MODIFIKASI

ALGORITMA DATA ENCRYPTION STANDARD (DES) 64 BIT

UNTUK PENGAMANAN PADA PENYIMPANAN FILE

ABSTRAK

Perkembangan teknologi yang pesat membuat kita semakin mudah mendapatkan informasi yang telah diolah dari data, hal mendasar dari sebuah infromasi adalah keaslian datanya. Beberapa ancaman pada keamanan sistem informasi yaitu dengan cara menambah, mengurangi, menyadap atau bahkan menghapus data yang akan olah menjadi sebuah informasi tanpa ada otentikasi terlebih dahulu, sehingga menjaga kerahasiaan dan integritas data dari sebuah data dalam bentuk *file* sangatlah penting untuk menghasilkan sebuah infromasi yang benar, baik informasi publik, terlebih informasi yang bersifat khusus dengan hak akses terbatas. Banyak hal yang dilakukan untuk mengamankan sebuah data dalam bentuk *file*, diantaranya dengan mempertahankan kerahasiaan dan integritas data tersebut yaitu dengan enkripsi dan dekripsi, sehingga menyulitkan pihak lain yang akan merubahnya dan menggunakan fungsi autentikasi data pengguna, salah satunya dengan menggunakan fungsi hash. Tujuan akhir dari penelitian ini untuk mengetahui dan membandingkan nilai *avalanche effects* dan *randomness test* dari hasil pengujian DES standar dengan DES modifikasi pada bagian *S-Box* dan *P-Box* yang dibuat dinamis tergantung pada kunci, sehingga data yang disimpan terenkripsi. Proses modifikasi menggunakan matlab dengan masukkan beberapa kunci kombinasi diantaranya kunci lemah DES, alphabet dan alfanumerik, sedangkan pengujian terbatas menggunakan php pada penyimpanan dokumen *file* dengan proses otentikasi pengguna dan enkripsi *file* dengan kunci yang dibangkitkan dari sha-256. Proses dekripsi akan terjadi saat pemilik mengunduh datanya, sehingga keamanan dan keaslian data bisa lebih terjamin. Kunci yang dibangkitkan berbeda tiap *file*, hal ini akan menyulitkan kriptanalis untuk mencuri data tersebut. Dengan melakukan modifikasi pada algoritma DES 64 *bits* ini diharapkan masalah keamanan data pada penyimpanan bisa dipersempit.

Kata Kunci : DES, Fungsi Hash, Simetris, Enkripsi, Dekripsi

MODIFICATION

ALGORITHM DATA ENCRYPTION STANDARD (DES) 64 BIT

FOR SECURITY IN STORAGE FILE

ABSTRACT

Rapid technological developments makes more easily get information that has been processed from data, the basics of infromation is authenticity of data. Some of threats to the security of information systems are like modifying, intercepting or even delete data that will process into an information without any authentication in advance, so as to maintain the confidentiality and integrity of data from data files is essential to produce right information, public information, especially information with limited access. Many things can be done to secure data in form of a file, such as by maintaining confidentiality and integrity of such data is with encryption and decryption, making it difficult for other party is going to change and use authentication function of user data, one of them by using hash function. The goal of this research to determine and compare value avalanche effects and randomness test of the test results between standard and modification DES in S-Box and P-Box are created dynamically depending on key, so the stored data is encrypted. Modification process using matlab to enter a few key combinations such weak DES keys, alphanumeric and alphabet, while the limited testing using php file document storage with the process of user authentication and file encryption with keys raised from sha-256. Decryption process will occur when the owners download data. Because of different key for each file, it will be difficult for cryptanalyst to steal data. By making modifications on DES algorithm is expected to issue data security on storage can be narrowed.

Keywords: DES, Hash Function, Symetric, Encryption, Decryption