ABSTRACT

RSA is one of the asymmetric algorithm used in the encryption and decryption of data. RSA is generally already have a good level of security, but still has some shortcomings. Some of them are the key length used and the separation of the authentication process to the encryption process. Where if you use short keys will easily factored. And separation of the authentication process to the encryption process resulted in common ciphertext received from anyone if the same encrypted message. To overcome these problems, in this final project designed a system security and authentication messaging using a modification of the RSA asymmetric algorithm.

In designing this final project, writer used a modified incorporation of n-prime function in key generation and modification merging each user authentication process with the process of encryption and decryption encryption system. Modification of n-prime gives the user the freedom to choose the number of primes in the generation of the key pair. While the incorporation of modifications authentication process with the encryption process is a modification in the system of encryption and decryption. Wherein each input message is converted into blocks of numbers. Block length depends on the length of the value of n in the sender's private key. Then do the authentication process with the sender's private key input. The results of this process will then be compiled into blocks of new numbers. Block length depends on the length of the value of n in the message recipient's public key. The results of this process is further encrypted into ciphertext row.

The system designed in this final project can only accept input type is text in the form of a combination of character letters and numeric characters. With the value of the test results of system design in this thesis can generate chi-square value is smaller than 3.481, the average value of the results of the avalanche effect is less than 50%, and the average value of a well-designed encryption system performance time of 1.84 times the performance system without modification and 1.62 times the performance of time with the RSA encryption system authentication Hash insertion.

Keywords: cryptography, encryption, authentication, RSA modified, n-prime