Abstract

The process give kriptografi value for document or file, where this value depends on document and sender called by digital signature. So, for the different document or/and different sender have a different digital signature value.

In this Final Task,explaine how to give digital signature value for file executable JAR. *This digital signature use hash function for get a message digest value from file then will be encryted use digital signature algorithm, RSA.*

The hash function in this aplication is MAC algorithm. Where this algorithm will be concated one way hash function with the private key. The use of key in MD5 can produce secure message digest, because the attacker must be knew the private key for decrypt of message digest.

Two aplication will be developed in this final task. PC base and Mobile device base. The PC base aplication consist of upload, sign, verify and download file executable JAR *facility and Mobile device base only have a download and verify signature facility.*

This Final task, can showing signature success if file or key is valid. And signature failed if one from file or key or both is change.

Key words : *Digital Signature, MAC algotrithm, RSA algorithm*