Cryptography

Cryptography is **technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it**.

Thus preventing unauthorized access to information.

The prefix “crypt” means “hidden” and suffix graphy means “writing”.

Understanding SHA256 Hash

Sha256 is a fingerprint for a digital document as a man have unique fingerprint. It is unique.

The algorithm behind sha256 was developed by NSA (National Security Agency)

Code of sha256 is opensource

Sha stands for **Secure Hash Algorithm** and 256 for no of bits it takes up for memory

Sha consists of 64 characters includes letters and digits because it is hexadecimal (16) hash (0-9, A-F) each character in the hash takes 4 bits.

This algorithm works for any digital things, not only for docs, pdf …

The same hash will be produced for the data if the data is removed and placed again.

Ex hello world: b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

After del and again input of same data

b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

if change a small thing in the data the hash will change entirely and i.e is called avalanche effect

ex: hello world!

Hash- 7509e5bda0c762d2bac7f90d758b5b2263fa01ccbc542ab5e3df163be08e6ca9

Doesn’t matter how much big is the data the hash will be 64 chars and 256 bits only.

The 5 requirements for hash algorithms

One-way

It means we can’t get data from based on hash.

Deterministic

Same hash for the same data like above example.

Fast computation

The avalanche effect

A tiny change in the data will effect on entire change of hash

Avalanche effect it is important in the application of blockchain.

Must withstand collisions

The collisions among the large amount of data like pigeon hole principle.

Source: on the secure hash algorithm family

<https://www.staff.science.uu.nl/~tel00101/liter/Books/CrypCont.pdf>