به نام خداوند جان و خرد

تمرین عملی تحویلی سوم

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

9931099

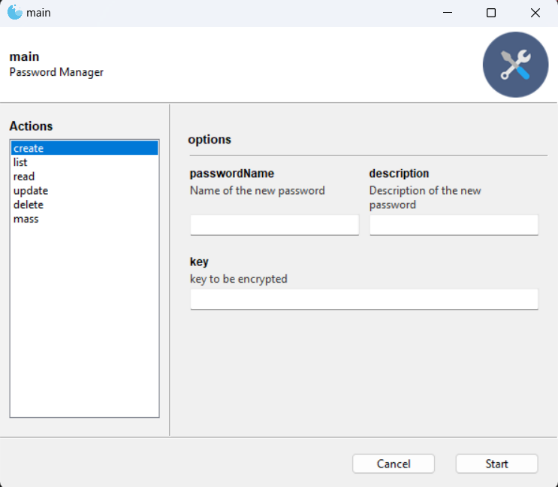
نحوه اجرای برنامه

نصب پکیج ها

در گام اول به نصب پکیج های مورد استفاده در برنامه می‌پردازیم. برای اینکار لازم است موارد زیر را انجام دهید:

* وارد پوشه code شوید.
* دستور pip install -r requirements.txt را اجرا کنید.

این برنامه به دو نحو اجرا می شود:

* ****دارای رابط کاربری
* Cli

**GUI**

برای اجرای برنامه با رابط کاربری نیاز است تا موارد زیر را به ترتیب انجام دهید.

1. پس از نصب پکیج ها در گام اول، وارد پوشه code شوید.
2. دستور python main.py را اجرا کنید تا رابط کاربری نشان داده شود.

**CLI**

برای این کار نیاز است تا decorator مورد استفاده برای رابط کاربری را کامنت کنید. برای این کار:

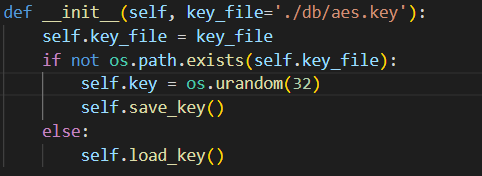
* وارد پوشه cli/utils شوید و فایل argParser را باز کنید.
* خط شماره 5 که شامل decorator است را، حذف یا کامنت کنید.
* در ادامه دستورات پیاده سازی شده برنامه و کارکرد قطعات کد، به طور مفصل توضیح داده خواهند شد.

**ساختار دستورات قابل استفاده**

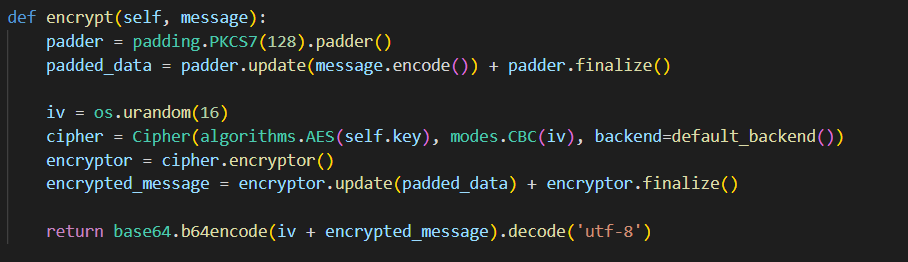
* دستور ساخت (create)
* python main.py create -n <name> -c <description> -key <key>

در این دستور نام، توضیحات و کلید مربوطه را می‌گیریم. سپس این کلید توسط الگوریتم AES رمزنگاری و به صورت یه فایل متنی آن را ذخیره می کنیم.

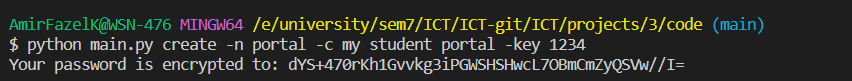
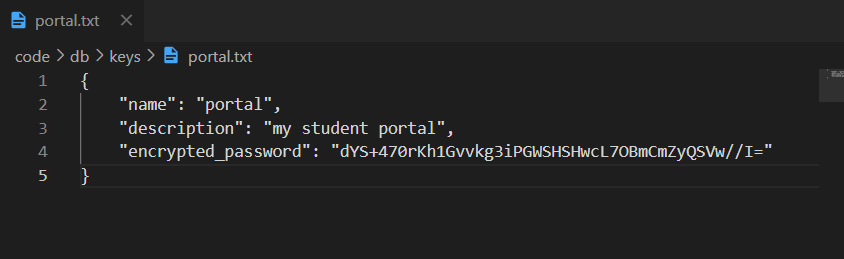
الگوریتم AES به دنبال کلید ذخیره شده در فایل می‌گردد. اگر آن را نیافت، آن را تولید می‌کند. در نهایت از این کلید برای رمزنگاری استفاده می‌کند:



تابع رمزنگاری نیز به شکل زیر پیاده سازی شده است:



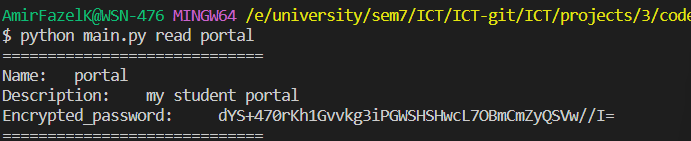
دمو:



* دستور خواندن (read)
* python main.py read <name>

این دستور، عملکرد بسیار ساده ای داشته، و صرفا در مخزن فایل های ما به دنبال رمز ذخیره شده مان می‌گردد. در نهایت آن رمز را به همرا اطلاعات دیگر ذخیره شده بر‌می‌گرداند.

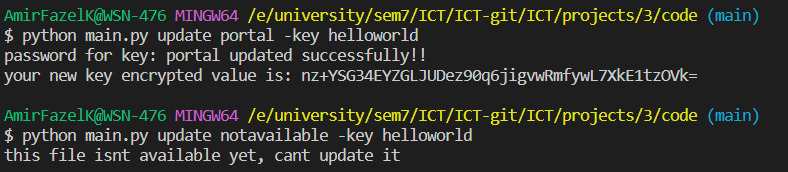
دمو

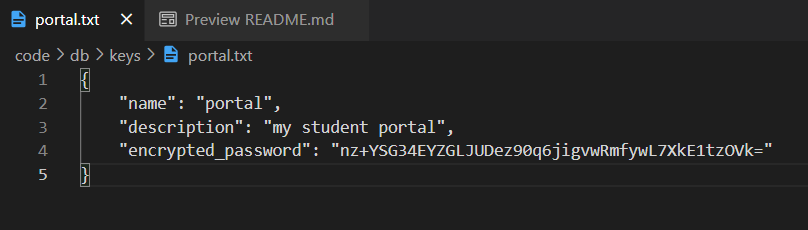


* بروزرسانی (update)
* python main.py update <name> -key <key>

با استفاده از این دستور می‌توانیم کلید رمز ذخیره شده فعلی خود را تغییر دهیم. برنامه در صورت موجود بودن رمز، آن را تغییر می‌دهد.

دمو

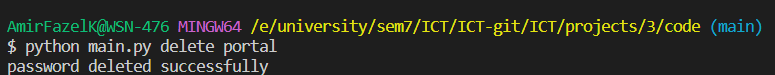


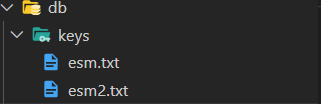


* حذف (delete)
* python main.py delete <name>

با به کارگیری این دستور، با صرفا دادن نام رمز، فایل مربوط به اطلاعات ذخیره شده درباره آن به کلی از سیستم محلی حذف می‌شود.

دمو



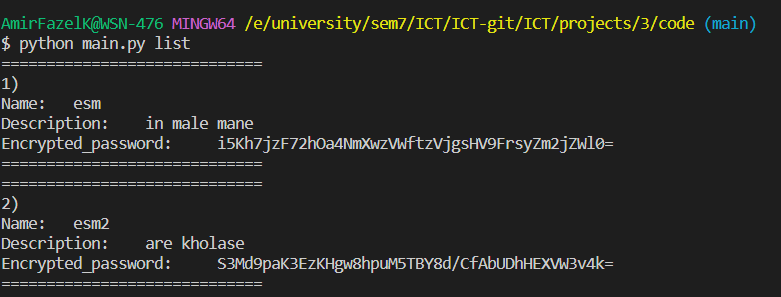


می‌توان مشاهده کرد که رمز مربوطه به کل حذف شده است.

* نشان دادن همه رمز ها (list)
* python main.py list

این دستور برای مشاهده همه کلید های رمز شده در این سیستم است.

از پیش برخی رمز ها را تعریف کرده ایم. در ادامه کارکرد این دستور را مشاهده خواهیم کرد.

دمو

بخش دوم

در این بخش به تولید و رمزنگاری انبوهی از گذرواژه ها خواهیم پرداخت و در نهایت با استفاده از ابزار statsgen این خروجی ها را بررسی خواهیم کرد.

فایل statsgen موجود در کورسز با ورژن فعلی پایتون تطابق نداشت پس مجبور به ایجاد برخی تغییرات در محتویات آن شدیم.

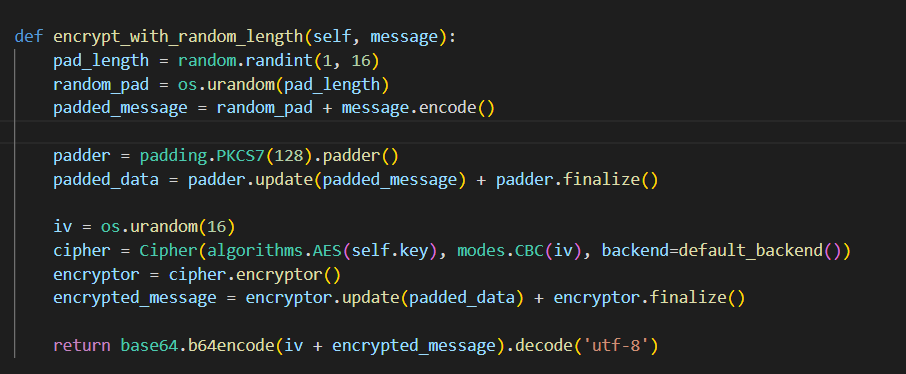
در ادامه به معرفی دستور دیگری از برنامه خود می‌پردازیم که وظیفه تولید مقدار بسیار زیادی نتیجه رمزنگاری شده از یک رشته دارد. رشته مورد استفاده "0000" است.

* دستور mass
* python main.py mass -key <key>

این دستور یک کلید را گرفته و تقریبا ده هزار بار آن را رمزنگاری می‌کند.

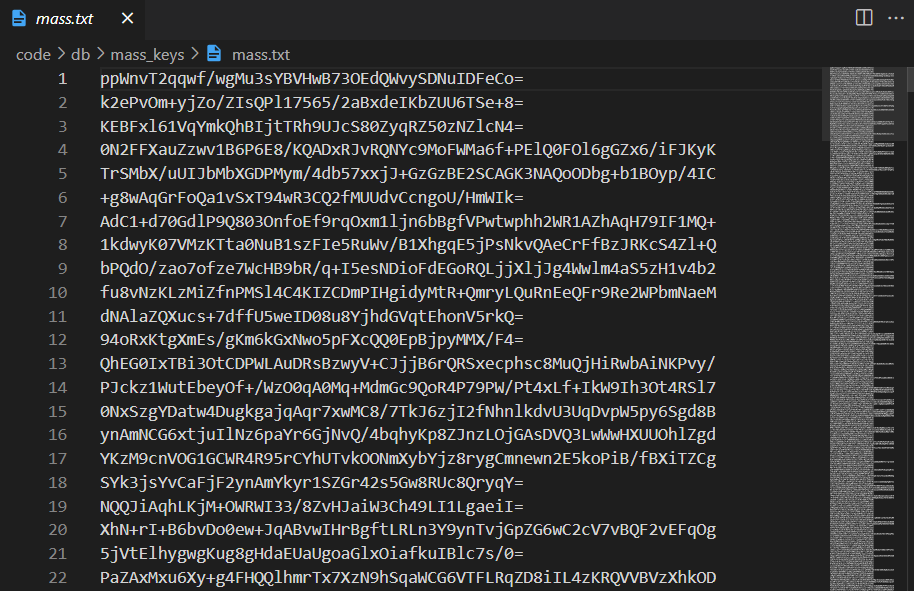
تابع مربوط به رمزنگاری استفاده شده در این بخش با تابع رمزنگاری قبلی اندکی تفاوت دارد.

این تفاوت صرفا به آن دلیل ایجاد شده تا بتوان خروجی هایی به طول های مختلف به دست آورد.



دمو





برای گام آخر، بیایید برنامه statsgen را برای فایل تکست خروجی اجرا کنیم تا از الگو های استفاده شده در آن، آگاه شویم: 