INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

MESSAGE ENCRYPTION USING NTRU ALGORITHM ON ANDROID

Amanpreet Kaur

Department of Computer Science Engineering, Rayat and Bahra College of Engineering & Biotechnology, Kharar (batthamanpreet@gmail.com)

Abstract

Short Message Service (SMS) is getting more popular now-a-days. SMS was first used in December 1992, when Neil Papworth, a 22-year-old test engineer used a personal computer to send the text message "Merry Christmas" via the Vodafone GSM network to the phone of Richard Jarvis in the UK. It will play a very important role in the future business areas of mobile commerce (M-Commerce). Presently many business organizations use SMS for their business purposes. SMS's security has become a major concern for business organizations and customers. There is a need for an end to end SMS Encryption in order to provide a secure medium for communication. Security is main concern for any business company such as banks who will provide these mobile banking services. Till now there is no such scheme that provides complete SMSs security. The transmission of an SMS in GSM network is not secure at all. Therefore it is desirable to secure SMS for business purposes by additional encryption. In this thesis, we have analyzed different cryptosystems for implementing to the existing Secure Extensible and Efficient SMS (SEESMS). We planned to implement NTRU cryptosystem into existing SEESMS frame. The NTRU public key cryptosystem was developed in 1996 at Brown University by three mathematicians J. Hoffstein, J.Pipher and J.H. Silverman. It is not that much popular cryptosystems like RSA, ECC and other traditional. The major advantages of NTRU cryptosystem is much faster generating key, encryption time and decryption time as compared to others. It is easily compatible with mobile devices and other portable devices. We have compared theoretically and analysis of NTRU with RSA and ECC cryptosystems at end of my papers. It is theoretically proposed here. We are expecting our novel scheme may show better result than others. So it will provide improve the current security level and fastest speed with respect to key generation, encryption decryption with small key size. This proposal will suitable to any kind of mobile device for SMS communication with suitable data security.

Keywords: message encryption, android, security, ntru

1. Introduction

Mobile phones are part of our daily life. Nowadays, Mobile phones provide us not only communication Services, but also many multimedia and other Function useful for human being. Mobile phones contain private or personal Data. This data is saved in a form of phone contacts, SMS, notices in a calendar, photos etc. Protection of the information depends also on a concrete user. The User should prevent against property of her/his with mobile phone. If the mobile phone is in wrong hands, most of the important information is available without a great effort (Received SMS). User registers the theft of the mobile phone almost immediately, but tapping not happens. The SMS tapping is possible in GSM network at some places. There could be used the encryption for securing of SMS. Encryption is most often realized through some user encryption applications. Therefore, there is a need to provide an additional encryption on the transmitted messages. Encryption can be classified into two categories Symmetric and Asymmetric. Symmetric encryption is the process where a single key is used for both encryption and decryption. It is somehow insecure to use. Asymmetric encryption uses two related keys, one for encryption and the other for decryption. One of the keys can be announced to the public as the public key and another kept secret as the private key. The major disadvantage of symmetric encryption is the key distribution that is mostly done through a third party. Key distribution through third party can negate the essence of encryption if the key compromised by the third party. Hence, Papers study is based on the use of asymmetric encryption technique in securing SMS. There are a lot of asymmetric encryption techniques but the commonly used in the literature are Rivest, Shamir and Adleman (RSA), ELGamal3DES Advance Encryption standard (AES), Blowfish And NTRU. Due to this reason, in this study of the mentioned algorithms have been done. This study introduces SMS, its security threats and the use of asymmetric encryption technique in securing SMS.

.

1. 1. Data encryption Algorithms:

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit weaknesses of DES, which made it an insecure block cipher. DES: As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods.

1.2. Advanced Encryption Standard: AES is the new encryption standard recommended by NIST to replace DES. It was originally called Rijndael (pronounced Rain Doll). It was selected in 1997 after a competition to select the best encryption standard. It has variable key length of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices Brute force attack is The only effective attack known against it, in which the attacker tries to test all the characters combinations toun lock the encryption. Both AES and DES are block ciphers.

1.3. NTRU: The NTRU encryption scheme is an interesting alternative to well- established .Encryption schemes such as, RSA, DES, ElGamal, and ECIES. The security of NTRU depends on the hardness of computing short lattice vectors and thus is a promising user for being quantum computer resistant. There has been extensive research on efficient implementation of the NTRU encryption scheme. In this paper, we present a new algorithm for showing the performance of NTRU. The proposed method is faster on average than the performance of NTRU. The proposed method is faster on average than the best previously known procedures.

2. Related work

Particularly about secure extensible and efficient SMS (SEESMS), the proposal presented by Alfredo De Santis and his team members in [1] which designed a Java based framework for exchanging secure SMS. They considered RSA, DSA and ECDSA algorithms. Here we have considered the same ECLIPSE frame with NTRU cryptosystems for SMS security purpose.

2.1. Message security

Now-a-days, SMS is used for M-Commerce purpose. SMS will play a very vital role in the future banking or commercial purpose because of its simplicity and cheapness. Upcoming payment system will be based on the mobile device by using SMS. Money can be debited or credited from the bank through the SMS by using the GSM network. But some security related services of SMS should be available when we go for such m-commerce or m-banking. Network operators are demanding spam control and anti-spoofing capabilities to protect their SMS network and subscribers. When customers have complaints regarding SMS, operators do have not any other options to block such types of SMS rather than blocking such SMS subscribers. There are some security gaps for SMS. Such as Snooping, SMS Interception, Spoofing, Modification, Faking, Flooding, Spam and other SMS-related scams are a global problem. There are many security threats to mobile subscribers and operators. It is easy to sneak a virus as a Trojan attachment in an SMS message.

2.3. Message encryption

SMS encryption is the process of transforming SMS information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information. Encryption is also used to protect data in transit, for example data being transferred via networks mobile telephones Encrypting data in transit also helps to secure it as it is often difficult to physically secure all access to networks. Encryption can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message. Successfully using encryption to ensure security may be a challenging problem. There are so many algorithms are available for SMS encryption. The application of SMS encryption algorithms is dependent upon operating system of the types of mobile device. The other factors like energy consumption, speed, security and others are to be considered while choosing the encryption techniques.

3. Objectives

The main goals of our application are:

1. Developing a secure SMS application.
2. Maintaining encrypted information of message recipients.
3. Decrypting of message as per users requirement.
4. Protection against misuse of message information.
5. High confidentiality and improved security

4. References

[1]. De Santis, A. Castiglione, A. Cattaneo, G. Cembalo, M. Petagna, F. Petrillo, U.F, "An Extensible Framework for Efficient Secure SMS," Complex, Intelligent and Software Intensive Systems (CISIS), International Conference, 15-18 Feb.2010, pp. 843-850, doi:10.1109/CISIS.201081

[2]. Hossain, A.; Jahan, S.; Hussain, M.M.; Amin, M.R.; Shah Newaz, S.H.; "A Proposal For Enhancing The Security System Of Short Message Service In GSM", Anti-counterfeiting, Security and Identification, 2nd International Conference, ASID 2008, doi: 10.1109/IWASID.2008.4688386.

[3]. http://en.wikipedia.org/wiki/Encryption.

[4]. ww.en.wikipedia.org/wiki/Android_%28mobile_phone_platform%29.

[5]. http://en.wikipedia.org/wiki/BlackBerry.

[6].Lisonek, David; Drahansky, Martin; “SMS Encryption for Mobile Communication”, Security Technology, SECTECH '08, International Conference, 2008, doi:10.1109/SecTech.2008.48.

[7]. Agoyi, Mary; Seral, Devrim; “SMS Security: An Asymmetric Encryption Approach,” Wireless and Mobile Communications (ICWMC), 6th International Conference, 2010, pp.448-452,doi: 10.1109/ICWMC.2010.87.

[8]. http://en.wikipedia.org/wiki/Mobile_application_development

[9]. http://en.wikipedia.org/wiki/NTRUEncrypt