ABSTRACT

The requirements of mobile information also become a background to the growth of data communications protection technology. It is often discovered the existence of criminal behaviour trying to enter this data communications gap. When conversing about data security, hence one of the thought up solution is cryptography. Cryptography is a mathematics science branch that exploits computing process to randomize data to be transmitted. Encryption is a data encoding process to prevent the unqualified party to see or modifying it.

This final paper implements three algorithms which are used in cryptography, such as hash function with MD5 and SHA1 algorithms, and also symmetrical cryptography with RC4 algorithm. These algorithms are solution which offered in the cryptography's world and commonly used in internet network. All implemented algorithm will adapted into system using J2ME platform.

The implemented system runs well in J2ME Wireless Toolkit emulator. Analysis within security subsistem has done based on some parameters, output data length, memory usage, process time, frequency distribution, variance, avalanche effect for RC4 algorithm, and brute force attack time for RC4 algorithm.

From the analysis result, it has compared which is better performance between hash function algorithms, MD5 and SHA1. The process has obtained that SHA1 algorithm has good point in output data length, process time with RC4 combination, frequency distribution, variance, and brute force attack time. MD5 algorithm has good point in memory usage, and process time without RC4 combination. Therefore, generally SHA1 algorithm has better performance than MD5 algorithm.