**4 — SHA-256**

A cryptographic hash function is a special type of function that **takes an input string** of a given length and converts it into an **alphanumeric string of fixed length**. In the case of Bitcoin, a **“Message”** is inputted, and a hash function, known as **SHA-256** (Secure Hashing Algorithm 256), gives an output known as a **“Hash”** or **“Message Digest”**. This means that however long the string of data (limit of 2²⁵⁶- 1 bits), the **output will always be 256-bits in length**. The process of hashing is **not a method of encryption** as it is only a **one- way process** and therefore **cannot be reversed** (decrypted). By running multiple outputs through SHA-256, we can see how different the output becomes, even when only changing a single character in the message. We can also see that despite having an input of longer length, the output length is the exact same (table 5.1). SHA-256 is also **deterministic**, meaning given the same input, the output will always remain the same.