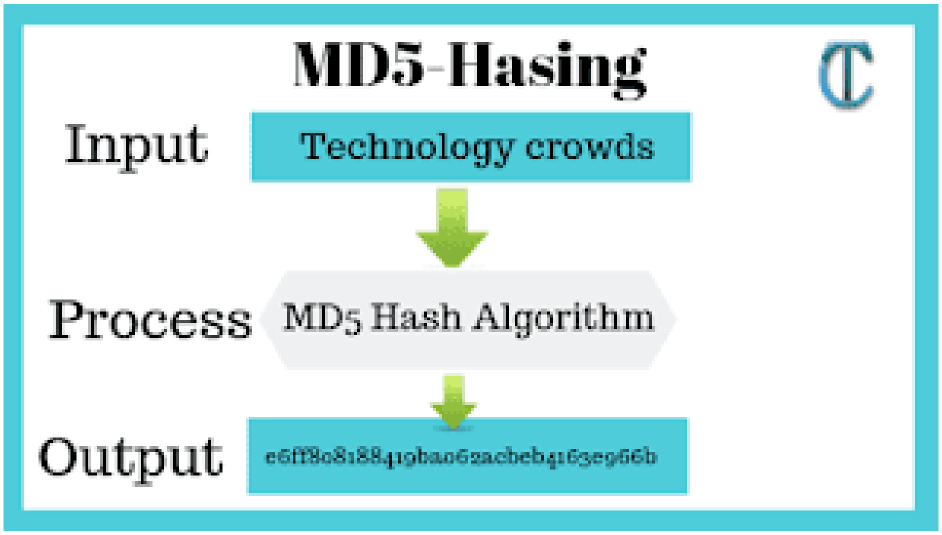
Introduction to MD5 Algorithm and SHA

- There are various algorithms used to protect the messages in communication. Two of them are MD5 and SHA.
- The MD5 is considered as cryptographically broken and cause collisions. On the other hand, SHA refers to a family of cryptographic hash functions developed by the National Institute of Standards and Technology (NIST).
- Overall, **SHA has versions such as SHA 256 and SHA 512, which are more secure than MD5.**

What is MD5

MD5 message-digest algorithm is the 5th version of the Message-Digest Algorithm developed by Ron Rivest to produce a 128-bit message digest. MD5 is quite fast than other versions of the message digest, which takes the plain text of 512-bit blocks, which is further divided into 16 blocks, each of 32 bit and produces the 128-bit message digest, which is a set of four blocks, each of 32 bits. MD5 produces the message digest through **five steps, i.e. padding, append length, dividing the input into 512-bit blocks, initialising chaining variables a process blocks and 4 rounds, and using different constant it in each iteration.**



Use of MD5 Algorithm

It was developed with the main motive of security as it takes an input of any size and produces an output if a 128-bit hash value. To be considered cryptographically secure, MD5 should meet two requirements:

1. It is impossible to generate two inputs that cannot produce the same hash function.
2. It is impossible to generate a message having the same hash value.

Initially, MD5 was developed to store one way hash of a password, and some file servers also provide pre-computed MD5 checksum of a file so that the user can compare the checksum of the downloaded file to it. Most Unix based Operating Systems include MD5 checksum utilities in their distribution packages.

What is SHA

SHA stands for **Secure Hash Algorithm**. National Institute of Standard and Technology published various versions of SHA. Some of them are as follows.

SHA-0: It is an original version of the 160-bit hash function. Later, SHA -1 replaced it.

SHA-1: It is a 160-bit hash function. It was designed as a part of the Digital Signature Algorithm. However, after 2010, it was not in use.

SHA-2: It consists of two equivalent hash functions with different block sizes. They are SHA 256 and SHA 512. SHA-256 uses 32-bit words, while SHA-523 uses 64-bit words. Moreover, there are truncated versions called SHA-224, SHA-384, SHA-512/224 and SHA 512/256.
SHA-3: Internal structure of SHA-2 is different from the rest of the SHA family. Additionally, it supports the same hash lengths as SHA-2.

CONCLUSION:
The **main difference** between MD5 and SHA is that **MD5 is not cryptographically stronger and not secure while SHA is more cryptographically stronger and secure with versions such as SHA 256 and SHA 512.**

TASK:

What is the Difference Between MD5 and SHA