Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Secure message encryption using Nth prime

Kumar shanu
Department of CSE, SEST
JamiaHamdard, New Delhi, India

Itiram Raza Khan
Department of CSE, SEST
JamiaHamdard, New Delhi, India

Abstract:This paper is intended to give a general outline about the use of cryptography in wireless communication, specific in mobile phones. The most recent couple of years have seen a true revolution in the mobile communication world. The functional principles of Public key and secret key cryptography, and in addition the general overview of Hashing, Random session key and Digital signature are described. Security assurance of messages is not yet that advanced and hard to implement in practice. Solutions, for example, encoded SMS ought to be considered if there is a need to send sensitive data through SMS.

Keywords:Random session key, Modulo, Nth prime number, Public key cryptography, Private Key cryptography, Hashing, Digital signature, SMS (Short Message Service) and secure cryptosystem.

I. INTRODUCTION

This application developed for end to end secure communication of the messages. The cryptosystem utilized is RSA cryptosystem and AES (Advanced Encryption Standard) cryptosystem. This paper additionally clarifies working of SMS, Hashing, Digital mark, RSA and AES cryptosystem and the working of our created application.

A. Requirement for secure information transmission

- Information security, sometimes abbreviated to Info-Sec, is the act of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.
- Encryption is the best approach to accomplish information security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. [6]
- Keeping up security in our personal communication is something everybody wants. As short message service (SMS) is currently broadly utilized as a business tool; its security has turned into a noteworthy worry for business organization and customers. [6]

II. LITERATURE REVIEW

A. Problem Statement

The SMS business being on such a great rise is vulnerable to attacks. Accordingly it has now turned out to be more basic to encode SMS before sending. Encrypted messaging isn't generally vital, but it can still be a welcome safeguard for whenever you, your family, or business partners need to communicate sensitive information from one side of the globe to the next.

Smart phones [3] have become an essential part in the life of the individuals and their priorities at the present time. The most prominent uses are in chatting and conversation applications. Most of these applications do not provide the required protection and privacy of the data exchanged between users. Yet there are very few mobile chat applications that provides an End-to-End (E2E) security and privacy-preserving service to their clients.

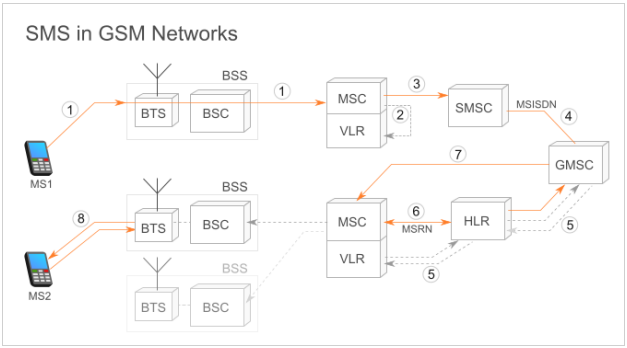

Figure 1

- With the plenty of cell phones out there, it's no big surprise BYOD [1] (bring your own device) has turned out to be so well known. Numerous organizations are under a lot of pressure to allow personal mobile device use on the enterprise wireless network. Look into firm J. Gold Associates reports that around 25%-35% of enterprise as of now have a BYOD [1] policy, and they anticipate that that will develop to more than half over the next two years.
- Many have already embraces BYOD [1], yet some are still fearful that this might cause significant challenges for IT departments. While the market hints at no abating, IT associations distinguish security as one of their most noteworthy worries about developing versatility. In this way, different encryption systems are utilized.
- In 2010, 6.1 trillion instant messages were sent. This translates into 192,192 SMS for each second. SMS has turned into a gigantic business industry, worth over $81 billion globally as of 2006. The worldwide normal cost for a SMS message is $0.11, while mobile networks charge each other interconnect fees of at least $0.04 when connecting between different phone networks.
- BYOD [1] is a relatively new initiative adopted by modern businesses which allows employees to use personal mobile devices to complete work in a convenient and flexible manner. Recent industry reports claim approximately 70% of businesses already utilize

BYOD [1] and agree they experience improvements including enhanced productivity, efficiency, morale and reduced hardware expenses. Of these, 50% of employees actively use pre-installed security measures on their device (eg. pass codes), yet less than 20% utilize extra methods (eg. anti-malware). In contrast, the rate of threats and attacks aimed towards mobile devices are increasing; especially software based attacks.

SMS (Short Message Service):
SMS means short message service. Basically, it is a method of communication that sends text between cell phones, or from a PC or handheld to a cell phone.

How it functions:

1. Messages in Short Message Service (SMS) must be no longer than 160 alphanumeric characters and contain no pictures or representation.
2. Once a message is sent, it is received by a Short Message Service Centre (SMSC), which must then get it to the appropriate mobile device.
3. To do this, the SMSC sends a SMS Request to the home location register (HLR) to discover the roaming client.
4. Once the HLR gets the request, it will react to the SMSC with the subscriber's status:1) inactive or active 2) where subscriber is roaming.
5. If the response is "inactive", then the SMSC will hold onto the message for a period of time. When the subscriber accesses his device, the HLR sends a SMS Notification to the SMSC, and the SMSC will attempt delivery.
6. The SMSC moves the message in a Short Message Delivery Point to Point format to the serving system. The system pages the device, and if it responds, the message gets delivered.
7. The SMSC gets verification that the message was received by the end client, then arranges the message as "sent" and will not attempt to send again.
8. By 2020, it is anticipated that 24 Billion devices will be connected with the Internet.

III. PROPOSED SOLUTION

Proposed scheme: We have programmed our application carefully considering different factors which might profit the client. The primary advantage is that it is very basic application, straightforward and simple to operate. UI is so straightforward and light weight that fundamental usefulness of encryption and decryption of SMS is carried out very efficiently.[7]For providing high message security we are using combination of following cryptographic algorithms [2][5].

- RSA (Ron Rivest, Adi Shamir, and Leonard Adleman)
- AES (Advanced Encryption Standard)
- SHA (Secure Hash Algorithm)
- DSA (Digital Signature Algorithm)

Short Message Service (SMS) is the text communication service component of mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between mobile phone devices. SMS framework allows two peers to exchange encrypted and digitally signed SMS messages. The communication between peers is secured by using public key cryptography. The identity validation of the contacts involved in the communication is implemented through DSA signature scheme. [4] [7]
Several Cryptography methods have been used to reduce the SMS security threats and provide enough security to mobile devices. But these encryption techniques can it perform their activity in a complete manner since it affects the performance of mobile devices in terms of power and battery life constraints [7].

Encryption steps:

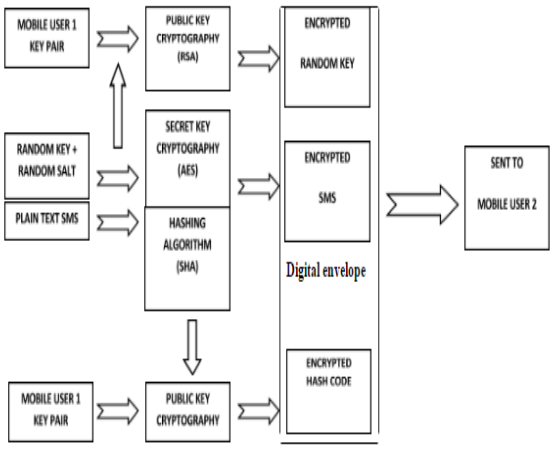

Figure 2

Decryption steps:

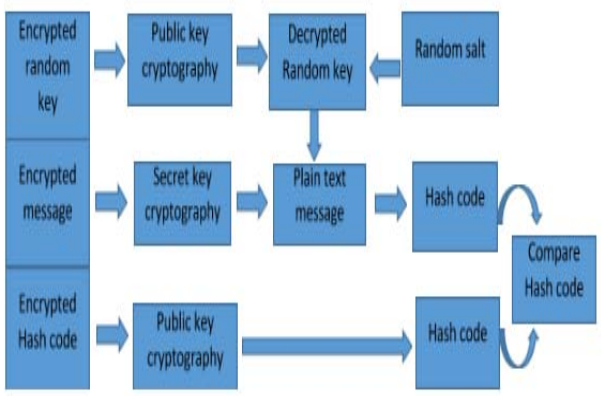

Figure 3

IV. IMPLEMENTATION

1. Generate N^{th} prime number using mobile numbers of Mobile User 1 and Mobile User 2 separately. **For example:** Assume Mobile User 1 having mobile number 8802647299 and Mobile User 2 having mobile number 7838039321. Then generate 8802647299th and 7838039321st prime number i.e. 220,741,275,211 and 195,602,710,439 respectively.
2. Select the large number among Mobile number 1 and Mobile number 2 and then find the difference between them i.e. Mobile number 1 – Mobile number 2 or Mobile number 2 – Mobile number 1 (if Mobile number 2> Mobile number 1).
   For example: In our case Mobile number 1 > Mobile number 2. Therefore calculate difference between mobile

number i.e. 8802647299 – 7838039321 = 964607978

3. Calculate Random key using difference between the mobile number and modulus function.
   For example: Random key : Mobile number mod Difference between them
   Sender : 8802647299 mod 964607978 = 121175497
   Receiver : 7838039321 mod 964607978 = 121175497

Encryption Process:

4. Generate Mobile User 1 key pair as {S_Public_Key; S_Private_Key} and Mobile User 2 key pair as {R_Public_Key; R_Private_Key}.
5. Calculate Hash value of the plain text SMS using SHA Hashing algorithm.
6. Now using Public key cryptography i.e., RSA algorithm encrypt Hash value obtained from plain text SMS using Mobile User 1 Private key pair as {S_Public_Key; S_Private_Key }.
7. On the other end, using Private key cryptography encrypt plain text SMS directly into encrypted cipher text by AES(Advanced Encryption Standard) using Random key + Random generated salt i.e. 121175497 + Random salt to generate Encrypted message.
8. Also encrypt the Random session key by Public key cryptography using Mobile User 1 Public key pair as {S_Public_Key; S_Private_Key} to generate Encrypted random key.
9. Finally transmit Encrypted random key, Encrypted message and Encrypted hash value of plain text SMS to the Mobile User 2.

Decryption Process:

10. Mobile user 2 receives Encrypted random key, d message and Encrypted hash value of plain text SMS.
11. Then using { R_Public-Key;R_Private_Key } decrypt Encrypted hash value of plain text SMS to get Hash value.
12. On the other end, decrypt Encrypted Random Key using { R_Public-Key;R_Private_Key } to get Random Key.
13. Finally decrypt Encrypted message using Random key + Random salt to get plain text SMS.
14. Calculate Hash value of the obtained plain text SMS and compare with decrypted Hash value obtained from step 1

V. RESULT

Securityservices:

Authentication: guarantees the recipient of a message the authenticity of the claimed source.
Non repudiation: ensures against sender/receiver denying sending/receiving a message.
Confidentiality: protects against unauthorized release of message content.
Data Integrity: guarantees that a message is received as sent.

Developed Application screenshots:

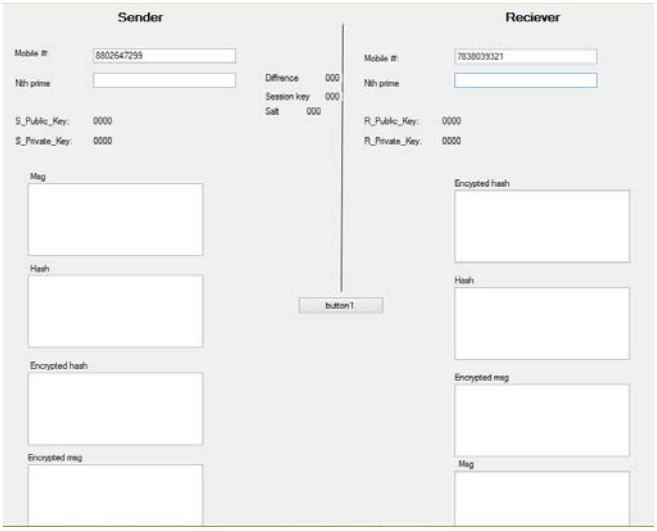

Figure 4

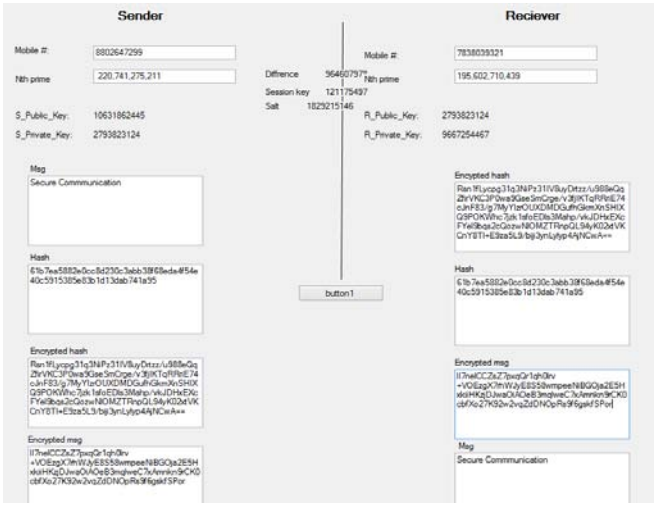

Figure 5

VI. CONCLUSION AND FUTURE WORK:

In this paper, we proposed new secure communication technique utilizing Mobile phone numbers of sender and recipient. After the examinations of the proposed algorithm, obviously this encryption technique fulfils the objectives that are required in any encryption technique to encode plain content of messages.
The algorithm is being implemented on C# programming language and it works out perfectly. In the future, we plan to design an app based on this technique which will target to use in secure mobile communication applications.

VII. REFERENCES

[1] Kathleen Downer, Maumita Bhattacharya, "BYOD Security: A New Business Challenge",vol. 00, no. , pp. 1128-1133, 2015, doi:10.1109/SmartCity.2015.221.

[2] PoonamMandavkar, GauriPatil, Chetana Shetty, Vishal Parkar, "SMS Security for Android Mobile Using Combine Cryptographic Algorithms", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 4, April 2014ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940

[3]"A Secure End-to-End Mobile Chat Scheme", 2014 Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), vol. 00, no. , pp. 472-477, 2014.

[4] NeeteshSaxena, Narendra S. Chaudhari, "A Secure Digital Signature Approach for SMS Security", IP Multimedia Communications A Special Issue from IJCA - www.ijcaonline.org

[5]Hellman, M. and J. Diffie, 1976. New Directions in Cryptography. IEEE transactions on Information theory, vol. IT-22, pp:644-654, November 1976

[6] Rohan Rayarikar, SanketUpadhyay, PriyankaPimpale, "SMS Encryption using AES Algorithm on Android", International Journal of Computer Applications (0975 – 8887) Volume 50– No.19, July 2012

[7]Muhammad Waseem Khan, "SMS Security in Mobile Devices: A Survey" Int. J. Advanced Networking and Applications Volume: 05, Issue: 02, Pages:1873-1882 (2013) ISSN : 0975-0290