The following scripts demonstrate the process of Python cryptography and hashing and how to use ‘Crypt’ and ‘hashlib’ module

‘Crypt’ - a function to check Unix passwords. This module implements an interface to the crypt(3) routine, which is a one-way hash function based upon a modified DES algorithm. Possible uses include storing hashed passwords so you can check passwords without storing the actual password, or attempting to crack Unix passwords with a dictionary. Notice that the behavior of this module depends on the actual implementation of the crypt(3) routine in the running system. Therefore, any extensions available on the current implementation will also be available on this module.

‘hashlib’ – a function module for generating secure hashes and message digests. This module implements a common interface to many different secure hash and message digest algorithms. Included are the FIPS secure hash algorithms SHA1, SHA224, SHA256, SHA384, and SHA512 (defined in FIPS 180-2) as well as RSA’s MD5 algorithm (defined in Internet RFC 1321). The terms “secure hash” and “message digest” are interchangeable. Older algorithms were called message digests. The modern term is secure hash.

Also demonstrate is how to write Hash algorithms.

Compiled and presented by Vakindu Philliam.