ABSTRAK

Nama : Muhammad Reza Aldifa

NIM : 1197010045

Judul Skripsi : Algoritma *Hybrid* : Vigenere-Hill Cipher Dan RSA (Rivest Shamri Adleman) Dengan Pembangkit Kunci Matriks Involusi dan ESRKGS

Algoritma simetri seperti Vigenere Cipher dan Hill Cipher telah menjadi pilihan utama dalam kriptografi klasik karena mudah untuk dibuat dengan fasilitas yang terbatas kala itu. Namun, dengan berkembangnya kajian mengenai kriptografi dan mulai ditemukannya teknik-teknik kriptanalisis seperti metode Kasiski dan known-plainteks attack, tingkat keamanan kedua algoritma ini menurun secara signifikan. Sebagai respons dari persoalam tersebut, penelitian ini mencoba mengkombinasikan algoritma kunci simetri tersebut dengan algoritma kunci asimetri seperti ESRKGS+RSA, algoritma RSA yang telah ditingkatkan keamanan kuncinya, yang memanfaatkan sepasang kunci terpisah: publik dan privat. Kombinasi algoritma simetri dan asimetris ini diharapkan dapat untuk meningkatkan tingkat keamanan secara substansial. Namun, untuk mencapai efisiensi dalam implementasi kombinasi ini, dibutuhkan kunci matriks involusi yang memiliki sifat invers, yang memungkinkannya berfungsi sebagai kunci untuk proses enkripsi dan dekripsi dengan mudah dan cepat.

Kata kunci : Algoritma Kunci Simetri, Algoritma Vigenere Cipher, Algoritma Hill Cipher, Algoritma RSA, Matriks Involusi, ESRKGS

ABSTRACT

Name **: Muhammad Reza Aldifa**

NIM **: 1197010045**

Tittle **: *Hybrid Algorithm: Vigenere-Hill Cipher and RSA (Rivest Shamir Adleman) with Involutory Matrix Key Generator and ESRKGS***

Symmetric algorithms such as Vigenere Cipher and Hill Cipher have been the primary choice in classical cryptography due to their ease of implementation with limited resources available at that time. However, with the advancement of cryptography studies and the emergence of cryptanalysis techniques such as the Kasiski method and known-plainteks attack, the security of these two algorithms has significantly declined In response to this issue, the research attempts to combine symmetric key algorithms with asymmetric key algorithms such as ESRKGS+RSA, an enhanced security version of the RSA algorithm, which utilizes a pair of separate keys: publik and pribadi. The combination of symmetric and asymmetric algorithms is expected to substantially enhance the security level. However, to achieve efficiency in implementing this combination, an involutory matrix key with invers properties is required, enabling it to function as a key for encryption and decryption processes quickly and easily.

Keywords: Symmetric Key Algorithm, Vigenere Cipher Algorithm, Hill Cipher Algorithm, Algorithm RSA, Involutory Matrix, ESRKGS