

Kleopatra

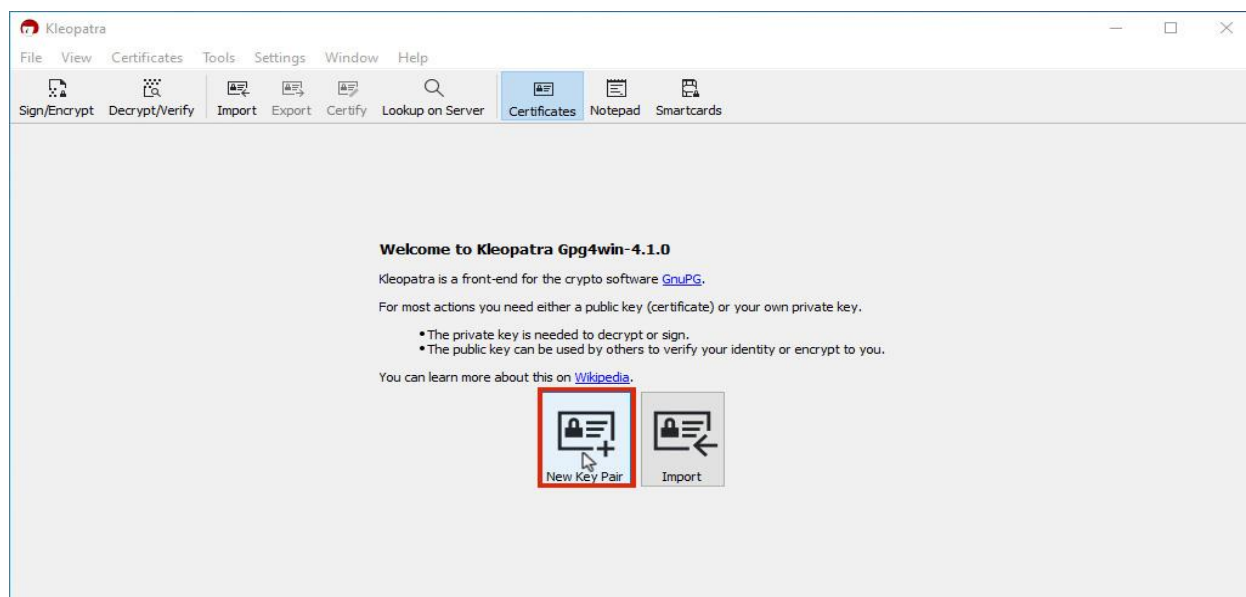
برای نصب نرم افزار Kleopatra می بایست ابتدا، نرم افزار `gpg4win` را از لینک زیر دانلود کرده و سپس نصب نمایید.

<https://gpg4win.org/thanks-for-download.html>

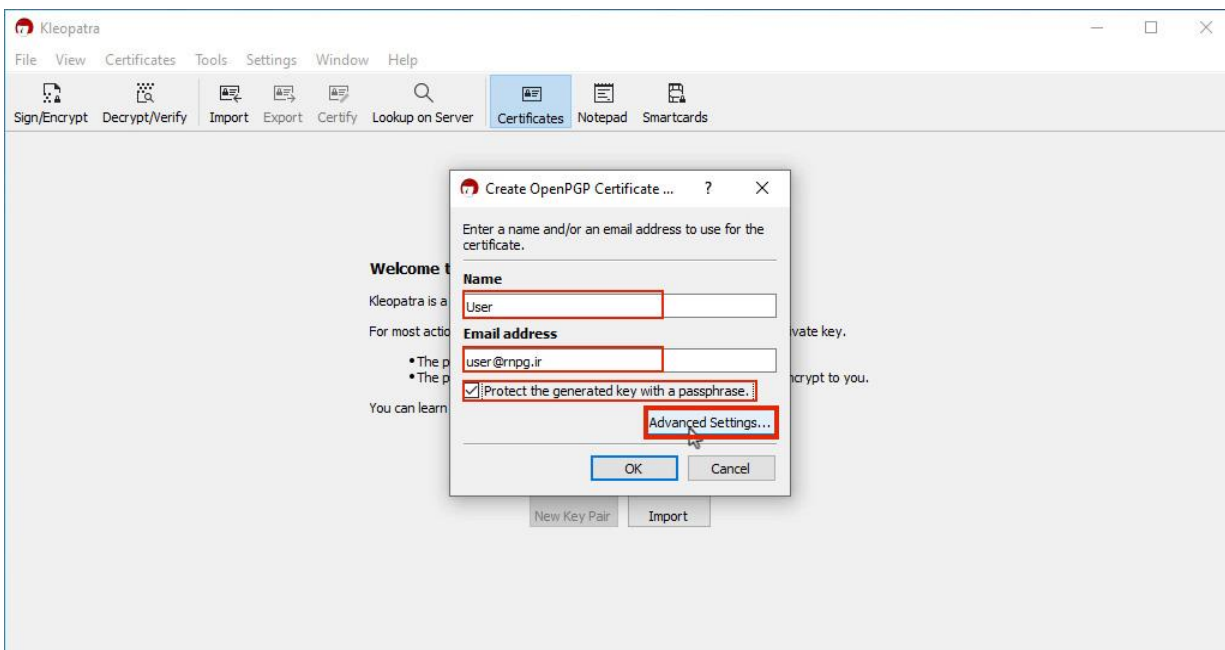
طی فرایند نصب `gpg4win` پیش نیاز های دیگری مثل `Kleopatra`، `GpgOL`، `GnuPG` و `GpgEX` نیز نصب می شوند.

۱. نحوه ساخت کلید

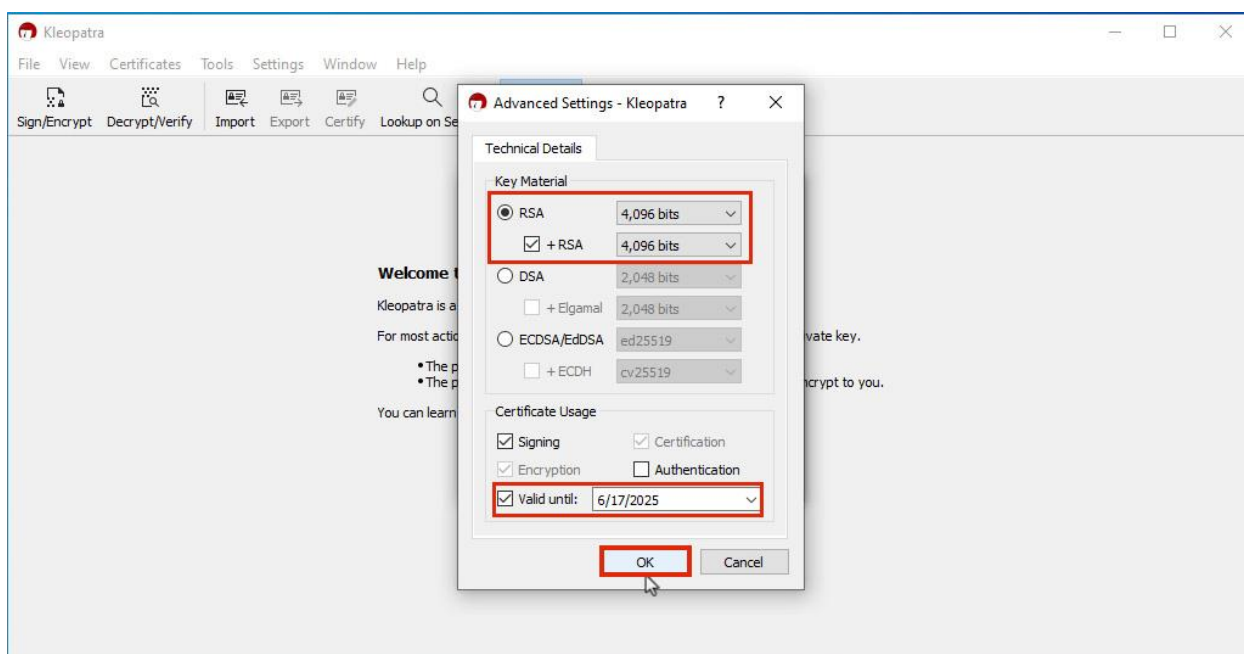
- وارد برنامه Kleopatra شده و بر روی دکمه "New Key Pair" مطابق تصویر زیر کلیک نمایید.



- در پنجره باز شده، می توان نام و ایمیل خود را به صورت اختیاری وارد نمایید.
- نکته: حداقل یک مورد باید تعریف شود.
- نکته: در صورت وارد نمودن نام، طول آن می بایست حداقل ۵ حرف باشد.
- برای حفاظت از کلید با رمز عبور، گزینه "Protect the generated key with a passphrase" را فعال کنید.
- سپس برای تغییر تنظیمات کلید، روی "Advanced Settings" کلیک نمایید.

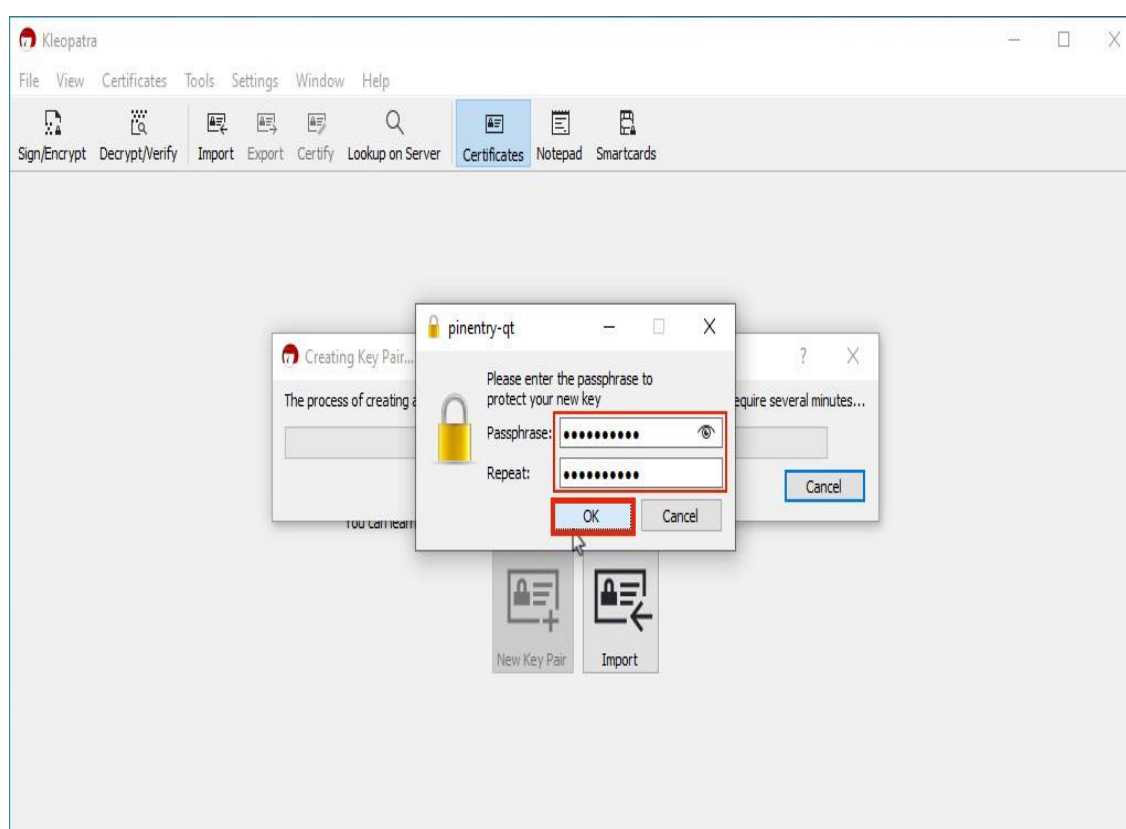


- سپس همانند تصویر زیر، الگوریتم رمزنگاری را RSA و طول آن را برابر با "4096 bits" قرار دهید. در ادامه می‌توانید تاریخ انقضا کلید را نیز تعیین نمایید.
- سپس روی "OK" کلیک نمایید



- همانطور که در تصویر زیر قابل مشاهده می باشد، در پنجره جدید، رمز عبور دلخواه خود را وارد نمایید و در فیلد "Repeat" رمز عبور وارد شده را مجددا وارد نمایید.

- نکته: بهتر است از رمز عبور پیچیده استفاده نمایید. رمز عبور پیچیده شامل رمز عبوری است که طولانی باشد، از حروف کوچک و بزرگ استفاده شده باشد، غیر قابل حدس باشد و اعداد و کاراکترهای خاص (مثل !، @، # و ...) نیز در آن وجود داشته باشد.



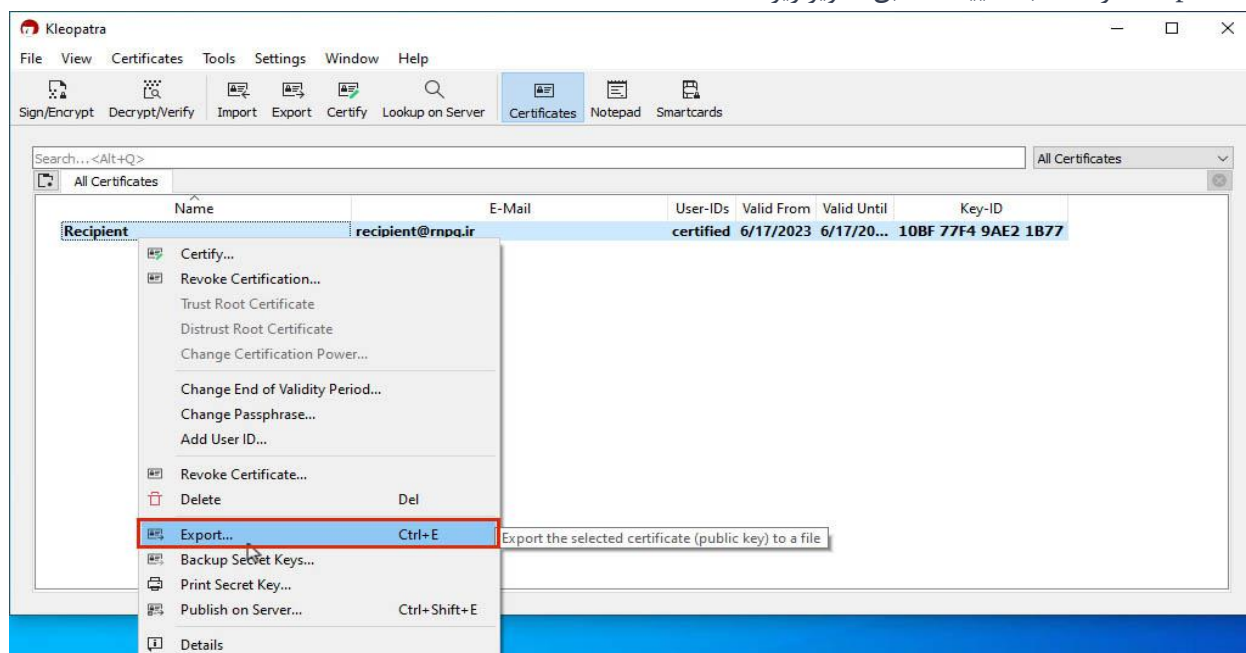
- در آخر بر روی گزینه "OK" کلیک نمایید.

۲. نحوه خروجی گرفتن کلید عمومی خود

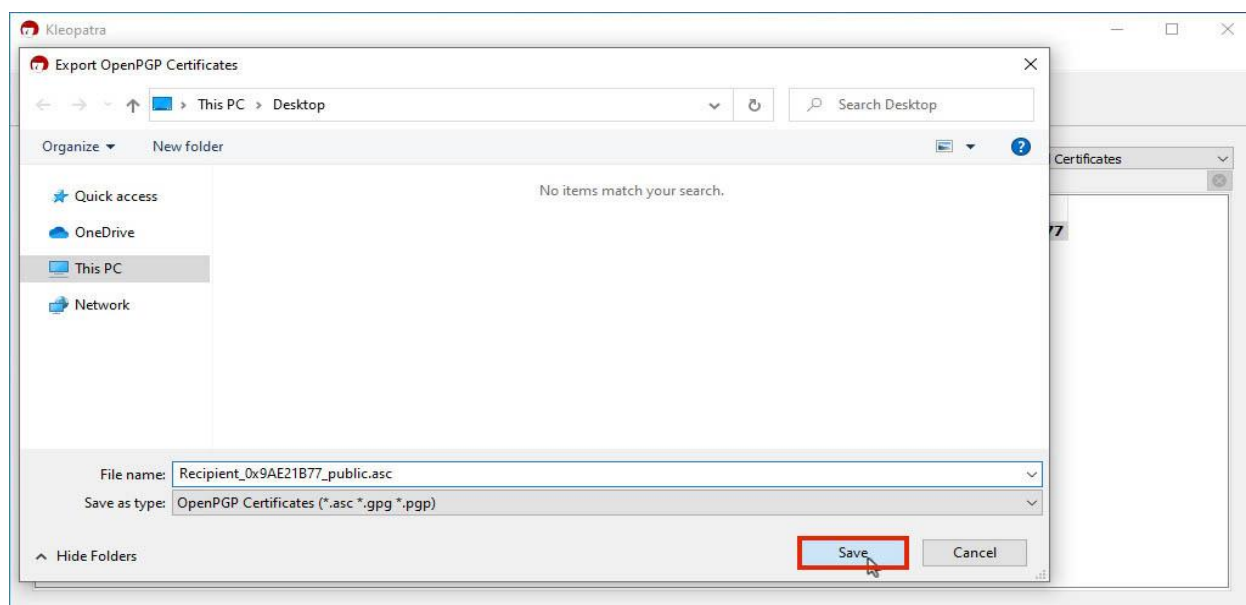
در مراحل بالا به آموزش ساخت کلید پرداخته شد. در ادامه، به نحوه خروجی گرفتن از کلید عمومی خود و ارسال آن به دیگران، جهت رمزگذاری فایل محرمانه توسط دیگران برای شما (با کلید عمومی شما) آموزش داده شده است.

تا به این مرحله، کلید عمومی و خصوصی ساخته شده است و در نرم افزار Kleopatra موجود می باشد. حال برای آن که دیگران بتوانند یک فایل محرمانه برای ما ارسال کنند که فقط ما قادر به رمزگشایی آن باشیم، می بایست کلید عمومی ما را در اختیار داشته باشند.

به منظور استخراج کلید عمومی خود، بر روی کلید ساخته شده در محیط نرم افزار Kleopatra کلیک راست نموده و گزینه "Export..." را انتخاب نمایید. (مطابق تصویر زیر)



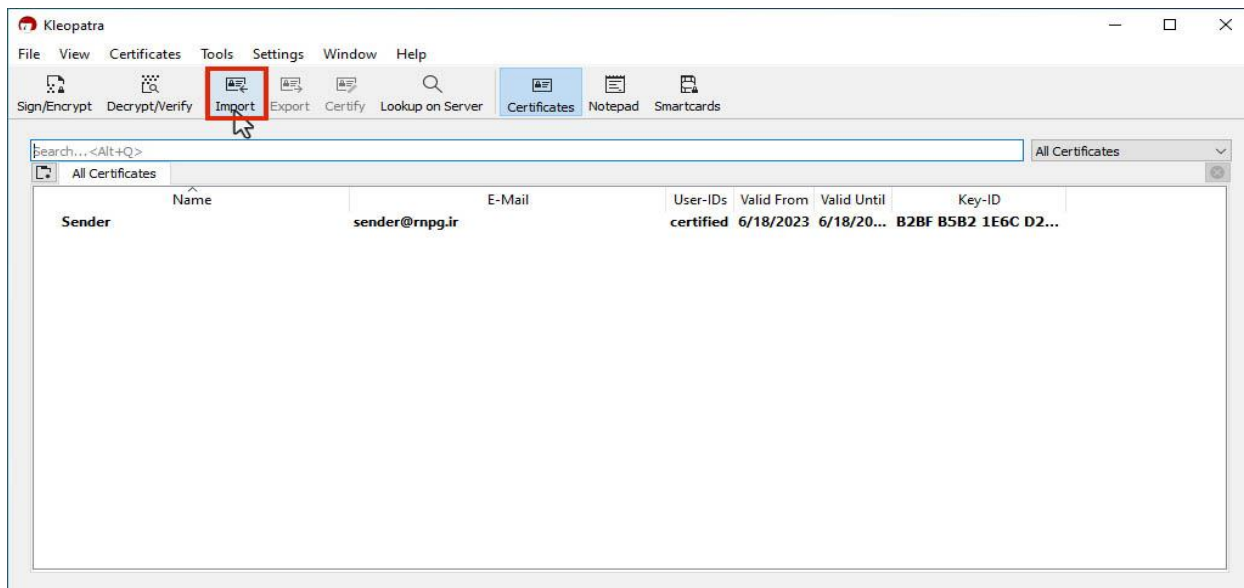
سپس آن را در مسیر دلخواه خود مطابق تصویر زیر، Save نمایید.



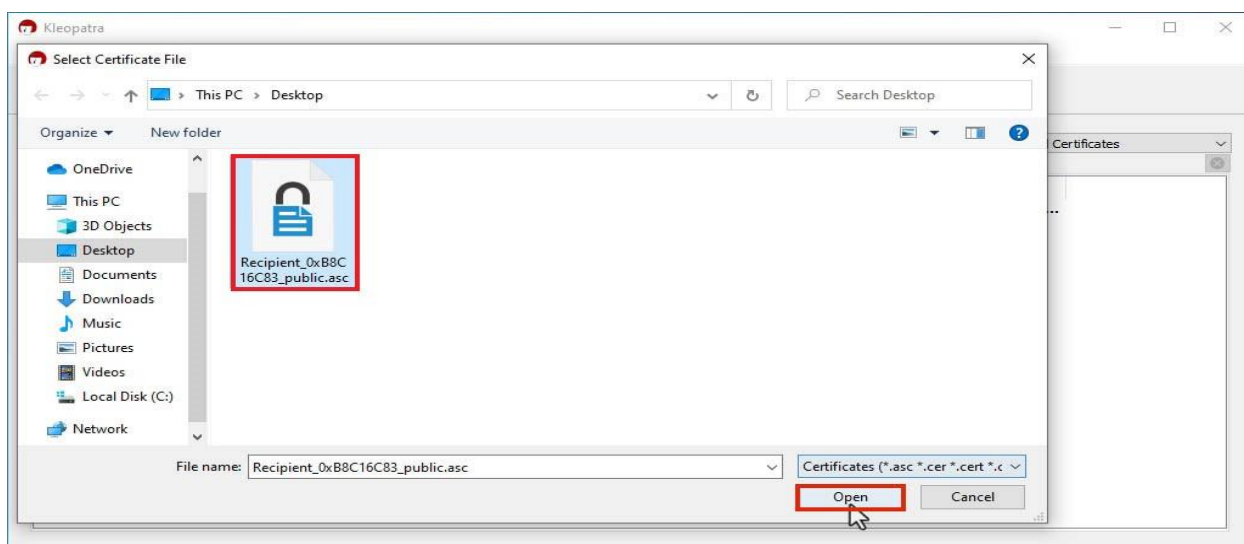
در آخر، فایل مذکور را می‌توان برای دیگران ارسال نمود تا فایل‌های محرمانه با کلید عمومی شما، رمز گذاری شوند و با کلید خصوصی خود، آن را رمزگشایی نمایید.

۳. نحوه وارد نمودن کلید عمومی دیگران

همانطور که پیش‌تر به آن اشاره شد، هنگامی که بخواهیم یک فایل محرمانه را برای دیگران رمزگذاری و ارسال کنیم، می‌بایست کلید عمومی گیرنده فایل را داشته باشیم تا با کلید عمومی او، فایل مذکور را رمزگذاری نماییم. به منظور وارد نمودن کلید عمومی دیگران در محیط Kleopatra، بر روی دکمه "Import" مطابق تصویر زیر کلیک نمایید.

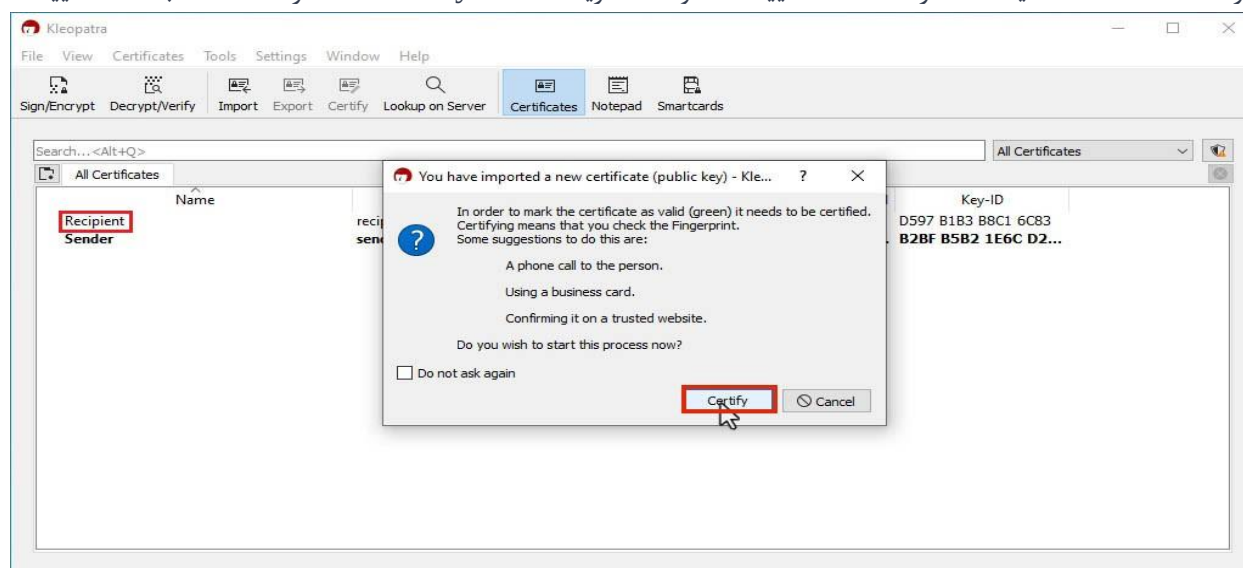


سپس مطابق تصویر زیر، کلید عمومی دریافت شده از شخص دیگر را انتخاب نمایید.

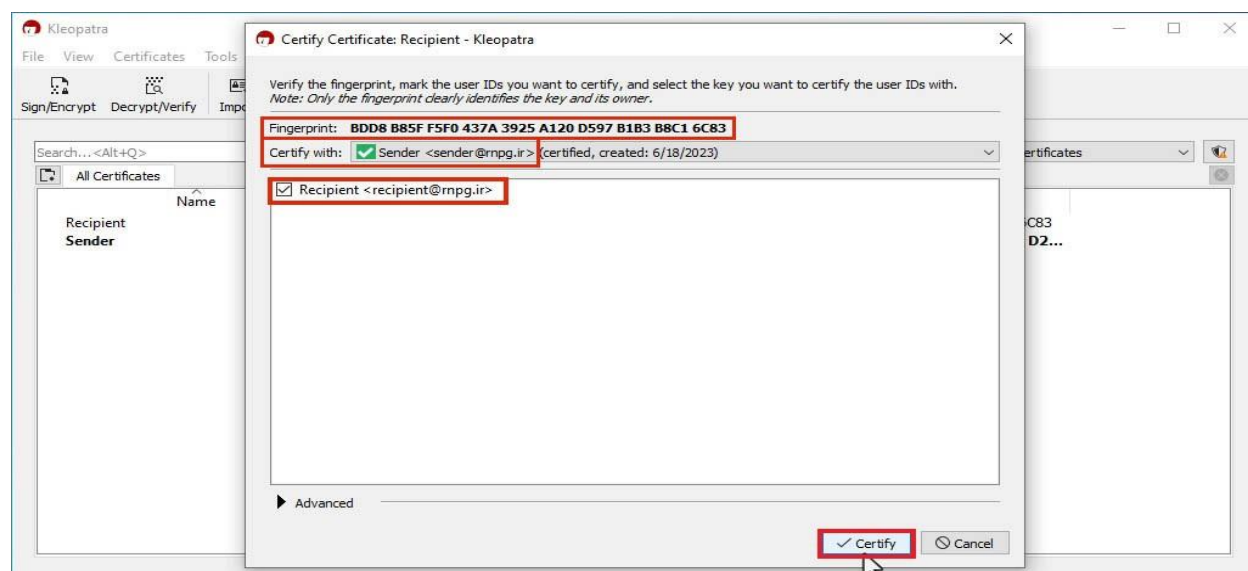


همانطور که در تصویر زیر قابل مشاهده می‌باشد، برای اینکه اطمینان حاصل کنید که کلید عمومی وارد شده دقیقاً همان کلید عمومی ارسالی از طرف مقابل می‌باشد، می‌بایست آن را Certify کنید، بنابراین بر روی گزینه "Certify" کلیک نمایید.

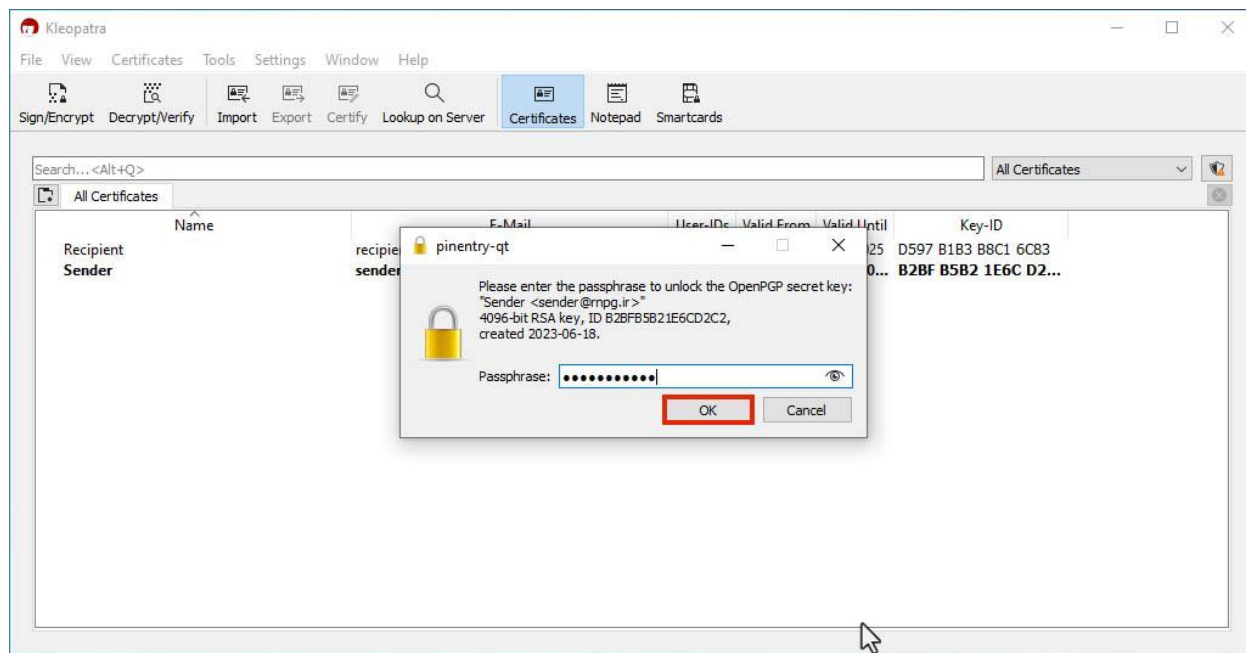
• نکته: در صورتی که پنجره مذکور نمایش داده نشد، می‌توانید وارد محیط نرم افزار Kleopatra شده و بر روی کلید عمومی وارد شده، کلیک راست نمایید و گزینه "Certify..." را انتخاب نمایید.



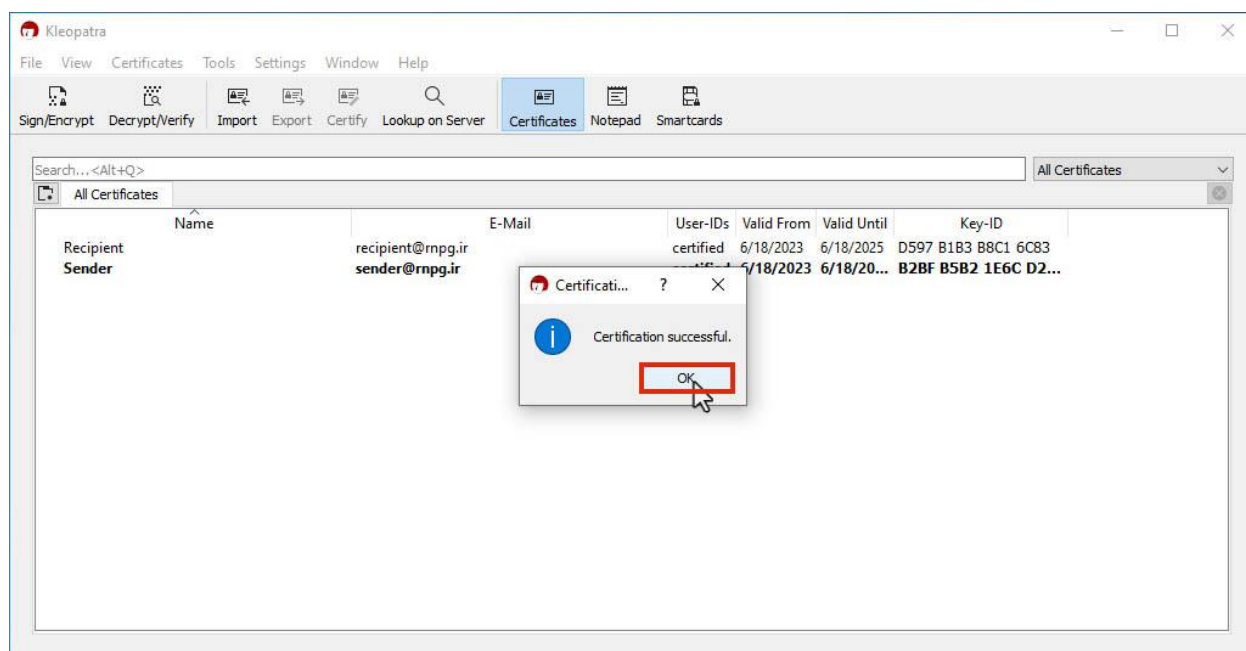
در ادامه، همانند تصویر زیر می‌بایست در قسمت "Certify with" مشخص نمایید که با کدام یک از کلیدهای خصوصی خود، قصد انجام این کار را دارید، سپس می‌بایست مقدار Fingerprint را که برابر با ۴۰ کاراکتر می‌باشد، از طریق یک بستر ارتباطی امن (به صورت حضوری، از طریق تماس تلفنی و ...) با طرف مقابل بررسی نمایید تا مغایرت نداشته باشد. در صورت عدم مغایرت، تیک کلید عمومی را فعال نموده و گزینه "Certify" را کلیک نمایید.



در آخر، رمز عبور کلید خصوصی خود را وارد نموده و روی OK کلیک نمایید.

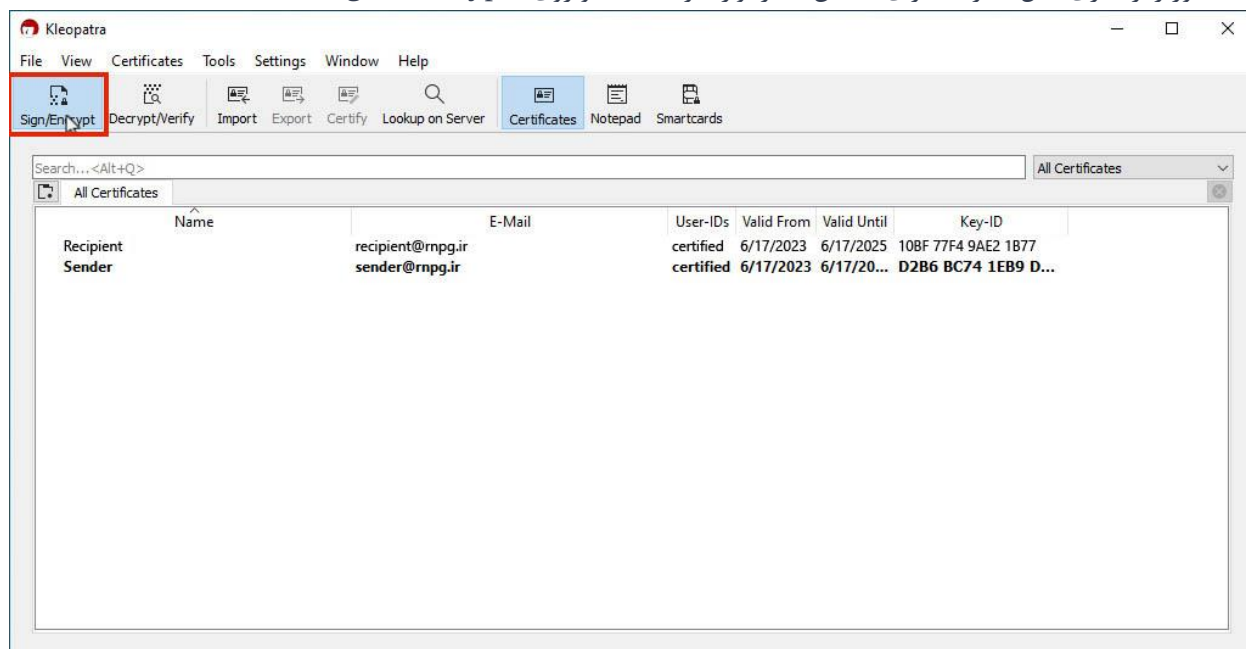


پس از دریافت پیام موفقیت، روی OK کلیک نمایید.

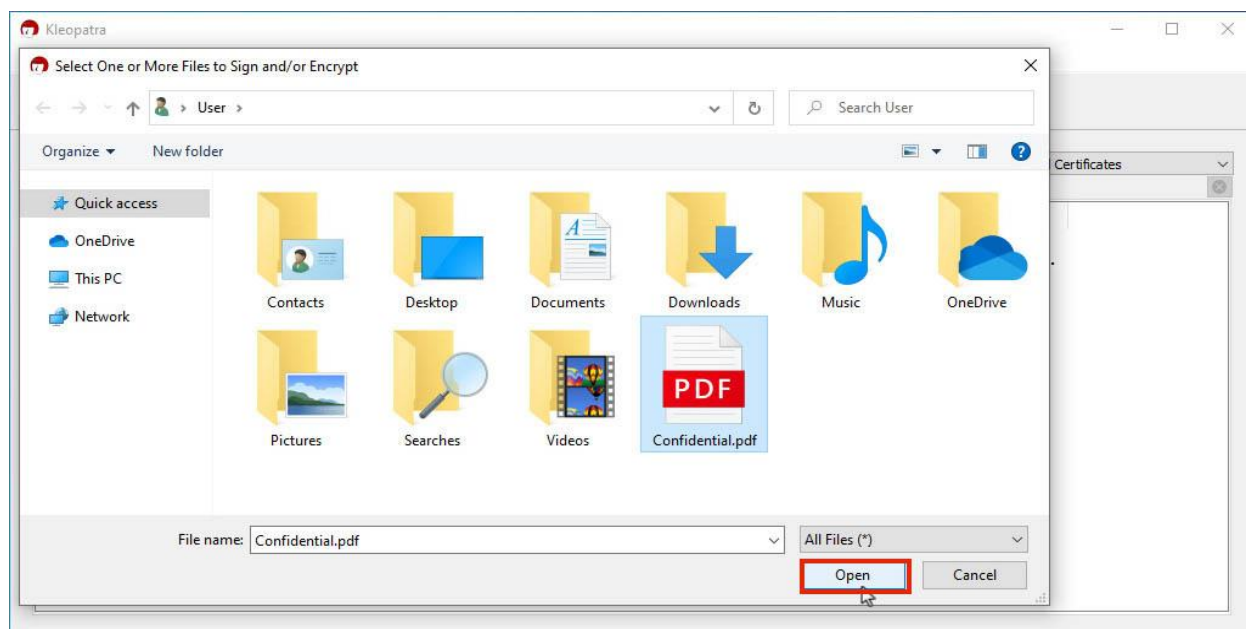


۴. نحوه رمزگذاری فایل برای دیگران

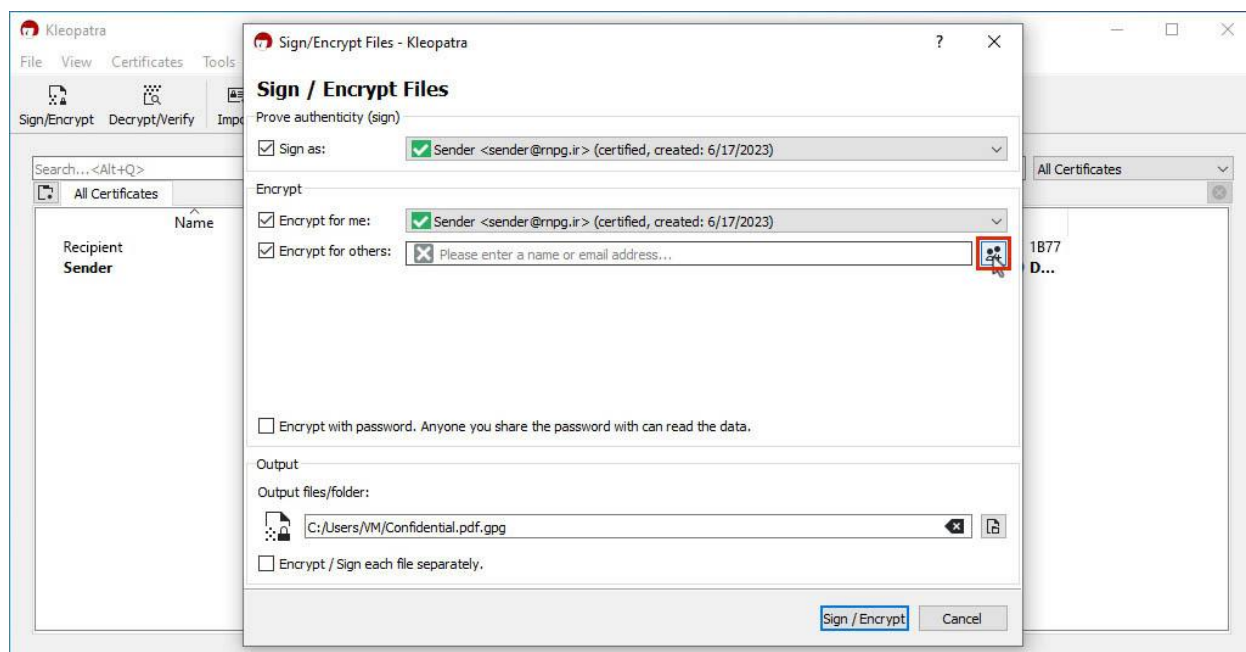
به منظور رمزگذاری فایل محرمانه برای شخص دیگر، وارد برنامه شده و روی "Sign / Encrypt" کلیک نمایید.



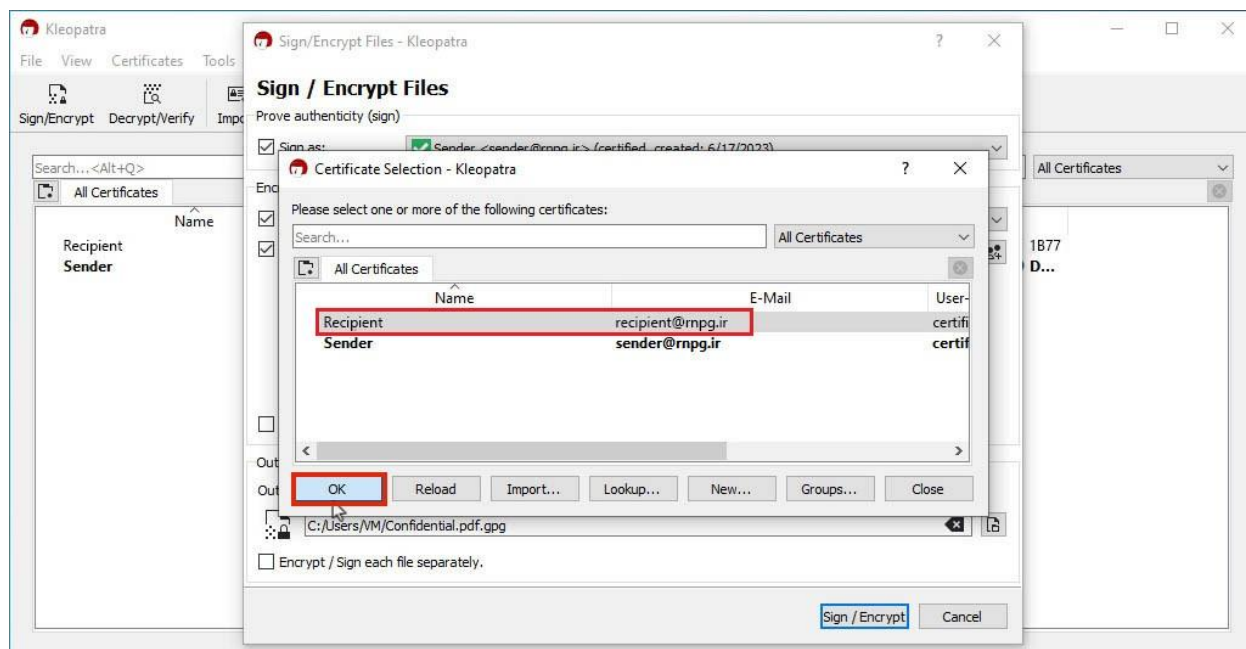
سپس فایل مورد نظر را انتخاب کرده، و روی "Open" کلیک نمایید.



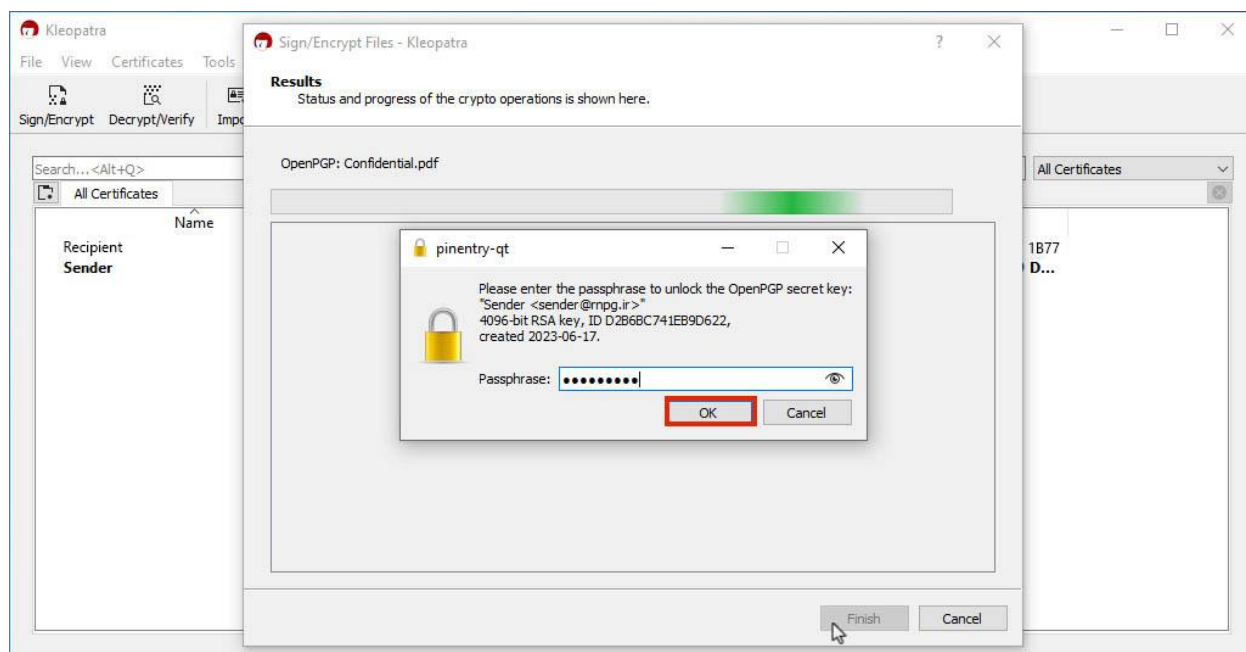
سپس مطابق تصویر زیر، روی دکمه نمایش داده شده کلیک نمایید.



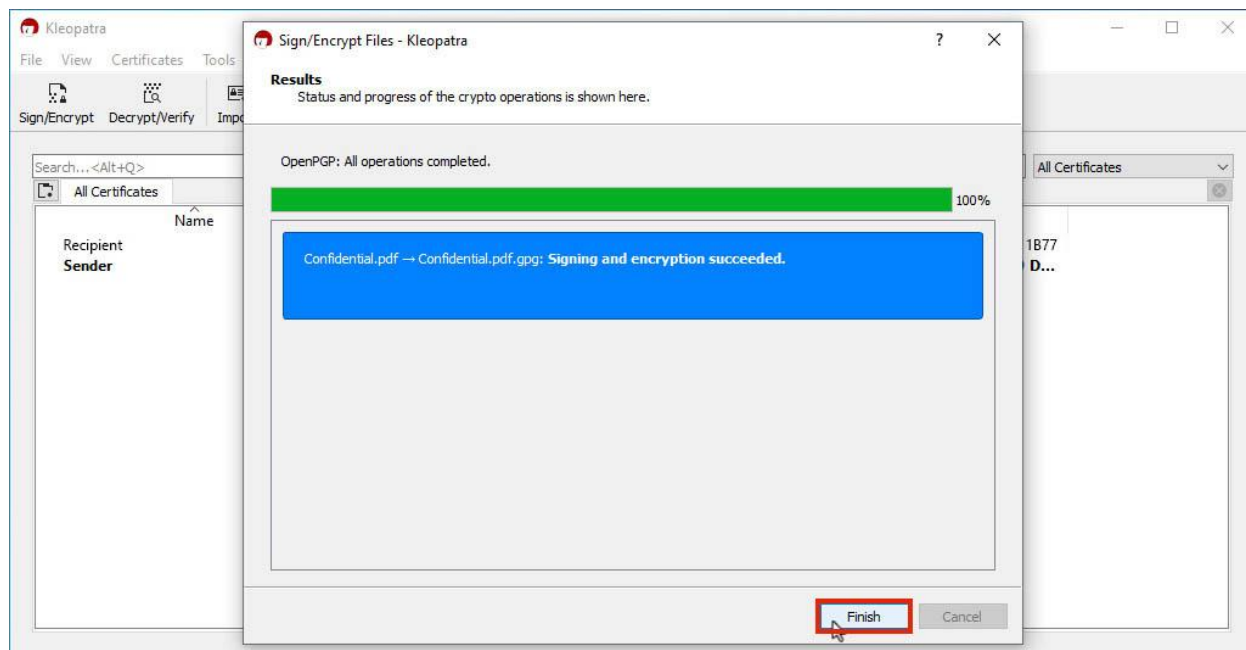
سپس از لیست نمایش داده شده، دریافت کننده پیام را انتخاب نموده و روی "OK" کلیک نمایید.



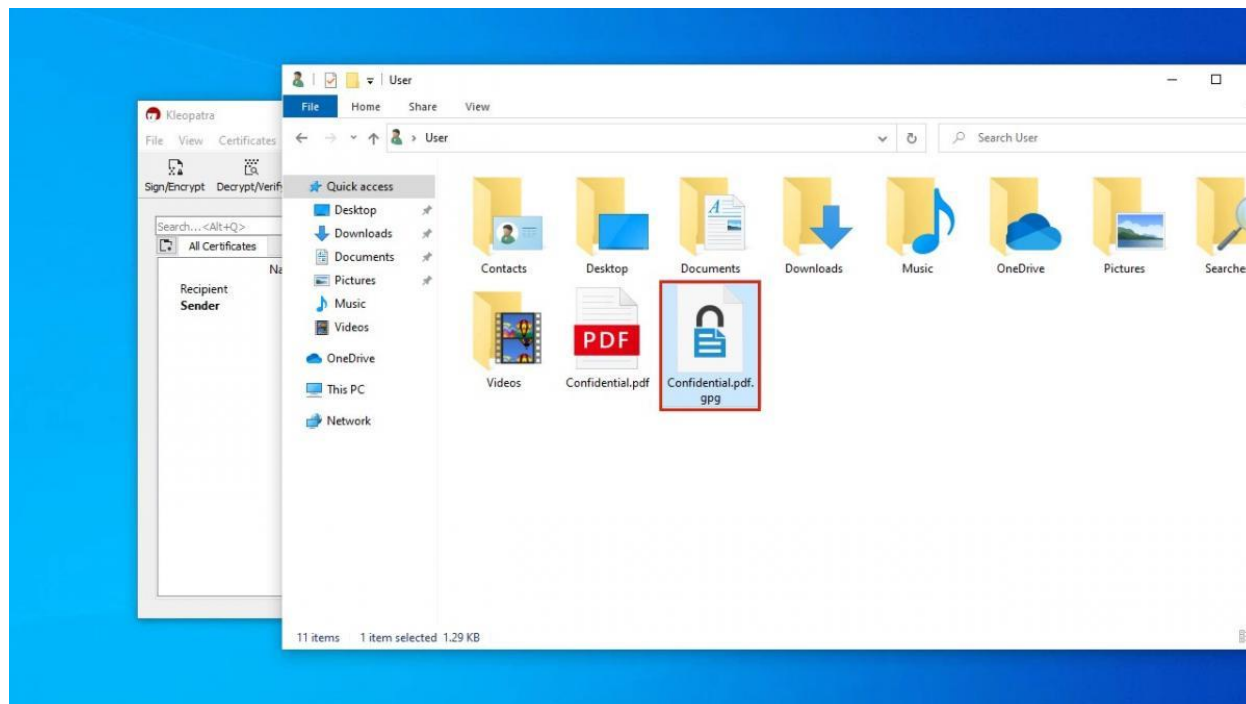
رمز عبور خود را وارد نموده و سپس روی "OK" کلیک نمایید.



پس از نمایش داده شدن پیام موفقیت، روی "Finish" کلیک نمایید.

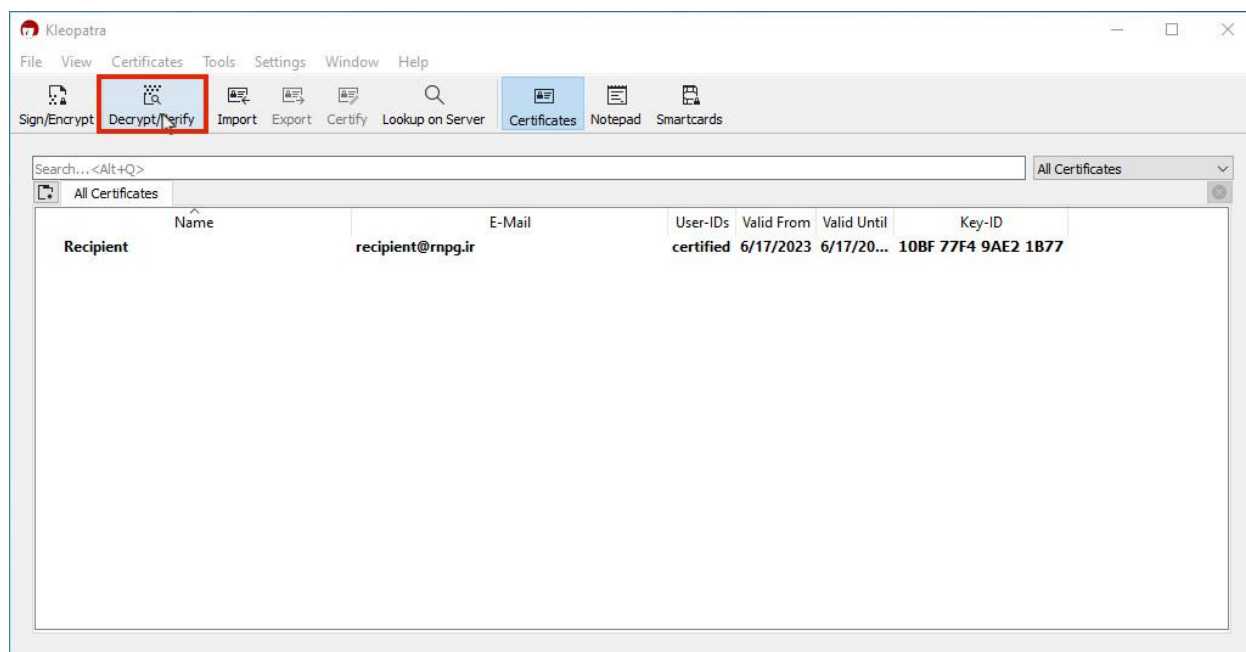


فایل رمزنگاری شده با پسوند **gpg** در کنار فایل اصلی ایجاد خواهد شد.

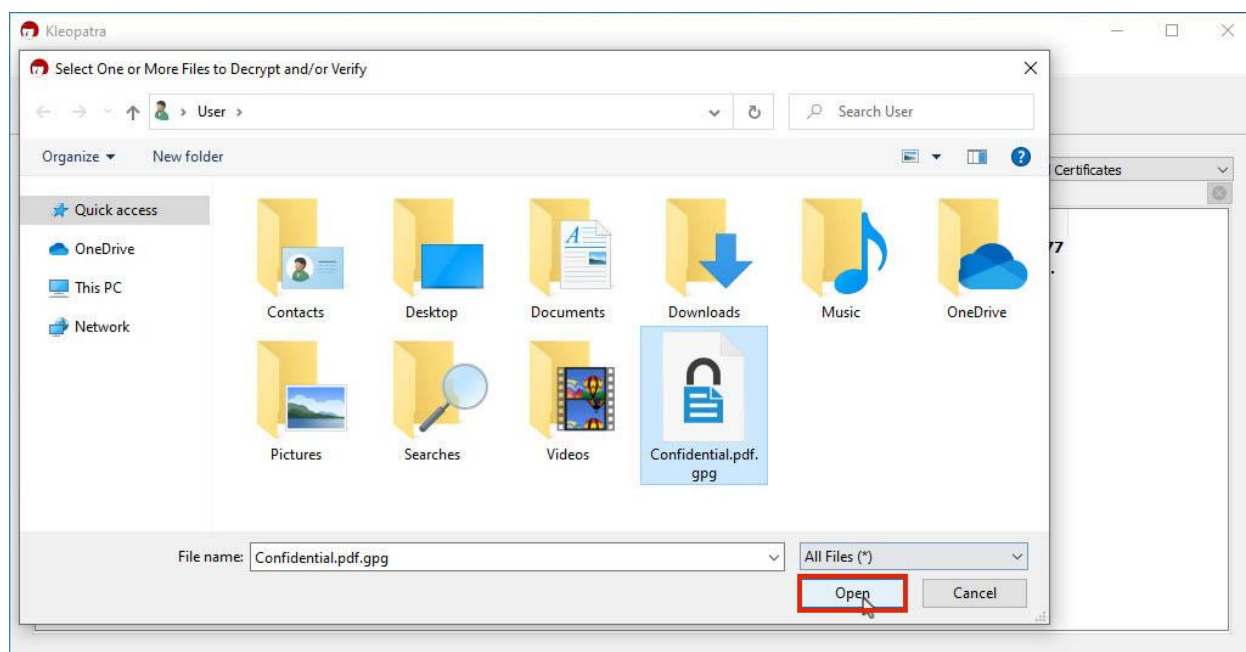


۵. نحوه رمزگشایی فایل

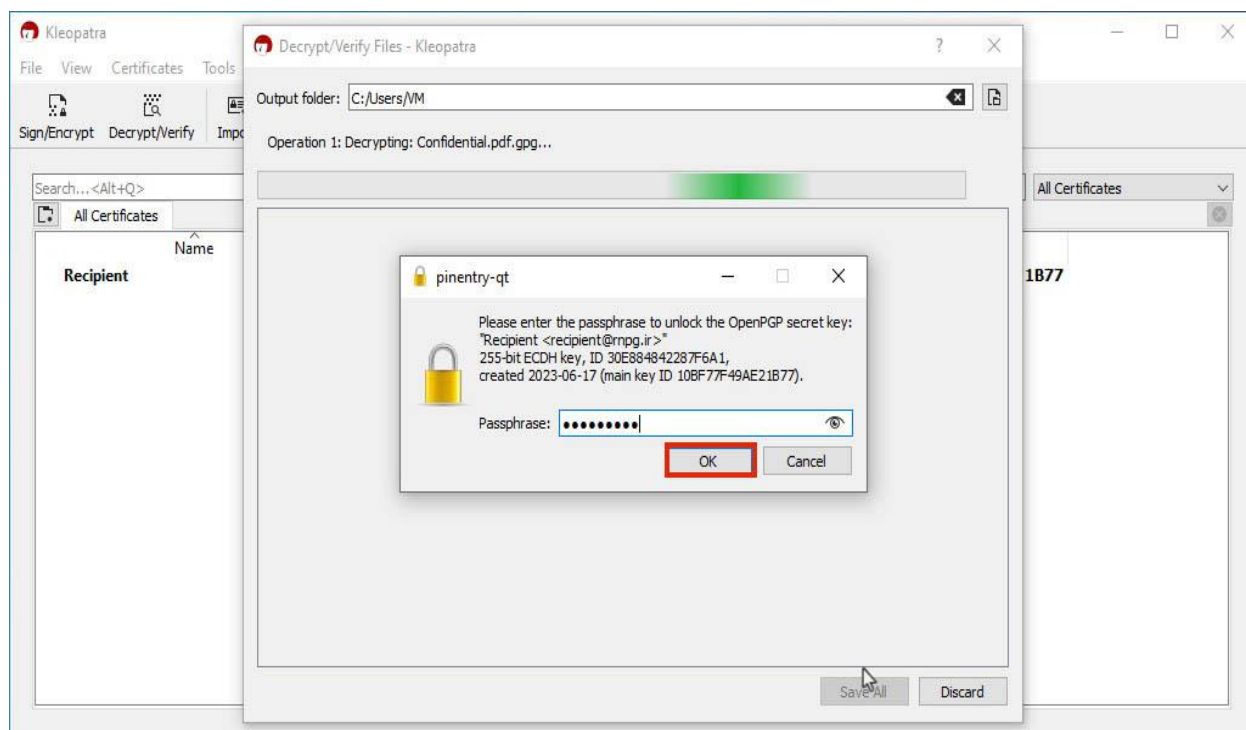
به منظور رمزگشایی فایل دریافتی، وارد برنامه شده و مطابق تصویر زیر، روی "Decrypt/Verify" کلیک نمایید.



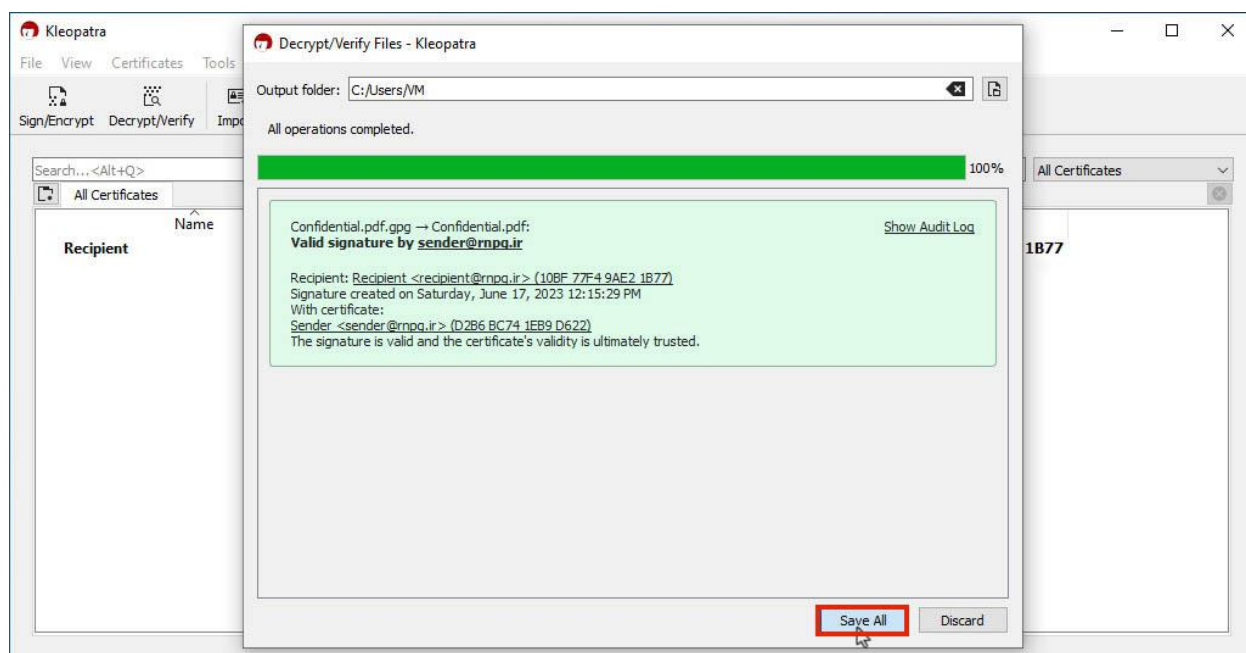
فایل رمزگذاری شده را انتخاب و سپس روی Open کلیک نمایید.



سپس رمز عبور تعریف شده در زمان ساخت کلید را وارد نمایید و روی "OK" کلیک نمایید.



در آخر بر روی گزینه "Save All" کلیک نمایید.



همانطور که در تصویر زیر قابل مشاهده می‌باشد، فایل Clear text در همان مسیر ایجاد و ذخیره می‌شود و می‌توان به محتویات آن دسترسی داشت.

