15.4. sha — SHA-1 message digest algorithm¶

Deprecated since version 2.5: Use the `hashlib` module instead.

This module implements the interface to NIST's secure hash algorithm, known as SHA-1. SHA-1 is an improved version of the original SHA hash algorithm. It is used in the same way as the `md5` module: use `new()` to create an sha object, then feed this object with arbitrary strings using the `update()` method, and at any point you can ask it for the *digest* of the concatenation of the strings fed to it so far. SHA-1 digests are 160 bits instead of MD5's 128 bits.

`sha.new`([*string*])¶

Return a new sha object. If *string* is present, the method call `update(string)` is made.

The following values are provided as constants in the module and as attributes of the sha objects returned by `new()`:

`sha.blocksize`¶

Size of the blocks fed into the hash function; this is always `1`. This size is used to allow an arbitrary string to be hashed.

`sha.digest_size`¶

The size of the resulting digest in bytes. This is always `20`.

An sha object has the same methods as md5 objects:

`sha.update`(*arg*)¶

Update the sha object with the string *arg*. Repeated calls are equivalent to a single call with the concatenation of all the arguments: `m.update(a); m.update(b)` is equivalent to `m.update(a+b)`.

`sha.digest`()¶

Return the digest of the strings passed to the `update()` method so far. This is a 20-byte string which may contain non-ASCII characters, including null bytes.

`sha.hexdigest`()¶

Like `digest()` except the digest is returned as a string of length 40, containing only hexadecimal digits. This may be used to exchange the value safely in email or other non-binary environments.

`sha.copy`()¶

Return a copy ("clone") of the sha object. This can be used to efficiently compute the digests of strings that share a common initial substring.

See also

Secure Hash Standard

The Secure Hash Algorithm is defined by NIST document FIPS PUB 180-2: Secure Hash Standard, published in August 2002.

Cryptographic Toolkit (Secure Hashing)

Links from NIST to various information on secure hashing.

Previous topic

15.3. `md5` — MD5 message digest algorithm

Next topic

16. Generic Operating System Services

This Page

- Show Source