ABSTRACT

Recently, there are many development in the field of cryptography. One of them uses a combination of biology ad cryptography that combines the characteristic of DNA. the cryptosystem called as DNA cryptography.. DNA cryptography is a new domain of cryptography is based on the field research on DNA computing and new technology like: PCR (Polymerase Chain Reaction) , microarray , etc. DNA cryptography uses the chacteristic of DNA to encode a plaintext . In the proposed implementation, DNA cryptography is implemented with the One -time pad method.

However, since the previous proposed DNA Cryptography uses vigenere chipher and subtitution table (for implementing the One Time Pad) which are weak against kasisi test and frequency analisys, then the method is weak against those attack as well. for overcoming the problem this research proposed DNA-based Cryptography One Time Pad which will be amplified using a random generator BBS.

Based on result that performed, DNA Cryptography resilient to attack both above and has a value Avalanche Effect close to optimal that is 53.03 % . But from memory usage , the results of the data encryption has nearly 3 times the initial plaintext. And then execute time is more longer than original one.

Keywords : ***Cryptography, One-Time-Padss, DNA Cryptography, Vigenere chipher, Subtitution table***