File Encryption with AES

Antonino Tan-Marcello

Overview

File encryption is the process of altering file data into unintelligible, meaningless data. Process must be reversible in order for decryption to work.

File can still be read by the computer, just is not meaningful / does not make any sense.

File decryption is converting the unintelligible data back into its original form, leaving no trace of altercations.

Applications

- Protecting information on an unattended or shared computer (school, work, home, etc).
- If device is lost or stolen, password somehow known, data will still be protected.
- Preventing information stolen by hackers (firewall breach / virus, etc).
- Storing files in a database system / cloud service.

Methodology

- Read target file’s contents as bytes.
- Run those contents through an encryption algorithm (AES at 128-bits) and retrieve new data.
- Delete previous file and write new, encrypted data to a file in the same directory to take its place.
- Using a symmetric key; decryption key is identical.

Two versions of program

1st Version:

- Uses Java’s crypto libraries, Cipher and CipherOutputStream
- Encrypts and decrypts any file type

2nd Version:

- Implements AES from scratch
- Encrypts and decrypts text files

Demonstration