

INTISARI

Kadang-kadang suatu informasi harus dijaga kerahasiaannya, karena informasi tersebut sangatlah penting dan tidak semua orang berhak mengetahui informasi tersebut. Kerahasiaan suatu data merupakan hal sangat dibutuhkan dalam kehidupan sehari-hari, misalnya dalam dunia militer dan perbankan. Salah satu cara yang dapat digunakan untuk pengamanan terhadap berkas yang dianggap rahasia adalah dengan penyandian data. Terdapat tiga jenis algoritma yang digunakan dalam tugas akhir ini, yaitu algoritma DES (*Data Encryption Standard*) dan algoritma RSA (Ron Rivest, Adi Shamir, dan Len Adleman) untuk berkas gambar (*.bmp) dan algoritma XOR untuk berkas teks (*.txt).

Berkas yang sudah dienkripsi mengalami pengacakan dan berkas yang sudah dienkripsi tidak mengalami perubahan ukuran. Jadi ukuran file asli dan file yang sudah dienkripsi sama. Dengan program ini diharapkan kerahasiaan suatu data dapat terjamin dengan baik sehingga informasi yang bersifat rahasia dapat terlindungi dengan baik.

ABSTRACT

Informations sometimes must be kept secret because these information are very important and not every body has the right to know it. The secret of a data is a thing which is very needed in daily life, such as in military world or banking world. One of the methods that can be used to keep the secret files is by encoding the data. There are three encryption algorithms that are discussed in this thesis, namely *Data Encryption Standard* (DES) algorithm , Ron Rivest, Adi Shamir, and Len Adleman (RSA) algorithm for formatted picture file (*.bmp) and XOR algorithm for text file (*.txt).

File that has been encrypted will be randomized, but its size will not be changed. Therefore, the size of the original file and the encrypted file will be the same. Hopefully, by this program the secret of the data will be guarantee so that the secret information can be protected.