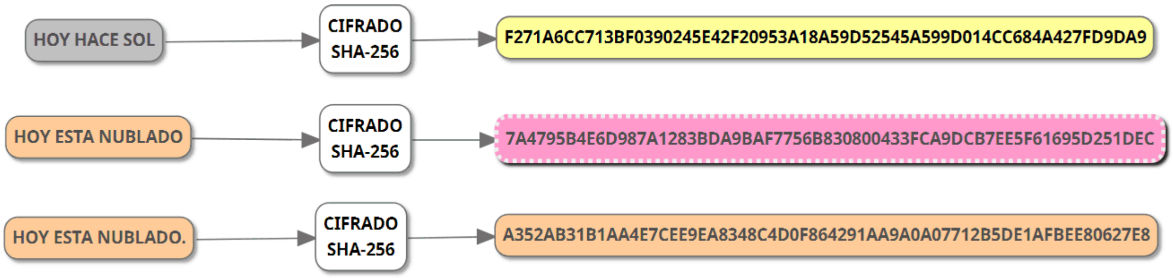
SHA-256

SHA-256 was first introduced in 2001, making it the newest algorithm out of the 3 I am using. It was published by the national security agency, as a successor to SHA-1. SHA-1 was another algorithm made by the national security agency which was published in 1995. SHA-256 is a hash function, this means the target data is scrambled to an unreadable state. This type of function is mainly used to verify data and files, the correct hash value can be published and the consumers of a software can compare the hash value they get to provide them with a sense of security knowing they have the correct download and not malware. SHA-256 is the most secure hashing function on the market currently. SHA-256 is also used for things like SSL handshakes, digital signature verification, and password hashing. SHA-256 has a single requirement, this requires the target object to be a multiple of 512, you can achieve this using padding. Padding is the process of adding bits to your target object, so it meets the requirements. SHA-256 takes the 512 block and breaks it into 16, 32-bit blocks then run these blocks into 4 rounds of 20 iterations meaning each block goes through 80 rounds of scrambling.


HOY HACE SOL
CIFRADO SHA-256
F271A6CC713BF0390245E42F20953A18A59D52545A599D014CC684A427FD9DA9
HOY ESTA NUBLADO
CIFRADO SHA-256
7A4795B4E6D987A1283BDA9BAF7756B830800433FCA9DCB7EE5F61695D251DEC
HOY ESTA NUBLADO.
CIFRADO SHA-256
A352AB31B1AA4E7CEE9EA8348C4D0F864291AA9A0A07712B5DE1AFBEE80627E8

REFERENCES

https://www.n-able.com/blog/sha-256-encryption

https://www.youtube.com/watch?v=nduoUEHrK_4

https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

https://academy.bit2me.com/en/sha256-bitcoin-algorithm/