Titan Newman

Security Algorithms

3/16/2022

# Project Proposal

My project will be a Microsoft Windows executable application that will take in a file and encrypt it with AES (128 bits). The application will not implement authentication as the files will not be leaving the local computer, it will randomly create a system key (i.e. a symmetric key), and it will enable the file to be decrypted based on a key given by the user. This means that the application will take in a set file, apply the AES encryption standard, and save it. We can then choose to either decrypt the file (based on its key) or leave it as is.