Secure hash algorithm (SHA):

In recent years, the most widely used hash function has been the Secure hash algorithm. Because virtually every other widely used hash-function had been found to have substantial cryptanalytic weakness. SHA was more or less the last remaining standardized hash algorithm developed by the National Institute of standards and Technology when weakness were discovered in SHA now known as SHA-0 a revised version was issued and is reffered to as SHA-1

SHA-1 produces a 160 bit hash value or message digest from the inputted data, which resembles the hash value of the MD5 algorithm. The message digest is usually then rendered as a hexadecimal number which is 40 digits long It uses 80 rounds of cryptographic operations to encrypt and Secure a data object.

Some of the protocol that uses SHA 1 include,

- Transport layer Security
- Secure Sockets layer
- Pretty Good privacy
- Secure Shell
- Internet protocol Security