Модуль hmac в Python, хеширование сообщений по ключу

Стандартная библиотека Python3. / Модуль hmac в Python, хеширование сообщений по ключу

Подписывание сообщении и файлов общим секретным ключом

Модуль hmac реализует алгоритм HMAC - хеширование по ключу для аутентификации сообщений, как описано в RFC 2104.

Алгоритм HMAC можно использовать для проверки целостности информации, передаваемой между приложениями или хранящейся в потенциально уязвимом месте.

Основная идея заключается в создании криптографического хеша реальных данных в сочетании с общим секретным ключом. Полученный хеш может затем использоваться для проверки переданного или сохраненного сообщения, чтобы определить уровень доверия, без передачи секретного ключа.

Примеры использования:

Пример подписи URL секретным ключом.

```
>>> import hashlib, hmac
>>> secret = 'mysecret'.encode()
>>> url = 'https://docs-python.ru/standart-library/'.encode()
>>> signing = hmac.new(secret, url, hashlib.sha256)
>>> signing.digest()
# b'\xcf\xa4C\x1e\xd2,\x1eE\xedVW\x16\xd2\x86YdjJ\xbe\x83>;y \x94\xa3B-#\xa7\xe5M'
>>> signing.hexdigest()
# 'cfa4431ed22c1e45ed565716d28659646a4abe833e3b792094a3422d23a7e54d'
>>> signing.digest_size
# 32
>>> signing.block_size
# 64
>>> signing.name
# 'hmac-sha256'
```

Пример подписи бинарного файла python3 секретным ключом.

```
import hashlib, hmac

secret_key = 'secret-shared-key'
```

```python
digest_maker = hmac.new(secret_key.encode(), digestmod='sha256')

with open('/usr/bin/python3', 'rb') as fp:
    while True:
        block = fp.read(1024)
        if not block:
            break
        digest_maker.update(block)

digest = digest_maker.hexdigest()
name = digest_maker.name
print(digest)
print(name)

# 301755e52acc33e777dce1149b6b781470e6212d9ec476323a26704756c1763d
# hmac-sha256
```

Содержание раздела:

Вверх