:mod:`secrets` --- Generate secure random numbers for managing secrets

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

Unknown directive type "module".

```
.. module:: secrets
   :synopsis: Generate secure random numbers for managing secrets.
```

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

Unknown directive type "moduleauthor".

```
.. moduleauthor:: Steven D'Aprano <steve+python@pearwood.info>
```

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

Unknown directive type "sectionauthor".

```
.. sectionauthor:: Steven D'Aprano <steve+python@pearwood.info>
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 9)

Unknown directive type "versionadded".

```
.. versionadded:: 3.6
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 11)

Unknown directive type "testsetup".

```
.. testsetup::

   from secrets import *
   __name__ = '<doctest>'
```

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

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 16); *backlink*

Unknown interpreted text role "source".

The :mod:`secrets` module is used for generating cryptographically strong random numbers suitable for managing data such as passwords, account authentication, security tokens, and related secrets.

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 20); *backlink*

Unknown interpreted text role "mod".

In particular, :mod:`secrets` should be used in preference to the default pseudo-random number generator in the :mod:`random` module, which is designed for modelling and simulation, not security or cryptography.

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 24); *backlink*

Unknown interpreted text role "mod".

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 24); *backlink*

Unknown interpreted text role "mod".

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 28)

Unknown directive type "seealso".

```
.. seealso::

   :pep:`506`
```

Random numbers

The :mod:`secrets` module provides access to the most secure source of randomness that your operating system provides.

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

Unknown interpreted text role "mod".

A class for generating random numbers using the highest-quality sources provided by the operating system. See :class:`random.SystemRandom` for additional details.

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 41); *backlink*

Unknown interpreted text role "class".

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 45)

Unknown directive type "function".

```
.. function:: choice(sequence)

   Return a randomly-chosen element from a non-empty sequence.
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 49)

Unknown directive type "function".

```
.. function:: randbelow(n)

   Return a random int in the range [0, *n*).
```

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

Unknown directive type "function".

```
.. function:: randbits(k)

   Return an int with *k* random bits.
```

Generating tokens

The :mod:`secrets` module provides functions for generating secure tokens, suitable for applications such as password resets, hard-to-guess URLs, and similar.

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 61); *backlink*

Unknown interpreted text role "mod".

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 65)

Unknown directive type "function".

```
.. function:: token_bytes([nbytes=None])

   Return a random byte string containing *nbytes* number of bytes.
   If *nbytes* is ``None`` or not supplied, a reasonable default is
   used.

   .. doctest::

      >>> token_bytes(16)  #doctest:+SKIP
      b'\xebr\x17D*t\xae\xd4\xe3S\xb6\xe2\xebP1\x8b'
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 77)

Unknown directive type "function".

```
.. function:: token_hex([nbytes=None])

   Return a random text string, in hexadecimal.  The string has *nbytes*
   random bytes, each byte converted to two hex digits.  If *nbytes* is
   ``None`` or not supplied, a reasonable default is used.

   .. doctest::

      >>> token_hex(16)  #doctest:+SKIP
      'f9bf78b9a18ce6d46a0cd2b0b86df9da'
```

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 88)

Unknown directive type "function".

```
.. function:: token_urlsafe([nbytes=None])

   Return a random URL-safe text string, containing *nbytes* random
   bytes.  The text is Base64 encoded, so on average each byte results
   in approximately 1.3 characters.  If *nbytes* is ``None`` or not
   supplied, a reasonable default is used.

   .. doctest::

      >>> token_urlsafe(16)  #doctest:+SKIP
      'Drmhze6EPcv0fN_81Bj-nA'
```

How many bytes should tokens use?

To be secure against brute-force attacks, tokens need to have sufficient randomness. Unfortunately, what is considered sufficient will necessarily increase as computers get more powerful and able to make more guesses in a shorter period. As of 2015, it is believed that 32 bytes (256 bits) of randomness is sufficient for the typical use-case expected for the :mod:`secrets` module.

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

Unknown interpreted text role "mod".

For those who want to manage their own token length, you can explicitly specify how much randomness is used for tokens by giving an :class:`int` argument to the various `token_*` functions. That argument is taken as the number of bytes of randomness to use.

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 112); *backlink*

Unknown interpreted text role "class".

Otherwise, if no argument is provided, or if the argument is `None`, the `token_*` functions will use a reasonable default instead.

Note

That default is subject to change at any time, including during maintenance releases.

Other functions

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 129)

Unknown directive type "function".

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

   Return ``True`` if strings *a* and *b* are equal, otherwise ``False``,
   in such a way as to reduce the risk of
   `timing attacks <https://codahale.com/a-lesson-in-timing-attacks/>`_.
   See :func:`hmac.compare_digest` for additional details.
```

Recipes and best practices

This section shows recipes and best practices for using :mod:`secrets` to manage a basic level of security.

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 140); *backlink*

Unknown interpreted text role "mod".

Generate an eight-character alphanumeric password:

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 145)

Unknown directive type "testcode".

```
.. testcode::

   import string
   import secrets
   alphabet = string.ascii_letters + string.digits
   password = ''.join(secrets.choice(alphabet) for i in range(8))
```

Note

Applications should not store passwords in a recoverable format, whether plain text or encrypted. They should be salted and hashed using a cryptographically-strong one-way (irreversible) hash function.

Generate a ten-character alphanumeric password with at least one lowercase character, at least one uppercase character, and at least three digits:

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 165)

Unknown directive type "testcode".

```
.. testcode::

   import string
   import secrets
   alphabet = string.ascii_letters + string.digits
   while True:
       password = ''.join(secrets.choice(alphabet) for i in range(10))
       if (any(c.islower() for c in password)
               and any(c.isupper() for c in password)
               and sum(c.isdigit() for c in password) >= 3):
           break
```

Generate an XKCD-style passphrase:

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 180)

Unknown directive type "testcode".

```
.. testcode::

   import secrets
   # On standard Linux systems, use a convenient dictionary file.
   # Other platforms may need to provide their own word-list.
   with open('/usr/share/dict/words') as f:
       words = [word.strip() for word in f]
       password = ' '.join(secrets.choice(words) for i in range(4))
```

Generate a hard-to-guess temporary URL containing a security token suitable for password recovery applications:

System Message: ERROR/3 (D:\onboarding-resources\sample-onboarding-resources\cpython-main\Doc\library\[cpython-main][Doc][library]secrets.rst, line 193)

Unknown directive type "testcode".

```
.. testcode::

   import secrets
   url = 'https://mydomain.com/reset=' + secrets.token_urlsafe()
```