ABSTRACT

The existing system on the aircraft black box is only limited as a storage media of all forms of flight activity. Aircraft black box does not yet have the ability to send information to other places as well as if there is information delivery process, aircraft black box does not yet have a security system. Data security is a very important part during the process of information exchange. Information that is exchanged may only be known and owned by the designated sender and receiver. The exchange process should not involve a man-in-the-middle attacker or a party not recognized by the sender or recipient. Therefore, to maintain the security, confidentiality and authentication of data, a cryptographic implementation is needed, which is the science and art to maintain the message security.

The stream cipher algorithm used is Dragon which belongs to the category of synchronous stream cipher in the process of encryption and decryption. Dragon is a candidate eStream Project algorithm, which can be implemented in software and hardware.

In this final project, designed a sound data security system on the cockpit voice recorder, by means of encryption, and then grant secure permissions to be decrypted by people who have the right to access of the data. The final results obtained from this research will be tested performance related to the process of encryption and decryption, avalanche effect, and data integrity. Will be obtained an algorithm that has a decent security system for cockpit voice recorder.

Keyword : Stream Cipher, dragon, cockpit voice recorder