ABSTRACT

In this final project will be discused about teks compression and encryption method, where the implementation is used on e-mail. Compression is used for preventing bandwidth limitation, encryption is used for security, that work for preventing data stealing at communication proccess by unauthorized individual. Therefore, in this final project, writer will do compression simulation using arithmetic code and encryption simulation using A5/2 algortihm. This final project is useful for text transmission, so bit size is minimize, and it encrypted so it can keep data integrity. For the future, this final project can be used for data stored, when the data is compressed and encrypted.

Arithmetic code represent as one of data compression, later the data would shape to be probability value, while A5/2 represent as encryption shape from LFSR (Linear Feedback Shift Register) who has output bits and will be Xor'ed with message bits. Then it will be counted how much compression factor, and encryption ability, and result expected from output decryption and decompression, would be like initialy text, like text who have no compression and encryption.

The best compression result can be achieved when the message is on very good condition, bigger number of iteration, and bigger number of character like the result, when compression factor and ratio for 1000 character and the number of iteration is 5 are 4.166666667 and 0.24, when compression factor and ratio for 10,000 character and number of iteration is 15 are 13.88888889 and 0.072. The number of iteration is bigger then compression time is faster.

Key words: *A5/2 encryption, arithmetic code, bandwidth, compression, cryptography, decryption, decompression, encryption, security*.