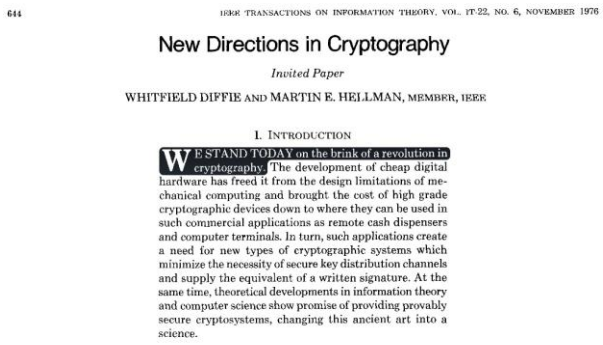
تاریخچه و راهنمای PGP: مقدمه

سی سال پیش، در اوایل ژوئن ۱۹۹۱، فیلیپ زیمرمن (Philip Zimmermann) نرم‌افزاری رو عرضه کرد که چهرهٔ حریم خصوصی رو برای همیشه تغییر و دنیا رو در مسیری تازه قرار داد.

اینجا خواهیم دید نتیجهٔ سال‌ها تلاش و فداکاری یک نفر چطور رمزنگاری رو از سلطهٔ دولت‌ها خارج کرد و به دست مردم عادی رسوند.

از راست به چپ، ویتفیلد دیفی، مارتین هلمن، و رالف مرکل



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

I. INTRODUCTION

WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

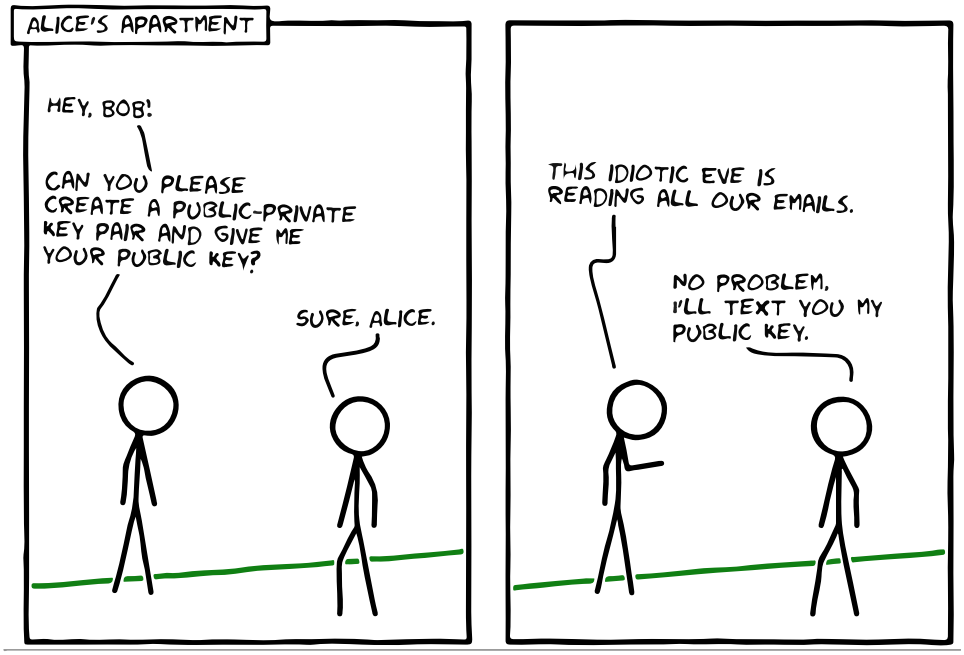
مقالهٔ انقلابی ویتفیلد دیفی و مارتین هلمن، نوامبر ۱۹۷۶

وقتی راجع به رمزنگاری مدرن صحبت می‌کنیم، باید به دههٔ ۱۹۷۰ برگردیم، زمانی که ویتفیلد دیفی، مارتین هلمن، و رالف مرکل پایهٔ رمزنگاری کلید عمومی رو بنا نهادن.

مرکل رو، که الهام‌بخش دیفی و هلمن در رسیدن به ایدهٔ رمزنگاری نامتقارن بود، ممکنه با طرح درخت مرکل (Merkle tree) بشناسیم.

ظهور رمزنگاری کلید عمومی

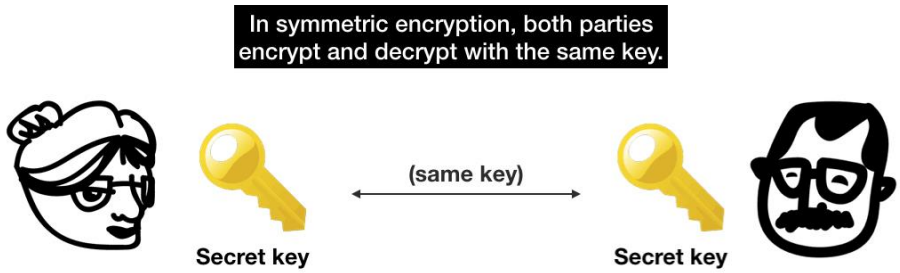
رمزنگاری کلید عمومی ایده‌ای خارق‌العاده و انقلابی بود. هر کاربر دو کلید داره: یکی عمومی و دیگری خصوصی. کلید عمومی می‌تونه با هر کسی به‌اشتراک گذاشته بشه، بدون اینکه امنیت رو به‌خطر بی‌اندازه. از کلید خصوصی، اما، باید از رمز حساب بانکی‌تون هم بیشتر محافظت کنید.



هرچیزی که با یکی از کلیدها رمز بشه، با کلید دوم گشوده می‌شه.

در اینجا، از دو اصطلاح متن آشکار (plaintext) و متن رمزنگاری‌شده (ciphertext) استفاده می‌کنیم. اگه من بخوام پیام امنی رو به دست شما برسونم، اون رو با کلید عمومی شما رمزنگاری و متن رمزنگاری‌شده رو برای شما ارسال می‌کنم.

شما، که کلید خصوصی مربوطه رو دارید، به‌راحتی می‌تونید متن رمزنگاری‌شده رو رمزگشایی و اون رو به متن آشکار تبدیل کنید.



در رمزنگاری متقارن، از یک کلید هم برای رمزنگاری و هم برای رمزگشایی استفاده می‌شه، به این معنا که فرستنده و گیرنده هر دو به یک کلید مشترک دسترسی دارن، و این، در بعضی موارد استفاده، می‌تونه ضعف محسوب بشه.

تا قبل از این، افراد از رمزنگاری متقارن استفاده می‌کردن. در این سیستم، دو طرف به یک کلید خصوصی مشترک دسترسی دارن، و ارسال کلید به روشی امن کار رو دشوار می‌کنه.

مسیری که فیلیپ زیمرمن هموار کرد

اما می‌رسیم به فیلیپ زیمرمن، نقشی که در دفاع از حریم خصوصی داشت، و دوره‌ای که بعدها به جنگ‌های رمزنگاری (Crypto Wars) معروف شد. جنگ جهانی دوم نشون داد رمزنگاری چقدر می‌تونه در استفاده‌های نظامی مهم باشه، و همین باعث شد این تکنولوژی در دستهٔ تسلیحات نظامی (munition) قرار بگیره.

باورش امروز ممکنه سخت باشه، اما تا ۱۹۹۲، رمزنگاری به‌عنوان تجهیزات نظامی کمکی (Auxiliary Military Equipment) در لیست تسلیحات ایالات متحده شناخته می‌شد، و صادرکردن هر نوع رمزنگاری‌ای—از روش‌ها گرفته تا حتی شرح اون‌ها—به‌شدت سخت‌گیرانه و نیازمند مجوز بود.

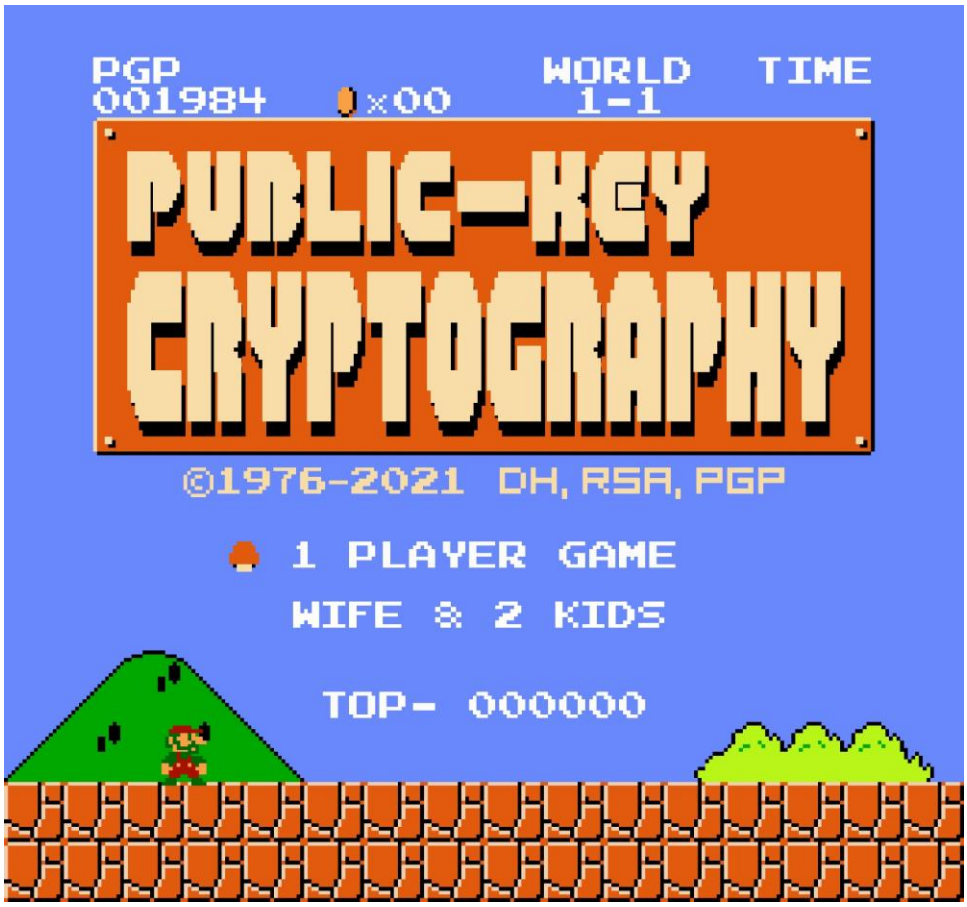
فیلیپ زیمرمن، خالق PGP

با انتشار عمومی الگوریتم‌های رمزنگاری مثل DES (استاندارد رمزنگاری داده‌ها) و روش‌های رمزنگاری نامتقارن، ظهور اینترنت، و البته تلاش‌ها و فداکاری عده‌ای در راستای حفظ حریم خصوصی (با وجود ریسک محاکمه‌شدن)، راه برای برچیده‌شدن چنین سیاست‌هایی هموارتر شد.

زیمرمن یکی از اون افراد بود.

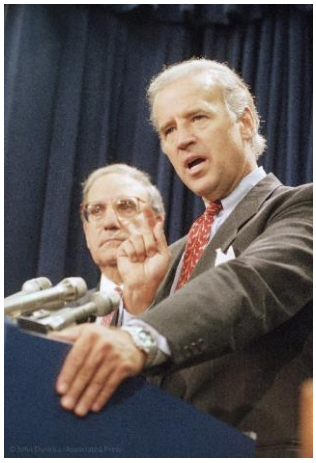
تا اون‌موقع، رمزنگاری قوی تنها در سلطهٔ دولت‌ها بود. اما چی می‌شد اگه نرم‌افزاری داشتیم که الگوریتم‌های رمزنگاری RSA رو به کامپیوترهای شخصی می‌آورد، و افراد عادی می‌تونستن مکالمه‌های روزمره و حتی فایل‌هاشون رو خودشون رمزنگاری کنن؟

این سؤالی بود که در ۱۹۷۷ به ذهن زیمرمن خطور کرد، اما کار جدی برای پاسخ به اون رو تا ۱۹۸۴ شروع نکرد. هرچی بیشتر به مشکلات پیرامون حریم خصوصی فکر می‌کرد، بیشتر به اهمیت این پروژه پی می‌برد. زیمرمن بعدها در شرح نرم‌افزارش حرف‌های قابل‌تأملی می‌نویسه، به‌ویژه در انتهای پاراگراف اول.



تشبیه فیلیپ زیمرمن به سوپر ماریو (تصویرسازی: MC Saeid)

زیمرمن، که تخصص ویژه‌ای در رمزنگاری نداشت، کند پیش می‌رفت. درحالی‌که شغل اصلی خودش رو داشت، دارای همسر و دو فرزند هم بود، و همین موضوع باعث می‌شد تا نتونه با اون سرعتی که می‌خواد پروژه رو پیش ببره. بااین‌حال، ازش دست نکشید. در ۱۹۸۶ موفق شد RSA رو پیاده‌سازی کنه.



۱۹۹۱ رسید، و زیمرمن همچنان نرم‌افزار کاملی برای عرضه نداشت، تا اینکه بایدن (که در اون زمان سناتور بود) قدمی برداشت که باعث شد زیمرمن چندین ماه بی‌وقفه روی پروژه کار کنه تا اون رو به‌پایان برسونه.

نقش بایدن چی بود، و چرا زیمرمن احساس می‌کرد باید هرچه‌زودتر نرم‌افزار رو منتشر کنه؟

در ژانویهٔ ۱۹۹۱، بایدن لایحهٔ ۲۶۶ رو پیشنهاد داد. جایی در این متن اومده که شرکت‌ها موظفن درصورت ارائهٔ درخواست قانونی، محتوای متنی، صوتی، و دادهٔ افراد رو دراختیار دولت قرار بدن. این همون آیندهٔ اورولی‌ای بود که زیمرمن تلاش می‌کرد ازش جلوگیری کنه.

همین موضوع به زیمرمن هدف تازه‌ای داد. حالا مسیرش مشخص بود. باید قبل از اینکه کنگره راهی پیدا می‌کرد تا جلوی ارتباط امن و خصوصی افراد رو بگیره، نرم‌افزارش رو آماده و عرضه می‌کرد. اقدام بایدن او رو مصمم کرد تا در ماه‌های آتی شبانه‌روز تلاش کنه و بالاخره پروژه رو سرانجام بده.

فیلیپ زیمرمن در ۱۹۹۶ (عکس: هلن دیویس)

۵ ژوئن ۱۹۹۱ روزی بود که فیلیپ زیمرمن، پس از گذر از مسیری پرپیچ‌وخم که چندین سال از عمرش رو صرفش کرده بود، بالاخره نرم‌افزارش رو عمومی کرد و نام اون رو PGP گذاشت—کوتاه‌شدهٔ Pretty Good Privacy یا «حریم خصوصی بسیار خوب».

فکر گرفتن کارمزد جهت استفاده از PGP از ذهنش عبور کرده بود، اما ازاونجایی‌که می‌ترسید روزی دولت استفاده از رمزنگاری رو ممنوع کنه، می‌خواست قبل از رسیدن چنین روزی همه تاحدامکان از ابزارهای حریم خصوصی بهره‌مند بشن. درنتیجه، تصمیم گرفت ثمرهٔ سال‌ها زحمتش رو مجانی منتشر کنه.

زیمرمن حتی تا مرز ازدست‌دادن خونهٔ خودش هم رفت چون از ابتدای ۱۹۹۱ تا زمان انتشار از پرداخت پنج قسط وام خونه‌ش عقب مونده بود و مجبور شد بانک رو قانع کنه تا خونه‌ش رو نگیره.

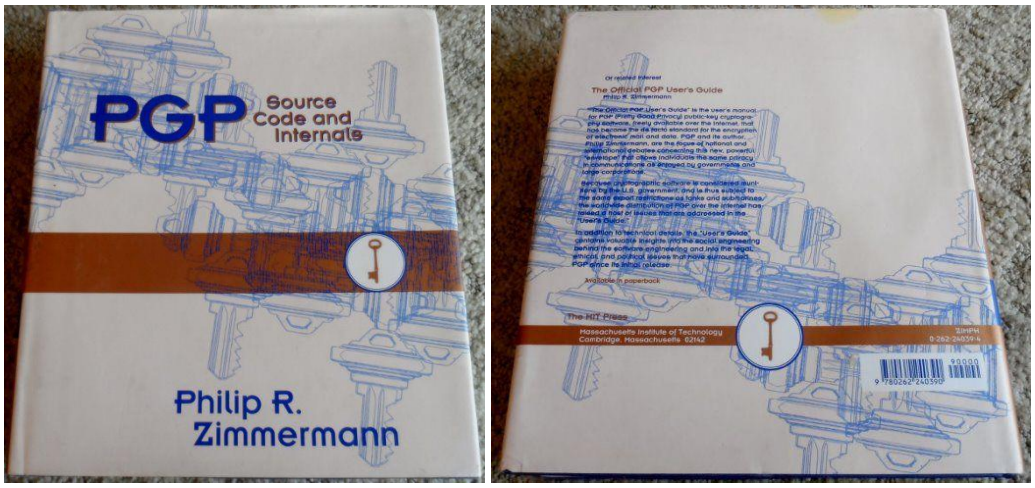
این، از دید من، نشون از فداکاری بزرگش داره.

دردسرهای حقوقی

زیمرمن، که در اون زمان اطلاعات چندانی راجع به اینترنت نداشت، اولین نسخهٔ PGP رو به دو نفر از دوستانش داد تا اون رو آپلود کنن. نرم‌افزار خیلی زود دست‌به‌دست شد و سر از اروپا و کشورهای دیگه درآورد.

«مثل هزاران دونهٔ قاصدک در دست باد»، زیمرمن توصیف می‌کنه PGP در اینترنت پخش می‌شد.

درحالی‌که استفاده از PGP در ایالات متحده آزاد بود، وقتی در کشورهای دیگه پدیدار شد (و PGP در زمان کوتاهی به محبوبیت بسیار بالایی بین کاربرها رسید)، دردسرهای قانونی‌ای برای زیمرمن درپی داشت. همون‌طور که می‌دونیم، صادرکردن چنین رمزنگاری قدرتمندی در اون زمان غیرقانونی محسوب می‌شد.



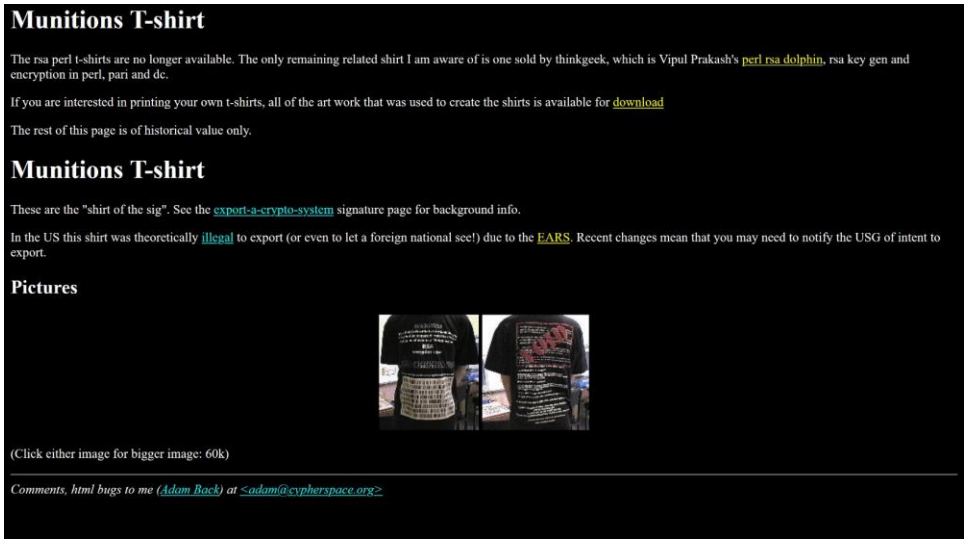
کتاب PGP: Source Code and Internals، انتشارات ام‌آی‌تی، ۱۹۹۵

سال ۱۹۹۳ و به مدت سه سال، زیمرمن درگیر یک پروندهٔ قضایی با دولت آمریکا شد. جرم؟ زیرپاگذاشتن قانون کنترل صادرات اسلحه (Arms Export Control Act).

زیمرمن در پاسخی زیرکانه، با همکاری انتشارات MIT، یکی از برجسته‌ترین ناشرها در سطح ملی و جهانی، سورس کد PGP رو در قالب کتاب منتشر کرد. براساس متمم اول (First Amendment) قانون اساسی ایالات متحده و زیرمجموعهٔ قانون آزادی بیان، نشر و صادرات کتاب هیچ‌گونه محدودیتی نداره. با انتشار کد PGP در قالب کتاب و فروشش در سطح جهانی، زیمرمن سعی داشت نشون بده اتهامش در صادرکردن «نرم‌افزار» بی‌معنیه.

برای دیدن تصویر بزرگ‌تر کلیک کنید.

پیش‌تر به تلاش‌ها و فداکاری عده‌ای در راستای هدفی بالاتر و با وجود دونستن ریسک‌ها اشاره شد. یکی از این نافرمانی‌های مدنی، از یکی از قدیمی‌ترین و شناخته‌شده‌ترین سایفرپانک‌هاست: آدام بک. روی این تی‌شرت پنج خط کد به زبان Perl وجود داره که RSA رو به شما می‌ده.



مشاهدهٔ سایت Cypherspace

اگه در ایالات متحده بودید، این تی‌شرت رو چاپ می‌کردید، و اون رو برای کسی در خارج از کشور می‌فرستادید و یا حتی به یک تبعهٔ خارجی (غیرآمریکایی) نشون می‌دادید، این کار جرم محسوب می‌شد.

درنهایت، همین تلاش‌ها بودن که باعث شدن رمزنگاری همه‌گیر بشه و ما امروز «حریم خصوصی» داشته باشیم. تا زمانی که اینجا هستیم، پیشنهاد می‌کنم دو مطلب بسیار مهم رو بخونید: A Cypherpunk's Manifesto و The Crypto Anarchist Manifesto. ترجمهٔ مطلب اول رو می‌تونید اینجا بخونید و ترجمهٔ مطلب دوم رو اینجا.

داستانی که خوندید تاحدامکان خلاصه شده و جزئیات ریز رو شامل نمی‌شه. چند دهه از اون دوران گذشته، و تنها راهی که می‌تونید تجربهٔ نزدیکی پیدا کنید (اگه بخواید) اینه که مصاحبه‌ها، کنفرانس‌ها، و مقاله‌های اون زمان رو ببینید و بخونید. در انتها منابعی رو برای کسانی که کنجکاون قرار می‌دم.

راه‌اندازی و استفاده از PGP

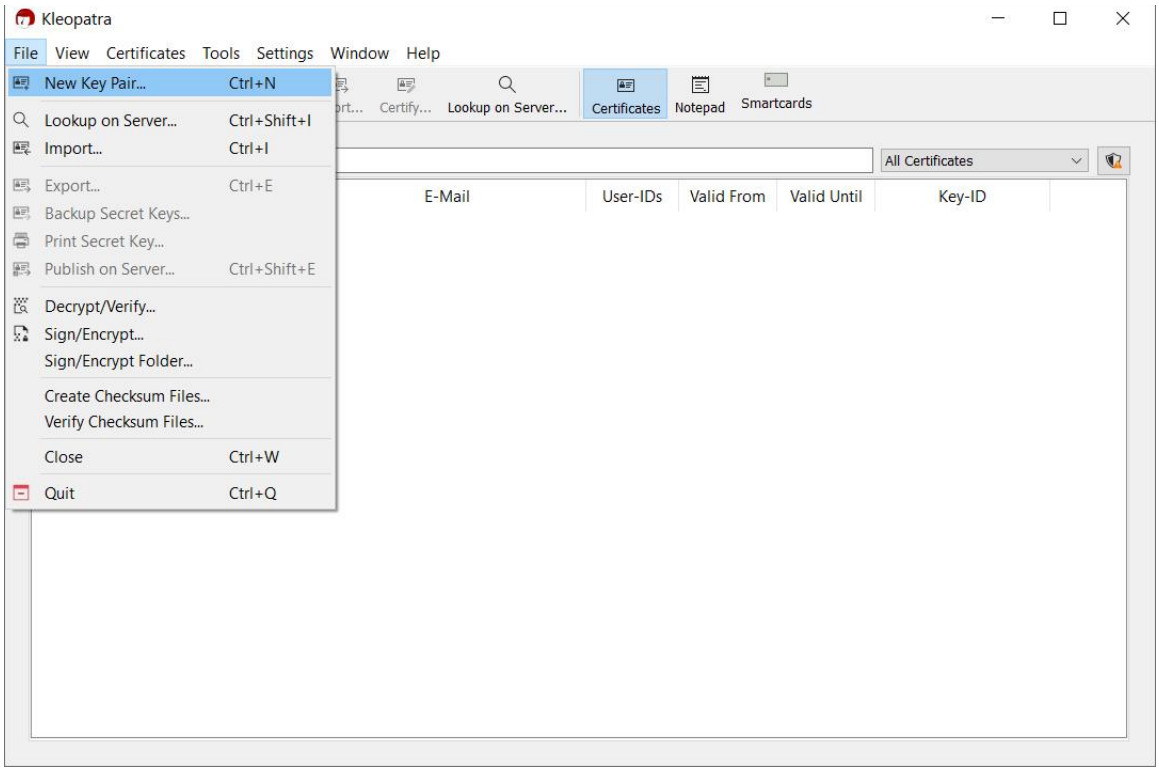
حالا که با تاریخچهٔ PGP آشنا شدیم، می‌تونیم کمی درمورد کاربرد و عملکردش صحبت کنیم. اولین قدم اینه که نرم‌افزارش رو دانلود و نصب کنیم و کلید خودمون رو بسازیم.

یکی از رایج‌ترین نرم‌افزارها GNU Privacy Guard یا GPG است. اگه کاربر ویندوز هستید (و این آموزش‌ها هم براساس این سیستم عامل هستن)، از Gpg4win استفاده کنید. لینک‌های دانلود برحسب سیستم عامل در سایت رسمی GnuPG قرار داده شده‌ن.

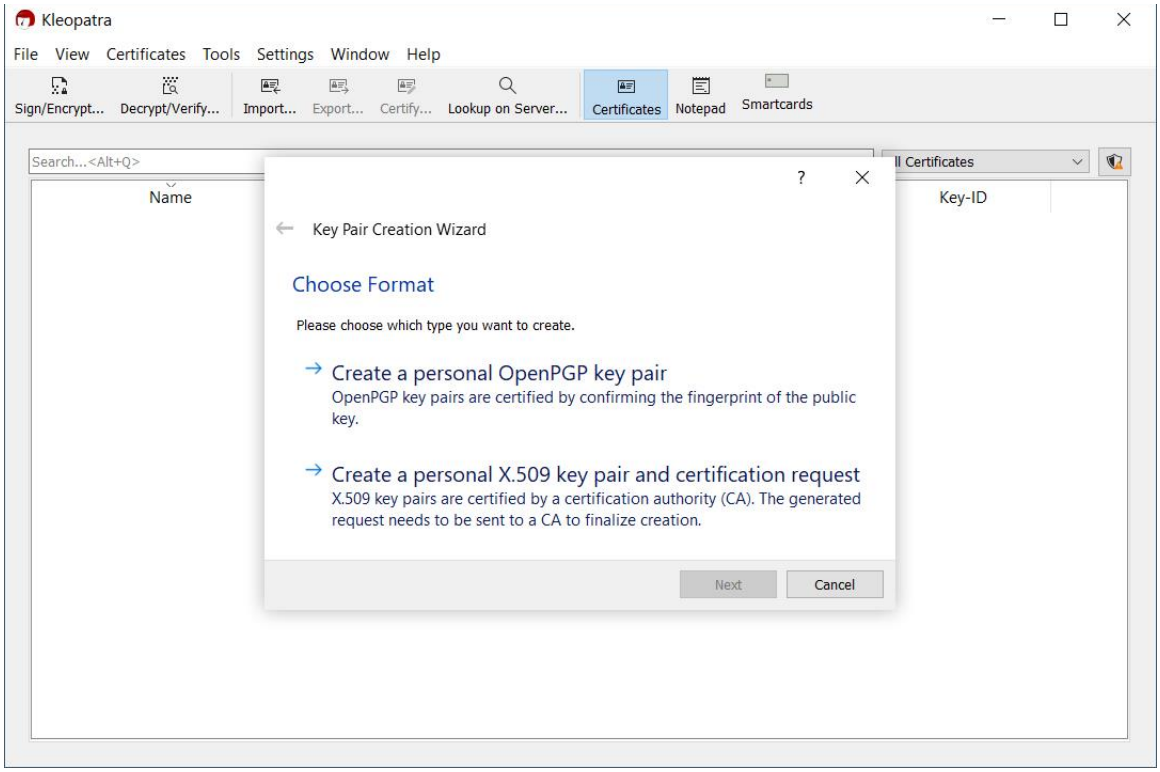
ساخت کلید

حقیقت جالب: کلئوپاترا (Cleopatra) آخرین فرعون مصر باستان و یکی از قدرتمندترین و بزرگ‌ترین پادشاه‌های زن در تاریخ بوده.

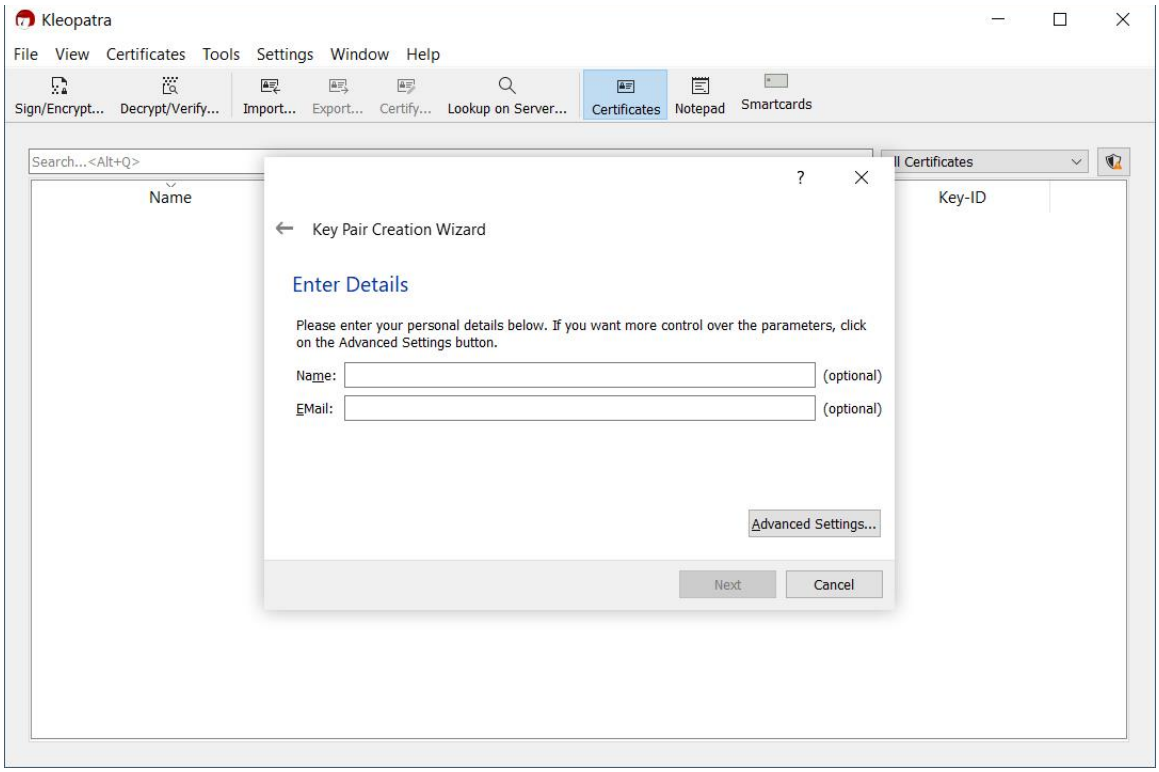
از نرم‌افزار Kleopatra برای تولید کلید شخصی، مدیریت کلیدها، رمزنگاری، و رمزگشایی استفاده می‌کنیم. به تصاویر صفحات بعد توجه کنید.



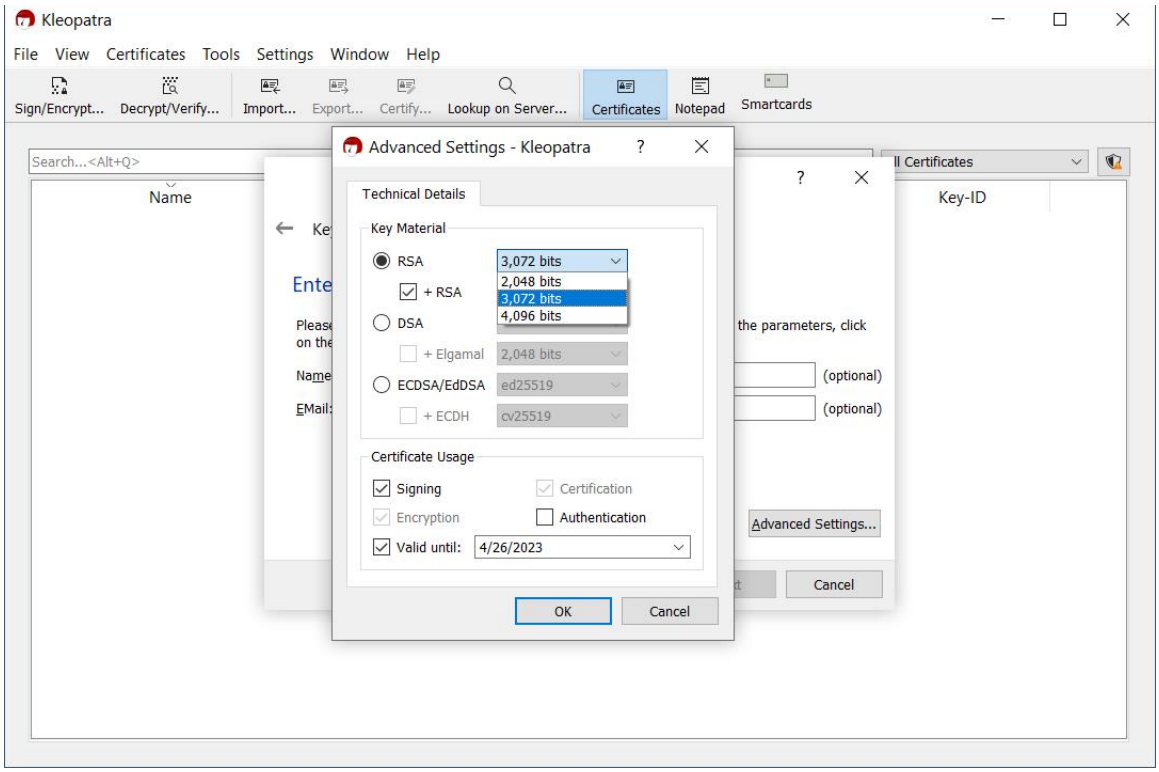
قدم اول در ساخت کلید: File → New Key Pair (یا استفاده از میانبر Ctrl + N)



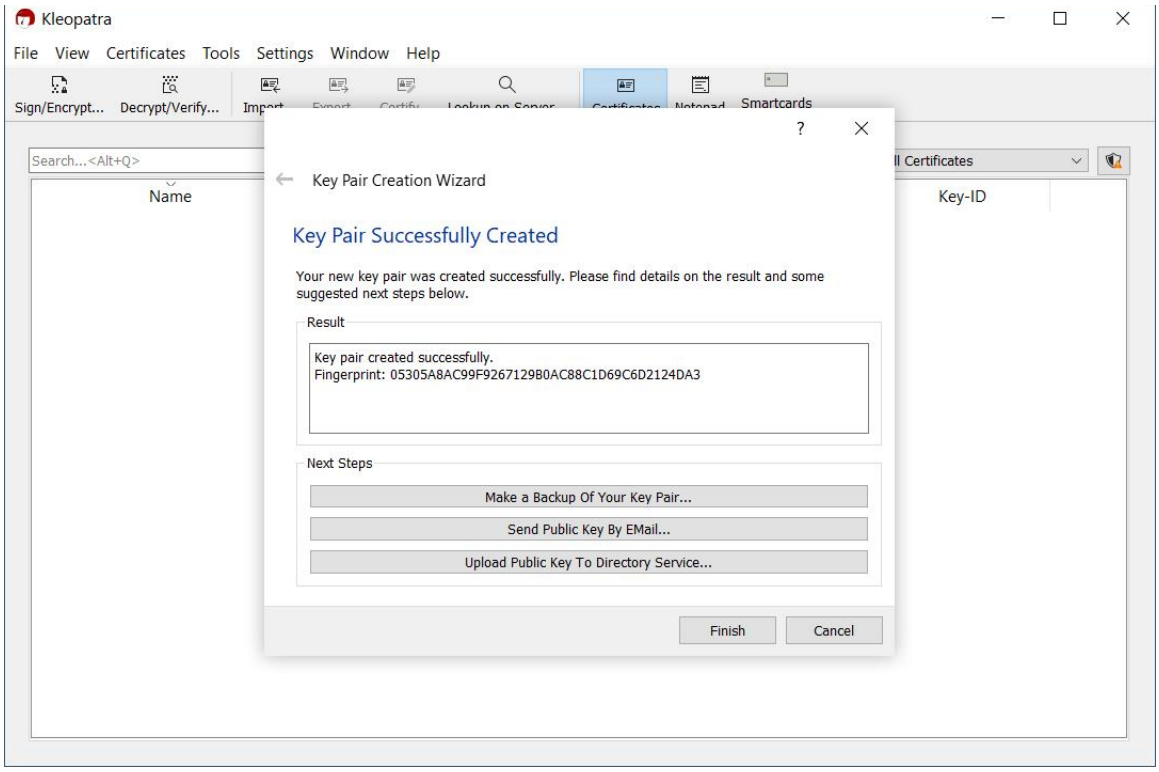
قدم دوم: انتخاب گزینهٔ Create a personal OpenPGP key pair



قدم سوم: واردکردن اطلاعات (اختیاری)



قدم چهارم: هنگام ساختن جفتِ کلید (key pair) می‌تونید از تنظیمات پیش‌فرض استفاده کنید، اما ضرری نداره اگه اندازهٔ کلید رو جهت امنیت بیشتر ۴۰۹۶ بیتی قرار بدید.



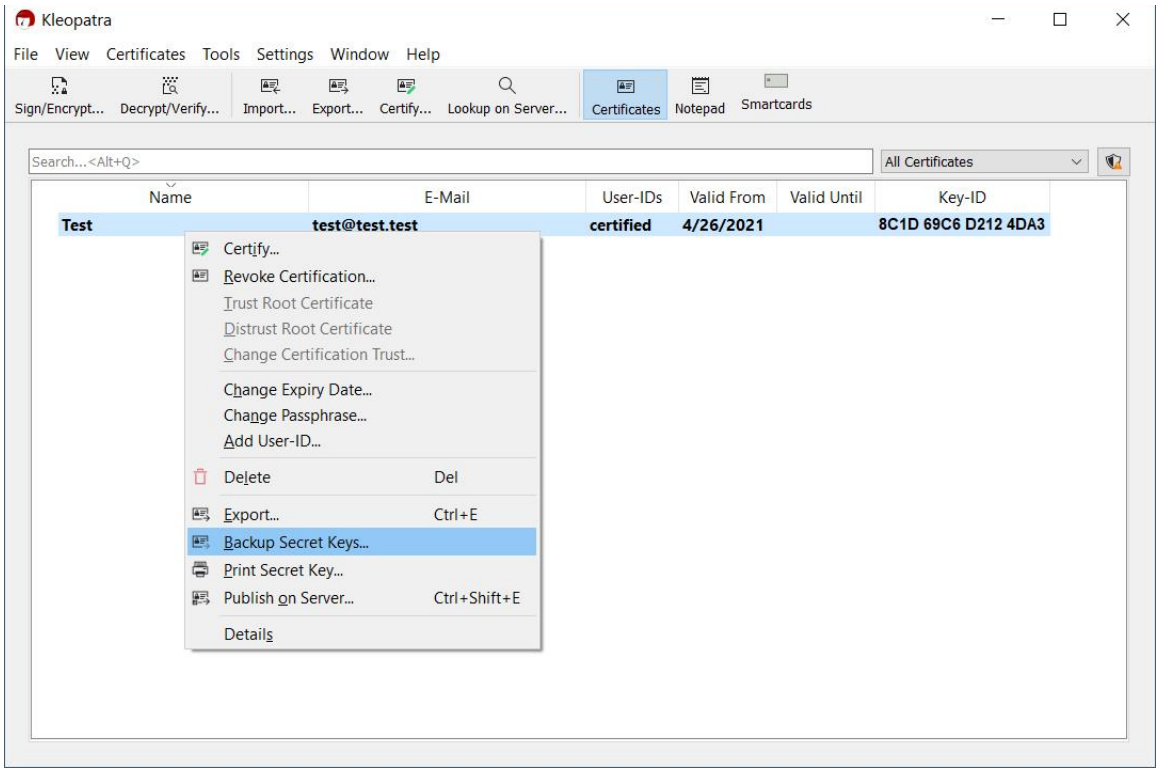
کلید شما با موفقیت ساخته شد.

اگه درمورد اجزای مختلف این پنجره کنجکاوید، سایت GnuPG یکی از جامع‌ترین و جذاب‌ترین سؤال‌های پرتکرار رو داره، که می‌تونید اینجا بخونید. درمورد امنیت و طول کلیدها کنجکاوید؟ این مکالمه رو در توئیتر دنبال کنید.

کلید خصوصی: تهیهٔ نسخهٔ پشتیبان و گواهی ابطال

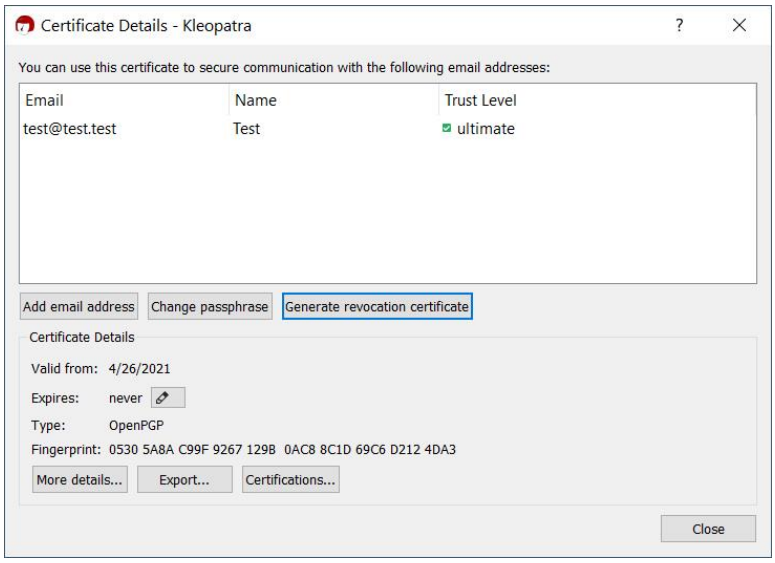
به تصویر بالا و گزینه‌های نمایش‌داده‌شده در چهارچوب Next Steps توجه کنید. از کلید خصوصی‌تون بک‌آپ تهیه کرده و اون رو در جایی امن نگه دارید. کل این فرآیند در امن‌نگه‌داشتن و محافظت از کلید خصوصی شما خلاصه می‌شه.

انجام این کار به روش‌های دیگه‌ای هم امکان‌پذیره، مثل تصویر زیر.



تهیهٔ نسخهٔ پشتیبان از کلید خصوصی (**بسیار مهم**)

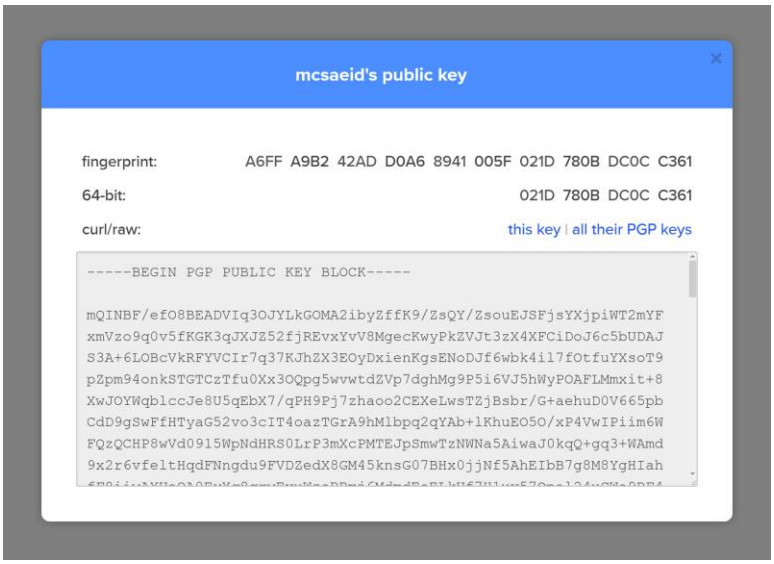
یکی از اولین کارهایی که انجام می‌دید باید تولید گواهی ابطال (revocation certificate) باشه. اگه زمانی کلیدتون گم بشه یا لو بره، با استفاده از این گواهی و انتشارش می‌تونید کلید رو باطل کنید. در ساخت کلید و ابطالش دقت کافی رو به‌خرج بدید. داشتن چند کلید باطل‌شده نشونهٔ چندان جالبی نیست.



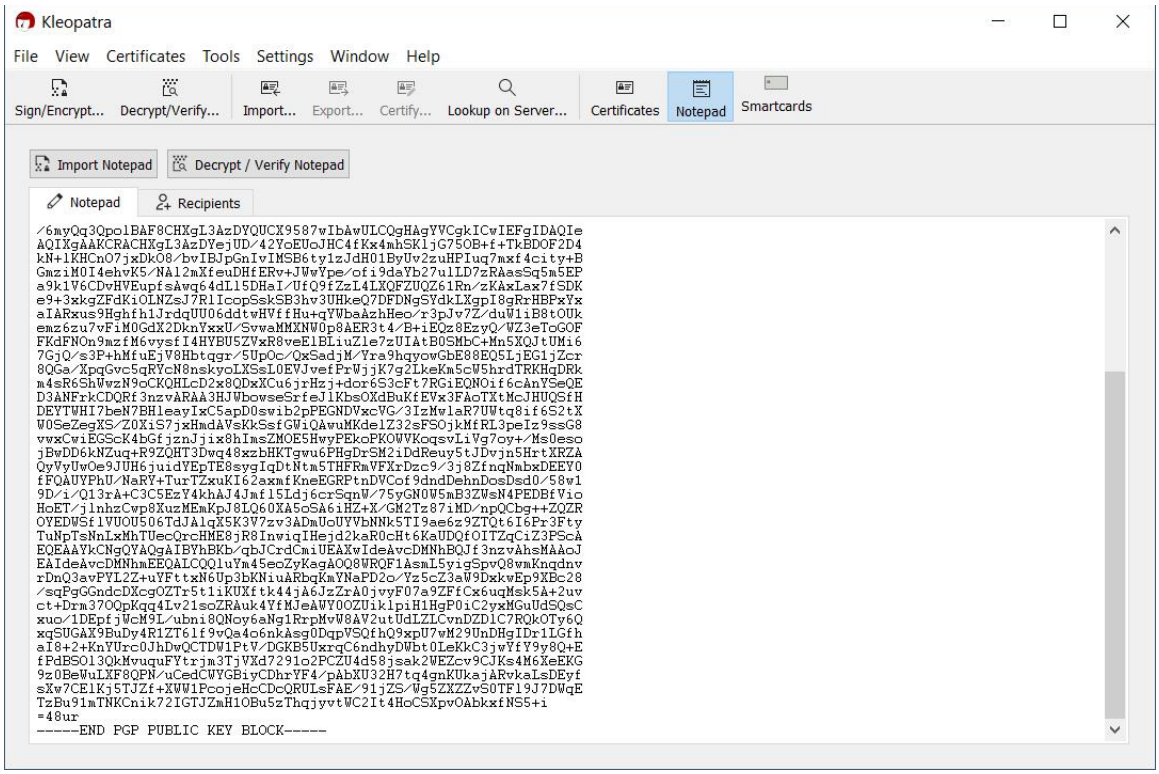
تولید گواهی ابطال

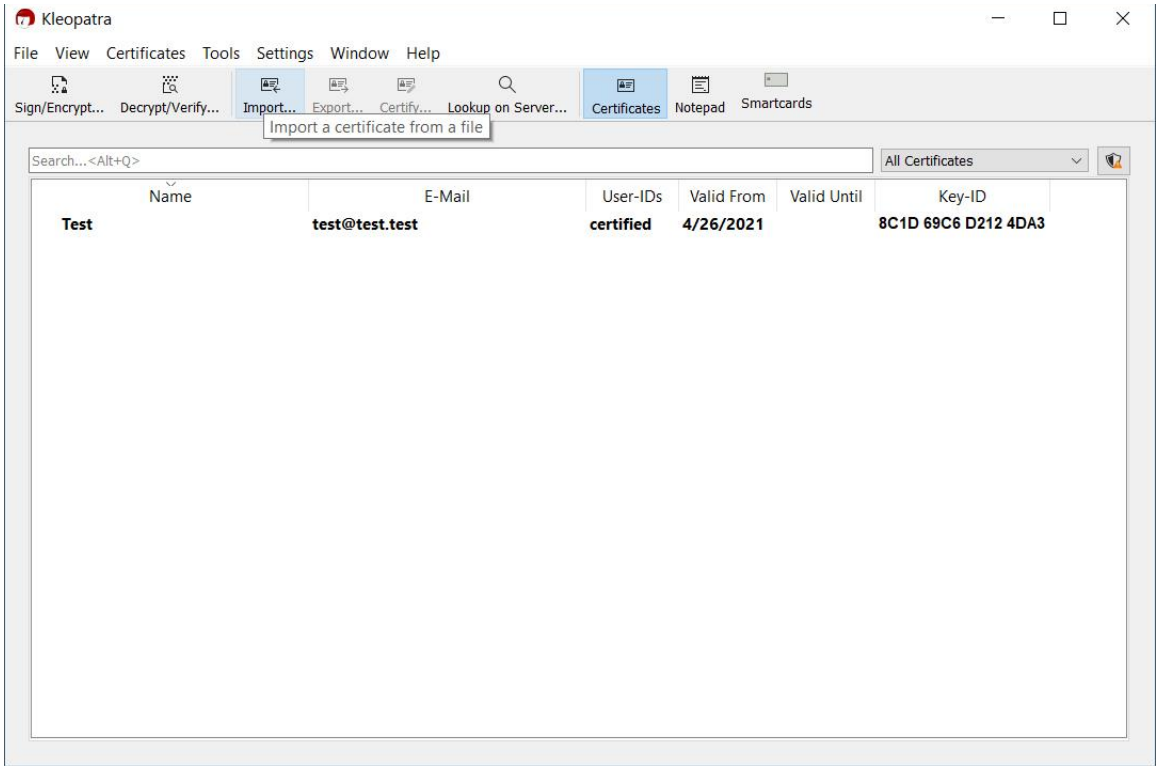
واردکردن کلید عمومی دیگران

برای اینکه بتونید با افراد مکالمهٔ رمزنگاری‌شده داشته باشید، ابتدا باید کلید عمومی‌شون رو وارد (import) کنید. روش‌های مختلفی برای انجام این کار وجود داره: ۱) کپی و پیست کلید عمومی در Notepad؛ ۲) ذخیرهٔ کلید عمومی به‌صورت فایل و سپس Import.



کلید عمومی من در Keybase





واردکردن کلید عمومی دیگران از طریق گزینهٔ ...Import یا Notepad

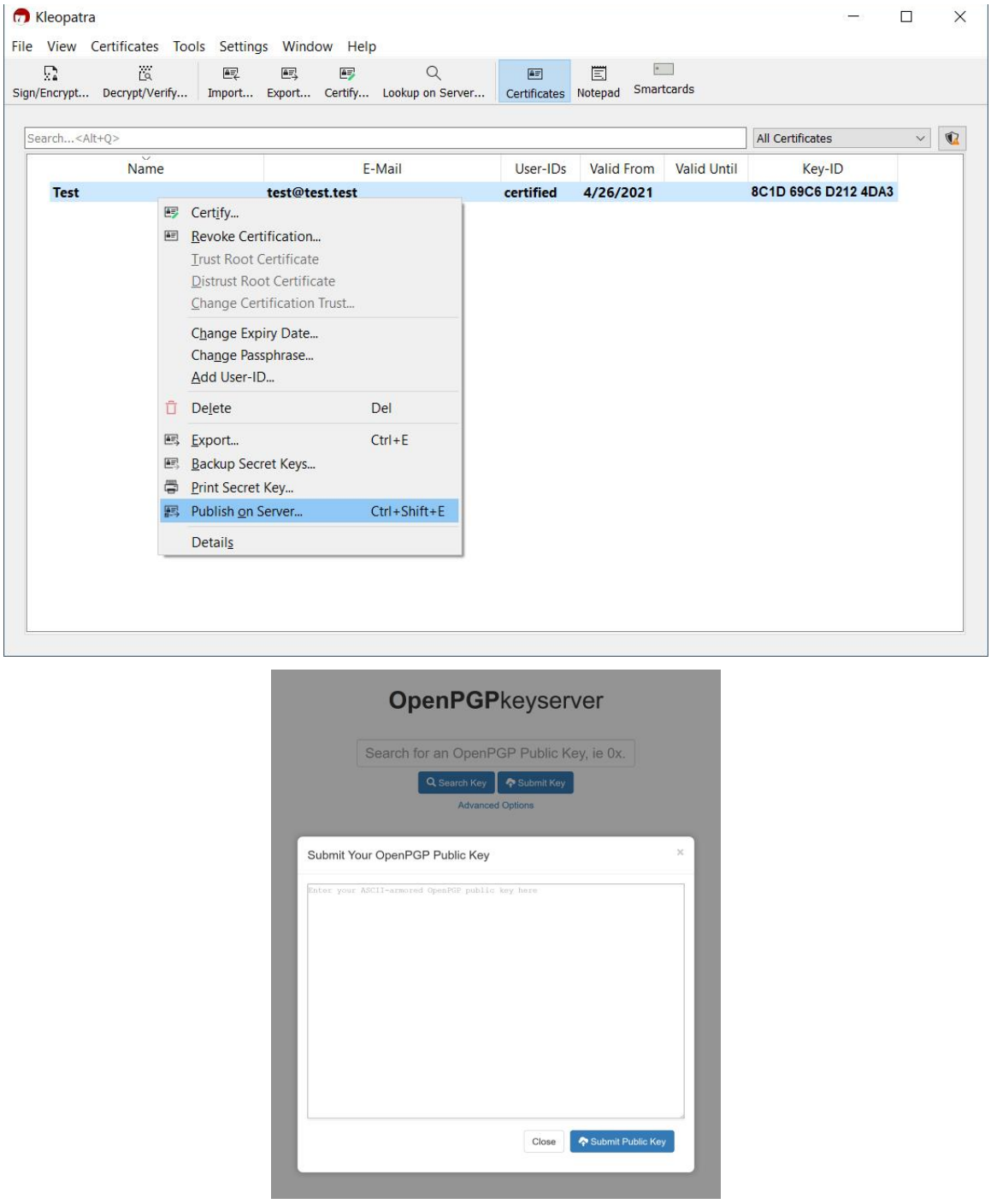
اگه کار با ترمینال رو یاد بگیرید، کارتون ممکنه راحت‌تر بشه.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Saeid> gpg --import pgp_keys.asc
gpg: key 021D780BDC0CC361: "MC Saeid <mcsaeid@protonmail.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
PS C:\Users\Saeid> gpg --keyserver keys.gnupg.net --search-keys mcsaeid@protonmail.com
gpg: data source: http://hkps.pool.sks-keyservers.net:11371
(1)     MC Saeid <mcsaeid@protonmail.com>
          4096 bit RSA key 021D780BDC0CC361, created: 2020-12-19, expires: 2030-12-20
Keys 1-1 of 1 for "mcsaeid@protonmail.com".  Enter number(s), N)ext, or Q)uit > 1
gpg: key 021D780BDC0CC361: "MC Saeid <mcsaeid@protonmail.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
PS C:\Users\Saeid> gpg --keyserver keys.gnupg.net --recv-keys 021D780BDC0CC361
gpg: key 021D780BDC0CC361: "MC Saeid <mcsaeid@protonmail.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
PS C:\Users\Saeid> gpg --keyserver keys.gnupg.net --search-keys "ziya sadr"
gpg: data source: http://hkps.pool.sks-keyservers.net:11371
(1)     Ziya Sadr <ziya_sadr@protonmail.com>
          4096 bit RSA key F97C47977F2EB716, created: 2018-06-27, expires: 2034-06-23
(2)     Ziya Sadr <ziyaamirisadr@gmail.com>
          2048 bit RSA key E28F1C1F3DCBEFCC, created: 2018-03-13
Keys 1-2 of 2 for "ziya sadr".  Enter number(s), N)ext, or Q)uit > 1
gpg: key F97C47977F2EB716: "Ziya Sadr <ziya_sadr@protonmail.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
PS C:\Users\Saeid> DONE_
```

برای واردکردن از فایل gpg --import [نام فایل]

جستجو در سرورهای کلید gpg --keyserver *keys.gnupg.net* --search-keys [نام شخص /آدرس ایمیل]

جستجو با اثرانگشت gpg --keyserver *keys.gnupg.net* --recv-keys [اثرانگشت]



انتشار کلید عمومی در سرور کلید از طریق نرم‌افزار یا به‌صورت دستی

شما می‌تونید کلید عمومی من رو با جستجو در سرورهای کلید مختلف پیدا کنید، اما این کار خودکار صورت نمی‌گیره. من از قبل کلید عمومی خودم رو در یکی از این منابع منتشر کرده‌م، و ازاونجایی‌که این سرورها همدیگه رو mirror می‌کنن، کلید عمومی من در جاهای دیگه هم قابل‌یافتنه.

اثرانگشت کلید عمومی

خب، حالا که کلید عمومی هم رو داریم، می‌تونیم به‌صورت امن مکالمه کنیم؟ نه، اصلاً. از کجا مطمئنید این کلید به من تعلق داره؟ شما ابتدا باید هویت من رو احراز کنید.

این خیلی مهمه. **هر کسی** می‌تونه با هر **آدرس ایمیلی** کلید بسازه. **هر کسی** می‌تونه اون کلید رو در **هر سروری** منتشر کنه. تنها درصورتی‌که هویت شخص رو احراز و اطمینان حاصل کنید کلید واقعاً به او تعلق داره، امنیت خواهید داشت.

ضیاء صدر در ویدئوی زیر مفصل دراین‌باره صحبت می‌کنه. پیشنهاد می‌کنم این ویدئوی بسیار خوب رو ازدست ندید، به‌ویژه که درمورد web of trust هم صحبت می‌کنه.

مشاهده در یوتیوب

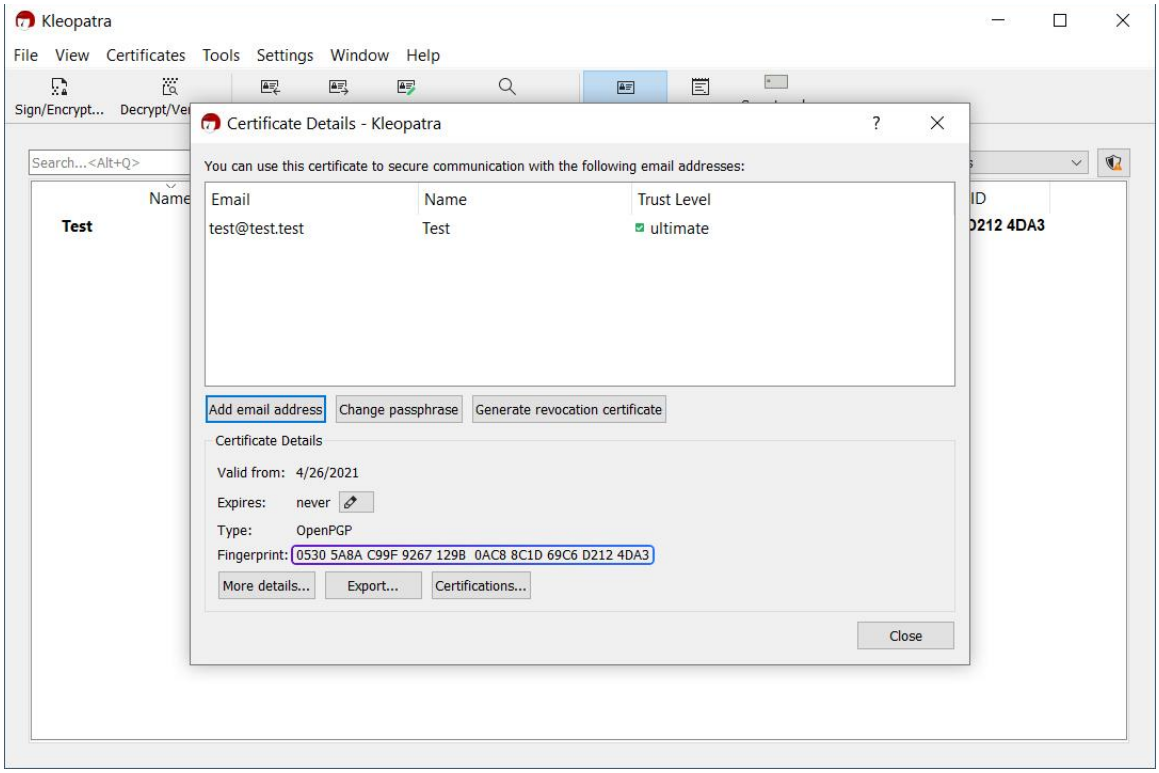
در مقالهٔ پیشین درمورد اثرانگشت مختصر صحبت شد. همون‌طور که پیش‌تر دیدید، کلیدهای عمومی بسیار طولانی‌ان، و امکان خوندن یا واردکردن اون‌ها به‌صورت دستی وجود نداره. ازاین‌رو، برای پیداکردن و همچنین احراز هویت افراد اثرانگشت کلید عمومی اون‌ها رو بررسی می‌کنیم.

Fingerprint:	A6FFA9B242ADD0A68941005F021D780BDC0CC361
Long Key ID:	021D780BDC0CC361
Short Key ID:	DC0CC361

توجه کنید که شناسهٔ بلند کلید (long key ID) و شناسهٔ کوچک کلید (short key ID) به‌ترتیب شونزده و هشت رقم آخر اثرانگشتن. شما با داشتن هرکدوم از این‌ها می‌تونید کلید عمومی من رو پیدا و وارد کنید.

احراز هویت کلید عمومی با اثرانگشت

یکی از راه‌های احراز هویت، مقایسه و تطابق‌دادن اثرانگشت شخصیه که قصد دارید باهاش ارتباط بگیرید. در این مورد حساسیت لازم رو به‌خرج بدید، مطالعه کنید، و دونسته‌های خودتون رو بالا ببرید.



با راست‌کلیک روی کلید و انتخاب گزینهٔ Details می‌تونید جزئیات اون رو ببینید، ازجمله اثرانگشت

احتمالاً اثرانگشت PGP افراد رو در وبسایت یا پروفایل توئیتر اون‌ها دیده‌اید. برای دستیابی به اثرانگشت کلیدتون به تصویر بالا توجه کنید، یا در ترمینال بنویسید:

gpg --fingerprint [آدرس ایمیل شما یا بخشی از اون]

مثال: gpg --fingerprint mcsaeid

توجه کنید، صِرفِ قراردادن اثرانگشت در پروفایل توئیتر، امضای ایمیل، تلگرام، و جاهای دیگه چیزی رو اثبات نمی‌کنه. در بهترین حالت، وقتی شخص رو چهره‌به‌چهره دیدید، کلید عمومی‌اش رو احراز کنید، و اگه قادر به ملاقات نیستید، از مفهوم web of trust—که بالاتر بهش اشاره شد—کمک بگیرید.

یک حقیقت جالب درمورد اثرانگشت لیست کلمات PGP است، که در ابتدا توسط پاتریک یولا (Patrick Juola) و فیلیپ زیمرمن در ۱۹۹۵ طراحی شد. هدف این بود که دو نفر حین مکالمهٔ صوتی بتونن اثرانگشت خود رو با هم مقایسه و احراز کنن—مشابه الفبای آوایی ناتو (NATO phonetic alphabet) اما با کلمات بیشتر.

اگه به لیست توجه کنید، هر بایت دارای دو کلمه‌ست: زوج (even) و فرد (odd). کلمه‌های زوج دوبخشی و فردها سه‌بخشی‌ان. اثرانگشت از چپ به راست خونده می‌شه، طوری‌که چپ‌ترین بایت معادل کلمهٔ زوج و راست‌ترین بایت معادل کلمهٔ فرده. برای مثال، در A6FF، کلمهٔ منصوب به A6 زوج و FF فرده.

A PGP public key fingerprint that displayed in hexadecimal as

`A6FF` `A9B2` `42AD` `D0A6` `8941`
`005F` `021D` `780B` `DC0C` `C361`

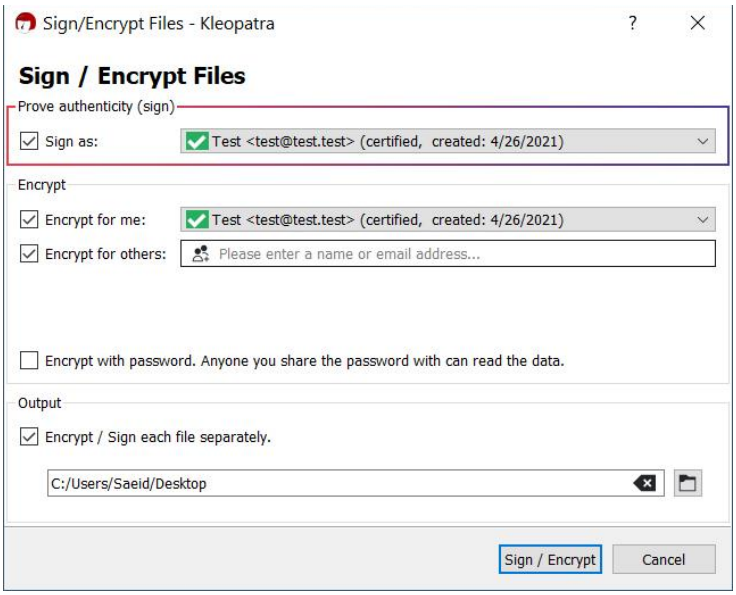
would display in PGP Words (the "biometric" fingerprint) as

`rematch Yucatan` `revenge pioneer` `crowfoot perceptive` `stagnate paragon` `nightbird decadence`
`aardvark forever` `accrue breakaway` `island armistice` `sweatband article` `snowcap frequency`

رمزنگاری

می‌رسیم به بخش جذاب ماجرا.

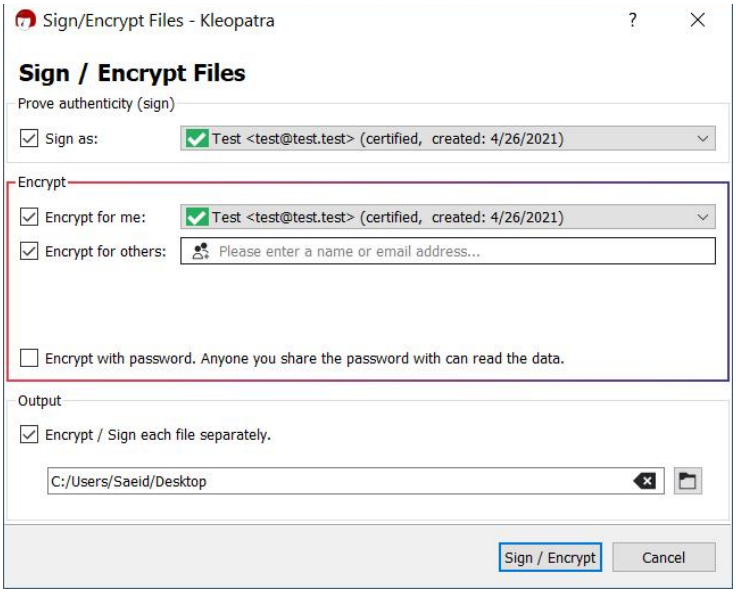
در نرم‌افزار Kleopatra به دو روش می‌تونید رمزنگاری کنید: متن و فایل. برای رمزنگاری فایل‌ها کافیه گزینهٔ Sign/Encrypt رو بزنید، فایل رو انتخاب کرده، و در پنجره‌ای که باز می‌شه گیرنده یا گیرندگان رو مشخص کنید. به تصاویر صفحهٔ بعد توجه کنید.



می‌تونید انتخاب کنید فایل رو با کلید خودتون امضا کنید

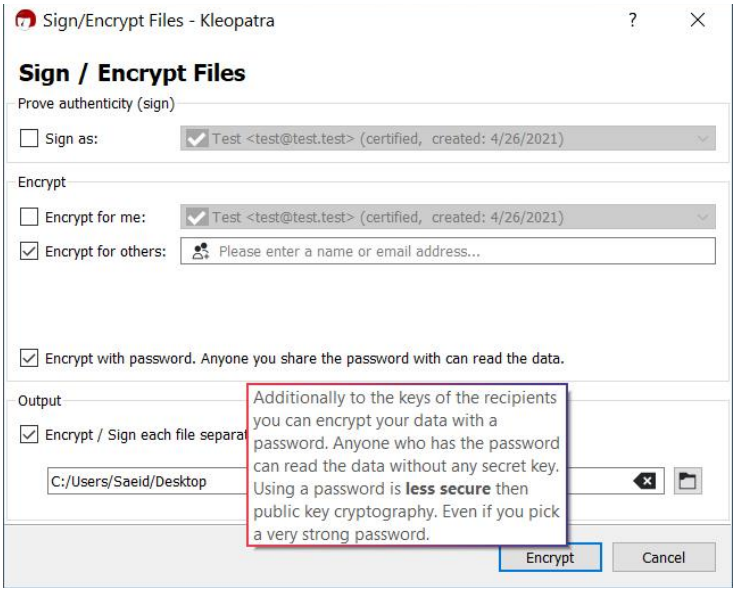
اینجا می‌تونید فایل رو امضا کنید. جلوتر بیشتر بهش خواهیم پرداخت. کسی که فایل رو رمزگشایی می‌کنه می‌بینه که شما اون رو امضا کرده‌اید، و می‌تونه اطمینان داشته باشه محتوا توسط شخص دیگه‌ای دست‌کاری نشده. هیچ‌کسی جز شما، بدون داشتن کلید خصوصی شما، قادر به ارائهٔ اون امضای منحصربه‌فرد نیست.

به هر دلیلی ممکنه نخواید امضا کنید، اما پیشنهاد می‌کنم همیشه فایل‌ها و پیام‌هاتون رو امضا کنید.



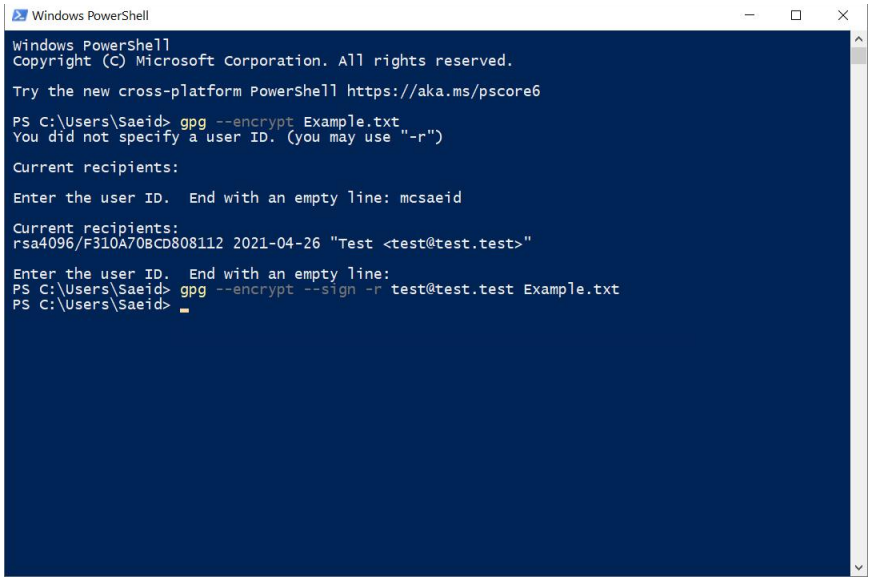
می‌تونید انتخاب کنید فایل رو برای خودتون، شخص دیگه‌ای، یا هر دو رمزنگاری کنید

در اینجا فایل به‌طور پیش‌فرض برای شما هم رمزنگاری می‌شه، مگه اینکه تیک Encrypt for me رو بردارید. (شاید نخواید فایل رو در آینده باز کنید، یا شاید اطلاعات حساسیه و نخواید که بتونید.)



می‌تونید فایل رو با یک گذرواژه هم رمزنگاری کنید

در Encrypt for others می‌تونید تعیین کنید فایل برای چه شخص یا اشخاصی (که کلید عمومی اون‌ها رو دارید) رمزنگاری بشه. اگه برای فایل رمز تعیین کنید (با گزینهٔ Encrypt with password)، هر کسی با داشتن رمز می‌تونه اون رو باز کنه. به این موضوع توجه داشته باشید. شما همچنین با اجرای دستور هم می‌تونید فایل‌ها رو رمزنگاری کنید.



ساده‌ترین دستور اینه:

gpg --encrypt [نام فایل]

در مرحلهٔ بعد از شما خواهد پرسید فایل رو می‌خواید برای چه کسی رمزنگاری کنید. دستور کامل‌تر می‌تونه این باشه:

gpg --encrypt --sign -r [آدرس ایمیل شما] [نام فایل]

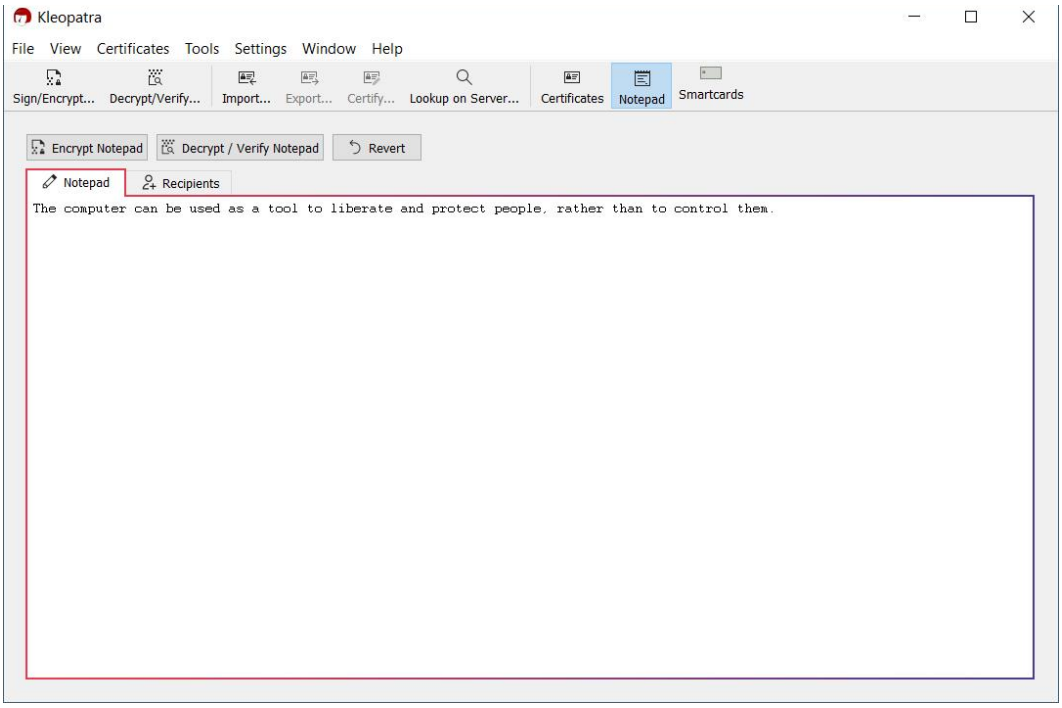
اینجا به توضیح کوتاهی درمورد پارامترها بسنده می‌کنم، که ممکنه جالب‌توجه باشه:

- رمزنگاری: --encrypt
- امضا: --sign
- افزودن گیرنده: -r (همچنین recipient)

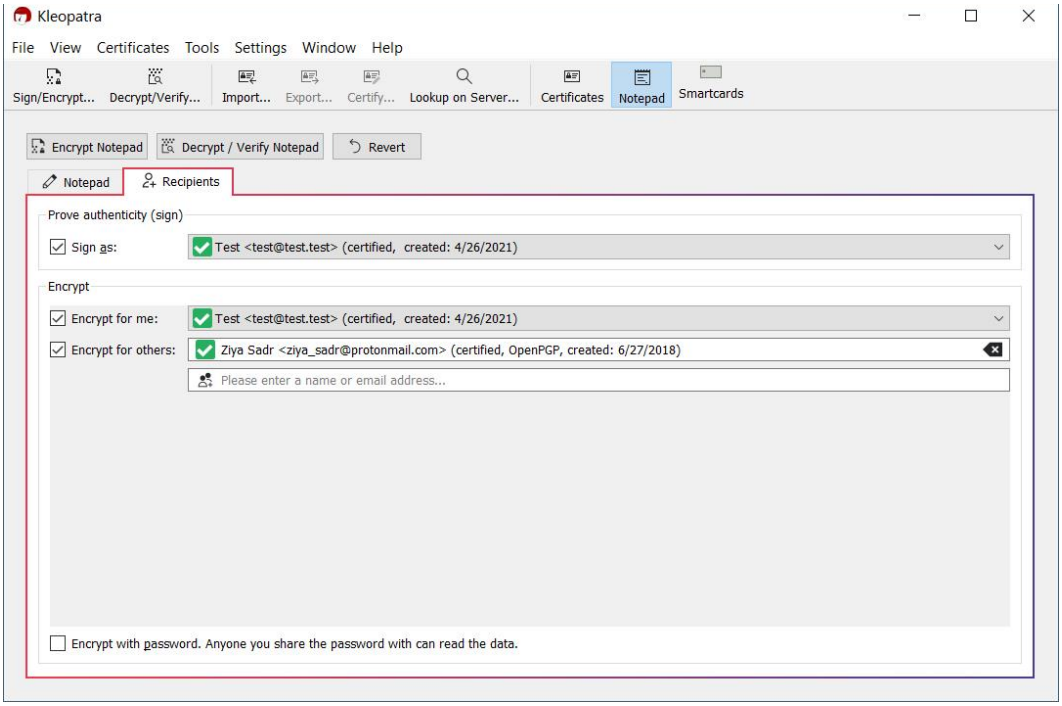
توجه مهم: اگه می‌خواید بتونید فایل رو رمزگشایی کنید، حتماً باید خودتون رو هم جزو گیرنده‌ها قرار بدید. درضمن، می‌تونید چند گیرنده داشته باشید؛ دراین‌صورت، چند مورد -r خواهید داشت.

توجه مهم: بعد از اینکه GPG فایلی رو رمزنگاری کرد، فایل اصلی رو دست‌نخورده نگه می‌داره. حواستون باشه اون رو حذف کنید، چه بسا به‌شکلی امن و غیرقابل‌برگشت. (اگه کاربر ویندوز هستید، درمورد SDelete بخونید.)

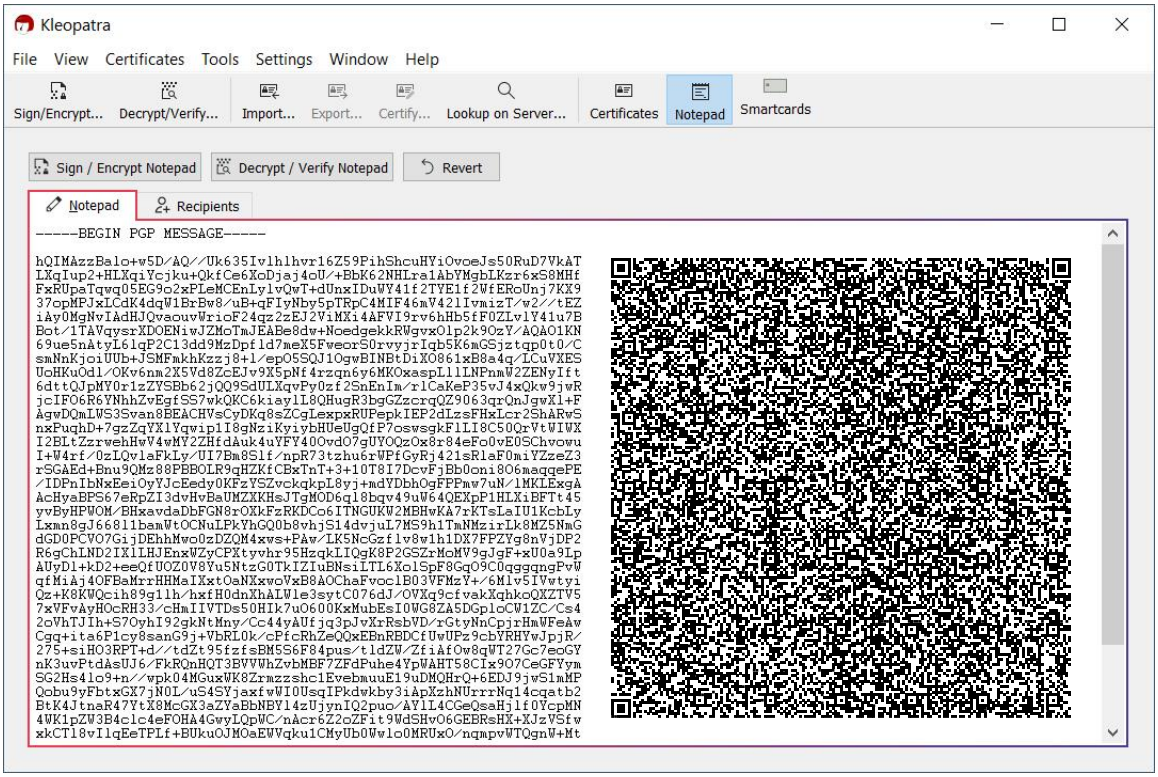
تا اینجا به رمزنگاری فایل‌ها پرداختیم، اما چطور یک متن رو رمزنگاری کنیم؟ خیلی ساده. از ابزار Notepad استفاده کنید.



برای رمزنگاری متن کافیه اون رو در Notepad بنویسید، سپس به سربرگ Recipient (گیرنده) برید



در سربرگ Recipient گیرنده یا گیرنده‌ها رو مشخص کرده و انتخاب می‌کنید نوشته رو از سمت خودتون امضا کنید یا نه

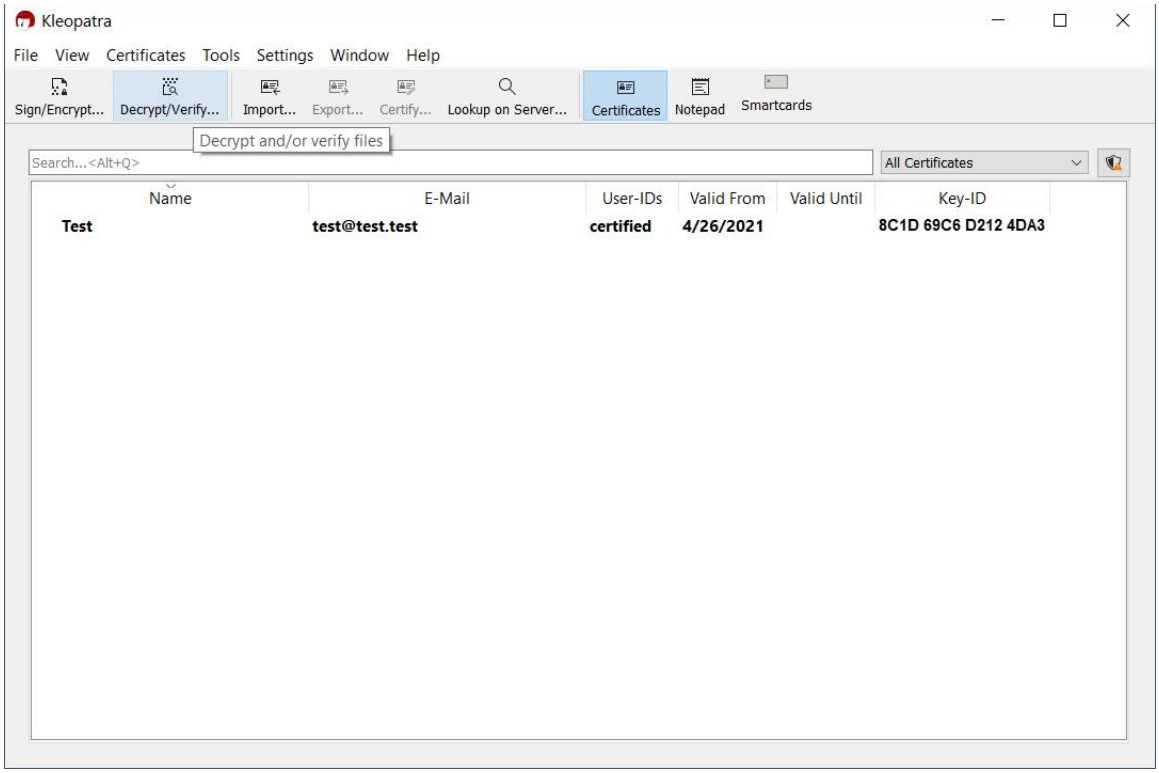


پس از نوشتن متن و تعیین گیرنده(ها)، با زدن گزینهٔ Sign / Encrypt Notepad متن رمزنگاری‌شده رو تحویل خواهید گرفت

برای مثال، اینجا پیامی رو برای خودم و ضیاء رمزنگاری کردم. او می‌تونه تصویر باکیفیتی رو از کد QR بالا ذخیره کنه (برای مثال، با زوم‌کردن و گرفتن یک اسکرین‌شات)، با ابزار QR Decoder اون رو decode کنه، و محتوای پیام رو بخونه. شما هم می‌تونید محتوای کد QR رو decode کنید اما decrypt نه چون به کلید خصوصی من یا ضیاء دسترسی ندارید و این پیام برای شما رمزنگاری نشده.

رمزگشایی

رمزگشایی پیام‌ها و فایل‌ها هم به آسونی رمزنگاری‌کردن اون‌هاست. برای فایل‌ها می‌تونید از گزینهٔ Decrypt/Verify استفاده کنید (یا روی فایل راست‌کلیک کرده و Decrypt and verify رو انتخاب کنید).



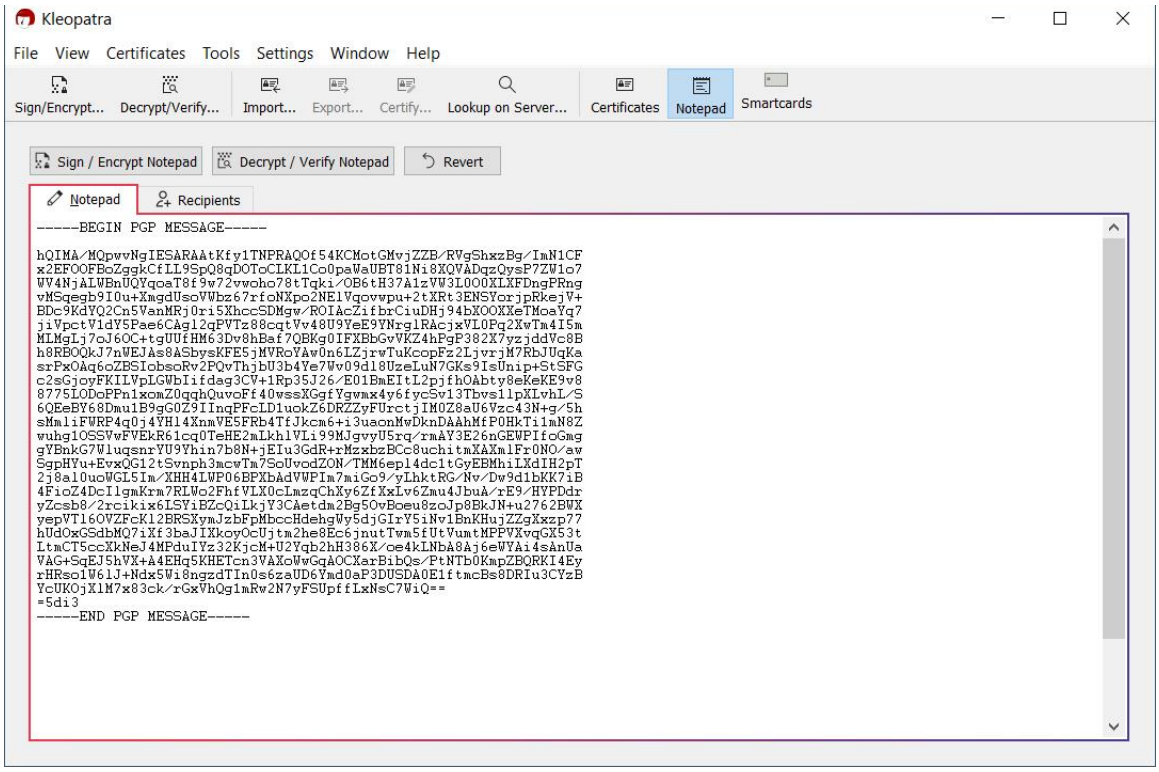
رمزگشایی فایل‌ها با گزینهٔ ...Decrypt/Verify

همچنین، می‌تونید از دستور زیر استفاده کنید:

gpg --decrypt [نام فایل]

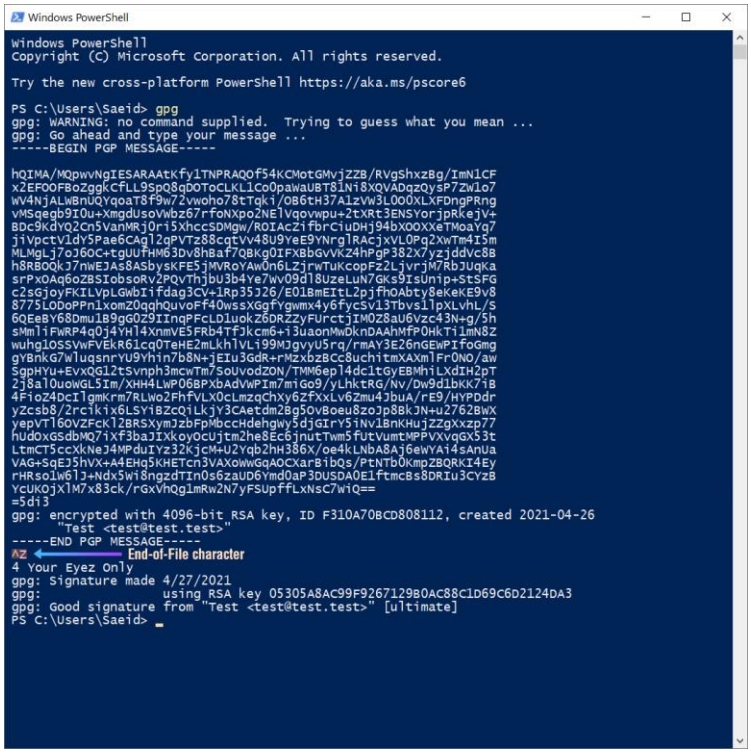
توجه مهم: بعد از اینکه GPG فایلی رو رمزگشایی کرد، کاری با فایل رمزنگاری‌شده نداره. بعد از بازکردن فایل یادتون باشه فایل اصلی رو حذف کنید، ترجیحاً به روشی امن. درضمن، اگه محتوای متنی رمزنگاری‌شده دارید، می‌تونید بدون اینکه ذخیره‌ش کنید محتوای اون رو ببینید:

gpg -d [نام فایل]



رمزگشایی متون با Notepad

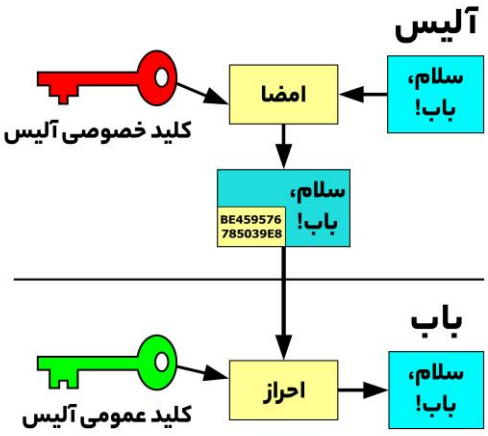
درضمن، اگه متن رمزنگاری‌شده دارید، می‌تونید اون رو در Notepad قرار بدید.



همچنین، اگه دوست دارید اون رو در ترمینال رمزگشایی کنید، ابتدا بنویسید gpg و enter بزنید، سپس پیام رو paste کنید، و در انتها برای پایان Ctrl + Z رو زده (کاراکتر End-of-File؛ Ctrl-D در Unix) و enter بزنید.

امضای دیجیتال

به مقولهٔ مهم امضاکردن (signing) می‌رسیم. GPG این امکان رو به شما می‌ده تا محتوای متنی یا فایلی خودتون رو دیجیتالی امضا کنید، که مزیت‌های مهمی داره. وقتی چیزی رو امضا می‌کنید، کسی جز شما قادر به تولید اون امضای منحصربه‌فرد نیست، و این، اطمینان می‌ده محتوا حین ارسال دست‌کاری نشده.

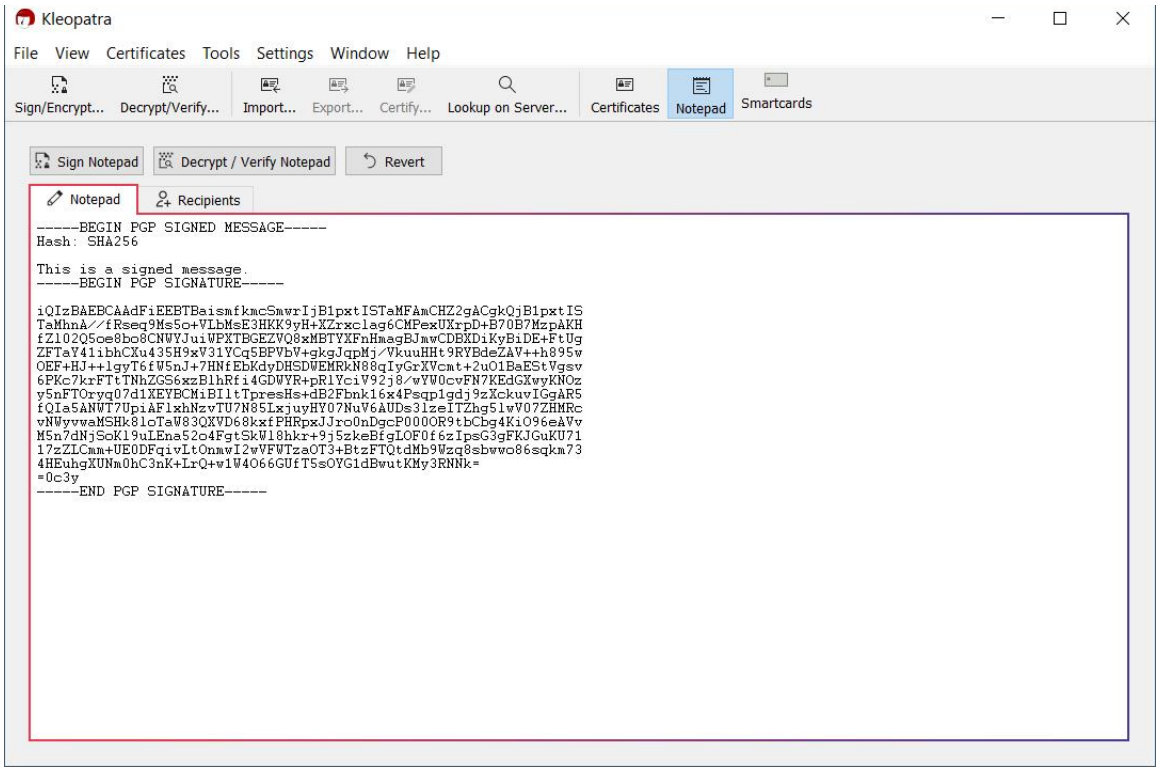


همچنین شخص مقابل، با داشتن کلید عمومی شما، می‌تونه امضای دیجیتال شما رو احراز (verify) کنه و مطمئن باشه از سمت شما اومده. اگه پیامی رو رمزنگاری می‌کنید، بهتره همیشه اون رو امضا کنید.

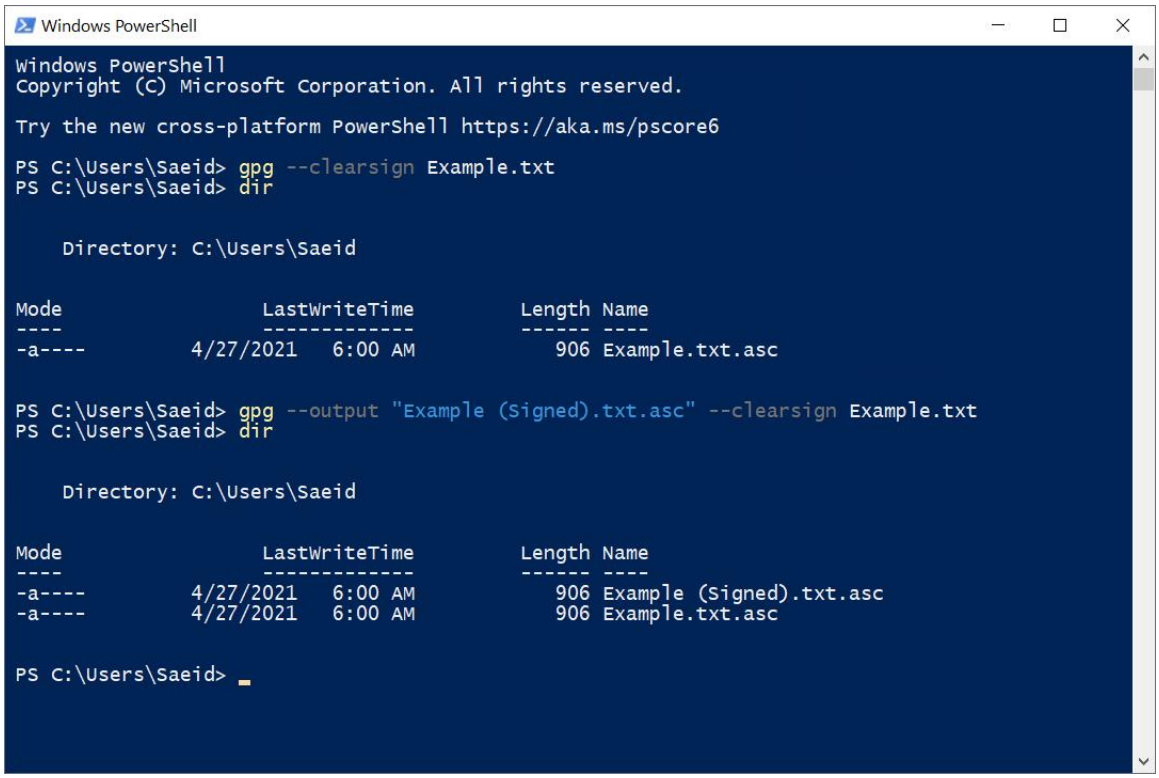
امضا می‌تونه کاربردهای متعددی داشته باشه، ازجمله:

- وقتی پیام مهمی ارسال می‌کنید؛ حین یک مکالمهٔ مهم
- دادن امکان صحت‌سنجی فایل‌ها به شخص دریافت‌کننده
- اثبات اینکه پیام واقعاً از سمت شما اومده و دست‌کاری نشده

با توجه به چیزهایی که تا اینجا یاد گرفتید، امضاکردن نباید کار سختی باشه، چه با نرم‌افزار و چه در محیط ترمینال. به نمونه‌های صفحهٔ بعد توجه کنید.

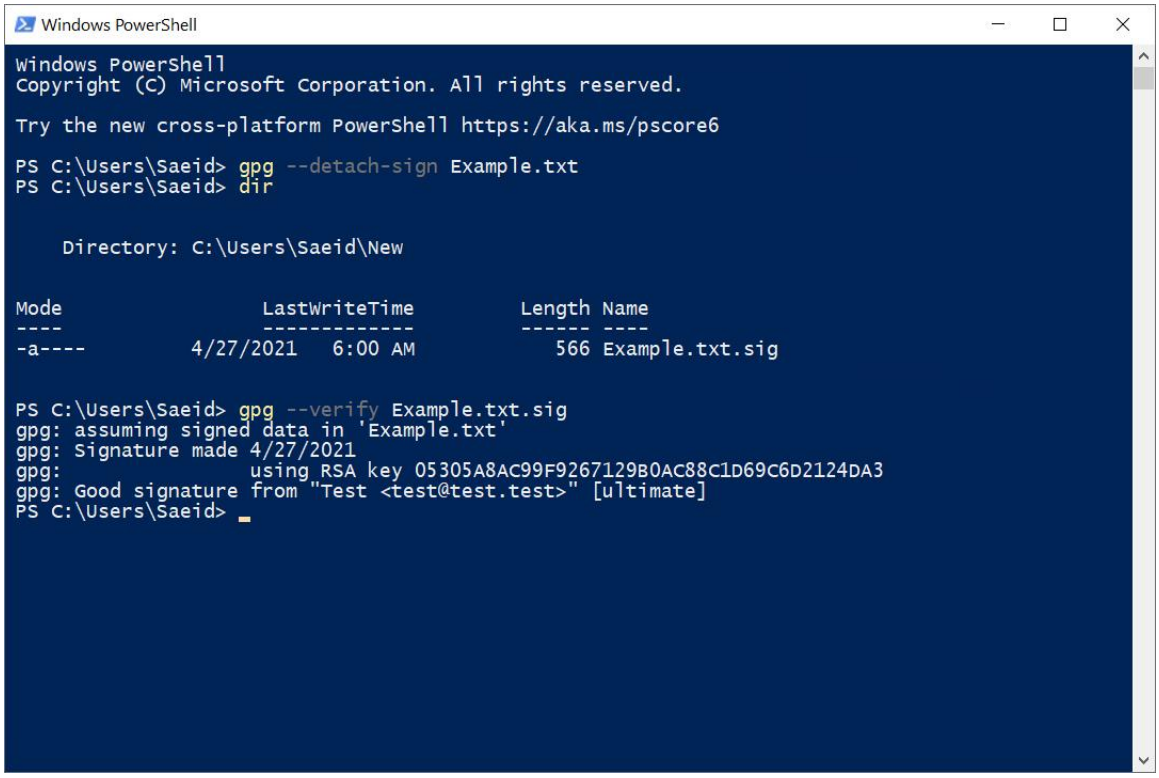


متن امضاشده در محیط نرم‌افزار



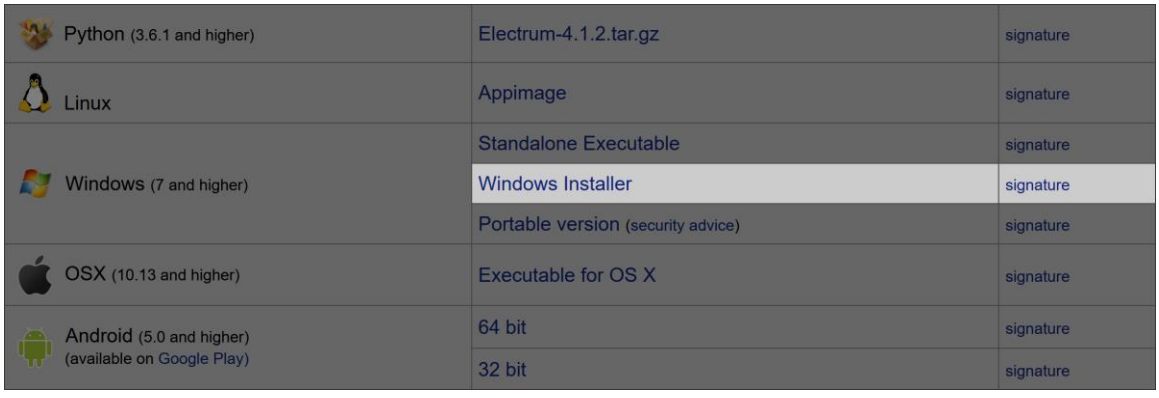
امضای فایل Example.txt با استفاده از ترمینال

پارامتر clearsign-- چیزی رو به شما می‌ده که در تصویر صفحهٔ قبل مشاهده کردید. درواقع، متن پیام درون امضا قرار می‌گیره. با دستور detach-sign-- می‌تونید فایل امضای مجزا تولید کنید.

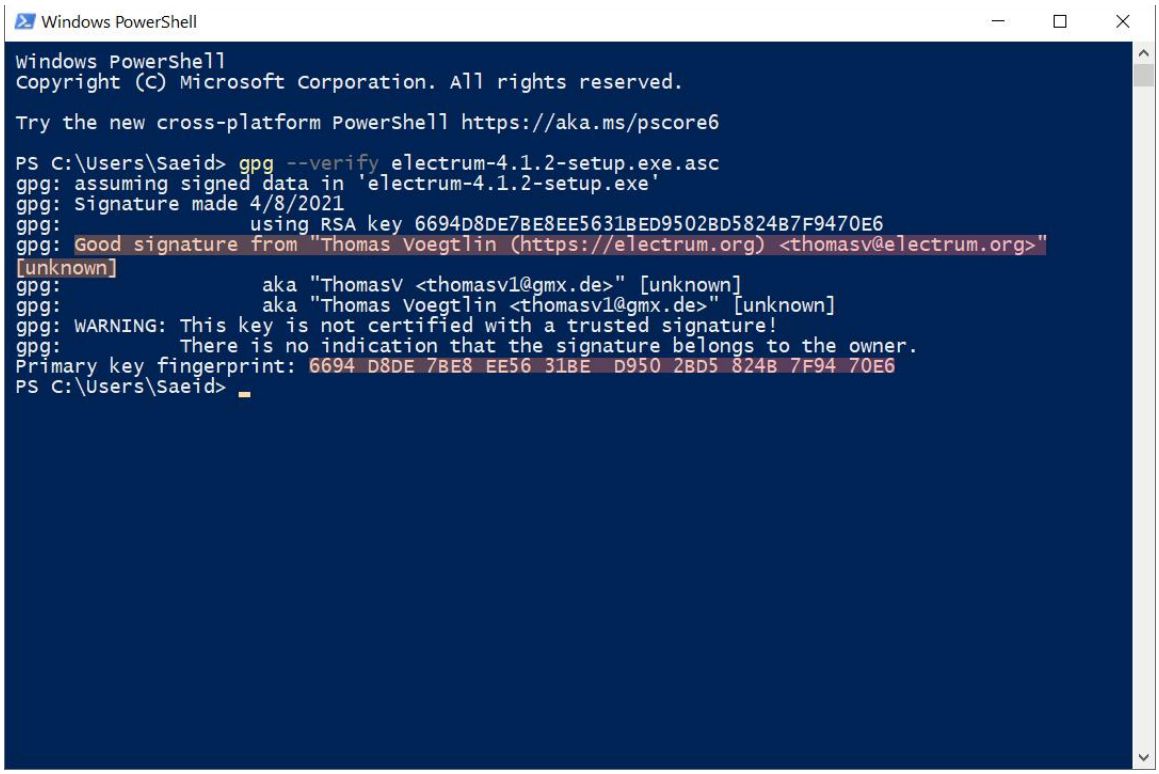


ایجاد فایل امضای مجزا و سپس احراز اون

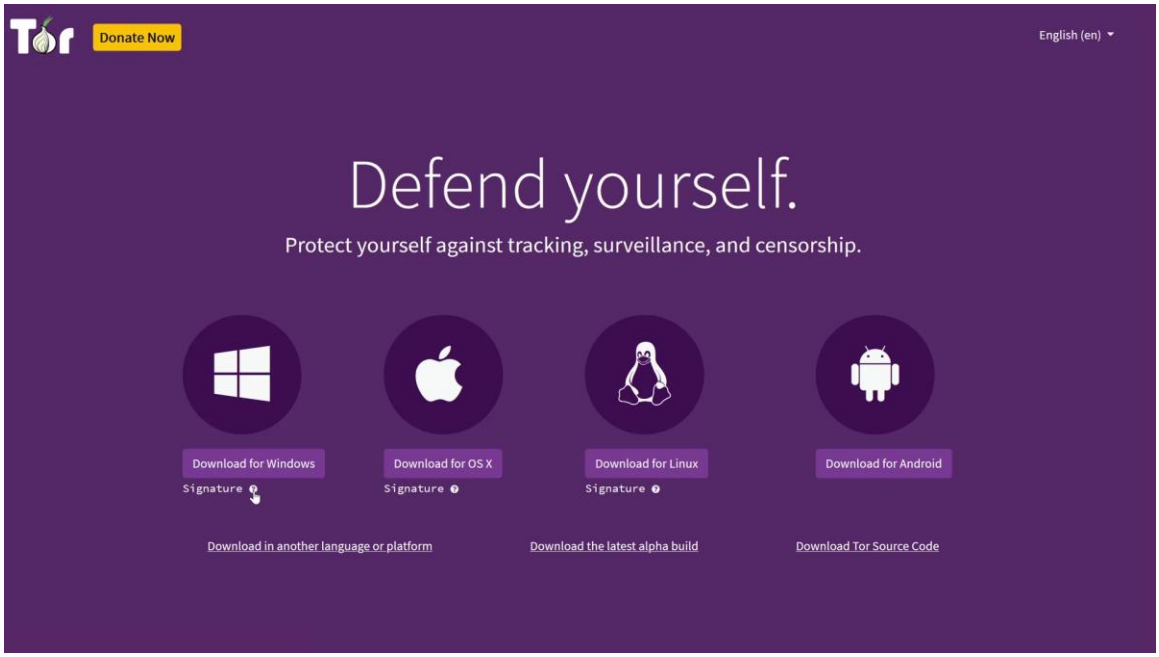
یکی از مهم‌ترین کاربردهای امضا در احراز و اصالت‌سنجی فایل‌هاییه که دانلود می‌کنیم، تا بدونیم از منبع معتبری اومدن.



امضاهای فایل‌های نصب کیف پول الکترام



احراز امضای توسعه‌دهندهٔ کیف پول الکترام



آموزش تصویری اصالت‌سنجی فایل‌ها در یوتیوب

سخن پایانی

اطلاعاتی که اینجا خوندید تنها بخش کوچکی از چیزهایی بودن که می‌تونید درمورد GPG یاد بگیرید، هرچند این‌ها نیاز کاربر عادی رو برطرف می‌کنن. راهنمای این نرم‌افزار بیش از ۲۰۰ صفحه‌ست، و حتی بعد از آشنایی کامل با عملکردش، همچنان نکات امنیتی زیادی هست که می‌شه یاد گرفت.

اگه تنها یک درس باشه که بخوام انتقال بدم اینه که به مقدار کمی دانش بسنده نکنید. جملهٔ زیر در ابتدا برام عجیب بود، اما هرچی بیشتر بهش فکر کردم، معناش برام قابل‌لمس‌تر شد. کنجکاو باشید، درمورد چیزهایی که علاقه دارید مطالعه کنید، و لذت ببرید.

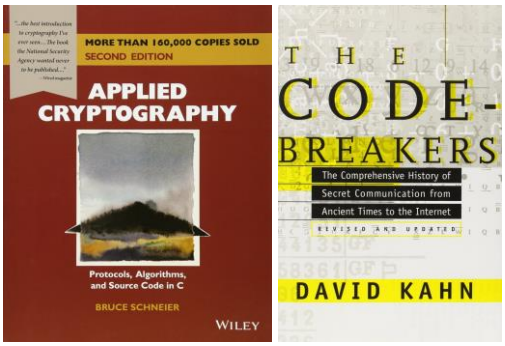
منابعی که در ادامه می‌ذارم برای اون یک نفریه که مثل من دوست داره همه‌چیز رو بدونه و مسیر یادگیری‌اش اینجا تموم نمی‌شه. (برای مقایسه، مسیر اصلی یادگیری من تازه از اینجا شروع شده.)

ازاونجایی‌که سطح انتظار بالایی برای quality content دارم، کم پیش میاد که مطلبی من رو شگفت‌زده کنه. یکی از بهترین، جامع‌ترین، و لذت‌بخش‌ترین منابعی که خوندم و حالا هرازگاهی بهش سرمی‌زنم، راهنمای GPG آلن ایلیاسون (Alan Eliasen) است. اگه دوست دارید آشنایی خوبی نسبت به GPG پیدا کنید، نباید ازدستش بدید. الهام‌بخش نوشتن این مقاله‌ها بود. اگه کنجکاوید راجع به نحوهٔ آشنایی من با این شخص و انگیزهٔ نوشتن این مطالب بدونید، این رشته‌توئیت رو بخونید.

جزئیات زیادی درمورد داستان زیمرمن و سایفرپانک‌ها هست که از حوصلهٔ این مطلب خارجه اما دونستنشون به شما کمک می‌کنه تصویر دقیق‌تری از اون روزها به‌دست بیارید. دو مقالهٔ عالی از Wired هستن که خوندنشون ضروریه: Crypto Rebels و Cypher Wars.

سایت شخصی زیمرمن به‌تنهایی منبع بسیار خوبی برای شروعه. اون‌قدر لینک و مقاله داره که چند روزی شما رو سرگرم نگه داره. پیشنهاد می‌کنم با متن ده‌سالگی PGP شروع کنید. یکی از بهترین روش‌ها برای آشنایی با یک موضوع اینه که اون رو از زبون سازنده یا سازنده‌هاش بشنوید. وقتی پای حرفشون می‌شینید، نکاتی رو می‌فهمید که ممکنه هیچ‌جای دیگه‌ای پیداشون نکنید. صحبت‌های زیمرمن در دف‌کان یازده شنیدنیه. حضور و صحبت‌هاش در Bitcoin Wednesday هم جالب و دیدنیه. وقتی یکی ازش می‌پرسه با توجه به سختی‌هایی که در چند دههٔ اخیر متحمل شده‌ای، آیا باز هم این کارها رو انجام می‌دادی، می‌گه، «آره، ولی احتمالاً از الگوریتم‌های بهتری در نسخهٔ اصلی PGP استفاده می‌کردم!»

برای پایان، دو کتاب معرفی می‌کنم، که خودم هنوز شروع نکرده‌م اما به‌شدت جذاب به‌نظر میان: رمزنگاری کاربردی (Applied Cryptography) از بروس اشنایر و رمزگشایان (The Codebreakers) از دیوید کان.



راهنماهای مرتبط

حریم خصوصی در عصر دیجیتال

رمزنگاری کلید عمومی RSA