DESAIN ALGORITMA KUNCI PUBLIK FISOYU SEBAGAI PENUTUP KELEMAHAN RSA

Afifah[1)], Sofu Risqi Y.S.[2)]
Sekolah Tinggi Sandi Negara
Jl.H.Usa Putat Nutug Ciseeng - Bogor, 16120
Telp : 085642863390
E-mail : afifahifaafi@gmail.com[1)], sofurizky@yahoo.com[2)]

Abstrak

Algoritma asimetris adalah algoritma yang menggunakan kunci berbeda pada proses enkripsi dan dekripsi yang dilakukan. Salah satunya adalah algoritma Fisoyu yang merupakan modifikasi dari algoritma RSA dan protokol Diffie Hellman. Kombinasi dari kedua algoritma tersebut dapat mempersulit kriptanalis dalam melakukan serangan sehingga usaha yang dilakukan jauh lebih besar dibandingkan dengan serangan pada RSA tanpa modifikasi.

Kata kunci: *RSA, Diffie Hellman, Fisoyu*

Abstract

Asymmetric algorithm is an algorithm that uses a different key in the encryption and decryption process is carried out. One of them is Fisoyu algorithm which is a modification of the algorithm RSA and Diffie Hellman protocol. The combination of these two algorithms can complicate cryptanalyst in an attack so that the work done is far greater than the attack on RSA without modification.

Kata kunci: *RSA, Diffie Hellman, Fisoyu*