توضیحات پروژه:
این پروژه رو با استفاده از پایتون و به صورت شی گرا (OOP) نوشتم
در این پروژه از پکیج rsa استفاده کردم
و برای اینکه بتوانیم از فایل پایتونی ران بگیریم قبل ازآن باید حتما پایتون نصب شده باشد و همچنین پکیج rsa هم نصب شده باشد
برای نصب پکیج rsa از دستور زیر در ترمینال میتوانیم استفاده کنیم

```
pip install rsa
```

مراحل اجرای فایل پایتونی:
ابتدا فایل زیپ را اکسترکت کنید
ترمینال یا CMD را در لوکیشن فولدر حاوی فایل پایتون باز کنید یا میتوانید ابتدا ترمینال را باز کنید و به مسیر پوشه مورد نظر بروید
حالا با وارد کردن این دستور میتوانید فایل پایتونی را اجرا کنید

```
python project.py
```

برنامه ساخته شده شامل ۸ دستور میباشد که با وارد کردن عدد هر دستور میتوانیم آن دستور رو اجرا کنیم

1.Generate a new keypair

با وارد کردن شماره این دستور میتوان key publick و private key جدید تولید کرد اگر از ابتدا هم این دستور رو وارد نکنیم به طور پیش فرض خودش میسازد

2. save key pair

private key و public key در فایل نوشته میشوند و در فایل های جداگانه ای با پسوند pem در همان فولدر ذخیره میشوند و می توان این فایل هارو با notepad باز کرد و آن هارا دید

3. load key pair

این دستور فایل هایی که در مرحله قبل ذخیره کردیم را در برنامه لود میکند و برنامه از این به بعد میتواند به public key و private key دسترسی داشته باشد

4. Encrypt

این دستور پیغام رو که به طور پیشفرض

```
'SeyedMohammadReza Mousavitabar ---> 39928441054130'
```

هست رو با استفاده از public key رمزگزاری میکند و در فایلی به نام encrypted.message ذخیره میکند

5. Decrypt

محتوای فایلی که در مرحله قبل ذخیره شده را با استفاده از private key رمزگشایی میکند و در خروجی نمایش میدهد

6. Sign

پیغام که به طور پیشفرض

```
"I have a new account on Twitter which is @madeupname453"
```

هست رو با استفاده از private key و متد SHA-256 هش میکند و امضا یا Signature ساخته می شود و در فایلی به نام signature ذخیره میشود

7. Verify

فایل ساخته شده در مرحله قبلی را میخواند و
Public key , message, signature
را با هم مقایسه میکند و اگر هر سه تا متغیر صحیح بودند متدی که پیغام رو با استفاده از آن هش کرده است رو نمایش میدهد.

توضیحات کلی راجب الگوریتم:

اگر فرضا مدیر یک سایت و کاربران رو در نظر بگیریم
کاربران میتوانند با استفاده از public keyکه مدیر سایت در اختیار آن ها گذاشته شده است پیغام خودشون رو encrypt کنند و برای مدیر سایت ارسال کنند
مدیر سایت با استفاده از private key میتواند پیغام رو decryptکند و پیغام اصلی رو مشاهده کند.

و حالا اگر مدیر سایت بخواهد پیغامی رو برای کاربران به صورت رمز گذاری شده ارسال کند از signمیتواند استفاده کند در این حالت پیغام با استفاده از private key و hash SHA 256 رمزگذاری میشود
در این صورت زمانی میتوانیم بگوییم که کاربران این پیغام رو به طور سالم دریافت کرده اند که signature و publick key درست باشد