MAHATMA EDUCATION SOCIETY'S

Pillai's HOC college of Engineering and Technology , Rasayani
Intercollegiate UG Project Competition

Group Id:- D15

Project Title :- "SMS Security Using Protocol"

Abstract

Nowadays, SMS or messages are very common way of communication. Even the various instant messaging apps are available but SMS are still one of the popular ways of communication because it doesn't require internet connection and of course sending an SMS is economical, fast and simple. It is very difficult to provide the security without Encryption. These papers propose solution that provides SMS security that guarantees provision of Confidentiality, Authentication, and Integrity service. We have used the Symmetric key cryptography algorithm Advanced Encryption Standards (AES) along with Asymmetric key cryptography algorithm RSA for encryption and decryption of the data. As AES provides strong encryption but the secret key has to share with other party in case of decryption which may turn into its shortfall, and RSA with is public key cryptography provide low encryption ratio but solves the problem of sharing key, hence the idea is to take the advantage of both algorithms and avoid the shortfalls of both to achieve a strong encryption. Every SMS has a character limit of 160 7bit characters as per the mandate provided by GSM regulatory body, and hence it require the solution to compact maximum character in SMS body and introduces economic and efficient value to your money.

Introduction

Mobile communication devices have become popular tools for gathering and disseminating information and data. When Confidential information is transmit using SMS, it is pivotal to protect the content from eavesdroppers as well as ensuring that the message is sent by a rightful sender. Using an encryption technique to secure SMS data increases its length and accordingly the cost of sending it. This project provides a compression and encryption technique to secure the SMS data. The proposed solution compresses the SMS to reduce its length, and then encrypts it using AES and RSA algorithm. A SMS in first encrypted with AES key and then it uses RSA algorithm to again encrypt it by receiver's public key and then it is sent to its destination.

SMS Security: What is needed? [7]

A. Authentication: Confirm true identities between sender and receiver, and prevent impersonation attack from illegal intruders.

B. Confidentiality: Ensure that decrypted messages are accessible only to those authorized senders and receivers.

C. Integrity: Ensure that receivers can check out whether the message has been altered, and prevent tampered messages.

Method

SMS ENCRYPTION

Many companies deal with securing of mobile communication today. Calls, SMS and data stored in mobile phone memory have to be secured. The applications are written for the most widespread programming platforms for mobile devices. Common model for SMS securing is to use asymmetric cryptography. [8]For SMS encryption, there is commonly used symmetric AES algorithm. AES algorithm demands small computing capability therefore, applications can be written for the most widespread programming platform like Java Platform, Micro Edition, and android. The major disadvantage of symmetric encryption is the key distribution that is mostly done through a mediator . Key distribution through third party can negate the essence of encryption if the key compromised by the third party. [10] The second option is to use an asymmetric cryptography, where the public key is distributed. The public key can also be known by an attacker Asymmetric cryptography can provide confidentiality, integrity and authentication information such asymmetric cryptography, but also provides a non-repudiation. Unfortunately, asymmetric cryptography is demanding the computing capability. Applications using the asymmetric cryptography must be written for the devices with more computing capability.

REQUIREMENTS ON ENCRYPTION ALGORITHM

The main requirement for an application is securing the confidentiality of the information sent in the SMS. Security should be sufficiently strong with the characteristics of modern cryptographic systems, but not overly annoying users. Users need not physically meet and/or have not a secure channel for the encryption keys distribution.

We can implement two types of cryptography algorithm.

1) Asymmetric Key Cryptography

2) Symmetric Key Cryptography

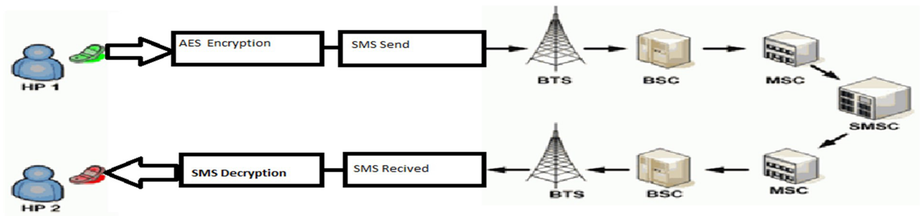
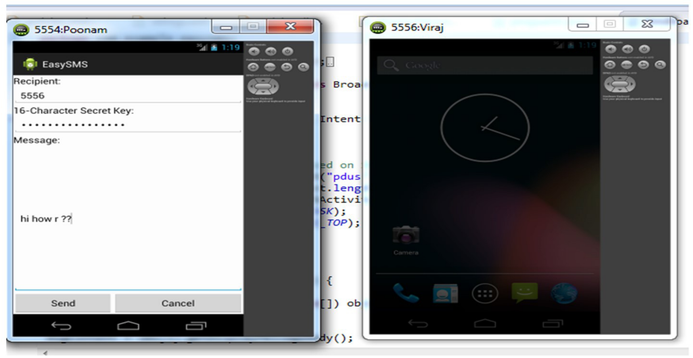
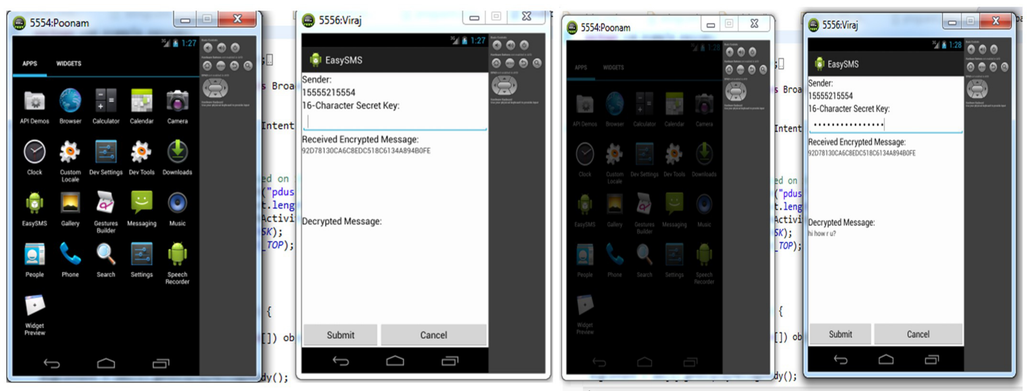


Fig. A System Architecture diagram

Result





Process

SMS Encryption and Compression

Encryption turns data into high breakup data, which is indistinguishable from a random stream. The encrypted message usually gets larger than the original message size leading to excessive charge in sending encrypted message. So data compression can be introduced here, but any compression algorithm relies on the principle of finding the patterns and assigning some shorter code to reduce its size. So if we apply encryption first, then all patterns present in SMS may loss. Compression before encryption also slightly increases your practical resistance against differential cryptanalysis, if the attacker can only control the plaintext, since the resulting output may be difficult to deduce.

The compression of original SMS and then applying encryption on compressed SMS, we get both compression as well as encryption of SMS and we can save a little cost per SMS.

Steps to follow at sender side:

Step 1: Write SMS.

Step 2: Compress SMS.

Step 3: Compressed text is transferred for Encryption. A random number generator function will generate any 16 digit random key for AES algorithm.

Step 4: Encrypt it with this random key(AES algorithm)

Step 5: Now this random key is appended at the end of encrypted text.

Step 6: Here we will be using Asymmetric public key algorithm- RSA.

Step 7: Above Cipher text with appended random key is again encrypted with receiver's public key (i.e. his/her Mobile no).

Step 8: Send the Encrypted SMS to its destination.

Steps to follow at receiver side:

Step 1: Enter private key to decrypt the random key and get original random key.

Step 2: Decrypt the SMS using this random key.

Step 3: Original SMS received.

References

[1] Rashmi Ramesh Chavan, Manoj Sabnees,| Secured Mobile Messaging| 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET]

[2] David Lisoněk, Martin Drahanský —SMS Encryption for Mobile Communication| 2008 International Conference on Security Technology

[3] Tarek M. Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahmed, Ahmed M. Mahfouz, —Hybrid Compression Encryption Technique for Securing SMS|, International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6)

[4] Rohan Rayarikar, Sanket Upadhyay, Priyanak Pimple — SMS Encryption using AES Algorithm on Android| *International Journal of Computer Applications (0975 – 8887) Volume 50– No.19, July 2012*

[5] Mohammed Al-laham & Ibrahiem M. M. El Emary 'Comparative Study Between Various Algorithms of Data Compression Techniques' Proceedings of the World Congress on Engineering and Computer Science 2007WCECS 2007, October 24-26, 2007, San Francisco, USA

[6] Priyanka Pimpale, Rohan Rayarikar and Sanket Upadhyay, —Modifications to AES Algorithm for Complex Encryption|, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011.

[7] Kahate A, "*Cryptography and network security*", 3rd ed., Tata McGrawHill, (2003).

[8] Ze-Nian Li and Mark S. Drew, —*Fundamentals Of Multimedia"*, Pearson Education, Inc.(2004)

[9] Senthil Shanmugasundaram and Robert Lourdusamy, —*A Comparative Study Of Text Compression Algorithms*|, International Journal of Wisdom Based Computing, Vol. 1 (3), December 2011

[10] Pravin Y Kumbhar, Prof. Shoba Krishnan

—*SMS Compression Using Arithmetic Coding Modification"*, Dept. of Electronics and Telecommunication, Vivekanand Education Society Institute of Technology Mumbai University, Mumbai (Maharashtra)

Conclusion

This application provides complete a secure communication between the users through SMS.

This application can run on any Android devices. AES algorithm creates more complexity during encryption which makes it very difficult for an attacker to interpret the encryption pattern and the plain text form of the encrypted data. The messages encrypted by the developed application are also resistant to Brute-Force and pattern attacks.

The application for security and compression of SMS has been designed and implemented, which prevents tapping and interception with efficient size and reduced cost. For securing, it has been chosen the combination of asymmetric cipher RSA and symmetric cipher AES. A user generated random key encrypts the SMS by AES and Public key used to encrypt that random key for secure transfer of key. The application is running in the mobile phone and does not require any additional encryption devices.

Mahatma Education Society's

Pillai HOC College of Engineering & Technology

Rasayani, Khalapur, Raigad – 410207

CERTIFICATE

This is to certify that Mr./Ms. Viraj Gujar
of B.E. IT won the First Prize
for the project titled Securing SMS Using Protocol

in

Intracollegiate Undergraduate Project Competition 2014-2015

held on Friday, 27th March 2015

Ms. Mansi Subhedar
(CONVENER)

Dr. Shrikant Charhate
(DEAN)

Dr. Chelpa Lingam
(PRINCIPAL)