



QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

Guide to the Secure Hash Standard

This Standard specifies secure hash algorithms, SHA-1, SHA-224, SHA-256, SHA-384, SHA512, SHA-512/224 and SHA-512/256. All of the algorithms are iterative, one-way hash functions that can process a message to produce a condensed representation called a message digest. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and message authentication codes, and in the generation of random numbers or bits.

Included in this ZIP file are:

- Intro Page.pdf
- Terms and Conditions.pdf
- Secure Hash Standard.pdf

Copyright © 2003-2012 IT Business Edge. All rights reserved.
<http://www.itbusinessedge.com>