ABSTRAKSI

Tanda tangan digital adalah skema tanda tangan untuk dokumen digital atau dokumen perangkat lunak. Tanda tangan digital atau biasa disebut Tanda tangan digital merupakan salah satu layanan keamanan pada kriptografi yang memberikan jaminan kepada pihak penerima pesan. Jaminan yang diberikan yaitu bahwa pihak pengirim pesan adalah sesuai yang diinginkan penerima pesan, bukan pihak ketiga dan pesan yang terima masih asli. *Elliptic Curve* Tanda tangan digital *Algorithm* (ECDSA) adalah salah satu kriptografi asimetri Publik Kunci dengan algoritma yang mendasarkan keamanannya pada permasalahan matematis kurva eliptik. Tidak seperti logaritma diskrit biasa dan masalah faktorisasi integer, masalah logaritma diskrit kurva elips tidak mengenal algoritma perkalian substansial daripada algoritma biasa. Selain itu, untuk melakukan implementasi tanda tangan digital perlu adanya verifikasi dari setiap pelaku bisnis yang terkait terhadap *agreement* yang sudah dilakukan. *Block Chain* merupakan metode enkripsi yang akan membagi-bagi *plaintext* yang akan dikirimkan dengan ukuran tertentu untuk dilakukan enkripsi dengan kriptografi *Advanced Encryption St*dan*ard* (AES) sehingga semua pihak yang terlibat dalam bisnis tersebut dapat mengetahui ketika *agreement* sudah berada di lain pihak. Pada tugas akhir ini dibahas masalah implementasi tanda tangan digital pada senderan dokumen dengan proses otentikasi, integritas dan, verifikasi dari pesan yang dikirimkan dengan menggunakan bahasa pemrograman *java*.

Kata Kunci : tanda tangan digital, kurva eliptik, aes, block chain, otentikasi, integritas.