International Journal of Multidisciplinary Research and Development
Online ISSN: 2349-4182, Print ISSN: 2349-5979, Impact Factor: RJIF 5.72
www.allsubjectjournal.com
Volume 3; Issue 5; May 2016; Page No. 67-69

Implementation of secured SMS for end to end communication using RSA algorithm

Sindhu UL

Assistant Professor, Department of Computer Science Engineering. Sri Krishna College of Technology, Kovaipudhur, Coimbatore-641042, Tamilnadu, India.

Abstract
Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation. Short Message Service (SMS) is established as a widely used and wide spread approach for text messaging in present day's immensely mobile reliant world. The current SMS hasn't achieved secure transmission of plaintext between different mobile phone devices. SMS doesn't have its own build-in mechanism to secure the transmitted data because security is not considered as a priority application for mobile devices. When this is the situation the imperative factor is "Security". One commonly used technique to provide security is Encryption. It plays a vital role when confidential data is proceeding in the network by serving as a fortification for the original raw data avoiding intrusion. Many SMS security schemes have been proposed by the researchers. There are many conventional and symmetric encryption algorithms available to bestow this, each having its own level of security and performance. Considering all aspects our proposed system a means of providing high authentication Rivest shamir Adleman (RSA) algorithm for security to the messages shared which can be efficiently used in small devices like mobile phones.

Keywords: Client-server, SMS, Mobile Communication, Security, Authentication

1. Introduction
Network security has become more important to personal com puter users,organizations, and the military. With the advent of the internet, security became amajor concern and the history of security allows a better understanding of the emergence of security technology.The architecture of the inter net, whenmodified can reduce the possibleattacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Nevertheless its versatility, SMS has some limitations that would be important for some unconventional applications. For some applications, like transactions, payments and monitoring, it would be helpful to incorporate some services that can provide confidentiality, integrity, authentication and non-repudiation services which are standard for network security.

Global System for Mobile Communications (GSM) is the most popular standard for mobile telephony systems in the world. In 1982, the European Conference of Postal and Telecommunications Administrations (CEPT) created the Group Special Mobile (GSM) to develop a standard for a mobile telephone system that could be used across Europe. The GSM Association estimates that 80% of the global mobile market uses the standard. GSM is used across more than 212 countries and territories. GSM pioneered low-cost implementation of the Short Message Service (SMS), also called text messaging, which has since been supported on other mobile phone standards as well.

In the GSM, only the airway traffic between the Mobile Station (MS) and the Base Transceiver Station (BTS) is optionally encrypted with a weak and broken stream cipher (A5/1 or A5/2). The authentication is unilateral and also vulnerable. The development of UMTS introduces an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user, whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no nonrepudiation.

2. Related Work
The necessity of providing security to SMS has been imperative since a long time and many algorithms and techniques have been implemented in various platforms to try and provide security to the messages. At present there are many algorithms based on symmetric cryptography that provides security to the messages transferred based on a shared secret key. The main disadvantage of a symmetric-key cryptosystem is related to the exchange of keys. There exists the problem of key distribution in them. Private-key systems need to use keys that are at least as long as the message to be encrypted. Symmetric encryption requires that a secure channel be used to exchange the key, which seriously diminishes the usefulness of this kind of encryption system when we talk about SMS.

- Mahmoud Reza Hashemi and Elahe Soroush et al [2], proposed a secure m-payment protocol for mobile devices. They used a 163-bit key for Enterprise Control component (ECC) computations, which is proven to be equivalent to a 1024-bit key for Rivest Shamir Algorithm (RSA). The results show that Elliptic Curve Digital Signature Algorithm (ECDSA) consumes less power than Digital Signature Algorithm (DSA). ECDSA and RSA

Digital Signature Algorithms (DSA) have complementary power costs. RSA performs signature verification efficiently, while ECDSA imposes a smaller cost for signature generation.

- S.Wu and C.Tan *et al* [3], proposed an implementation of public key cryptosystem for SMS in mobile phone network has been presented in java based public key infrastructure for SMS messaging. A secure SMS is considered to provide mobile commerce services presented in paper a high security framework for SMS and is based on public key cryptography
- H. Rongu, Z. Guolei, C. Chaowen, X. Hui, Q. Xi and Q. Zheng *et al* [5], proposed an application system based on the payment system. This application is based on the high security foundation. This application generates the shared key for each period and transfer the secure information between two peers.
- P. Mondal, P. Desai, S.K. Ghosh and J. Mukherjee *et al* [6], proposed an application design for the public health care. This application is based on the java public key cryptography. This application stored all the medical data of each person and secure message transfer from one mobile phone to another the table 2.1 shows the various reviews of authors discussed.

3. Proposed Work

Cryptography is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again to plain text (known as decryption). The key feature of asymmetric cryptography system is encryption and decryption procedure are done with two different keys - public key and private key. Private Key cannot be derived with help of public key that provides much strength to security of cryptography

The proposed RSA algorithm is widely used in encrypted connection, digital signatures and digital certificates core algorithms. Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA). It is the main operation of RSA to compute modular exponentiation. Since RSA is based on arithmetic modulo large numbers, it can be slow in constraining environments. Especially, when RSA decrypts the cipher text and generates the signatures, more computation capacity and time will be required. Reducing modulus in modular exponentiation is a technique to speed up the RSA decryption. The security of RSA comes from integer factorization problem. RSA algorithm is relatively easy to understand and implement RSA algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent RSA is used in security protocols such as IPSEC/IKE, TLS/SSL, PGP, and many more applications. The public and private keys are functions of a pair of large prime numbers and the necessary activities required to decrypt a message from cipher text to plaintext using a public key is comparable to factoring the product of two prime numbers.

4. Experimental Results

Sometimes, we send the confidential information like password, pass code, banking details and private identity to our friends, family members and service providers through an SMS. But the traditional SMS service offered by various mobile operators surprisingly does not provide information security of the message being sent over the network. In order to protect such confidential information, it is strongly required to provide end-to-end secure communication between end users. SMS usage is threatened with security concerns, such as SMS disclosure, man-in-the-middle attack, replay attack and impersonation attack. There are some more issues related to the open functionality of SMS which can incapacitate all voice communications in a metropolitan area, and SMS-based mobile botelnet as Android botnet.

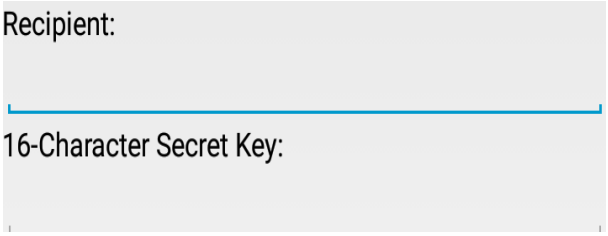

Fig 1: Entering number and key.

Fig 2: Sending the Encrypted message.

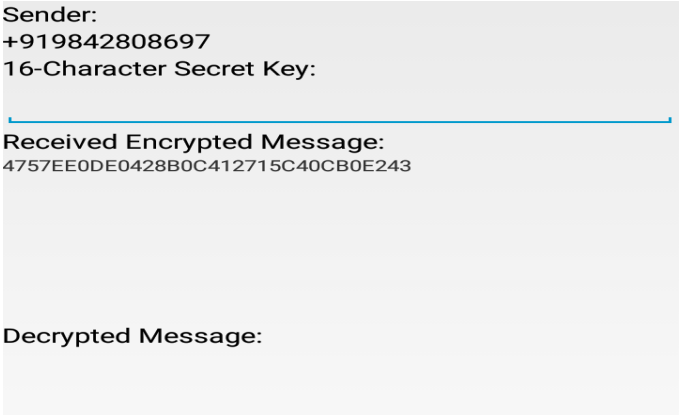

Fig 3: Receiving Decrypted message

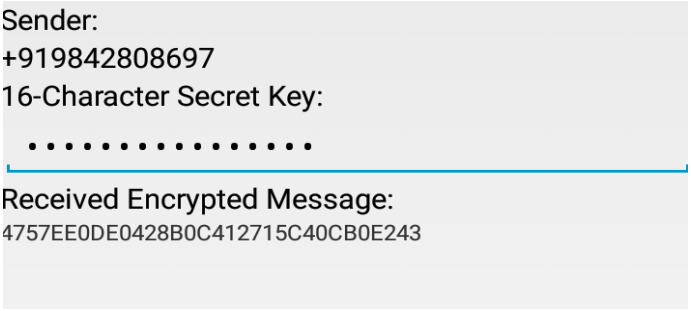

Fig 4: Entering the key of user.

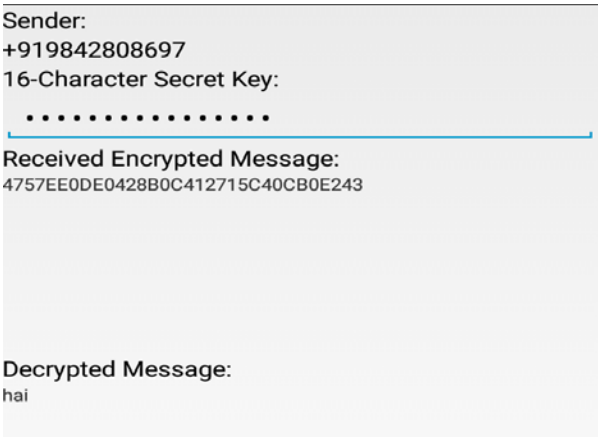

Fig 5: Decryption of message

5. Performance Analysis

Precision is also known as positive predictive value and it is defined as the ability of the system to present all relevant data. The number of manipulated Apps by individually analysing the ranking, rating, review based evidences. The precision value for each of the evidences has been computed by considering the total number of manipulated Apps obtained on aggregation.

Recall is also known as sensitivity and is the ratio of relevant instances that have been retrieved. The number of manipulated Apps by individually analysing the ranking, rating, review based evidences. The recall value for each of the evidences has been computed by considering the total number of manipulated Apps obtained on aggregation.

A comparison of the overall performance of the existing and proposed system has been depicted in Figure 6.3. The results show that the proposed system provides better results than the existing system.

6. Conclusion

Secured SMS application is successfully designed in order to provide end-to-end secure communication through SMS between mobile users. The analysis of the proposed application using RSA algorithm, shows that it is able to prevent various attacks. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. This produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged ratio during authentication. It consumes very low bandwidth and provides a good data security than SMSSEC. This system contains a high security authentication mechanism and it also ensures message integrity and confidentiality. The most of using this means of secure communication is that both the sender and the receiver should be using the same application and should be active at the same time. This ensures high authentication and the fact that the SMS can be decrypted only when it was sent and thus protected from others who try to decrypt it at a later point of time.

References

1. Bertalmio M, Sapiro G, Caselles V, Ballester C. “Image inpainting”, in Proc. SIGGRAPH, 2000; 417-424.
2. Criminisi A, Perez P, Toyama K. “Region filling and object removal by exemplar-based image inpainting. IEEE Transactions on Image Processing, 2004; 13(9):1200-1212.
3. Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, Stanley Osher. “Simultaneous Structure and Texture Image Inpainting”, IEEE Transactions on Image Processing, 2003; 12(8).
4. Yassin MY, Hasan, Lina J, Karam. “Morphological Text Extraction from Images”, IEEE Transactions On Image Processing, 2000; 9(11).
5. Eftychios A, Pnevmatikakis, Petros Maragos. “An Inpainting System for Automatic Image Structure-Texture Restoration with Text Removal”, IEEE trans. 978-1-4244-1764, 2008.
6. Bhuvaneswari S, Subashini TS. “Automatic Detection and Inpainting of Text Images”, International Journal of Computer Applications. 2013; 61(7):0975-8887.
7. Aria Pezeshk, Richard L, Tutwiler. “Automatic Feature Extraction and Text Recognition from Scanned Topographic Maps”, IEEE Transactions on geosciences and remote sensing, 2011; 49(12).
8. Xiaoqing Liu, Jagath Samarabandu. “Multiscale Edge-Based Text Extraction from Complex Images”, IEEE Trans., 1424403677, 2006.
9. Nobuo Ezaki, Marius Bulacu Lambert, Schomaker. “Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons”, Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer Society, 2004; 2: 683-686.
10. Mr. Rajesh H Davda1, Mr. Noor Mohammed. “Text Detection, Removal and Region Filling Using Image Inpainting”, International Journal of Futuristic Science Engineering and Technology, ISSN 2320–4486, 2013; 1(2).
11. Uday Modha, Preeti Dave. “Image Inpainting-Automatic Detection and Removal of Text from Images”, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 2012; 2(2).
12. Muthukumar S, Dr. Krishnan N, Pasupathi P, Deepa S. “Analysis of Image In painting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighbourhood Methods”, International Journal of Computer Applications (0975 – 8887), 2010; 9(11).