Abstract

SMS is a short messaging service via mobile phones. Although it is a part of the earlier interface of the GSM standard capabilities, SMS is still a service that widely used by communities. The use of SMS becomes popular among the people so easily because we can exchange information without any restrictions of distance and time with a fast and low cost.

Currently, the development of mobile devices goes through very rapid developments. The various features and facilities offered for the users of mobile devices such as internet, multimedia chat, and many other features. It makes the mobile devices become an important part of people's lifestyles. Along with the development of technologies on mobile devices, problems associated with the security level on mobile devices increase, such as eavesdropping, theft of information and others. The risk when we communicate via SMS is the sent message will be stored in the SMSC (Short Message Service Center) before it is sent to the destination. Messages that formatted in plaintext can be wired by anyone who is able to have access to the SMSC. As a result, important information such as passwords, pin numbers, etc. can be read by unwanted people. It is a harmful condition if the stolen or intercepted information is information that considered as personal or confidential.
From the problems that have been previously described, this final assignment develops software that serves as the SMS application, which is able to encrypt and decrypt SMS messages on mobile devices using Rabin cryptographic method. This method uses three main processes; generating key pairs, encryption, and decryption. The process of generating key will generate a public key; which is used to encrypt; and private key; which is used to decrypt. The Rabin technique always develop four possible decryption results, all given to a person that carry out the secret message decryption. Next, the person should be able to determine which message is correct between the four results of the decryption. Although the decryption generates four different outcomes, but ultimately the message recipient can select the correct message and it is not too difficult, because the correct message should be obvious when compared with the other third decryption result.

This Final assignment is more focused on the development of Android operating system, since it is supported by appropriate technology and available in various smart-phone types and brands. By utilizing the Rabin cryptographic method, SMS service is expected to be more secure because the encryption algorithm used is quite tough and the result of encryption is difficult to solve.

Keywords: Android, cryptography, public key, Rabin, SMS, Smartphone.