such as saving data (texts, photos, etc.), reminders, alarms and running some apps, etc. Short message service (SMS) is the cheapest way of exchanging ideas considering communication modes. Because of that, most of the customers are using SMS for exchanging ideas. Security is an essential factor for not only in phone communication but also in all sorts of communication system. Further, security is essential for all the data stored in the mobile phones and data which are being transmitted to and from mobile phones. Cryptography is a common method used to maintain security. Further, user level security options are not yet implemented or reported. When user level security methods are implemented, anybody can maintain their data safely and securely. When the options are given to users for choosing method for encryption and decryption, they can be sure about their own security.

II. Cryptography

Cryptography is a commonly used method for securing information during the transmission. Cryptography is used to protect data being transferred between devices such as mobile telephones, automatic teller machines (ATM), etc. Several methods are used in cryptography. We can divide the cryptographic methods into two major categories called symmetric and asymmetric cryptography. Cryptography was used by kings and security forces during wars those days to securely exchange messages. Later that idea has been enhanced for better security. Still researches are being carried out for enhancing the methods for encryption/decryption.

T. Arudchelvam and W. W. E. N. Fernando are with the Department of Computing and Information Systems, Wayamba University of Sri Lanka, Kuliyapitiya, Sri Lanka (e-mail: tarudchelvam@gmail.com, arul@wyb.ac.lk).

III. Encryption and Decryption

In this work, following encryption/decryption methods are used:

A. Caesar Cipher

This is a simple encryption method which replaces the letter of alphabet with a letter that is three places ahead of it [1], [2]. Now this method can be modified in different ways. For example, instead of 3rd letter ahead, nth letter ahead can be chosen, where n can be any number which should be preferably less than 26 because there are 26 letters. Further, in this method, digits and symbols such as ",", ".", ":", etc. are not considered. But, digits and symbols can also be considered and they can be arranged in an order and replaced by nth symbol. This idea is implemented in this work as well. Caeser cipher is enhanced and presented by Mishra [3].

B. Rail Fence Cipher

This method is also very easy and simple for implementing. In this method the plain text is written downwards on successive "rails" of an imaginary fence, starting a new column when the bottom is reached. The message is then read off in rows. During the decryption the number of rails that was used to encrypt, must be known by the person who is going to decrypt. Break up the letters into equal groups for each rail. Finally, stack the groups on top of each other and read off the message vertically [4]. But, this method can easily be cracked. Anyway, when number of rails is changed regularly, it is a bit difficult to crack the message by unauthorised people. This is implemented in this work.

C. Vigenere Cipher

The Vigenere cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. In this cipher, Vigenere table or Vigenere square is used. It consists of alphabets written out 26 times in different rows, each alphabet shifted cyclically to the previous alphabet, corresponding to the 26 possible Caesar ciphers. This method is enhanced and presented in [4], [5]. Changing the keyword regularly may be useful because all the time hackers cannot guess the keyword. Further, the table used in this method also only has the English alphabets. But, by

adding symbols and numbers to this table, the level of the security will be enhanced. Even if those symbols and numbers are added randomly in between alphabets, the level of the security will be further enhanced.

D. RSA

RSA [2], [4] is considered as the most secured method for encryption/decryption. This has some mathematical calculations for which a bit of high computational power is needed. This computational power cannot be increased in mobile phones as we like.

The steps to be followed for key generation in the RSA are given below:

a. Choose two distinct prime numbers p and q
b. Compute $n = p*q$
c. Compute $\varphi(n) = \varphi(p)*\varphi(q) = (p-1)(q-1)$, where φ is Euler's function.
d. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co-prime.
e. Determine d as $d \equiv e-1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e(modulo $\varphi(n)$)

Because of the limited power available in mobile phones, following ranges of p, n, and e are chosen during the implementation:

1. $p > 250$,
2. $n < 100{,}000$,
3. $e < 10{,}000$.

IV. Cryptography and SMS

References [6], [7] discuss the need and ways to secure data when they are being transmitted through a network. Reference [8] discusses the details of implementing cryptography for computer privacy. Reference [9] discusses the theoretical aspects of cryptography. Our concern in this work is to secure data in mobile phones and during the transmission of messages between mobile phones. Users sometimes are sensitive in securing their data in mobile phones. They may want to hide the exact message which might be saved in mobile phones. Sent messages and received messages are saved in phones. These messages sometimes might be taken/seen/misused by unauthorised people intentionally or even sometimes unintentionally. But anyhow, after knowing the message, it may be useful to others or sometimes may be misused by those people. In order to save messages from unauthorised people, in this application, users are able to choose or use cryptography. In this work, users have the given options to choose one cryptographic method from a list of available methods.

Caesar Cipher, Rail Fence Cipher, Vigenere and RSA are implemented in this work. Further, a user can encrypt any message using any cipher method available in this application. If the message is encrypted before sending the message, the cipher method and the key should be notified to the receiver secretly. In addition to that cipher method and the key can regularly be changed. Therefore, the chance for hacking can be reduced. If a message is encrypted after receiving that, the owner of the phone should remember the cipher method and the key in case if they want to save that message for future use.

V. Implementation

The user interface for the above application is given in Fig. 1. There are two buttons for encryption and decryption. When the encryption button is clicked, the message in the message box will be encrypted using the key in the "Secret Key" area of Fig. 1. When the "Decrypt" button is clicked, immediately the received the messages in the message box will be displayed. Then, a message to be decrypted has to be chosen. Then, that chosen message will be decrypted using the key given in the "Secret key" area of Fig. 1. It should be noted that the key used for encrypting a message has to be given for decrypting that as well. Different messages can be encrypted using different keys. It is better and secured to change keys regularly for any methods. If the same key is always used and if somebody could guess or find the key, then all messages can be hacked. The secret key has to be given in a particular format. The format of the secret key for Caesar and Rail Fence is given in Fig. 2. The formats of the secret key for RSA and Vigenere cipher are given in Figs. 3 and 4, respectively. In all the formats, 1st box contains the method number. Caesar, Rail Fence, Vigenere and RSA are indicated by 1, 2, 3, and 4, respectively. If the "Clear" button is clicked, the message area will be cleared.

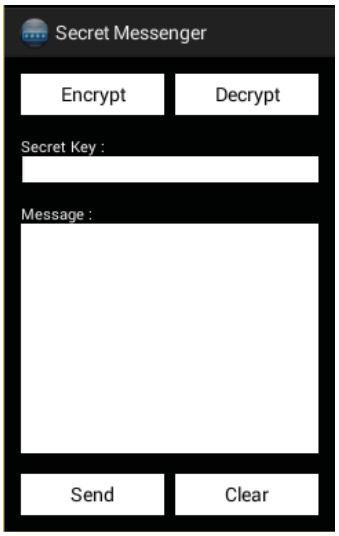

Fig. 1 Interface of the application

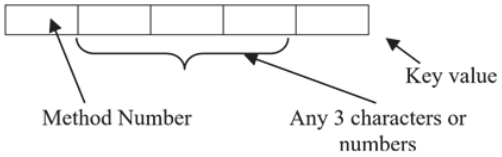

Fig. 2 Format of Secret key for Caesar and Rail Fence

Cesar cipher and Rail Fence cipher methods are having only one key value. In Caesar cipher, the key value indicates the

number of characters to be shifted, and in Rail Fence cipher it is the number of rails. Further, 3 digits or characters are added after the method number in all formats. This is just for confusing the hackers and not for anything else.

The fifth box of the format of secret key of Vigenere cipher (Fig. 3) contains the number of keys to be used in this method. Number of keys can also be changed at every attempt. This will increase security and confuse the hackers. Depending on the number of keys in Vigenere cipher, the number of boxes after fifth box will vary. That is the number of keys and the number of boxes after fifth box should be the same.

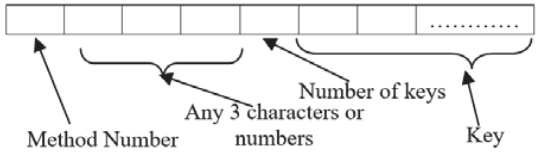

Fig. 3 Format of Secret key for Vigenere cipher

In the format of the RSA (Fig. 4), last four boxes are filled by just random numbers or characters.

As the number of boxes is to be the same for all the cipher methods, one character or a digit is included in the last box of the RSA cipher.

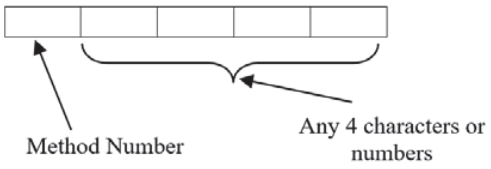

Fig. 4 Format of Secret key for RSA

In this application, keys for Caesar, Rail Fence and Vigenere cipher are to be shared by both the sender and the receiver. But for the RSA it is not needed. But the method number needs to be shared.

Steps to be followed by the sender are given below:

1. Enter the message to be sent in the Message text field.
2. Enter the secret key in the prescribed format in the "Secret Key" field.
3. Click on the "Encrypt" button. Now you get the encrypted message in the message field.
4. Click on the "Send" button.
5. Now user is expected to enter the phone number.
6. After giving the phone number, press the send button for sending the message.

Steps to be followed by the receiver are given below:

1. Enter the secret key in the "Secret Key" field.
2. Click on "Decrypt" button.
3. Now the message is displayed in the message field. The user can read the message. When the application is exited, decrypted message will be vanished. Further, text in the message field can be cleared using the "clear" button.

In this application any time or every time user can change the secret key. This will increase the security. But only thing is that, every time the password is to be shared with the receiver. Further, some people are keeping credit/ATM/debit cards' passwords, email password, etc. in the mobile phone and if the phone is lost, it may be a big threat to the owner of the phone. But using this application user can safely keep the valuable information in the phone. In this case the user will be the sender and the receiver. This application has been successfully tested with Android 2.3 (Gingerbread), Android 4.2.2 (Jelly Bean) and Android 4.4.4 (KitKat).

VI. Results and Discussion

Caesar Cipher, Rail fence Cipher and Vigenere Cipher are successfully implemented and properly tested. Every message can be encrypted and decrypted.

TABLE I
VALUES OF VARIABLES FOR SUCCESSFUL ENCRYPTION AND DECRYPTION

p	q	N	phin	e	D
251	383	96133	95500	9999	2999
251	359	90109	89500	9999	17499
251	317	79567	79000	9999	8999
251	269	67519	67000	9999	8999
251	257	64507	64000	9999	21999
257	379	97403	96768	9997	9157
257	359	92263	91648	9999	22511
257	349	89693	89088	9997	15301
257	347	89179	88576	9999	17903
257	317	81469	80896	9999	23535
257	281	72217	71680	9999	4079
257	269	69133	68608	9999	2031
257	263	67591	67072	9999	13295
263	347	91261	90652	9999	24823
263	337	88631	88032	9997	5125
263	307	80741	80172	9997	409
263	281	73903	73360	9999	719
269	313	84197	83616	9995	20195
269	281	75589	75040	9999	6319
271	359	97289	96660	9997	7213
271	337	91327	90720	9997	21253
271	311	84281	83700	9997	8833
271	281	76151	75600	9997	6133
277	349	96673	96048	9997	22261
277	317	87809	87216	9997	18949
277	317	85039	84456	9997	20605
277	281	77837	77280	9997	14533
281	311	87391	86800	9999	10799
281	283	79523	78960	9997	14533
283	349	98767	98136	9997	20173
283	311	88013	87420	9997	3253
283	307	86881	86292	9997	15097
283	293	82919	82344	9997	22429
293	313	91709	91104	9995	13955
307	317	97319	96696	9997	13261
307	311	95477	94860	9997	19993
311	317	98587	97960	9999	5839

But for RSA, there are limitations in this application. Computing power is a big factor in mobile phones. In RSA, though the messages are encrypted, it is not sure that whether it is correct or not. If encrypted message is decrypted

successfully, then the encryption should also be correct. But if the decrypted message of an encrypted message is wrong, there are two possibilities. One is that the decryption may be wrong or else sometimes the encryption may also be wrong. Therefore, it is not a good idea to say that all the messages are encrypted successfully. But, instead of that it can be told that the encryption and decryption are done successfully. Several ranges of data are tested for encryption and decryption using RSA. Values of the variables for successful encryption and decryption using RSA are shown in Table I. p, q, n, phin, e, and d are same as the variables in the steps to be followed for key generation in the RSA given in the previous section. Further, there is a big set of unsuccessful data. Further, since some additional characters/numbers are to be given as the key, it gives more security. Hackers may be confusing on additional data to be given.

The limitation of this application is that the sender and the receiver have to remember the key values.

VII. Conclusion

In this work, an Android application is developed for implementing cryptography. The users are able to choose desired encryption method in this application. Caesar cipher, Rail Fence, Vigenere cipher, and RSA are implemented in this application. The sender and the receiver should exchange the secret key secretly. As it is the user level security, this is essential. Caesar cipher, Rail Fence and Vigenere cipher are successfully implemented. But for RSA, the ranges of variables are reported for successful encryption and decryption. This application is useful for exchanging messages and storing secret data and messages by the user. Though the phone or the mobile device is lost, those data which are stored using this methods, cannot be handled by unauthorized people.

Acknowledgment

Authors thank the Wayamba University of Sri Lanka for the support given for this work.

References

[1] William Stalling, "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
[2] Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks, 5th ed*, Prentice Hall, New York, 2011.
[3] Anupama Mishra, "Enhancing Security of Caesar Cipher Using Different Methods", International Journal of Research in Engineering and Technology, Vol. 02, Issue. 09, pp: 327-332. Sep 2013.
[4] Simon Singh, *The Code Book,* DELACORTE PRESS, New York, 2001.
[5] Md. Khalid Imam Rahmani1, Neeta Wadhwa1 and Vaibhav Malhotra "Alpha-Qwerty Cipher: An Extended Vigenère Cipher", Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012.
[6] William Stalling, Network Security Essentials (Applications and Standards), Pearson Education, 2004.
[7] Stallings. W, Cryptography and Network Security, 2nd edition, Prentice Hall, 1999.
[8] H. Feistel, "Cryptography and computer privacy," *Scientific American*, vol. 228, pp. 15-23, 1973.
[9] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL. 1997.