

Abstract

Data storage on computer system needs an effort to keep data secrecy and safety. One of the alternatives is to secure data using cryptography. Cryptography is a discipline that studies about how to keep a data secretly to avoid unauthorized access. FAT file system is very often used in Windows operating-system and can be accessed across many other platforms. At Windows driver level, one layer can be added to secure data on physical media transparently (background-operated). This layer is implemented as non– plug & play device driver on Windows platform.

The reason of using hybrid cryptosystem is to ensure powerful [enough] data security and simplify key-management so that users will conveniently secure their respective data. This hybrid cryptosystem consists of asymmetric cryptograph with RSA algorithm, and symmetric cryptograph with RC6 algorithm. Key length can be adjusted to measure up to computer hardware specification. This adjustment is needed to maintain seamlessly (less user awareness) data encryption/decryption and avoid significant computer performance degradation.

Keywords: windows driver, hybrid cryptosystem, RC6, RSA, FAT file system.