Why use HMAC-SHA256?

I decided to use HMAC-SHA256 because it takes SHA 256 out of the public domain, in that the generator of the hash needs to have the secret key. Whereas with SHA anyone can derive the hash. This can cause problems. For example, in the context of my project I have a database holding the hash values of files. If the database is compromised, the hash values can be replaced by the hash value of the maliciously altered file. Upon checking there would be no detection of file alteration.

SHA 256

Function of up to 2^64 input bits

Broken into 512-bit blocks.

256-bit output.

Problems: secret key storage.

Talk about that…