| | |
|---|---|
| Thesis Title | Development of Software Package for Digital Wireless Mobile Data on WorldData Network |
| Student | Mr. Rangsarn Noychinda |
| Thesis Advisor | Assoc.Prof. Kaset Sirisantisamrid |
| Degree | Master of Engineering in Electrical Engineering |
| Year | 1999 |


## Abstract

The digital wireless mobile data communication is on a World Data network. The data communicates be utilizing the packet switching technology at a speed of 19.2 kbps and radio frequency of 800 MHz. The protocol utilized to transfer information between the mobile terminal and the radio packet modem is known as NCL (Native Command Language) which is an asynchronous transaction.

In each input data frame would be compressed before sending. We propose the compression method improved will be the Lempel-Ziv algorithm by prediction. It works by searching for redundant the longest data context in the input data. If an appropriate match is found, then the match length is written. If no appropriate match is found, then the literal is written. At this point, the Static Huffman coding algorithm will look at the frequency of occurrence of the literal and match length symbol are computed first, and then constructs a full binary tree with shorter bit patterns.

After data compression processed, the data encrypted by RC5 (Rivest Cipher) algorithm that is a symmetric block cipher. The plaintext and ciphertext are fixed-length bit blocks which can be utilized by processors of difference word-lengths. This is because a 16-bit, 32-bit, or a 64-bit processors are capable of effectively increasing computation speed. Furthermore, RC5 has a variable-length secret key and a variable number of rounds which provide flexibility in its security level. We called the RC5 key is secret key. We propose to use the RSA encryption method for RC5 key exchange. In the RSA (Rivest, Shamir, Adleman) method, each person has a pair of keys, One key is a public key, and the other one is a private key. The public key will be available for all to see, but the private key will be kept by each person. We can only decrypt by a private key. The RC5 and RSA key generator used random number sources from mouse click timing, keystroke timing, time and clock. The random output run its through MD5 (Message Digest) algorithm to produce the bits are all independent. The attacker difficult to guess and break the key.