Assignment = 5

Name = Muhammad Shaheer.
Roll No = 20p-0480.
Subject = Information Security.

Title:- Merkle Damgard Construction

Merkle damgard construction is a technique used to construct a hash function from a collision resistant hash function

It is a method to create a hash function that is both collision-resistant and second pre-image resistant.
The basic idea is to use the collision resistant hash function to produce a hash value for a portion of the input message and then use the second pre-image resistant hash function to produce a hash value for the remaining portion of the input message.

Partial Example:-
Bit coin hash function, Ethernet hash function, SHA-3, they all uses a common hash function based on this algorithm.

Code:- High level outline of merkle construction.

Python Code:-

```
Import hashlib
def merkle-damgard(message):
    # divide input into fixed size prefix
    and suffix

    prefix = message[:32]

    suffix = message[32:]

# use Collision-resistant hash function
    prefix-hash = hashlib.sha256(prefix.
                  encode()).hex.digit()

# use pre-image hash function

    suffix.hash = hashlib.512(suffix.encode())
                  .hex.digit()

    merkle_hash = prefix-hash + suffix hash.
    return merkle_hash.
```

NOTE:- This is just high Level implementation of merkle damgard construction.