ABSTRAK

PERANCANGAN SISTEM KEAMANAN DATABASE MENGGUNAKAN ENKRIPSI MERKLE–HELLMAN KNAPSACK DAN ADVANCED ENCRYPTION STANDARD (AES)

Oleh

AZIZ TRI NUGROHO

19102253

Aspek informasi perlu menerapkan keamanan agar tidak terjadinya kebocoran data. menurut BSSN (Badan Siber dan Sandi Negara), Letnan Jenderal TNI (Purn) Hinsa S. telah mengungkapkan, bahwa Serangan siber semakin banyak untuk tiap tahunya terutama pada tahun 2019 yang mengalami 182.034.863 kali serangan siber sedangkan pada tahun 2020 sudah mencapai 423.244.053 serangan. Hal ini tentunya menjadi sinyal bahwa keamanan digital harus ditingkatkan.Keamanan memilliki peranan penting dalam sebuah sistem. Salah satunya dalam mengamankan *database* atau basis data.Masalah tersebut menginspirasi peneliti untuk melakukan penelitian ini. Penelitian ini menggunakan enkripsi dua tahap menggunakan *merkle-hellman knapsack dan* AES 256 pada sistem yang dibangun dengan objek situs web berbasis *PHP Native* dan tersimpan di web hosting serta penggunaan MySQL sebagai tipe *database* dengan implementasi enkripsi menggunakan library OpenSSL.hasil pengujian ini menghasilkan enkripsi dua tahap *merkle-hellman knapsack dan* AES 256 I dapat di impementasikan pada kolom selain id_anggota yang ditunjukan dimana kolom selain id_anggota terenkripsi dan terjadi error Ketika melakukan SQL Injection pada situs web.

Kata Kunci : ***Enkripsi, Database,Merkle-Hellman Knapsack, AES, Openssl***