:mod:`hmac` --- Keyed-Hashing for Message Authentication

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst`, line 1); *backlink*

Unknown interpreted text role "mod".

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst`, line 4)

Unknown directive type "module".

```
.. module:: hmac
   :synopsis: Keyed-Hashing for Message Authentication (HMAC) implementation
```

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst`, line 7)

Unknown directive type "moduleauthor".

```
.. moduleauthor:: Gerhard HÃ¤ring <ghaering@users.sourceforge.net>
```

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst`, line 8)

Unknown directive type "sectionauthor".

```
.. sectionauthor:: Gerhard HÃ¤ring <ghaering@users.sourceforge.net>
```

Source code: :source:`Lib/hmac.py`

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst`, line 10); *backlink*

Unknown interpreted text role "source".

This module implements the HMAC algorithm as described by RFC 2104.

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst`, line 17)

Unknown directive type "function".

```
.. function:: new(key, msg=None, digestmod='')

   Return a new hmac object.  *key* is a bytes or bytearray object giving the
   secret key.  If *msg* is present, the method call ``update(msg)`` is made.
   *digestmod* is the digest name, digest constructor or module for the HMAC
   object to use.  It may be any name suitable to :func:`hashlib.new`.
   Despite its argument position, it is required.

   .. versionchanged:: 3.4
      Parameter *key* can be a bytes or bytearray object.
      Parameter *msg* can be of any type supported by :mod:`hashlib`.
      Parameter *digestmod* can be the name of a hash algorithm.

   .. deprecated-removed:: 3.4 3.8
      MD5 as implicit default digest for *digestmod* is deprecated.
      The digestmod parameter is now required.  Pass it as a keyword
      argument to avoid awkwardness when you do not have an initial msg.
```

**System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 36)

Unknown directive type "function".

```
.. function:: digest(key, msg, digest)

   Return digest of *msg* for given secret *key* and *digest*. The
   function is equivalent to ``HMAC(key, msg, digest).digest()``, but
   uses an optimized C or inline implementation, which is faster for messages
   that fit into memory. The parameters *key*, *msg*, and *digest* have
   the same meaning as in :func:`~hmac.new`.

   CPython implementation detail, the optimized C implementation is only used
   when *digest* is a string and name of a digest algorithm, which is
   supported by OpenSSL.

   .. versionadded:: 3.7
```

An HMAC object has the following methods:

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 53)

Unknown directive type "method".

```
.. method:: HMAC.update(msg)

   Update the hmac object with *msg*.  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)``.

   .. versionchanged:: 3.4
      Parameter *msg* can be of any type supported by :mod:`hashlib`.
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 63)

Unknown directive type "method".

```
.. method:: HMAC.digest()

   Return the digest of the bytes passed to the :meth:`update` method so far.
   This bytes object will be the same length as the *digest_size* of the digest
   given to the constructor.  It may contain non-ASCII bytes, including NUL
   bytes.

   .. warning::

      When comparing the output of :meth:`digest` to an externally-supplied
      digest during a verification routine, it is recommended to use the
      :func:`compare_digest` function instead of the ``==`` operator
      to reduce the vulnerability to timing attacks.
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 78)

Unknown directive type "method".

```
.. method:: HMAC.hexdigest()

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

   .. warning::

      When comparing the output of :meth:`hexdigest` to an externally-supplied
      digest during a verification routine, it is recommended to use the
      :func:`compare_digest` function instead of the ``==`` operator
      to reduce the vulnerability to timing attacks.
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 92)

Unknown directive type "method".

```
.. method:: HMAC.copy()

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

A hash object has the following attributes:

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 100)

Unknown directive type "attribute".

```
.. attribute:: HMAC.digest_size

   The size of the resulting HMAC digest in bytes.
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 104)

Unknown directive type "attribute".

```
.. attribute:: HMAC.block_size

   The internal block size of the hash algorithm in bytes.

   .. versionadded:: 3.4
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 110)

Unknown directive type "attribute".

```
.. attribute:: HMAC.name

   The canonical name of this HMAC, always lowercase, e.g. ``hmac-md5``.

   .. versionadded:: 3.4
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 117)

Unknown directive type "deprecated".

```
.. deprecated:: 3.9

   The undocumented attributes ``HMAC.digest_cons``, ``HMAC.inner``, and
   ``HMAC.outer`` are internal implementation details and will be removed in
   Python 3.10.
```

This module also provides the following helper function:

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst, line 125)

Unknown directive type "function".

```
.. function:: compare_digest(a, b)

   Return ``a == b``.  This function uses an approach designed to prevent
   timing analysis by avoiding content-based short circuiting behaviour,
   making it appropriate for cryptography.  *a* and *b* must both be of the
   same type: either :class:`str` (ASCII only, as e.g. returned by
   :meth:`HMAC.hexdigest`), or a :term:`bytes-like object`.
   .. note::

      If *a* and *b* are of different lengths, or if an error occurs,
      a timing attack could theoretically reveal information about the
      types and lengths of *a* and *b*â€”but not their values.

   .. versionadded:: 3.3

   .. versionchanged:: 3.10

      The function uses OpenSSL's ``CRYPTO_memcmp()`` internally when
      available.
```

System Message: ERROR/3 (`D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]hmac.rst`, line 147)

Unknown directive type "seealso".

```
.. seealso::

   Module :mod:`hashlib`
      The Python module providing secure hash functions.
```