Required plugins: PyCrypto

Python Version Used: 2.7

Usage:

1. Run ‘Hashing-DaviesMeyerMerkleDamgardConstruction.py
2. Enter ‘g’ to start hash generation process
3. Enter the password that will be used for the hashing process. It must be 8 bits so that it may be used to encode the first 8-bit block of the message in DES. E.g. Pass= ‘password’
4. Hashing process will run and generate a hash code. E.g. ‘94ae67befce6d213’
5. Program then returns to main menu, type ‘m’ to begin MAC check
6. Enter the password that has been agreed upon for generating hashed. E.g. ‘password’
7. Enter the hash that was supplied along with the message. E.g. ‘94ae67befce6d213’
8. Program will then run the hashing function with the password supplied and message and return ‘Success’ if the supplied hash matches up with the generated one, or ‘Failure’ if this is not the case.