به نام خداوند جان و خرد

پروژه تحویلی اول

درس مبانی امنیت اطلاعات

امیرفاضل کوزه گر کالجی

9931099

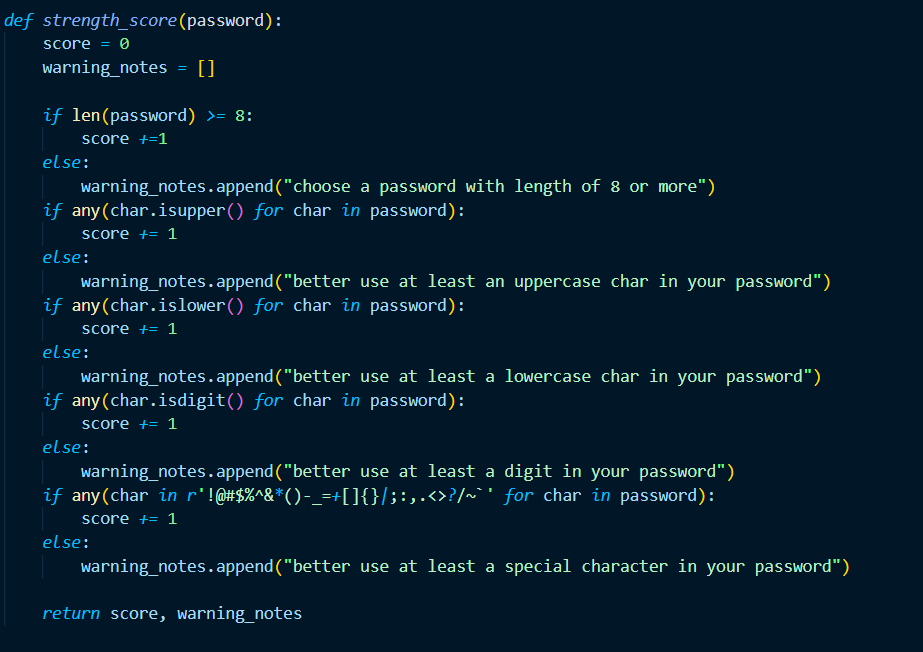
فاز اول

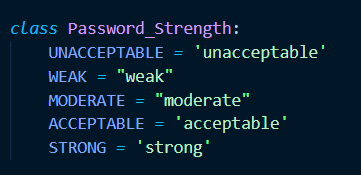
بخش اول:

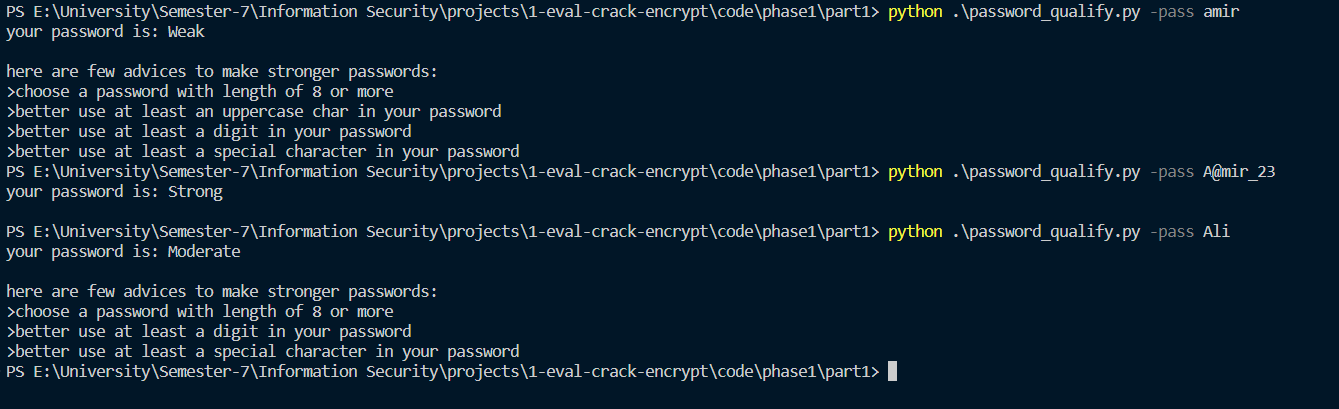
در این بخش برنامه ای توسعه داده شد تا میزان قدرت یک رمز را بسنجد. معیار های ارزیابی رمز در این برنامه به شکل زیر است:

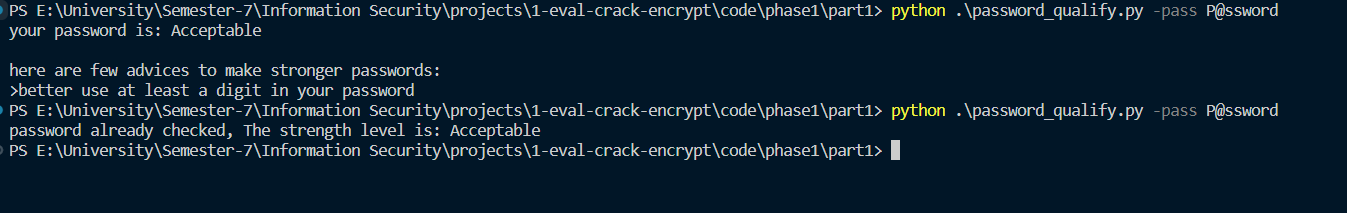
* طول رمز
* وجود کاراکتر های lowercase
* وجود کاراکتر های uppercase
* وجود کاراکتر های خاص
* وجود رقم

ارضا شدن هر یک از 5 معیار نام برده یک امتیاز مثبت برای رمز ما خواهد داشت. به همین سبب، در نهایت بر اساس هر امتیازی که رمز کسب کرده است، عنوانی برای نشان دادن میزان قدرت آن نشان می دهیم.





در شکل زیر نتیجه برنامه را برای برخی پسورد های امتحانی نشان می‌دهیم:

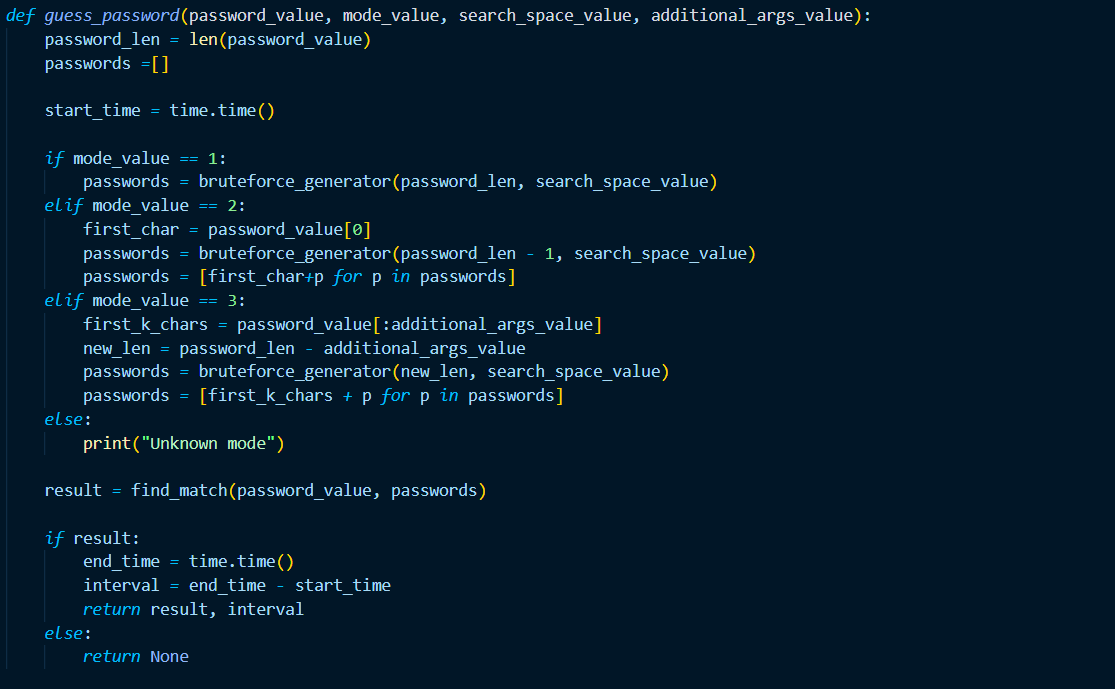
همچنین رمز هایی که استفاده می‌شوند همراه با سطح خود، در یک فایل json ذخیره می‌شوند زیرا که اگر بعدا همین رمز وارد شد سریعتر به مقدار آن دسترسی داشته باشیم و از محاسبات اضافی بپرهیزیم:

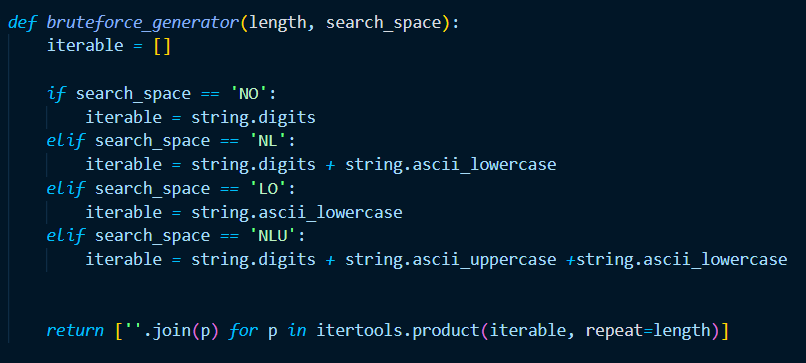
بخش دوم:

در این بخش، طبق گفته های دستورکار یک ابزار برای حدس رمز طراحی و توسعه داده شده است که دارای مود ها و فضای جست و جو های متفاوتی می‌باشد.

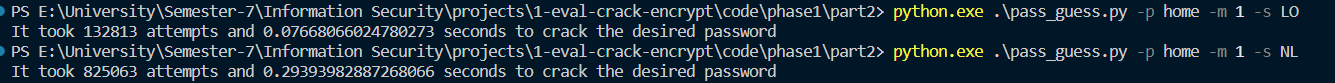
برای توسعه این برنامه از کتابخانه itertools استفاده شده است تا برای ما لیستی از تمام ترکیبات ممکن را فراهم آورد.

رفتار برنامه بر اساس مود های ذکر شده، به شکل زیر تعیین می‌شود:



رفتار برنامه بر اساس محیط های جست و جو ذکر شده نیز، به شکل زیر تعیین می‌شود:

در این میان، هنگام اجرای برنامه و جست و جو به دنبال رمز داده شده، میزان تلاش ها و زمان سپری شده نیز ضبط و در انتها اعلام می‌شود:







تصاویر فوق، نمونه هایی از اجرای برنامه مدنظر می‌باشند.

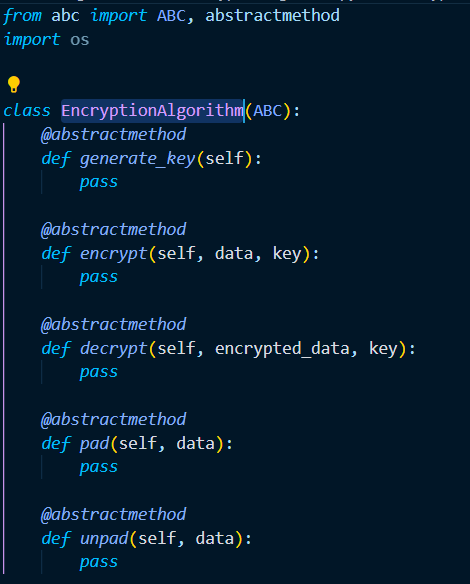
فاز دوم

در این فاز از ما خواسته شده تا یک برنامه بنویسیم که محتوای فایل ها را رمزگذاری و رمزنگاری کند.

این برنامه با زبان پایتون و با درنظر گرفتن text بودن فایل های دریافتی توسعه داده شده است.

در این برنامه یه روش رمزنگاری AES، DES، و RSA پیاده سازی شده است. که غیر از RSA باقی الگوریتم ها متقارن محسوب می‌شوند.

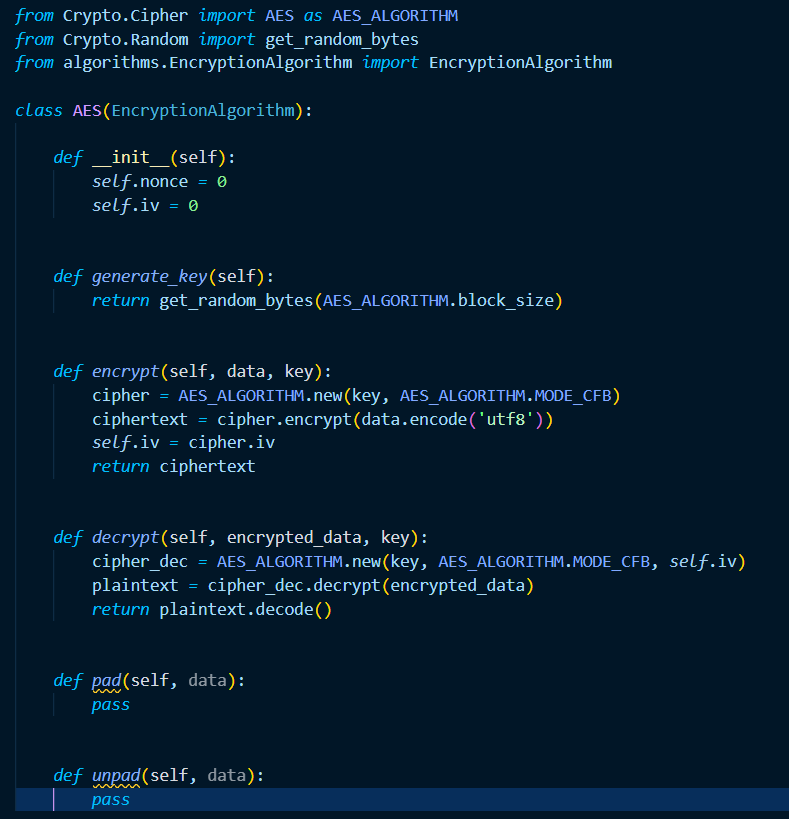
تمامی الگوریتم ها از توابع یکسانی برخوردارند پس همه آنها از یک کلاس ابسترکت ارث بری می‌کنند:

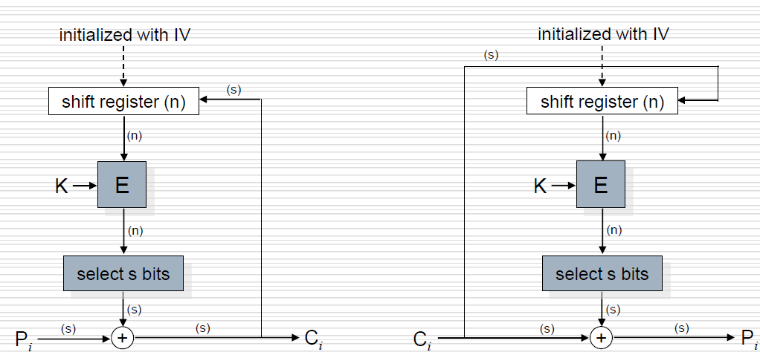


الگوریتم ها

AES

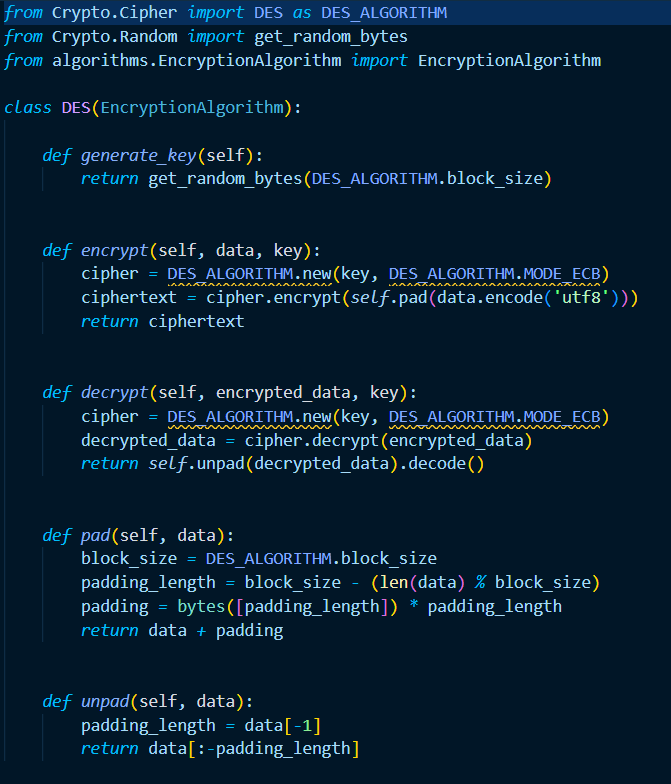
در پیاده سازی این الگوریتم از کتابخانه Crypto استفاده شده است تا به صورت واضح تمامی قابلیت های الگوریتم AES را در اختیارمان قرار دهد.



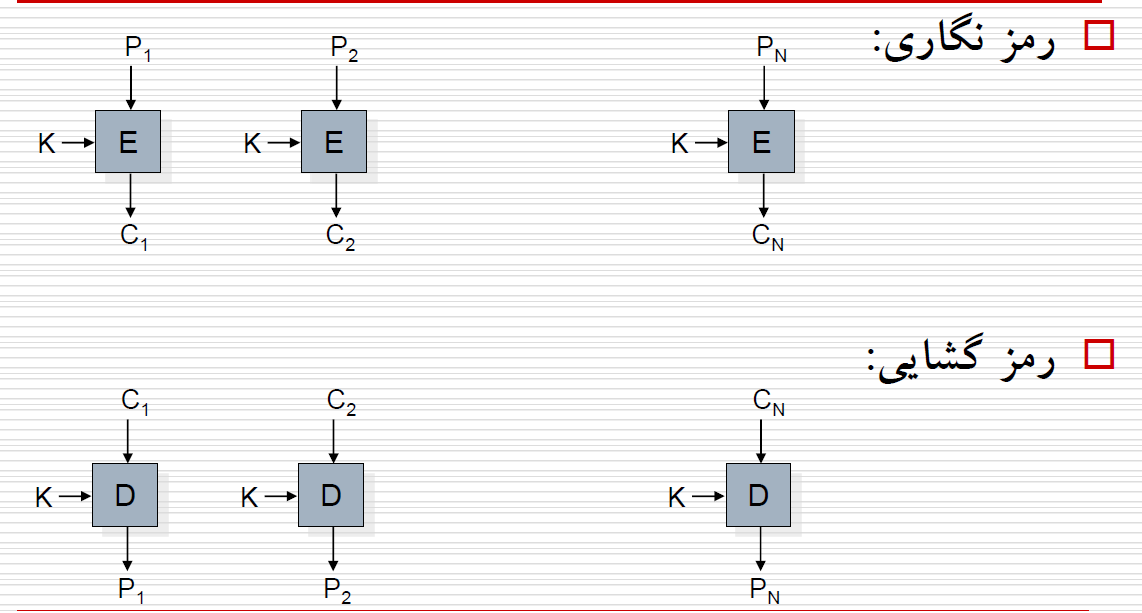
طبق قطعه کد فوق، می‌توان دریافت که این الگوریتم از مد CFB یا Cipher feedback استفاده می‌کند. اساس کار CFB به شکل زیر می‌باشد:

DES

همانند AES، در پیاده سازی این الگوریتم نیز از کتابخانه Crypto استفاده شده است.



همانطور که طبق کد فوق قابل مشاهده است، الگوریتم DES با مد ECB، طراحی یافته است:

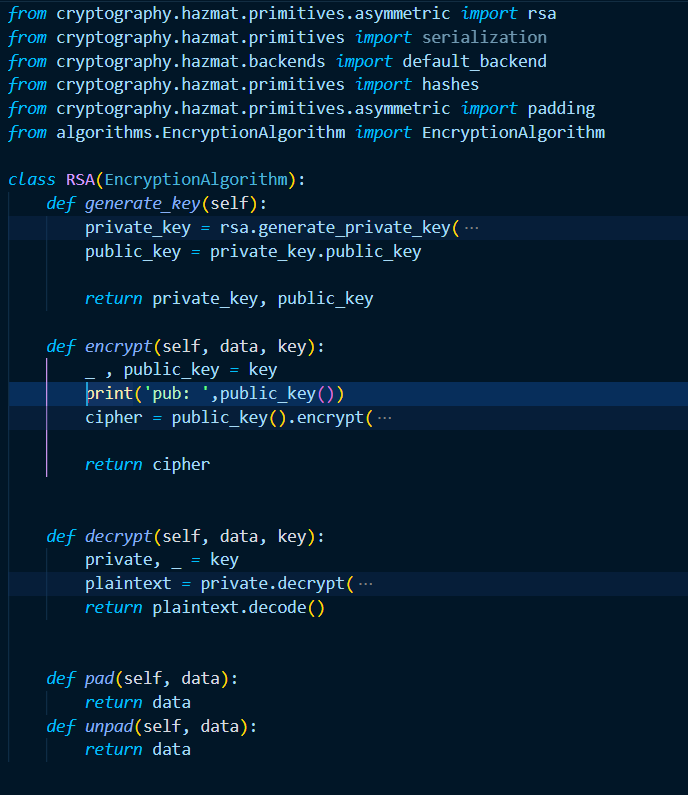


دو متد pad و unpad مناسب با نوع عملکرد DES رفتار می کنند و بیت هایی را به داده اصلی الحاق یا از آن جدا می‌کنند.

RSA

این الگوریتم با دو کلید انجام می‌پذیرد. یکی کلید عمومی و دیگری کلید خصوصی. پس باید هنگام کار با آن دو کلید تولید کنیم. با کلید عمومی داده را رمز کنیم، و با کلید خصوصی داده را رمزگشایی کنیم.

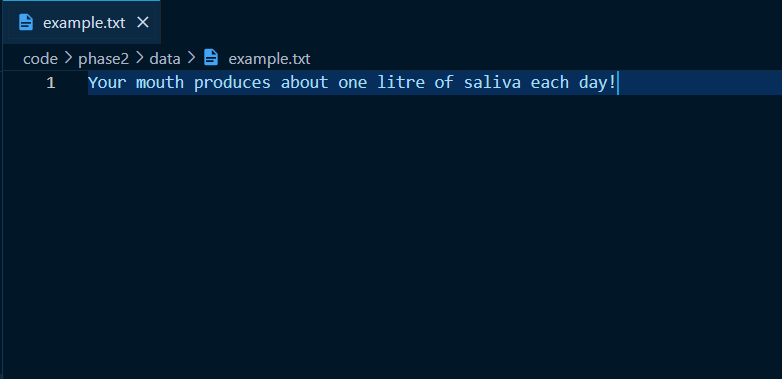
با توجه به توضیحات بیان شده، بهتر است نگاهی به قطعه کد نوشته شده داشته باشیم:



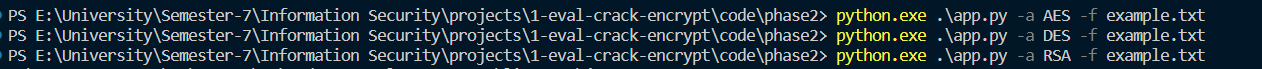
همانطور که قابل مشاهده است این بار از کتابخانه cryptography استفاده کردیم زیرا که به ما امکان تولید کلید های عمومی و خصوصی را می‌داد. در ادامه منطق توضیح داده در ابتدا را می‌توان به صورت کد، مشاهده کرد(عملیات رمز کردن و رمزنگاری کردن).

حال نتیجه برنامه را در هر 3 حالت مشاهده خواهیم کرد:

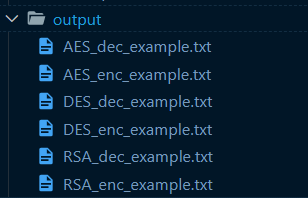
فایل example.txt فایلی است که باید رمز شود:



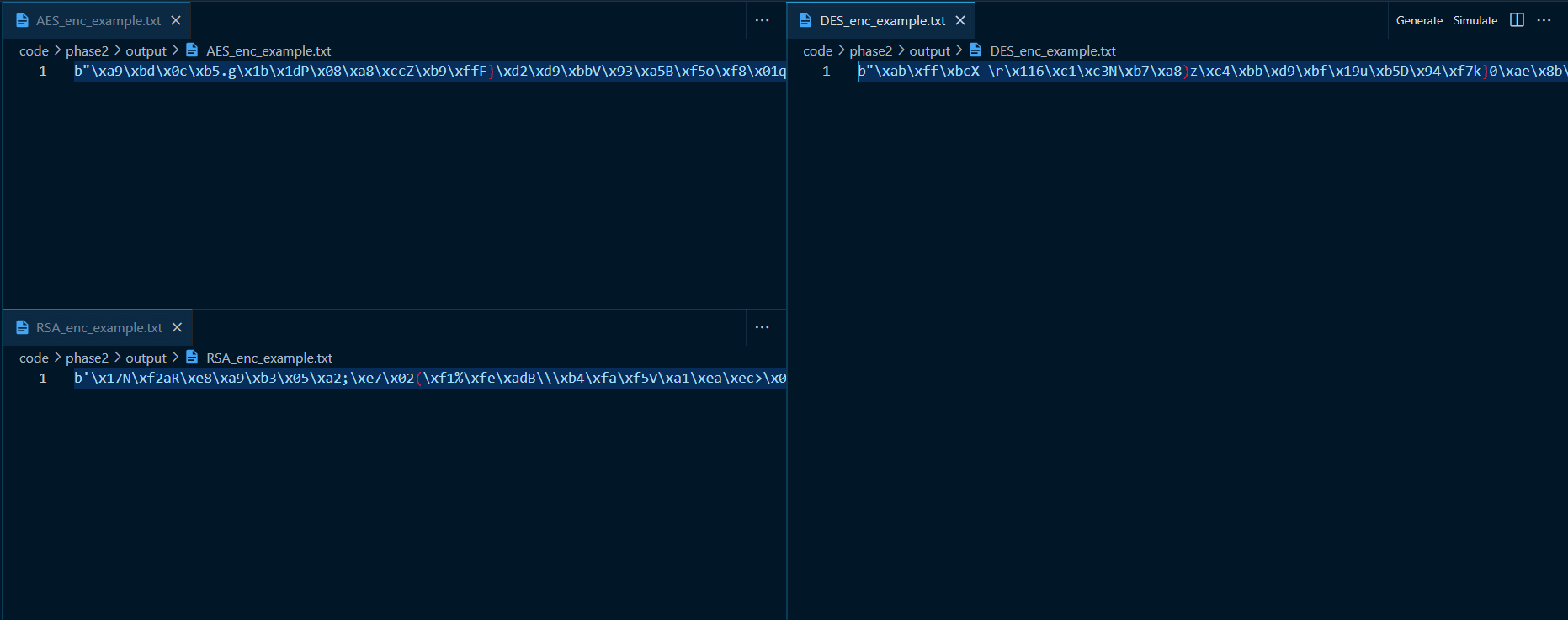
برنامه را به ازای هر سه الگوریتم اجرا می‌کنیم:



در پوشه output که برای قرار دادن خروجی ها، تعبیه شده فایل های زیر ظاهر خواهند شد:



محتوای رمز شده به ازای هر الگوریتم را می‌توانید از شکل زیر مشاهده کنید:



و در نهایت فایل رمزگشایی شده به ازای هر یک را، می توان در فایل های مربوطه مشاهده کرد:

