

**دانشگاه صنعتی امیرکبیر**

**(پلی‌تکنیک تهران)**

**دانشکده مهندسی کامپیوتر**

**مبانی امنیت و اطلاعات**

**(پاییز ۱۴۰۱)**

**تمرین عملی دوم**

**محمد چوپان ۹۸۳۱۱۲۵**

**گزارش پروژه :**

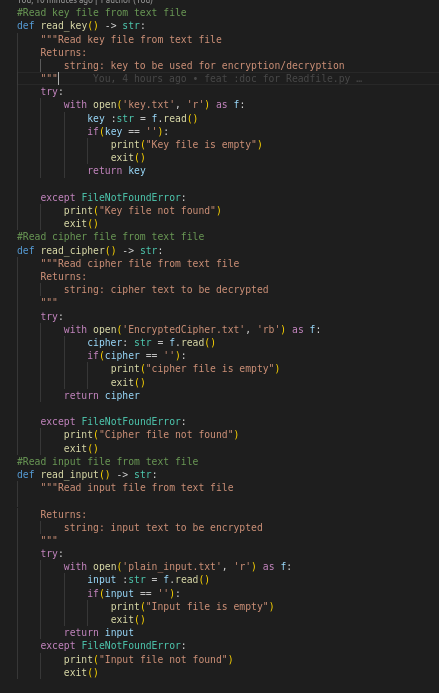
توضیحات فایل ها و کد ها درون کد موجود می باشد.

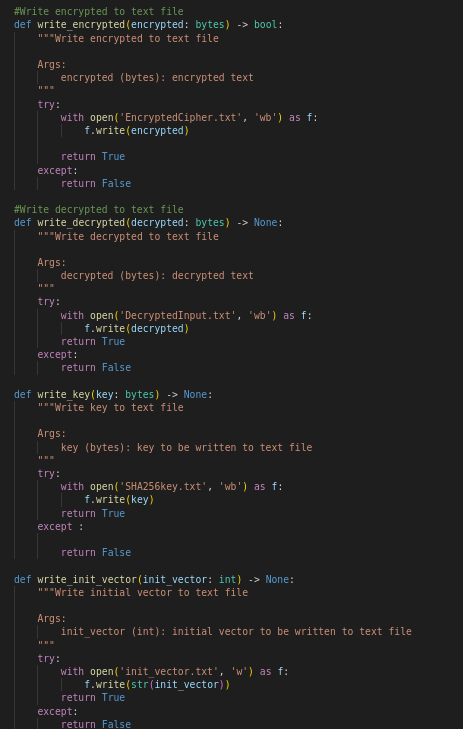
**توضیحات کد :**

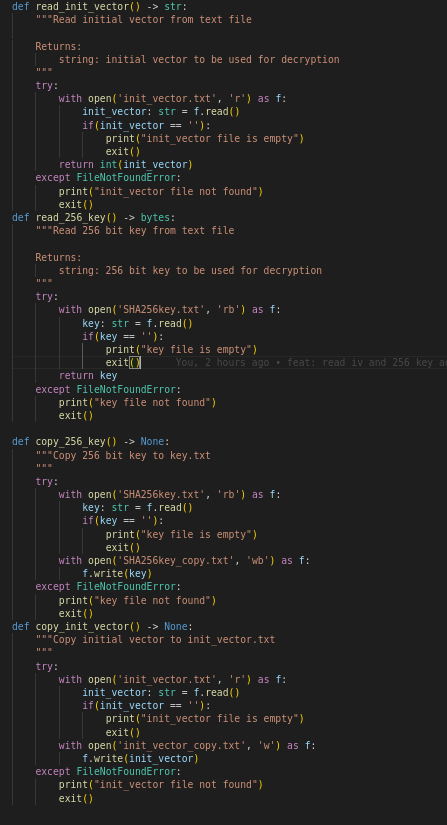
در ابتدا یک فایل با اسم handleFile.py برای کار با فایل ایجاد کرده و تمامی توابع موجودی که برای کار با فایل نیاز داریم را پیاده سازی میکنیم . برای خواندن کلید ، خواندن ورودی، خواندن متن رمزنگاری شده و نوشتن در مقدار های جدید همچنین ۲ فایل برای ذخیره سازی بردار ورودی و کلید همراه با سالت نیز اضافه میکنیم.

به این منظور که در هر بار رمزنگاری کلید ها عوض می شود برای نگهداری آن ها هم ۲ فایل کپی برای کاربر در نظر میگیریم. این توابع به خواندن و نوشتن در فایل کمک می کنند.

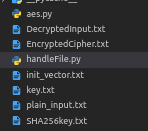
به صورت زیر :







**در کل پروژه فایل ها به صورت زیر است :**



فایل key.txt :

برای کلید اولی

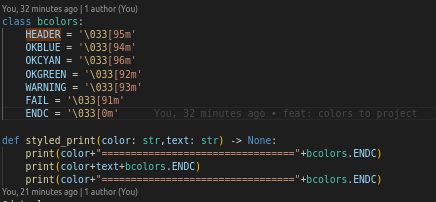
فایل SHA256key.txt :

فایل کلید به همراه سالت

فایل init\_vector.txt فایل بردار ها است.

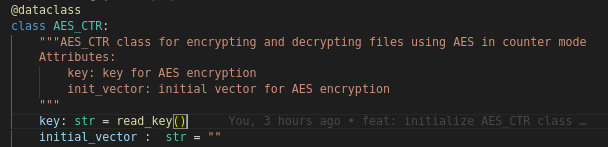
فایل های دیگر هم از نام گذاری آن ها مشخص است.

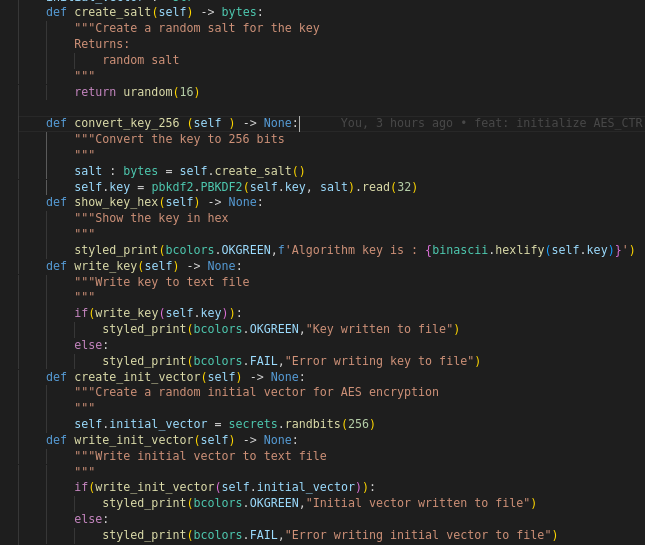
درون فایل aes.py که فایل اصلی ما است به شکل زیر است :

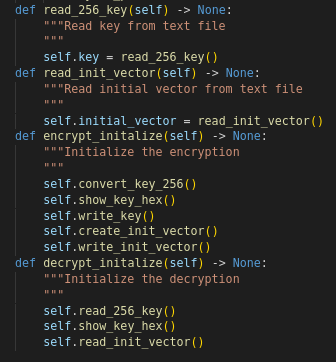


یک کلاس و تابع پرینت برای پرینت های رنگی

**کلاس AES\_CTR** که مقدار کلید و بردار را نگهداری میکند توضیح توابع درون عکس ها موجودند.

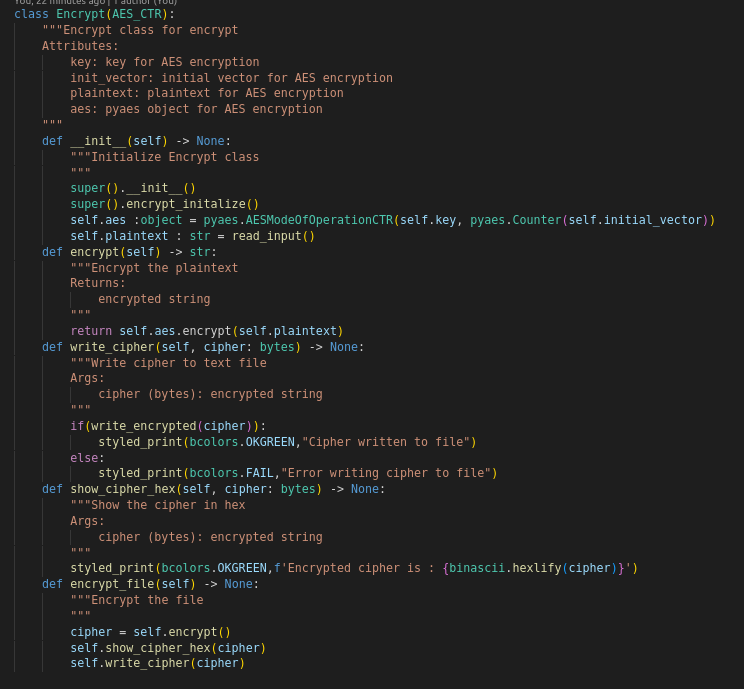




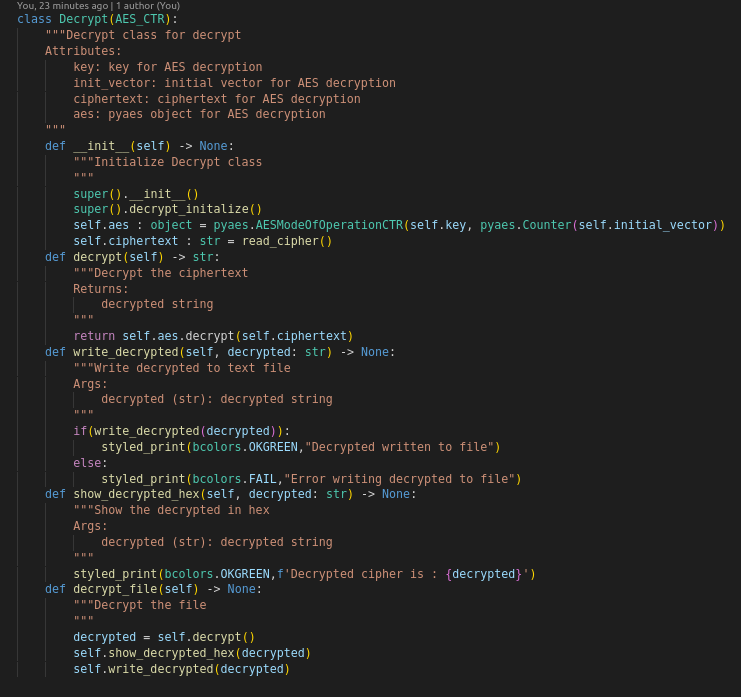


دو تابع initialize برای این هستند که اگر رمزنگاری هست کلید تولید کند و اگر رمزگشایی قبلی ها را از فایل ها بخواند.

**کلاس Encrypy :**



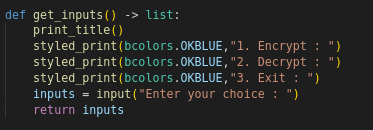
**کلاس Decrypt:**



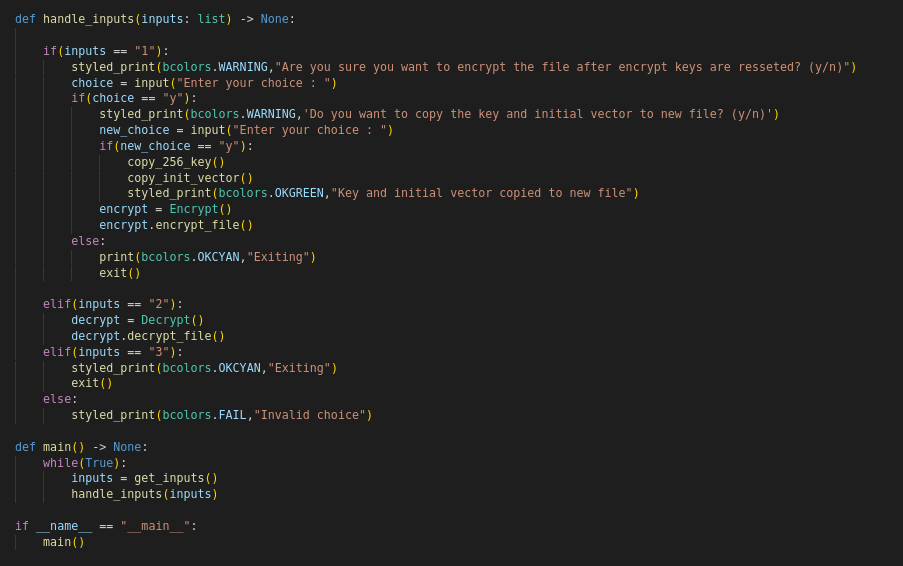
**تابعی برای نمایش هدر برنامه :**



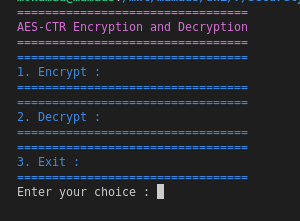
**تابعی برای ورودی:**



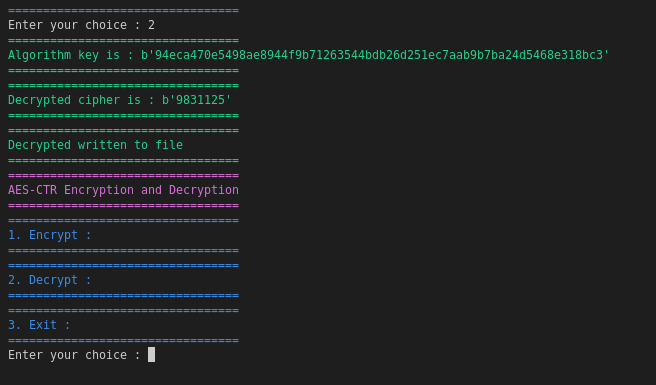
**و تابعی برای پردازش ورودی ها و main**



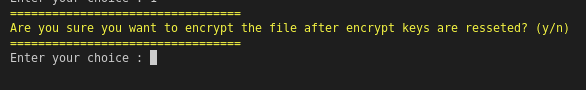
**در نهایت در صورت اجرای برنامه به این شکل است که در صورت اجرا فایل :**



اگر گزینه ۳ انتخاب شود از برنامه خارج می شود در صورت انتخاب گزینه ۲ :



در صورت انتخاب گزینه ۱ :

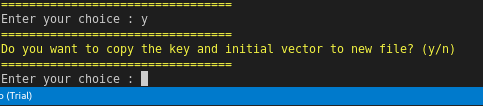


اخطار می دهد که کلید ها از اول تولید می شوند آیا می خواهید ادامه دهید.

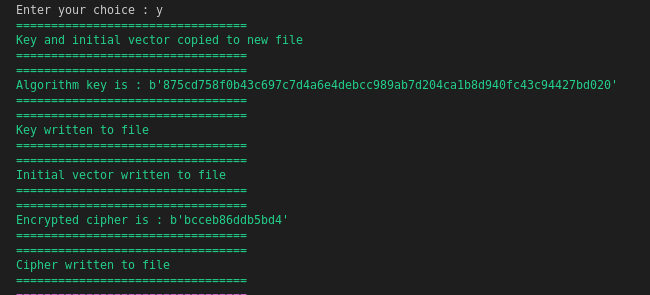
اگر خیر بزنیم از برنامه خارج می شود .



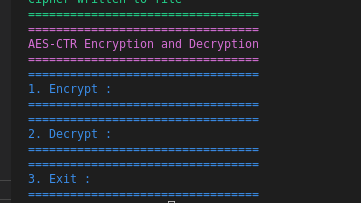
اگر بله بزنیم :



میگوید که آیا میخواهید کلید های قبلی را کپی کنید : اگر بله بزنیم کلید ها را در دو فایل کپی جایگذاری میکند.



و فرایند جدد تکرار می شود :



تمامی فایل ها در پروژه موجود است.

همچنین در صورت نبود فایل ها key.txt و plain\_input برای رمزنگاری با خطا مواجه می شویم.

