

توابع درهم سازی که توسط hashlib پشتیبانی میشود دو مدل هست :

1 . مدل اول را algorithms_available، شامل تمام الگوریتم های درهم سازی هست که در مفسر پایتون شما وجود داره.

2 . مدل دوم را algorithms_guaranteed، یعنی الگوریتم هایی که به طور قطعی توسط پایتون پشتیبانی میشه.

تابع ها :

md5()

sha1()

sha224()

sha256()

sha384()

sha512()

blake2b()

blake2s()

sha3_224

sha3_256

sha3_384

sha3_512

shake_128

shake_256

- آشنایی با متد های update() و digest()

```
1.py - C:/Users/Asus/Desktop/hashlib/1.py (3.9.1)
File Edit Format Run Options Window Help

import hashlib
a=hashlib.md5()
a.update(b'python')
print(a.digest())

IDLE Shell 3.9.1
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:/Users/Asus/Desktop/hashlib/1.py =====
b'#\xee\xeb\xbd\xd2k\xfc~\xe9\xa3\xb7U\xdd'
>>>
```

Update() = این متد برای اضافه کردن مقدار هست

Digest() = دایجست, مقدار پاس داده شده رو در قالب Byte Object بر می گرداند

- آشنایی با متد hexdigest()

```
2.py - C:/Users/Asus/Desktop/hashlib/2.py (3.9.1)
File Edit Format Run Options Window Help

import hashlib
a=hashlib.md5()
a.update(b'python')
print(a.digest())

IDLE Shell 3.9.1
File Edit Shell Debug Options Window Help
Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:/Users/Asus/Desktop/hashlib/2.py =====
b'#\xee\xeb\xbd\xd2k\xfc~\xe9\xa3\xb7U\xdd'
>>>
```

Hexdigest() = مثل متد digest هست با این تفاوت که خروجی رشته ای در مبنای هگزادسیمال است

* copy() = یک کپی از hash object میگیره.

به مثال زیر توجه کنید (استفاده از sha256)

```
3.py - C:/Users/Asus/Desktop/hashlib/3.py (3.9.1)
File Edit Format Run Options Window Help

import hashlib

data = ['bardial23', 'amir456', 'ho3ein789']

for d in data:
    print(hashlib.sha256(d).hexdigest())
```

```
IDLE Shell 3.9.1
File Edit Shell Debug Options Window Help

Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:/Users/Asus/Desktop/hashlib/3.py =====
aab402afb3eb4f28414f082b0f7413ad5b95d275b09a02ac950a8eld44d09337
10f8a56b4e8c21ddfd10d53c433c81040e8ff58d26d06d448872d5e8b3fba6c8
9167561ab34ea46936e9d34f939e685778ed6a2c949664edcdcl46cb68db05dc
>>>
```

* یک لیست از یوزر ها داده و با تابع sha256 آن ها را هش میکنیم

*** در مثال زیر یک برنامه نوشته شده که از چندین تابع مرتبط با hashlib استفاده شده

```
4.py - C:/Users/Asus/Desktop/hashlib/4.py (3.9.1)
File Edit Format Run Options Window Help

import hashlib

print("""
[+] -1 md5
[+] -2 sha1
[+] -3 sha224
[+] -4 sha256
[+] -5 sha384
[+] -6 sha512
""")

inputer = input("Enter Your password for hashing : ")
model = input("select the number options : ")

if model == "1":
    md5 = hashlib.md5()
    md5.update(inputer.encode())
    print("[*] md5 your password is > ",md5.hexdigest())
elif model == "2":
    sha1 = hashlib.sha1()
    sha1.update(inputer.encode())
    print("[*] sha1 your password is > ",sha1.hexdigest())
elif model == "3":
    sha224 = hashlib.sha224()
    sha224.update(inputer.encode())
    print("[*] sha224 your password is > ",sha224.hexdigest())
elif model == "4":
    sha256 = hashlib.sha256()
    sha256.update(inputer.encode())
    print("[*] sha256 your password is > ",sha256.hexdigest())
elif model == "5":
    sha384 = hashlib.sha384()
    sha384.update(inputer.encode())
    print("[*] sha384 your password is > ",sha384.hexdigest())
elif model == "6":
    sha512 = hashlib.sha512()
    sha512.update(inputer.encode())
    print("[*] sha512 your password is > ",sha512.hexdigest())
else:
    exit()
```

```
IDLE Shell 3.9.1
File Edit Shell Debug Options Window Help

Python 3.9.1 (tags/v3.9.1:1e5d33e, Dec 7 2020, 17:08:21) [MSC v.1927 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: C:/Users/Asus/Desktop/hashlib/4.py =====
[+] -1 md5
[+] -2 sha1
[+] -3 sha224
[+] -4 sha256
[+] -5 sha384
[+] -6 sha512

Enter Your password for hashing : bardial23
select the number options : 6
[*] sha512 your password is > Sde6fa22ee6d77cd85d5921ee78193cf387d3030e313e9034
54702d9a3fa553d79f4ecda43f02575365626ac34dd2786e01220dalc7855ff6385101c9a52cc5
>>>
```

