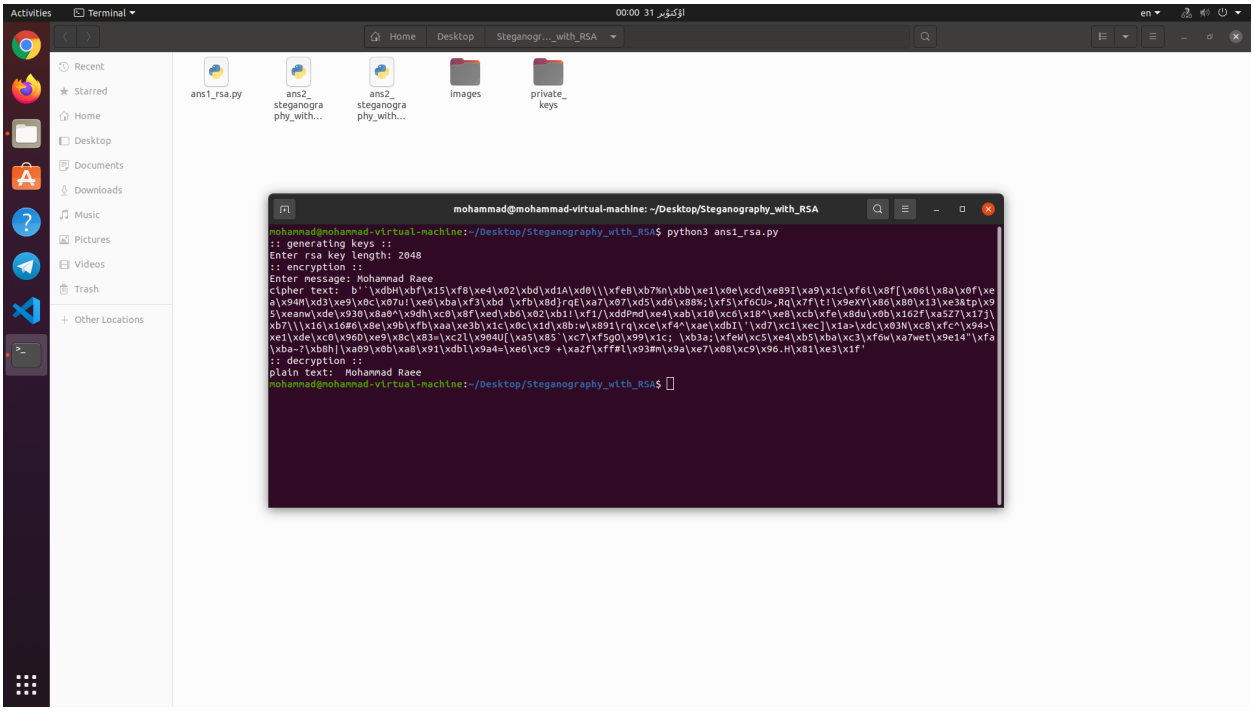
پاسخ سوال ۱ : پاسخ این سوال در فایل Ans1_rsa.py قرار داده شد. که ضمیمه و ارسال شد. در این فایل ۳ تابع داریم . تابع اول generate_key هست که طول کلید rsa را گرفته و دو کلید public و private ایجاد میکند. تابع دوم encryption است که با گرفتم کلید عمومی و دریافت یک متن از کاربر رمز نگاری را انجام میدهد و cipher_text را در خروجی نمایش میدهد. و تابع سوم decryption است که با دریافت کلید خصوصی و متن رمز شده، متن اولیه یا همان plain_text را نمایش میدهد .

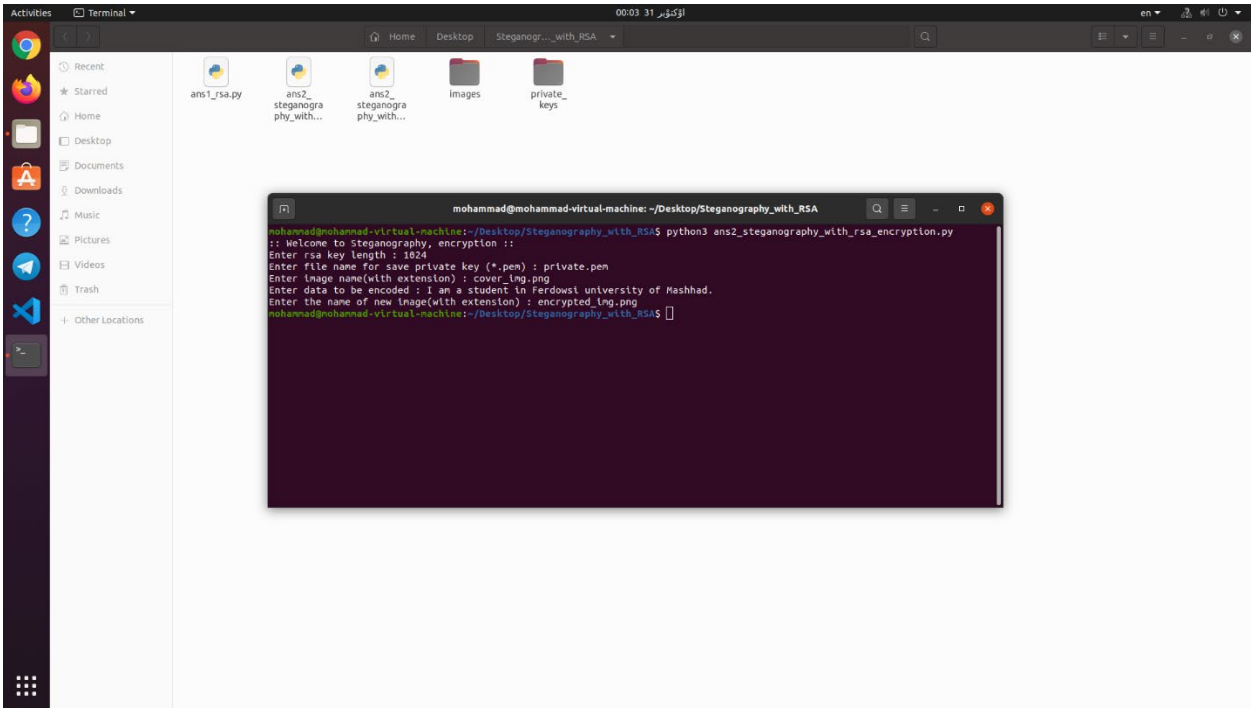
خروجی Ans1_rsa.py را در تصویر زیر میبینیم:



پاسخ سوال ۲ : پاسخ این سوال در دو قسمت داده شد. **قسمت اول یعنی بخش رمز نگاری در فایل ans2_steganography_with_rsa_encryption.py قرار داده شد.** کامنت گذاری ها به طور کامل انجام شده است . در این فایل ابتدا تابع encode اجرا میشود که در آن یک عدد صحیح برای ساخت کلید rsa از کاربر میگرد. سپس نام فایلی که کلید خصوصی میخواهد در آن ذخیره شود را از کاربر میگیرد (این فایل باید با پسوند pem. باشد) سپس کلید خصوصی را در پوشه private_keys فایلی با همان نام ایجاد میکند و در آن ذخیره میکند. در ادامه متن ورودی را از کابر میگیرد و به همراه کلید عمومی به تابع encryption میدهد. در این تابع ابتدا متن با کلید عمومی رمز میشود و سپس تابع hash256 روی آن اجرا میشود و پس از آن مقدار hash شده دوباره با کلید عمومی رمز میشود و این مقدار به cipher_text میچسبدو به عنوان خروجی میدهد. سپس از کاربر نام تصویری که میخاد نهان نگاری در آن انجام شود را میگیرد (این عکس در پوشه ی images قرار داد و این نام به همراه خروجی encryption به تابع encode_enc داده میشود تا به جای بیت های سمت راست پیکسل های درون عکس قرار بگیرد. سپس آدرس عکسی را میخواهید تصویر نهان

نگاری شده در آن ذخیره شود را از کاربر میگیرد.(این تصویر نیز در پوشه ی images ذخیره میوشد.

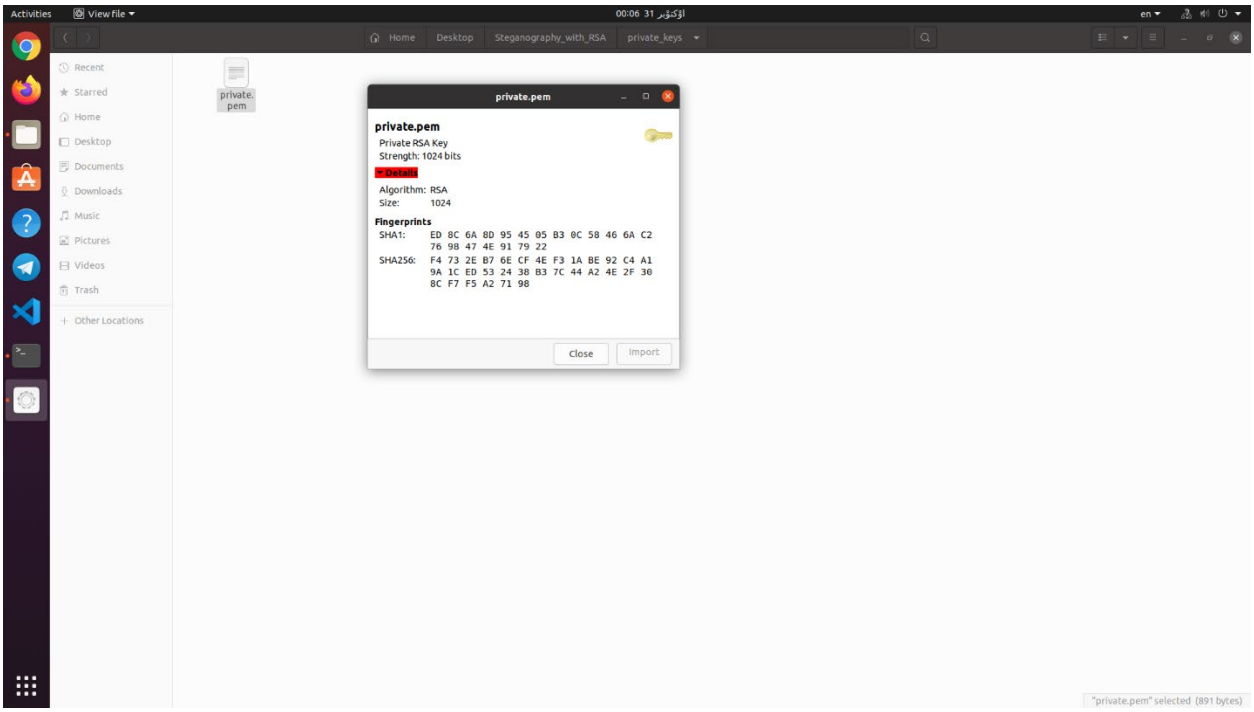
خروجی دستوران خط فرمان ans2_steganography_with_rsa_encryption.py را در تصویر زیر میبینیم:



تصویر اولیه که با نام cover_img.png است را در تصویر زیر مشاهده میکنید:

تصویر نهان نگاری شده که با نام encrypted_img.png ذخیره شده را در تصویر زیر مشاهده میکنید:

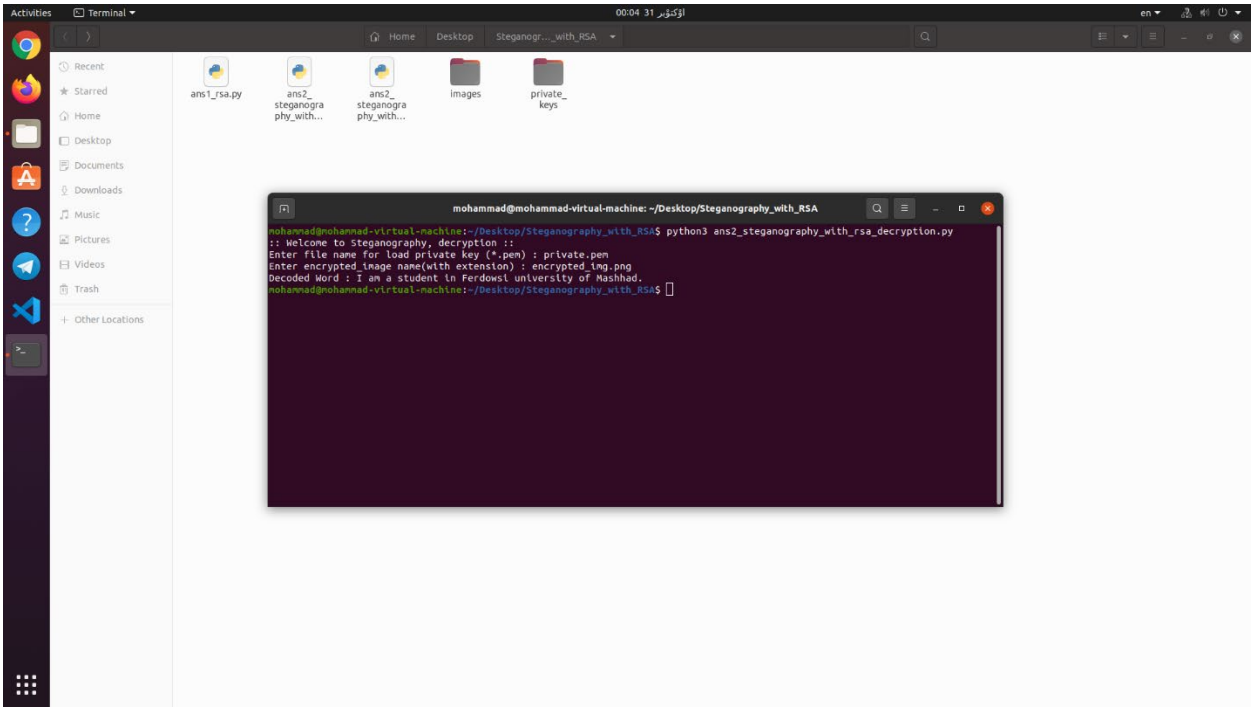
همچنین تصویر فایل حاوی کلید خصوصی را که با نام private.pem ذخیره شد، در تصویر زیر مشاهده میکنید:



قسمت دوم یعنی بخش رمز گشایی در فایل ans2_steganography_with_rsa_decryption.py قرار داده شد. در این فایل ابتدا نام عکسی را که باید رمز از آن استخراج شود از کاربر میخواهد(این تصویر در پوشه ی imges قرار دارد)

سپس نام فایلی که باید کلید private برای رمز گشایی از آن استخراج شود را از کاربر میخواهد(این فایل در پوشه ی private_keys) قرار دارد. حال تابع decryption را صدا میزند. این تابع ابتدا مقدار نهان نگاری شده در تصویر مذکور را استخراج میکند و که این مقدار حاصل concat دو مقدار cipher_text و مقدار رمز شده ی هش cipher_text است .
خب این دو مقدار را از هم جدا میکند و بخش دوم را ابتدا با private_key رمز گشایی میکند و سپس بخش اول را با hash256 رمز میکند و دو مقدار را با هم مقایسه میکند، اگر یکی بودند پس integrity تایید میشود و سپس cipher_text را با private رمز گشایی کرده و نمایش میدهد و در صورت عدم مطابقت، پیام عدم تایید integrity را میدهد.

خروجی دستوران خط فرمان ans2_steganography_with_rsa_decryption.py را در تصویر زیر میبینیم:



پاسخ سوال ۳ : در پاسخ به دو مورد از کاربرد های رمز نگاری اشاره میکنیم. کاربرد نخست یک کاربرد در دنیای اقتصاد یعنی رمز ارز هاست. رمز ارزها یکی از مهم‌ترین کاربردهای بلاک‌چین می‌شود و از کلیدهای عمومی و خصوصی برای حفظ آدرس کاربران بلوک‌چین بهره می‌گیرد. در مورد رمزنگاری در بلاکچین، کلیدهای خصوصی به‌عنوان آدرس فرد استفاده می‌شود و کلیدهای عمومی به صورت جهانی و برای همگان قابل مشاهده است. کلید خصوصی، مقدار مخفی است و برای دسترسی به آن و مجوز هریک از آن «آدرس» است که به‌طورکلی تراکنش‌ها هستند، به کار می‌رود. امضاهای دیجیتال به طور خاص برای ارزهای دیجیتال استفاده می شوند. آن‌ها را برای ارزیابی معامله‌ها با امضای آنها به صورت ایمن (آفلاین) استفاده می‌کنند و همچنین برای قراردادهای چند امضایی کیف پول دیجیتال در لاکچین نیز کاربرد دارند.

کاربرد دوم در مورد کاربرد روزمره رمز نگاری در وای فای خانگی و فشای اینترنت است. همانطور که می‌دانید اولین محل اتصال شما با دنیا از شبکه‌های وای‌فای(wi-fi) است، بنابراین اولین قسمتی است که نیاز به رمزنگاری و محافظت از همین

شبکه‌های خانگی دارد. شبکه‌ها وای‌فای توسط پروتکل‌های محافظتی مانند WPA و WPA2 رمزنگاری شده‌اند. که از شبکه‌های وای‌فای شما در برابر ترافیک اطلاعاتی شما محافظت میکند. همچنین موتورهای جستجوگر مدرن از پروتکلی به نام Secure Sockets Layer (SSL) استفاده می‌کنند تا جستجو و تبادلات شما را امن کنند. عملکرد SSL به این صورت است که از یک کلید برای رمزنگاری و از کلید دیگری برای رمزگشایی رمز استفاده می‌کندکه همان نام‌نگاری است. زمانی که عبارت HTTPS را در محل تایپ آدرس(URL) می‌بینید، بدین معناست که به دور از چشمان شما، SSL در حال تامین امنیت در اینترنت است.