سپهر مقیسه

مبانی امنیت اطلاعات

تکلیف عملی دوم

پاییز ۱۴۰۱

طبق روش گفته شده کلید را میسازیم و به کاربر نشان می دهیم:

مبنای کد استفاده از کتابخانه pyaes و binascii است

```
salt = os.urandom(16)
final_key= pbkdf2.PBKDF2("2022*ICTSec*A", salt).read(32)
```

```
here's the encrypted key: b'6165b4eeabcf7f259f0bb031e90115dc3235dabd4874c96aeb54e2bfbc1c5f83'
```

سپس هنگامی که E را کاربر انتخاب میکند

شماره دانشجویی کد شده در فایل قرار میگیرد.

```
24d54e0949aec3
```

این کد به صورت hexs شده در فایل ذخیره میشود

سپس در هنگام انتخاب D به همین صورت از کد بیرون می اید

```
elif enter == 'D':
    with open("result.txt", "r+b")as file:
        cipher = file.readline()
        cipher = binascii.unhexlify(cipher)
        file.close()
    with open("decode.txt", 'wb') as file:
        file.write(aes2.decrypt(cipher))
        file.close()
```