

ABSTRAK

Pengamanan database itu sendiri adalah sebuah teknik yang melakukan perubahan informasi menjadi sesuatu yang tidak bisa dimengerti orang lain, dengan menggunakan sebuah kunci matematis. Kunci daripada proses enkripsi bisa berupa aturan, angka, arahan, kata maupun kalimat, salah satu cara mengamankan data itu memberikan pengamanan karena data adalah data pribadi jadi untuk mengamankan memerlukan algoritma dalam memberikan pengamanan database, algoritma yang digunakan metode DES yang beroperasi pada 16 kali putaran. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal. Kunci internal dibangkitkan dari kunci eksternal yang panjangnya 54 bit. Sebelum putaran pertama, terhadap blok plainteks dilakukan permutasi awal initial permutation. Tujuan permutasi awal adalah mengacak plainteks sehingga urutan bit-bit di dalamnya berubah karena ada 16 putaran, maka dibutuhkan kunci internal sebanyak 16 buah. Kunci-kunci internal ini dapat dibangkitkan sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci eksternal panjangnya 64 bit atau 8 karakter.

Kata kunci: Android, DES, Enkripsi, Dekripsi, Database, Security