File Encryption on Storage Devices
By: Antonino Tan-Marcello

A hard drive is a piece of computer hardware that has the ability to hold very important documents, sensitive information and other files. Due to this, its is important that these files on one's hard drive is secure and not accessible to unauthorized individuals. To solve this issue, a person could put a password on there computer, so nobody could get access to their files. However, what if an external hard drive or USB thumb drive is lost or stolen? USB thumb drives are not usually password protected. Also, if a computer falls into the wrong hands, someone with the proper equipment could access the data directly. Taking all this into account, a best approach someone could take would to encrypt the files on their storages, or specifically encrypt certain files that need to always be confidential. That way, if someone wanted to view these files, they would need to be decrypted first. Otherwise, they are completely indecipherable. This method also works if an attacker, somehow has remote access to one's system. They can potentially see that there is something on the storage drives, but they are encrypted and without the proper encryption key, information cannot be obtained. A specific set of algorithms could be utilized to encrypt files. These algorithms would implement AES at 128 bits, an advanced and secure encryption system. I plan to utilize this encryption system and use it to encrypt specific data stored on a hard drive (i.e documents). This encryption system would convert given data, known as plaintext into ilegible code, known as ciphertext, using the encryption system's cipher. In order to decrypt these files an encryption key would be required, which is accessible with a set password, and the data then would be converted back into its original, plaintext form. An individual could use this method to encrypt their files when not in use and decrypt them only when they need to access them. Nowadays, as well as in the past, computer security is an issue due to hackers trying to get access to sensitive information. It is always best to take precautions and I believe that encrypting files on any form of storage is an effective way to prevent data theft.