Cryptotool: A Secure Data Storage Software

Yildiran Yilmaz * and Basel Halak*[+]

*Electronics and Computer Sciences, Southampton University

[+]Institute for Learning Innovation and Development

Abstract. Confidentiality and personal information security has always been a big problem in the world of cyberspace. There exist a number of solutions which are based on encryption methods, however such tools are typically file-format specific and/or do not give sufficient control to the user to choose the cryptographic algorithm. In this study, a private key encryption software is presented; it supports two main security features. The first is encryption that supports all file formats and several encryption algorithms such as AES, 3DES and RC2. The second feature is integrity using Hash functions, the latter ensures that unauthorised modifications of stored files can be detected. In addition, the tool has an easy-to-use interface which allows the user to choose from several encryption algorithms and define the encryption key. The software also allows the user to combine a number of cryptographic algorithms to build stronger ciphers for more enhanced security. In addition, the Crypto Tool can be used as an education tool as it supprts a number of classic ciphers and provides opportunity to compare different cryptographic encrypting techniques.