INTISARI

Kadang-kadang suatu informasi harus dijaga kerahasiaanya. Kerahasiaan, tidak bisa disangkal masih dibutuhkan dalam kehidupan sehari-hari. Misalnya dalam dunia militer, keamanan informasi merupakan hal yang sangat perlu untuk dijaga. Berdasarkan hal itu, perlu dipikirkan bagaimana cara agar kerahasiaan informasi dalam komputer tersebut tetap terjaga. Salah satu cara adalah dengan penyandian atau pengacakan, sehingga informasi yang disimpan atau dikirimkan tetap terjaga kerahasiaanya. Terdapat dua jenis algoritma yang digunakan dalam tugas akhir ini, yaitu algoritma DES (*Data Encryption Standart*) dan algoritma RSA (Ron Rivest, Adi Shamir, dan Len Adleman) . Adapun format citra yang dipakai adalah citra ber-format *.BMP.

Dimana citra yang telah dienkipsi akan mengalami pengacakan, tetapi hasil enkripsinya sendiri memiliki ukuran *file* yang sama besarnya dengan citra sebelum dienkripsi. Setelah program dijalankan beberapa kali dapat dilaporkan bahwa enkripsi dengan algoritma RSA menghasilkan citra yang benar-benar teracak, karena kunci-kunci yang digunakan lebih banyak sehingga akan menghasilkan kombinasi yang lebih baik. Demikian juga dari segi keamanan algoritma RSA lebih sulit untuk dipecahkan dan membutuhkan waktu yang lebih lama dibandingkan dengan algoritma DES, karena nilai untuk proses dekripsi berbeda dengan nilai untuk proses enkripsi nilai yang dimaksud adalah nilai e sedangkan nilai p dan q sama, dimana pada waktu dekripsi dimasukan nilai e yang merupakan kebalikan dari nilai e ketika proses enkripsi dilakukan.

ABSTRACT

Sometimes an information have to be taken care of secret. Secret, cannot be denied still be required in everyday life. Form example in the world of military, informatio security represent very matter need to be taken care. Pursuant to that matter, require to be estimated how to be information secret in the computer remain to be awaked. One of way is encodedly or random, so that information kept or delivered reamin to be awaked secret. There are two type algorithms used in final daty, that is DES (*Data Encryption Standart*) algorithms and RSA (Ron Rivest, Adi Shamir, and Len Adleman) algorithms. As for image format weared is image format *.BMP.

Where image which have encryption will experience of the random, but the result of encryption self own the size measure same file level of with the image before encryption. After program run several times can be by reported that encryption with the RSA algorithms yield the really random image, because keys by used more amount so that will yield the better combination. And so do from facet of security RSA algorithms more difficult to be solved and many more time to be compared to by DES algorithms, because value to proses the decryption differ from the value to proses the encryption. Such value is value e of while value of p and q is equal, where when our decryption is input assess the e representing reverse from value e of when process encryption conducted.