Izaan
P20-0613

The Merkle-Damgard Construction is widely used technique in crypotography for building cryptographic hash function. Two inventors are Ralph and Ivan. This construction is used to turn compression function into hash function and it forms basis for many hash function like MD5, SHA1 ans SH 2.

The construction works by taking a message of arbitary length and breaking it into fixed size block. These block are processed by compression function. Then compression function takes both the current and output of previous compression and produces a fixed size output. The final output is the hash of entire message.

```
Import hashlib
md5_hash = hashlib.md5()
message = "Hello, world!"
md5_hash.update(message.encode(utf,8)
hash_result = md5_hash.hexidigest( )
print ("MD5 Hash, result())
```

One of vulnerabitis of MD construction is its susceptibility to length extension attacks. means attacker can take the hash of message and easily append additional data without knowing the orignal message