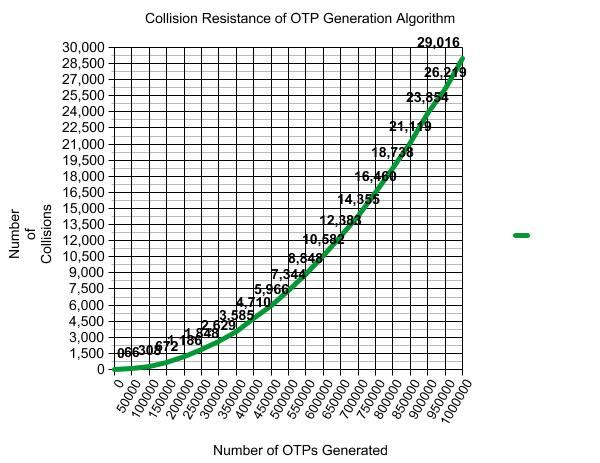
Andrew Montgomery and Ulysess S

Assignment #2

Collision Resistance Analysis



The program initially shows very little collisions per OTP generated, but as the number of OTP’s generated increases, the number of collisions per OTP generated also increase. The result was about a 0.1% collision rate at 50 thousand OTP’s generated, and a 3% collision rate at 1 million OTP’s generated. This still clearly shows the strength of sha256 for generating unique hashes, and the collisions are a result of only choosing the six least significant digits of the hash. A potential way to increase the collision resistance of the OTP generation algorithm would be to randomly select six digits from the entirety of the hash generated by the sha256 algorithm, which would increase variability and potentially result in less collisions.