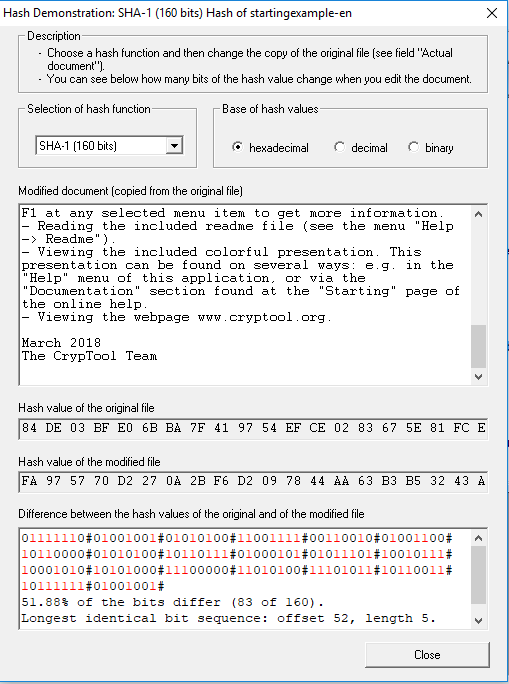
Matthew Austin

Cryptology

Anwar

November 2016

Crypto Hashes

* 2e.) A non-keyed hash produces an output that depends only on the input data. A keyed hash produces an output that depends both on the input data, and a key. If Ubuntu Linux is hosted on a mirror site for many users to download a non keyed hash would be used for verification. The hash would be used for verification in Alice and Bob’s case would be keyed hash procedures. There are no known ways faster than brute force as well as random chance to find the key used and find the correct output.
* 3c.) 51.88% of the bits differ. This is called collision resistance. The avalanche or domino effect exhibits the same effect.
* 
* 4.) is attached in the zip file.