A study of Bitmap File Format Encryption with DES Using Electronic Codebook and Cipher Block Chaining Modes of Operation

Marius Cristian URECHE

Abstract

The Data Encryption Standard (DES) specifies a Federal Information Processing Standard (FIPS) approved cryptographic algorithm. This article provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) "bitmap" file format images. It presents two modes of operation - Electronic Codebook (ECB) and Cipher Block Chaining (CBC) - and shows the main characteristics of the software implementation using Java Cryptography Extension (JCE).