ABSTRAK

Penggunaan ponsel pintar (smartphone) di masyarakat saat ini sangat luas. Android menjadi yang paling diunggulkan oleh para pengguna dan juga produsen smartphone karena fiturnya yang sangat menarik. Namun demikian, meskipun teknologi dari smartphone ini memiliki banyak fitur, pengguna masih memiliki perhatian khusus terhadap SMS (Short Message Service). Sayangnya, fitur SMS ini memiliki keterbatasan terutama dalam keamanan pertukaran informasi yang bersifat rahasia, sehingga dibutuhkan sistem yang dapat memberikan pengamanan terhadap pertukaran informasi pada SMS berbasis android. Oleh karena itu, diperlukan metode untuk mengamankannya, salah satunya dengan menggunakan metode kriptografi. Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (message). Kriptografi telah banyak diimplementasikan di banyak hal. Smart card, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia (plainteks) ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia (cipherteks). Proses transformasi plainteks menjadi chiperteks diistilahkan dengan enkripsi. Sedang proses pengembalian pesan chiperteks menjadi plainteks diistilahkan dengan dekripsi. Ada banyak algoritma kriptografi, dalam penelitian ini aplikasi kriotografi yang dikembangkan menggunakan algoritma DES (Data Encryption Standard) dengan bahasa pemrograman Java. DES menggunakan sandi blok kunci simetrik dengan ukuran blok 64-bit dan ukuran kunci 56-bit dan Advance Encryption Standard (AES) dengan ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit.

Kata Kunci: *Kriptografi, keamanan komunikasi data, kriptograpi Data Encryption Standard (DES), Advance Encryption Standard (AES), Android.*

ABSTRACT

The use of smart phones (smartphones) in today's society is very broad. Android became the most favored by the users and manufacturers of smartphones due to its very attractive. However, although the technology of this smartphone has many features, users still have special concern for SMS (Short Message Service). Unfortunately, this SMS feature has limitations, especially in the security of the exchange of confidential information, and so we need a system that can provide security for the exchange of information on the SMS-based android. Therefore, methods are needed to secure it, one of them by using cryptographic methods. Cryptography is the science to maintain the security of the message (message). Cryptography has been widely implemented in many ways. Smart cards, Automated Teller Machine (ATM), Pay TV, Mobile Phones, and Computers are a few examples of products that use cryptographic technology to its safety. It works by changing the original message that can be understood / human readable (plaintext) into another form that can not be understood / read by humans (ciphertext). The process of transformation of plaintext into chiperteks termed encryption. Being the process of returning a message chiperteks be termed decrypted plaintext. There are many cryptographic algorithms, in this study kriotografi applications developed using algorithms DES (Data Encryption Standard) with the Java programming language. DES uses a symmetric key block cipher with a block size of 64-bit and 56-bit key size and Advanced Encryption Standard (AES) with a block size and the key remains at 128, 192, 256 bits.

Keywords: *Cryptography, The Security of Data Communications, Kriptograpi Data Encryption Standard (DES), Advance Encryption Standard (AES), Android.*

.