

## ABSTRACT

The flight data recorder (FDR) is part of the black box to collect and record aircraft data , such as, altitude, data rate, data machine, air speed and other parameters. Black box is analyzed to know the cause of plane crash, so it can avoid from similar accidents in the future.

This research aims to design a data security system on Flight Data Recorder (FDR) until the condition is ready to be sent to the system on the ground during the flight. This is done to avoid data alteration and theft which is conducted by unauthorized parties or man in the middle during the transmission process takes place. .

The security system use cryptographic method. The cryptographic algorithms which implemented is the Variably Modified Permutation Composition (VMPC) stream cipher algorithm, which use symmetric keys on encryption and decryption process. This research analyzed in terms of encryption and decryption process, avalanche effect and the integrity of data. Follows to the resarch VMPC algorithm has avalanche effect as much as 44,19% for 100-parts and 44,11% for 250 -parts.

*Keyword: stream cipher, Variably Modified Permutation Composition, flight data recorder.*