ABSTRACT

Digital Signature is a Signature scheme for digital documents or software documents. Signing digitals or so-called Signature digital is one of the security services in cryptography that provides assurance to the receiver message. The guarantee provided is that the sender of the message is what the receiver of the message wants, not the third party and the received message is still authentic. Elliptic Curve Tanda tangan digital Algorithm (ECDSA) is one of Public Key asymmetry cryptography with algorithms that base its security on the mathematical problems of elliptic curves. Unlike ordinary discrete logarithms and integer faktorization problems, the discrete logarithmic problem of the elliptic curve does not recognize substantive multiplication algorithms rather than the usual algorithm. In addition, to carry out the implementation of digital signature there is a need verification from every business related to the agreement that has been done. Block Chain is an encryption method that will divide the plaintext that will be sent to a certain size for enkripsi with Advanced Enkripsi Stdanard (AES) cryptography so that all parties involved in the business can know when the agreement is on the other side. In this final project discussed the problem of digital signature implementation on the delivery of documents with the process of authentication, integrity and, verification of messages sent by using java programming language.

Key Words : digital signatures, elliptic curves, aes, block chain, authentication, integrity.