



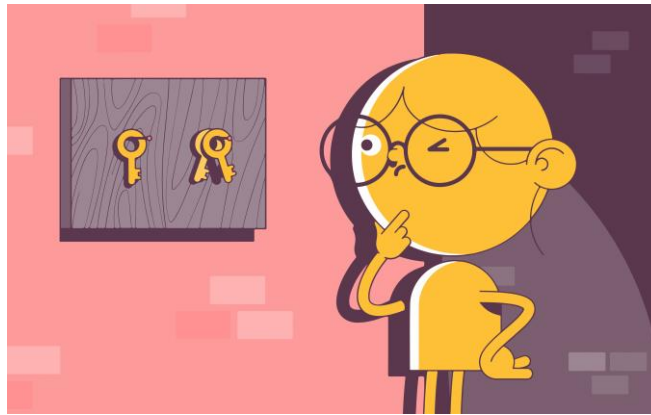
معرفی سیستم رمزنگاری RSA

به همراه راهنمای عملی به کارگیری ابزار PGP

رمزنگاری کلید عمومی RSA

سیستم رمزنگاری کلید عمومی RSA (آراس‌ای) یکی از قدیمی‌ترین و جذاب‌ترین‌هاست، و در این مطلب می‌خواهیم تاریخچه، کاربرد، و اهمیتش در امنیت اطلاعات رو با هم مرور کنیم. با معرفی RSA در ۱۹۷۷، دنیای رمزنگاری وارد عصر جدیدی شد. خیلی از ما، از جمله من، چهار دهه بعد از خلقش باهاش آشنا می‌شیم.

به‌طور کلی، دو نوع رمزنگاری داریم: **متقارن (symmetric)** و **نامتقارن (asymmetric)**. 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.

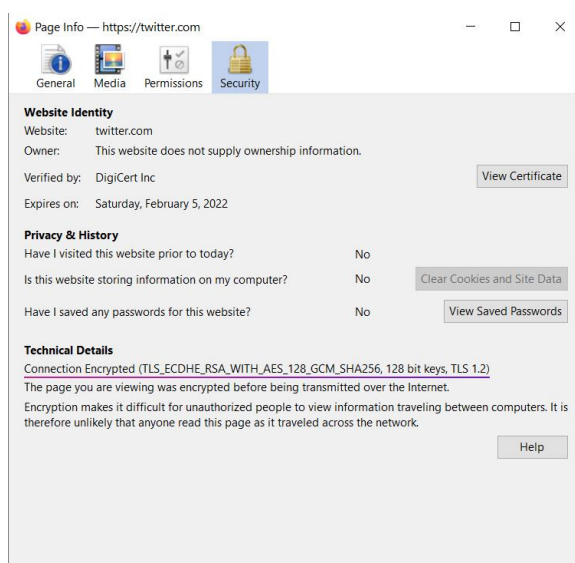


رمزنگاری نامتقارن فرآیند پیچیده‌تری داره: دو کلید دارید، یکی عمومی و دیگری خصوصی.

رمزنگاری کلید عمومی

در این روش، شما با استفاده از کلید عمومی خودتون چیزی رو رمزنگاری می کنید، و اون پیام یا داده تنها با کلید خصوصی مرتبط قابل رمزگشاییه. درحالی که این دو کلید یکی نیستن و با هم فرق دارن، از طریق ریاضی به هم مرتبطن.

رمزنگاری نامتقارن (یا رمزنگاری کلید عمومی) امنیت بسیار خوبی رو ارائه می ده، از این جهت که رسیدن به رابطه بین دو کلید و پیدا کردن کلید خصوصی دشواره—به لطف **تابع یه طرفه ای** که جلوتر بهش می پردازیم. از طرفی، رمزنگاری نامتقارن روش کندتری در مقایسه با رمزنگاری متقارن به حساب میاد.



یکی از رایج ترین الگوریتم های رمزنگاری متقارن **AES** (استاندارد رمزنگاری پیشرفته) است. همین الان مرورگر شما برای اتصال امن به توئیتر از این نوع رمزنگاری استفاده می کنه.



« ۱۲۸ بیتی یا ۲۵۶ بیتی؟ » تفاوت امنیت کلیدها در یوتیوب

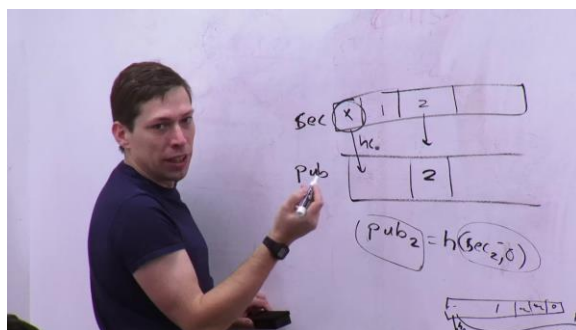


معرفی AES در یوتیوب

وقتی راجع به رمزنگاری متقارن صحبت می‌کنیم، طول کلید در ارائه امنیت بیشتر مهم و تأثیرگذاره، اما تنها فاکتور نیست. کلیدها در این نوع رمزنگاری—متشکل از رشته‌ای از حروف و اعداد—به‌طور معمول ۱۲۸، ۱۹۲، و ۲۵۶ بیتی‌ان. ویدئوهای صفحه قبل رو برای آشنایی بیشتر با تفاوت امنیت کلیدها ببینید.

طول کلیدها در رمزنگاری کلید عمومی بسیار بلندتره (۲۰۴۸ بیت به بالا)، اما روش سنجش امنیتش از رمزنگاری متقارن متفاوت. برای مثال، به کلید عمومی ۳۰۷۲ بیتی از نظر امنیت کم‌وبیش با یک کلید ۱۲۸ بیت AES برابره. درموردش بخونید. (کلیدواژه‌ها: طول کلید (key size)، سطح امنیت (security level))

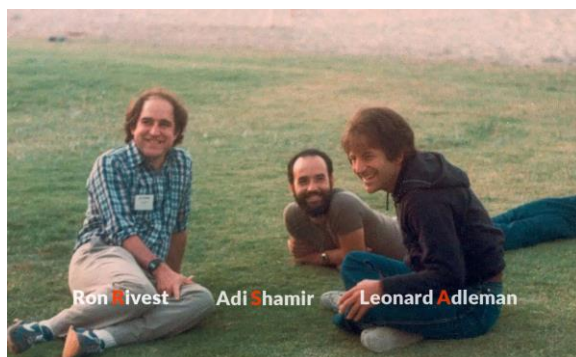
دو نمونه از سیستم‌های نامتقارن RSA و ECC (رمزنگاری منحنی بیضوی) هستن. اولی موضوع صحبت ماست، و دومی سیستمیه که در بیت‌کوین به کار رفته و کلیدهای عمومی و خصوصی شما بر پایه‌ش ساخته می‌شن.



رمزنگاری منحنی بیضوی در یوتیوب

سیستم رمزنگاری RSA

سیستم RSA اسم خودش رو از نام خانوادگی سه شخصی گرفته که در اختراعش نقش داشتن: ریوست، شامیر، و آدلمن.



سال ۱۹۷۶، ویتفیلد دیفی و مارتین هلمن ایده رمزنگاری نامتقارن رو مطرح کردن—ایده‌ای نو و انقلابی—اما راه‌حل عملی‌ای براش ارائه ندادن.

ریوست، شامیر، و آدلمن هر سه در ام‌آی‌تی تدریس می‌کردن، و ارتباط نزدیکی با هم داشتن. روزی یکی از شاگردهای ریوست مقاله دیفی-هلمن رو بهش نشون می‌ده و می‌گه، «ممکنه برات جالب باشه»، و واقعاً بود. ریوست و شامیر، که در حوزه کامپیوتر فعالیت داشتن، تصمیم می‌گیرن روی این مسئله کار کنن.

این دو ماه‌ها تلاش می‌کنن تابع یه طرفه‌ای رو پیدا کنن که محاسبه‌ش از یه سمت سریع اما از سمت دیگه بسیار سخت باشه، و درعین حال ضعف امنیتی‌ای نداشته باشه که برگشت‌پذیری‌اش رو ساده کنه. آدلمن، که ریاضی‌دان بود، مسئولیت این رو داشت که توابع پیشنهادی رو بشکنه و نقاط ضعفشون رو پیدا کنه.

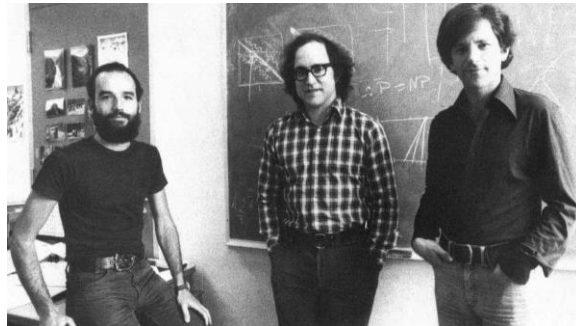


مرور تاریخچه RSA با لئونارد آدلمن در یوتیوب

شبی در آوریل ۱۹۷۷، این سه توسط یکی از دانشجویها به مهمونی پِسَح (عیدی یهودی) دعوت می‌شن. بعد از برگشتن به خونه‌هاشون، ریوست، که خوابش نمی‌بره، شروع می‌کنه به کار روی مسئله و بالاخره تابع یه طرفه رو پیدا می‌کنه. به آدلمن زنگ می‌زنه، مطرحش می‌کنه، و آدلمن همونجا بهش تبریک می‌گه. ریوست تمام شب رو بیدار می‌مونه و تا صبح مقاله‌ش رو می‌نویسه.

داستان انتخاب اسم RSA هم یکی از اون چیزهاییه که شانس‌ی اما فوق‌العاده اتفاق می‌افته. ریوست ابتدا قصد داشت نویسنده‌های مقاله رو به ترتیب معمول «آدلمن، ریوست، شامیر» بنویسه، اما آدلمن، که حس می‌کرد بیشتر کار رو اون‌ها انجام دادن، موافق نبود اسمش لحاظ بشه. درنهایت، بعد از کلی صحبت و فکر، قبول می‌کنه اما می‌گه اسم من رو آخر بذارید، و این طوری RSA خلق می‌شه.

ریوست، شامیر، و آدلن سال ۲۰۰۲ **جایزه تورینگ** (بالاترین جایزه در حوزه کامپیوتر و به نوعی نوبل علوم کامپیوتر) رو به خاطر عملی ساختن رمزنگاری کلید عمومی بردن.



در این عکس معروف، یه شوخی بامزه روی تخته هست، که ریوست می گه احتمالاً من نوشتم. (درمورد مسئله برابری پی و ان پی بخونید.) اگه علاقه مندید با ریوست و کارهای آشنا بشید، «**تاریخ شفاهی رونالد ریوست**» رو ببینید. به طبع، مصاحبه کامل آدلن با ACM (انجمن اعطاکننده جایزه تورینگ) رو هم پیشنهاد می کنم.

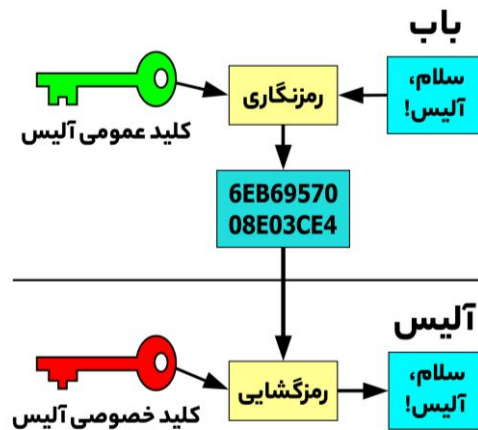
عملکرد RSA

اما RSA دقیقاً چطوری کار می کنه؟

با RSA، شما یه کلید عمومی و یه کلید خصوصی دارید. کلید عمومی رو می تونید در اختیار همه قرار بدید. می تونید اون رو در سایت شخصی خودتون بذارید، در امضای ایمیل، در بایوی توئیتر، یا روی **کارت ویزیت**. هرچیزی که با کلید عمومی شما رمزنگاری بشه، تنها با کلید خصوصی شما قابل رمزگشاییه.

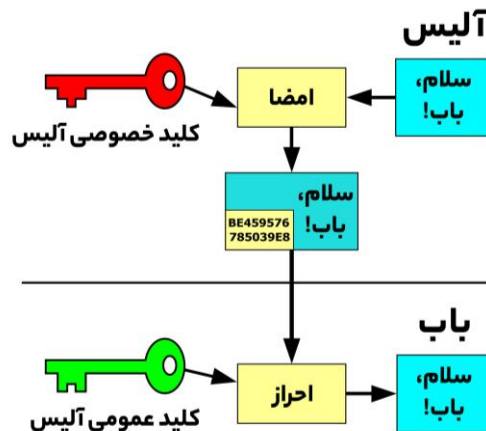
افراد می تونن از کلید عمومی شما برای ارسال پیامی محرمانه استفاده کنن، و اون شخص و شما می تونید مطمئن باشید کسی جز شما (دارنده کلید خصوصی مرتبط با اون کلید عمومی) قادر به خواندن پیام نیست.

رمزنگاری و رمزگشایی



به این مثال توجه کنید. باب می‌خواهد پیامی رو برای آلیس ارسال کنه اما نمی‌خواد کسی جز آلیس از محتوای پیام باخبر بشه. پیام خودش رو با «کلید عمومی آلیس» رمزنگاری می‌کنه. باب پیام رمزنگاری شده رو برای آلیس ارسال و آلیس با داشتن «کلید خصوصی» خودش می‌تونه اون رمزگشایی کنه و بخونه.

اصالت‌سنجی / احراز هویت



رمزنگاری کلید عمومی همچنین امکان اصالت‌سنجی / احراز هویت (authentication) رو به ما می‌ده، و این در بعضی شرایط می‌تونه حیاتی باشه، مثل زمانی که می‌خواهید هویت شخصی ناشناس رو احراز کنید.

شخص پیامی رو با کلید خصوصی اش «امضا» می کنه، و شما با داشتن کلید عمومی اش قادر به احرازش هستید. در اینجا کمی وارد موضوع PGP می شیم—که جلوتر مفصل درموردش صحبت خواهیم کرد—اما قبل از اینکه من و ناداو ایوگی، از توسعه دهنده های قدیمی حوزه بیت کوین، شروع به همکاری کنیم، نیاز بود هویت هم رو احراز کنیم. بهترین اقدام این بود که پیامی رو با مشخصات من و موضوع صحبتمون در اون لحظه امضا و ارسال کنه و من احراز کنم.

```
gistfile1.txt Raw
1 -----BEGIN PGP SIGNED MESSAGE-----
2 Hash: SHA1
3
4 I'm shesek on freenode, chatting with lmushix23 about eznode
5 -----BEGIN PGP SIGNATURE-----
6 Version: GnuPG v1
7
8 iQEcBAEBAGAGBQJgPWRZAAoJEIH2EEzQ8VD8PAEH/RmxTaZbfSgrCibnALBDTOfo
9 vCJW+av2v57BYX7ecPB81tgj4/uoQ99s87hpGRtjWJRixIFpJxWnoWxoZSRfVtRW
10 D0Ty2cqP7wV27SBgQP0o5pREYHVzvV0ka/9260pJXMCTbfyVpvA3zoNc1fRcdWBA
11 xu89fDa+y/SOEMQ5IHL/poI2REeWEQcBjBU/1WLAsyGsrkZ2uR3o/dwjt0b9VdfG
12 KC97EahJ1EFLesV1fWy62hULFWxmKZVP3mbd047P4CQUXE9LIztiFXFwXctmLIzK
13 VOCqr9S5jFEhP3nIViETZkIGW+RL6mLmDXd7qVGLZwyPRs1geyK3YVfNvH5Rvt4=
14 =2MGG
15 -----END PGP SIGNATURE-----
```

در اینجا، ناداو پیام رو امضا و برای من ارسال کرد، و من با وارد کردن (import) کلید عمومی اش و صحت سنجی این پیام موفق به احراز هویتش برای خودم شدم. بهتر می بود آگه زمان رو هم لحاظ می کرد، به ساعت هماهنگ جهانی (UTC).

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

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

PS C:\Users\Saeid> gpg --verify .\1f7483d020d72b07852790c755012e5b.txt
gpg: Signature made 3/2/2021
gpg: using RSA key 81F6104CD0F150FC
gpg: Good signature from "Nadav Ivgi <nadav@shesek.info>" [unknown]
gpg: aka "Nadav Ivgi (Bitrated) <nadav@bitrated.com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg: There is no indication that the signature belongs to the owner.
Primary key fingerprint: FCF1 9B67 8665 62F0 8A43 AAD6 81F6 104C D0F1 50FC
PS C:\Users\Saeid>
```




Nadav Ivgi
@shesek

Ambassador at @BitcoinEmbassy · @eznode_ · min.sc · bwt.dev · Spark Wallet ⚡ · PGP: FCF1 9B67 8665 62F0 8A43 AAD6 81F6 104C D0F1 50FC · Cypherpunks write code.

اثرانگشت کلید عمومی ناداو ایوگی

اصالت‌سنجی فایل‌ها، به‌ویژه در دنیای نرم‌افزار آزاد، بسیار مهمه. شما می‌خواید که مطمئن باشید نرم‌افزاری رو که دریافت می‌کنید صحیحه. اگه نرم‌افزار بیت‌کوین یا کیف پولی رو دانلود می‌کنید، مهمه که اصالتش رو قبل از استفاده احراز کنید، و این با مفهوم کلید عمومی و امضای دیجیتال ممکنه.

نکته: کلیدهای عمومی به‌طور معمول بسیار بلندند، و این، کار رو برای انتقال و وارد کردنشون سخت می‌کنه. ازاین‌رو، از **اثرانگشت کلید عمومی** استفاده می‌کنیم. ما می‌تونیم کلید عمومی خودمون رو با تابع رمزنگارانه خاصی هش کنیم و به اثرانگشت برسیم، که بسیار کوتاه‌تره. توجه کنید که همه این‌ها، از تولید کلید عمومی و خصوصی گرفته تا ساختن اثرانگشت، در محیط نرم‌افزار اتفاق می‌افته. جلوتر به این نرم‌افزارها اشاره می‌کنم.

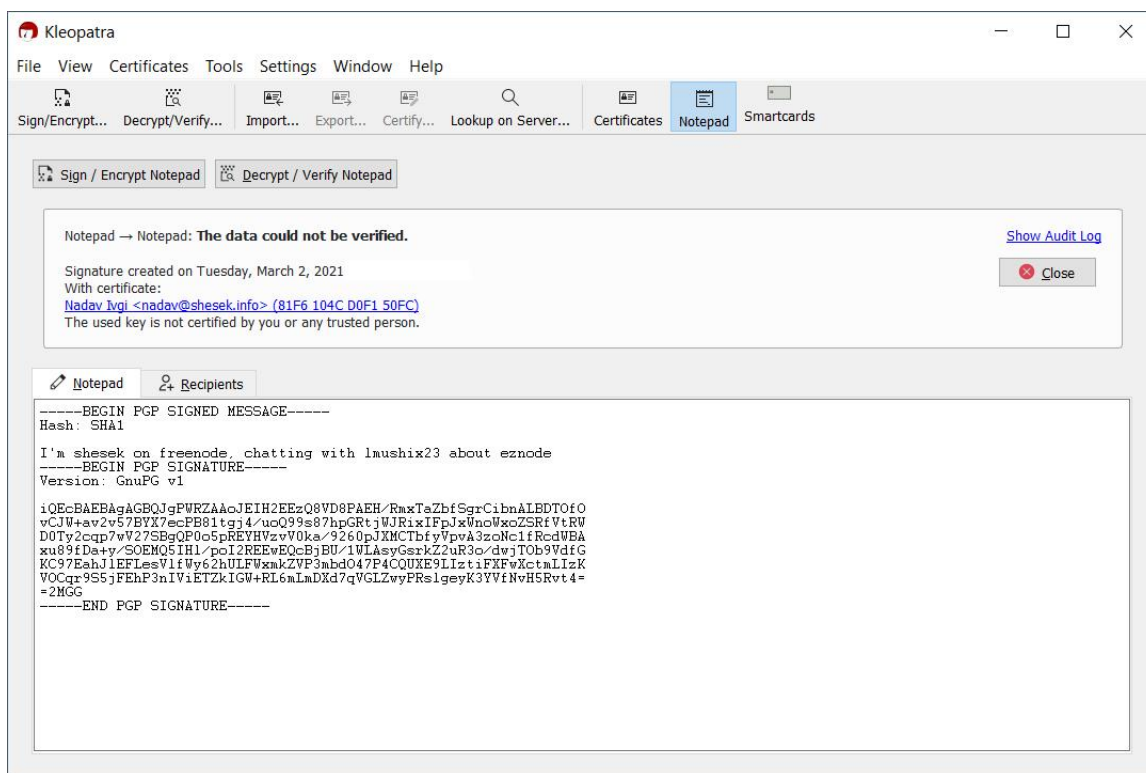
ممکنه اثرانگشت PGP بعضی رو در وبسایت یا پروفایل توئیترشون باشید. شما با داشتن این اثرانگشت می‌تونید به کلید عمومی شون برسید.

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

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

تولید کلید عمومی و خصوصی

یکی از رایج‌ترین نرم‌افزارها GNU Privacy Guard یا GPG است. آگه کاربر ویندوز هستید، از Gpg4win استفاده کنید. لینک‌های دانلود برحسب سیستم عامل در سایت رسمی **GnuPG** قرار داده شدن.



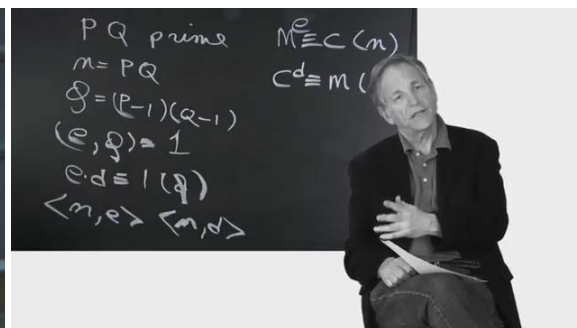
نرم‌افزار کلتوپاترا

سخن پایانی

ریاضی پشت کلید عمومی RSA بسیار جذابه آگه علاقه‌مند و کنجکاو به دوستتس هستید. توضیحش در قالب این مطلب کمی سخته، اما **ویدئویی** رو پیشنهاد می‌کنم که قدم‌به‌قدم توضیح می‌ده، و حتی آگه فکر می‌کنید در ریاضی قوی نیستید، می‌تونید نحوه کارش رو درک کنید.



داستان ریوست-شامیر-آدلمن در یوتیوب



شرح RSA از زبان سازندگان اون در یوتیوب

از دید من، RSA، در کنار نوآوری‌های دیگه‌ای مثل پروتکل تبادل کلید دیفی-هلمن (Diffie-Hellman Key Exchange)، چهره رمزنگاری و ارتباطات رو برای همیشه تغییر داد. به لطف این افراد و تلاش هاشون، ما امروز فضای اینترنت و ارتباطات امن‌تری داریم. شما این‌طور فکر نمی‌کنید؟

در ادامه، با گذشته و نحوه کار با نرم‌افزار PGP آشنا خواهیم شد.



تاریخچه و راهنمای جامع استفاده از نرم افزار PGP

تاریخچه و راهنمای PGP: مقدمه

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

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

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

WHAT 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.



مقاله انقلابی ویتفیلد دیفی و مارتین هلمن، نوامبر ۱۹۷۶

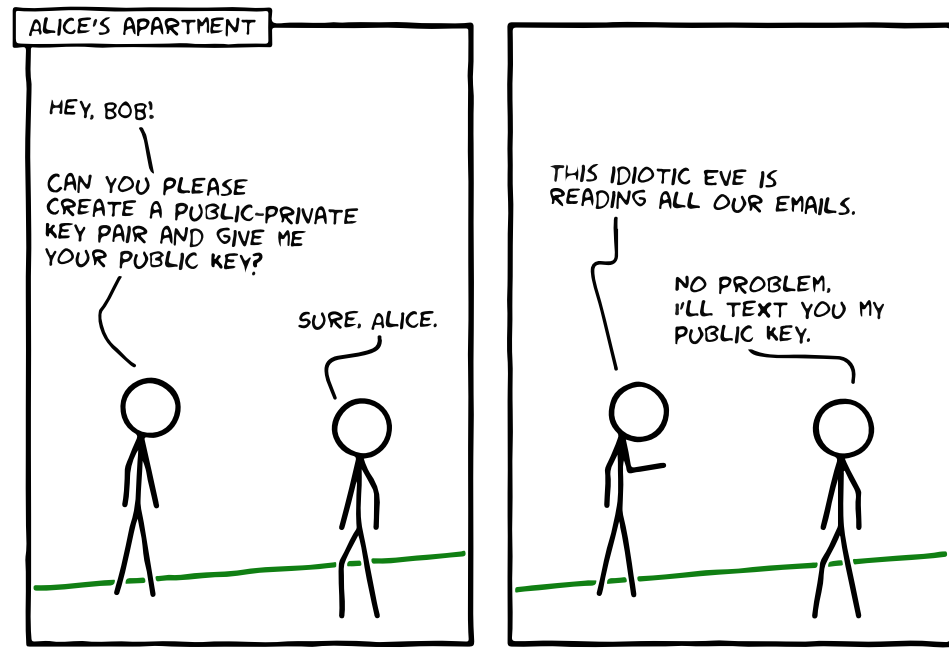
از راست به چپ، ویتفیلد دیفی، مارتین هلمن، و رالف مرکل

وقتی راجع به رمزنگاری مدرن صحبت می کنیم، باید به دهه ۱۹۷۰ برگردیم، زمانی که ویتفیلد دیفی، مارتین هلمن، و رالف مرکل پایه رمزنگاری کلید عمومی رو بنا نهادن.

مرکل رو، که الهام بخش دیفی و هلمن در رسیدن به ایده 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 دارد: یکی عمومی و دیگری خصوصی. کلید عمومی می‌تونه با هر کسی به اشتراک گذاشته بشه، بدون اینکه امنیت رو به خطر بی‌اندازه. از کلید خصوصی، اما، باید از رمز حساب بانکی تون هم بیشتر محافظت کنید.



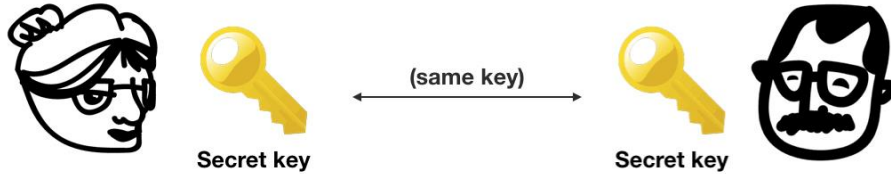
هرچیزی که با یکی از کلیدها رمز بشه، با کلید دوم گشوده می‌شه.

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

شما، که کلید خصوصی مربوطه رو دارید، به راحتی می‌تونید متن رمزنگاری شده رو رمزگشایی و اون رو به متن آشکار تبدیل کنید.

Symmetric encryption

In symmetric encryption, both parties encrypt and decrypt with the same key.



در رمزنگاری متقارن، از یک کلید هم برای رمزنگاری و هم برای رمزگشایی استفاده می‌شود. به این معنا که فرستنده و گیرنده هر دو به یک کلید مشترک دسترسی دارند، 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 دارند، 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 دسته 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 سخت گیرانه و نیازمند مجوز بود.



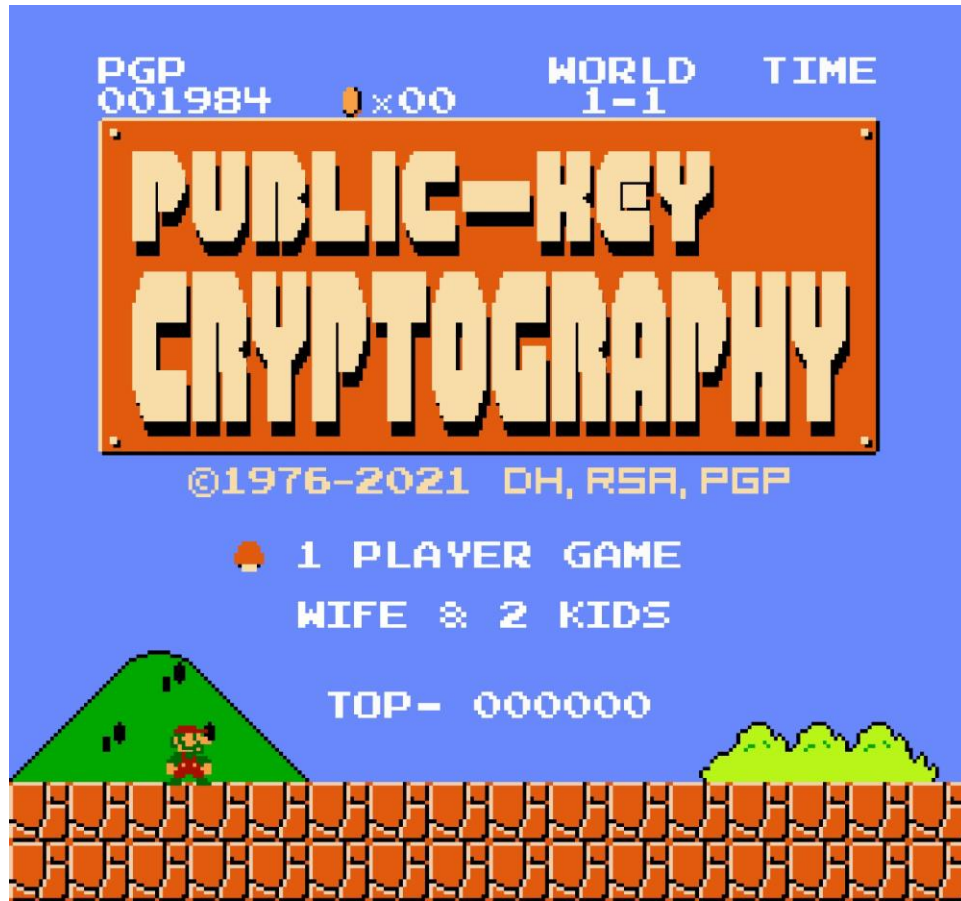
فیلیپ زیمرمن، خالق PGP

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 اون موقع، رمزنگاری قوی تنها در سلطه 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 قابل تأملی 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 تنونه با اون سرعتی که می‌خواد پروژه رو پیش ببره. باین حال، 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 به پایان برسونه.

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

در ژانویه ۱۹۹۱، بایدن **لایحه ۲۶۶** رو پیشنهاد داد. جایی در این متن اومده که شرکت‌ها موظفن در صورت ارائه درخواست قانونی، محتوای متنی، صوتی، و داده افراد رو در اختیار دولت قرار بدن. این همون آینده **اورولی** ای 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 پریچ‌وخم 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 از اونجایی که می‌ترسید روزی دولت استفاده از رمزنگاری رو ممنوع کنه، می‌خواست قبل از رسیدن چنین روزی همه تا حد امکان از ابزارهای حریم خصوصی بهره‌مند بشن. در نتیجه، تصمیم گرفت ثمرهٔ سال‌ها زحمتش رو مجانی منتشر کنه.

زیمرمن حتی تا مرز ازدست دادن 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.

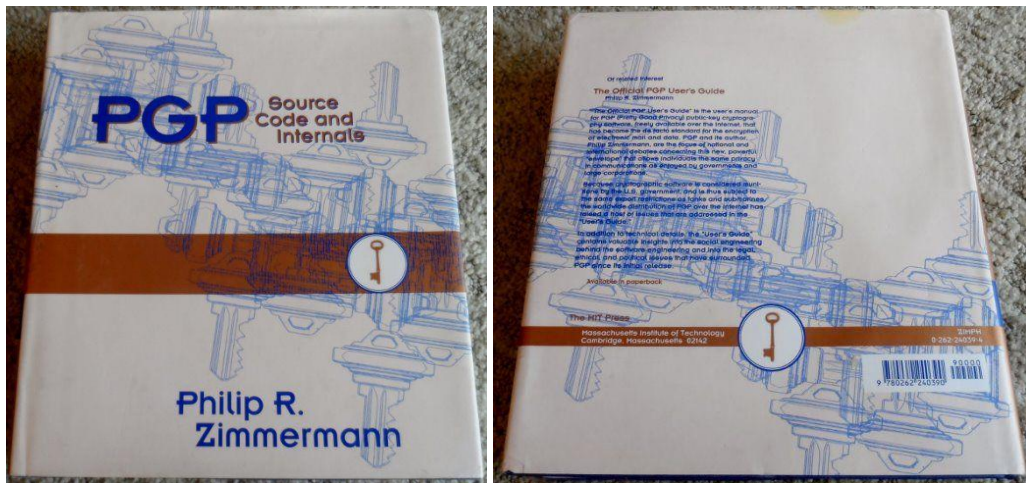
این، از دید من، نشون از فداکاری بزرگش داره.

دردسره‌های حقوقی

زیمرمن، که در اون زمان اطلاعات چندانی راجع به اینترنت نداشت، اولین نسخه 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 دونه 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)، دردسره‌های قانونی‌ای برای زیمرمن در پی 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 پرونده قضایی با دولت آمریکا شد. جرم؟ زیرپا گذاشتن 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 زیرمجموعه 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 بزرگ تر کلیک کنید.

پیش تر 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 دارد که RSA رو به شما می‌ده.

Munitions T-shirt

The rsa perl t-shirts are no longer available. The only remaining related shirt I am aware of is one sold by thinkgeek, which is Vipul Prakash's [perl rsa dolphin](#), rsa key gen and encryption in perl, pari and de.

If you are interested in printing your own t-shirts, all of the art work that was used to create the shirts is available for [download](#)


The rest of this page is of historical value only.

Munitions T-shirt

These are the "shirt of the sig". See the [export-a-crypto-system](#) signature page for background info.

In the US this shirt was theoretically [illegal](#) to export (or even to let a foreign national see!) due to the [EARS](#). Recent changes mean that you may need to notify the USG of intent to export.

Pictures



(Click either image for bigger image: 60k)

Comments, html bugs to me ([Adam Back](#)) at adam@cypherspace.org

مشاهده سایت Cypherspace

اگره در ایالات متحده بودید، این تی‌شرت رو چاپ می‌کردید، و اون رو برای کسی در خارج از کشور می‌فرستادید و یا حتی به یک تبعه 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](#). ترجمه مطلب اول رو می‌تونید [اینجا](#) بخونید و ترجمه مطلب دوم رو [اینجا](#).

داستانی که خونید تاحدامکان خلاصه شده و جزئیات ریز رو شامل نمی‌شه. چند دهه از اون دوران گذشته، و تنها راهی که می‌تونید تجربه 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

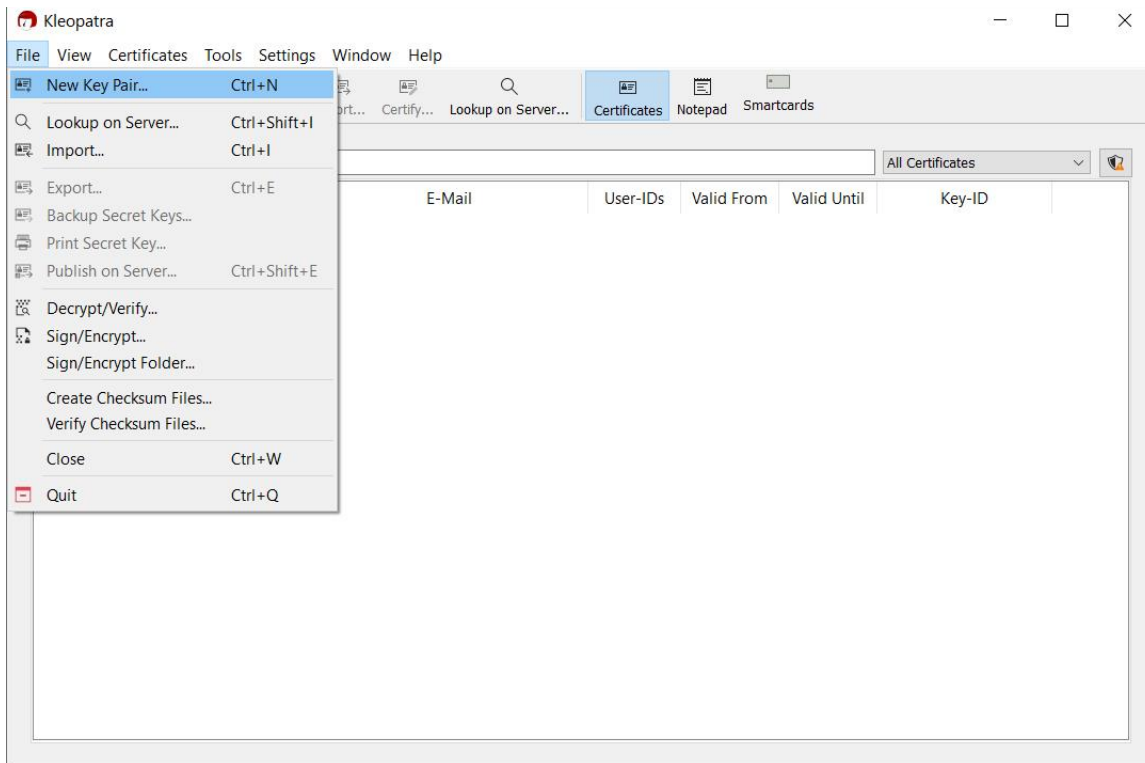
حالا که با تاریخچه PGP آشنا شدیم، می‌تونیم کمی در مورد کاربرد و عملکردش صحبت کنیم. اولین قدم اینه که نرم‌افزارش رو دانلود و نصب کنیم و کلید خودمون رو بسازیم.

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.

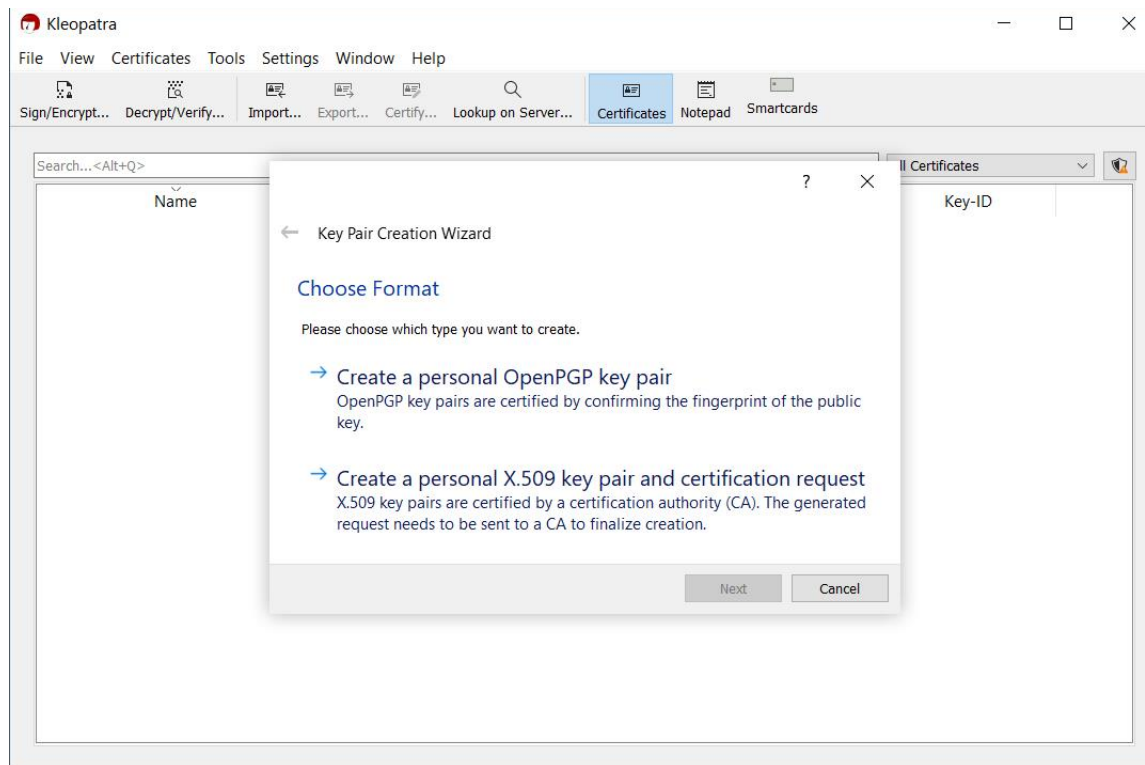
ساخت کلید

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

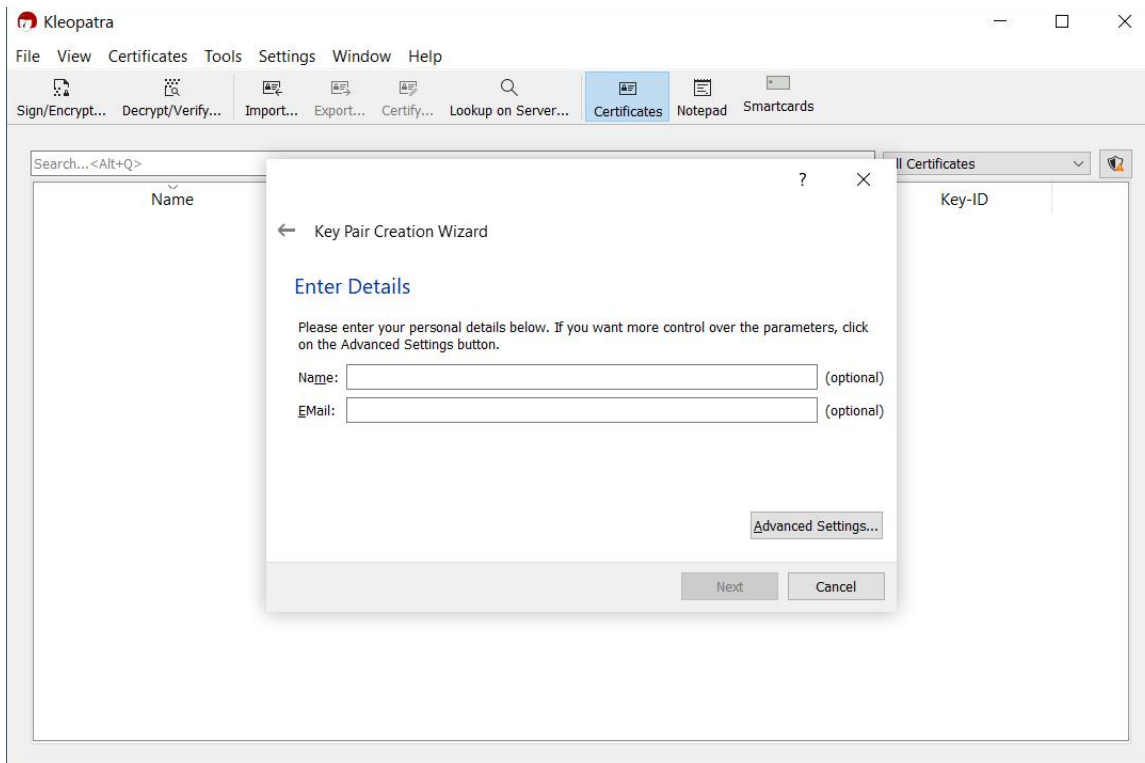
از نرم‌افزار Kleopatra برای تولید کلید شخصی، مدیریت کلیدها، رمزنگاری، و رمزگشایی استفاده می‌کنیم. به تصاویر صفحات بعد توجه کنید.



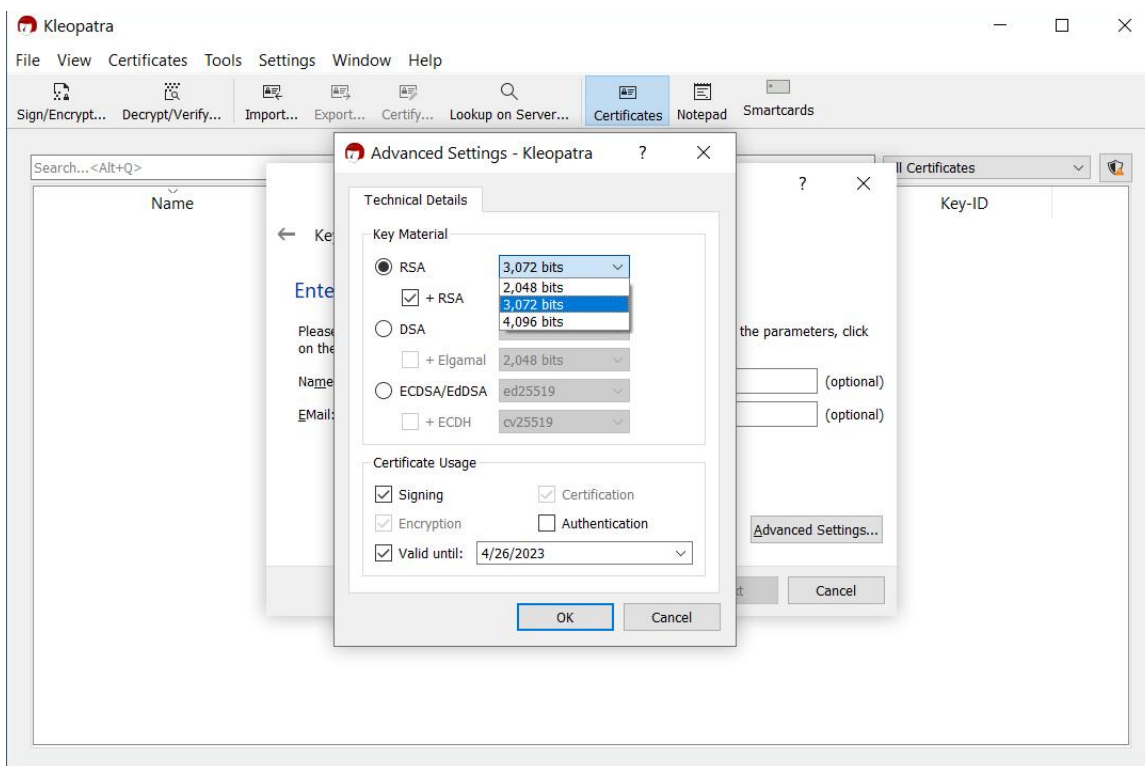
قدم اول در ساخت کلید: File → New Key Pair (یا استفاده از میان‌بر Ctrl + N)



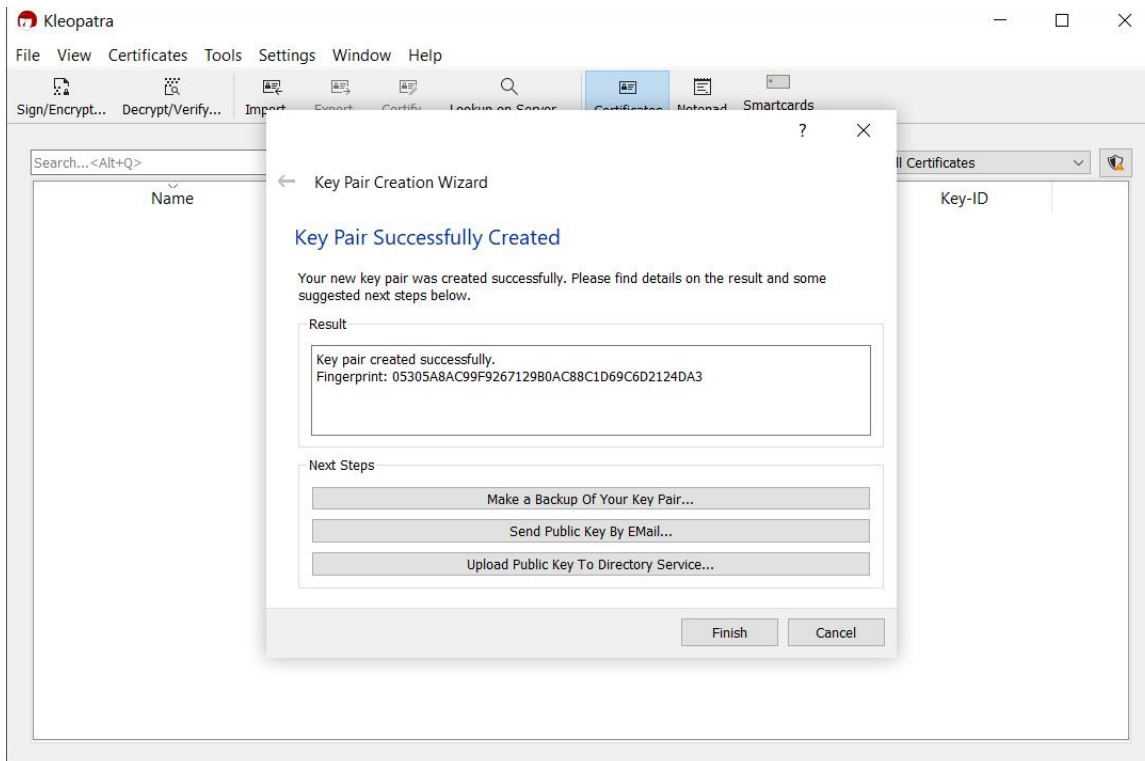
قدم دوم: انتخاب گزینه Create a personal OpenPGP key pair



قدم سوم: وارد کردن اطلاعات (اختیاری)



قدم چهارم: هنگام ساختن جفت کلید (key pair) می‌توانید از تنظیمات پیش فرض استفاده کنید، اما ضروری نداده اگه اندازه کلید رو جهت امنیت بیشتر ۴۰۹۶ بیتی قرار بدید.



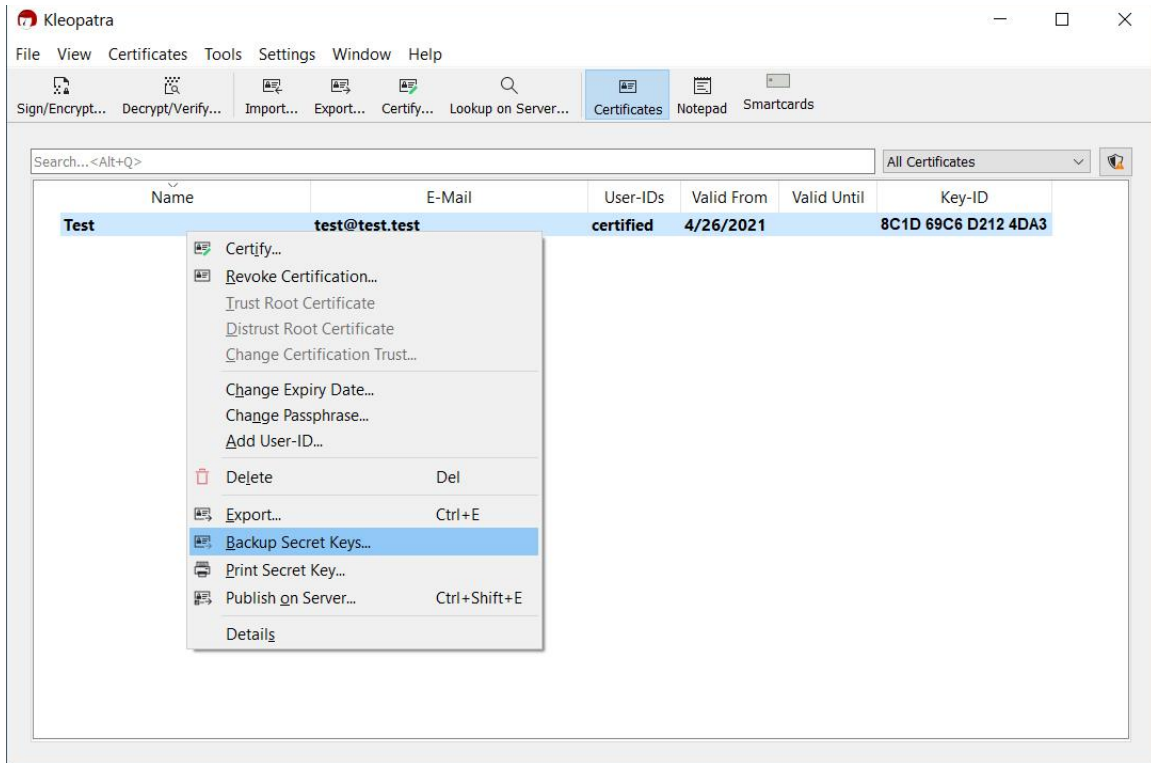
کلید شما با موفقیت ساخته شد.

اگره در مورد اجزای مختلف این پنجره کنجکاوید، سایت GnuPG یکی از جامع‌ترین و جذاب‌ترین سؤال‌های پرتکرار رو داره، که می‌تونید [اینجا](#) بخونید. در مورد امنیت و طول کلیدها کنجکاوید؟ [این مکالمه](#) رو در توئیتر دنبال کنید.

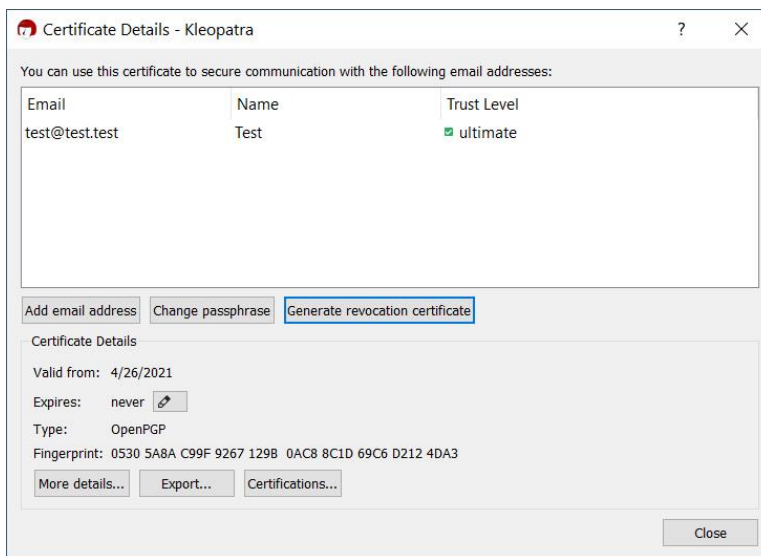
کلید خصوصی: تهیه نسخه پشتیبان و گواهی ابطال

به تصویر بالا و گزینه‌های نمایش داده شده در چهارچوب Next Steps توجه کنید. از کلید خصوصی تون بک آپ تهیه کرده و اون رو در جایی امن نگه دارید. کل این فرآیند در امن نگه داشتن و محافظت از کلید خصوصی شما خلاصه می‌شه.

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



تهیه نسخه پشتیبان از کلید خصوصی (بسیار مهم)

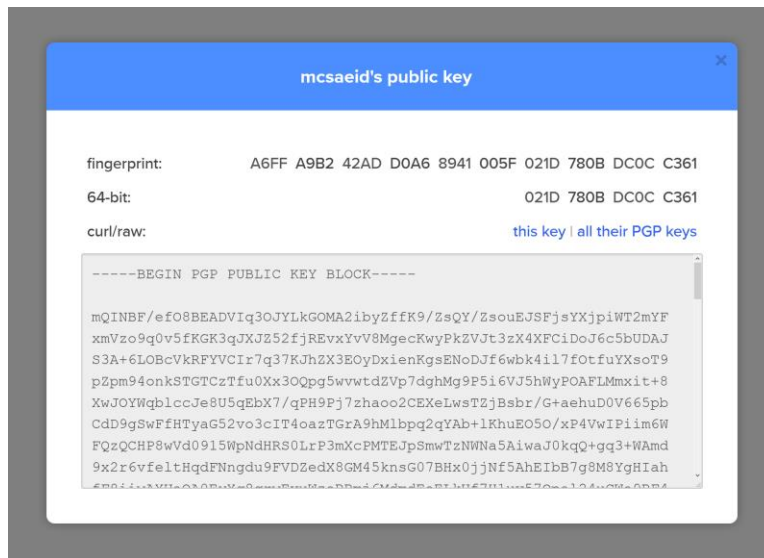


یکی از اولین کارهایی که انجام می‌دید باید تولید گواهی ابطال (revocation certificate) باشد. آگه زمانی کلیدتون گم بشه یا لو بره، با استفاده از این گواهی و انتشارش می‌تونید کلید رو باطل کنید. در ساخت کلید و ابطالش دقت کافی رو به‌خرج بدید. داشتن چند کلید باطل شده نشونه چندان جالبی نیست.

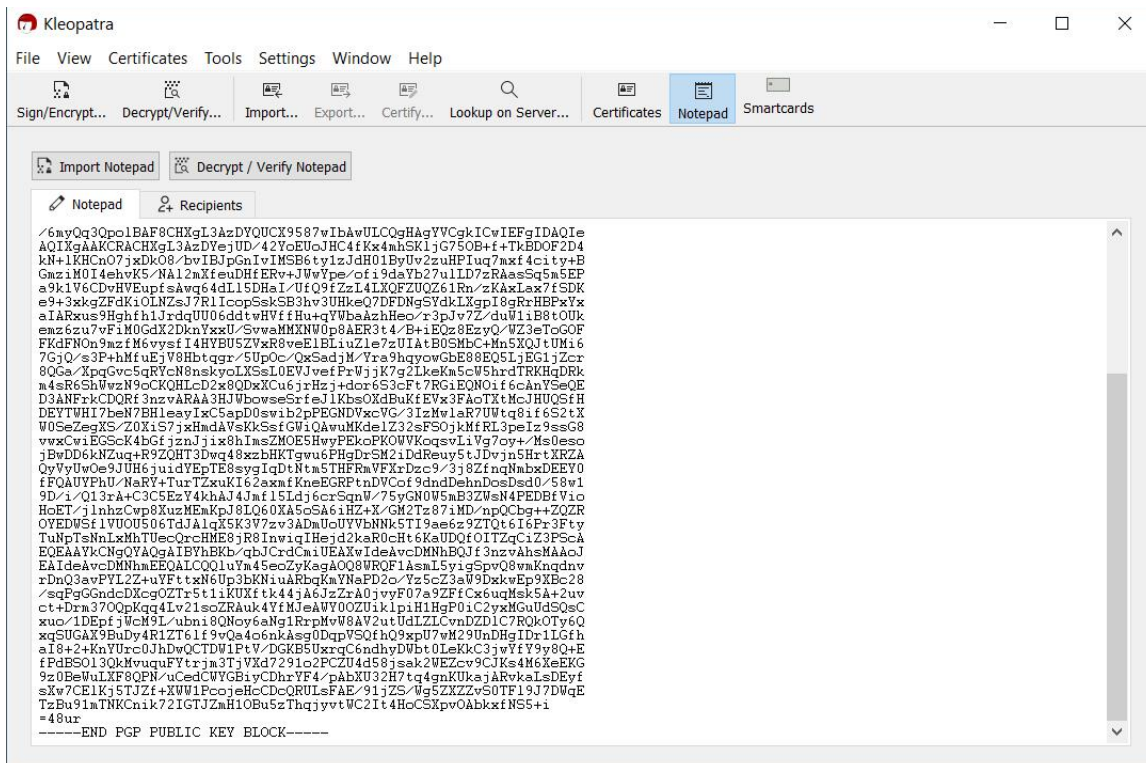
تولید گواهی ابطال

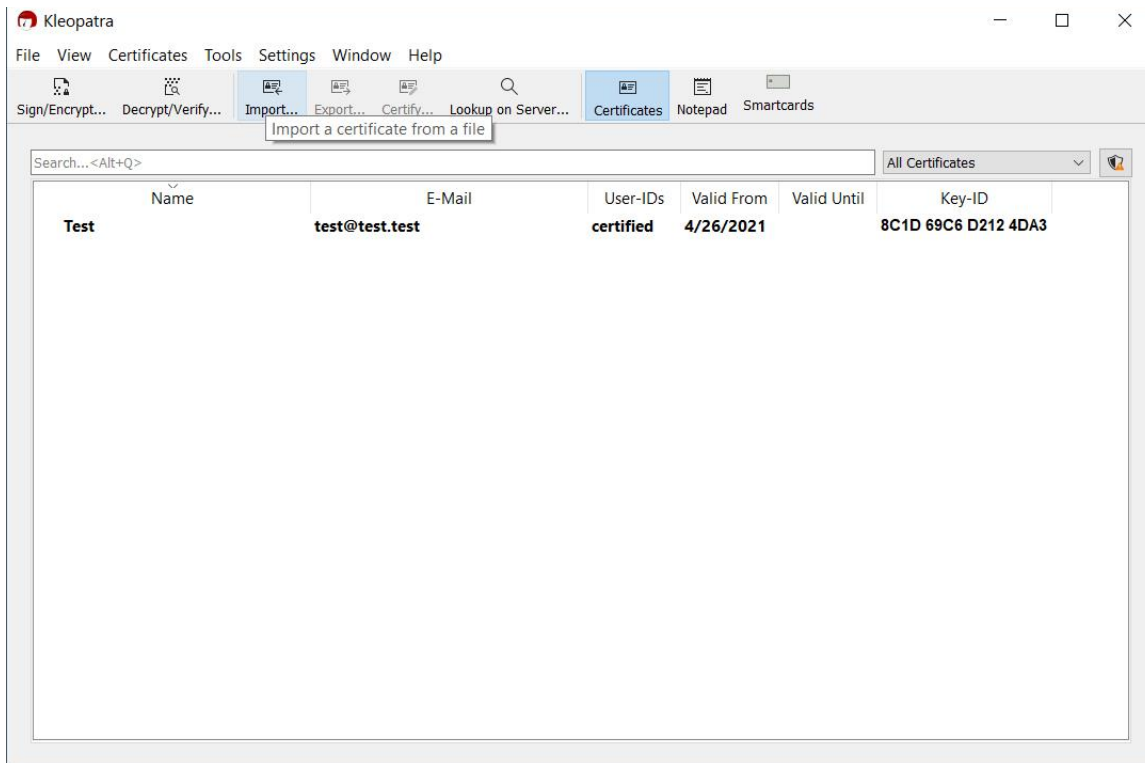
وارد کردن کلید عمومی دیگران

برای اینکه بتوانید با افراد مکالمه رمزنگاری شده داشته باشید، ابتدا باید کلید عمومی شون رو وارد (import) کنید. روش های مختلفی برای انجام این کار وجود داره: (۱) کپی و پیست کلید عمومی در Notepad؛ (۲) ذخیره کلید عمومی به صورت فایل و سپس Import.



کلید عمومی من در Keybase





وارد کردن کلید عمومی دیگران از طریق گزینه `Import...` یا `Notepad`

اگر کار با ترمینال رو یاد بگیرید، کارتون ممکنه راحت تر 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 gpg_keys.asc
gpg: key 021D780B0C0CC361: "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-keyserver.net:11371
(1)  MC Saeid <mcsaeid@protonmail.com>
    4096 bit RSA key 021D780B0C0CC361, 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 021D780B0C0CC361: "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 021D780B0C0CC361
gpg: key 021D780B0C0CC361: "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-keyserver.net:11371
(1)  Ziya Sadr <ziya_sadr@protonmail.com>
    4096 bit RSA key F97C4797F2EB716, created: 2018-06-27, expires: 2034-06-23
(2)  Ziya Sadr <ziyaamir@sadr@gmail.com>
    2048 bit RSA key E28F1C1F3DC8EFCC, created: 2018-03-13
Keys 1-2 of 2 for "ziya sadr". Enter number(s), N)ext, or Q)uit > 1
gpg: key F97C4797F2EB716: "Ziya Sadr <ziya_sadr@protonmail.com>" not changed
gpg: Total number processed: 1
gpg:   unchanged: 1
PS C:\Users\Saeid> DONE_

```

`gpg --import` [نام فایل]

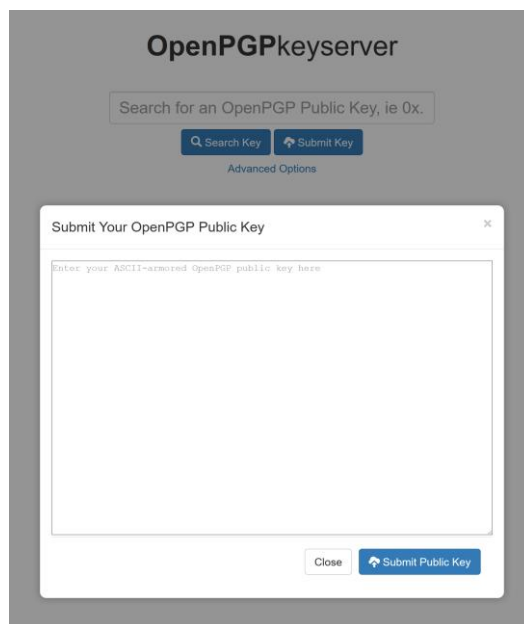
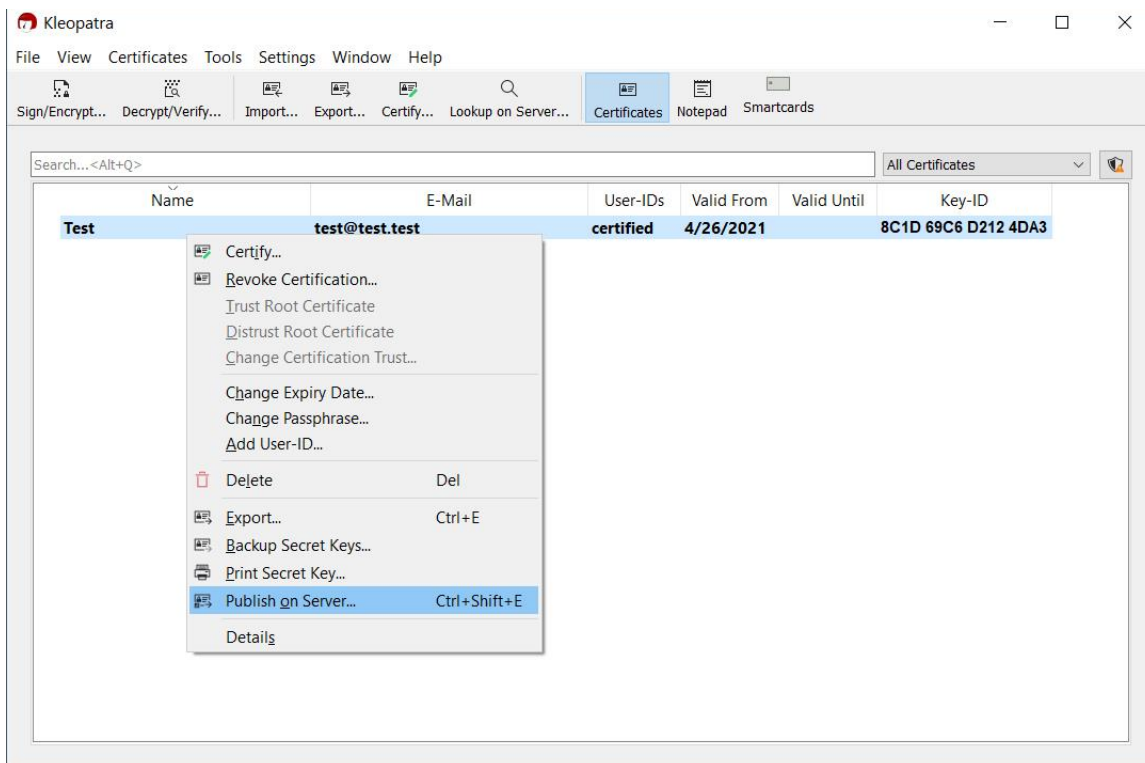
برای وارد کردن از فایل

`gpg --keyserver keys.gnupg.net --search-keys` [نام شخص / آدرس ایمیل]

جستجو در سرورهای کلید

`gpg --keyserver keys.gnupg.net --recv-keys` [اثر انگشت]

جستجو با اثر انگشت



انتشار کلید عمومی در سرور کلید از طریق نرم افزار یا به صورت 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 از اونجایی که این سرورها همدیگه رو mirror می‌کنن، کلید عمومی من در جاهای دیگه هم قابل یافته.

اثرانگشت کلید عمومی

خب، حالا که کلید عمومی هم رو داریم، می‌تونیم به صورت 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 در صورتی که هویت شخص رو احراز و اطمینان حاصل کنید کلید واقعاً به او تعلق داره، امنیت خواهید داشت.

ضیاء صدر در ویدئوی زیر مفصل در این باره صحبت می‌کنه. پیشنهاد می‌کنم این ویدئوی بسیار خوب رو از دست ندید، به ویژه که در مورد web of trust هم صحبت می‌کنه.



مشاهده در یوتیوب

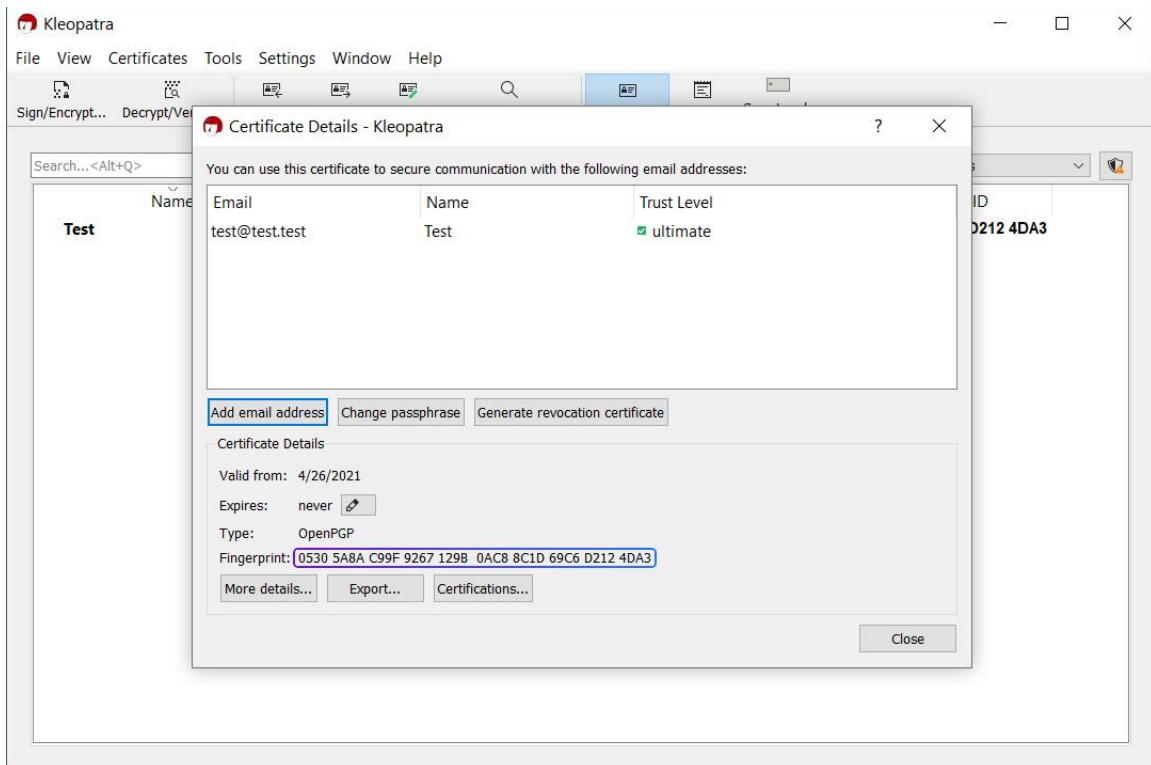
در مقاله پیشین در مورد اثرانگشت مختصر صحبت شد. همون‌طور که پیش‌تر دیدید، کلیدهای عمومی بسیار طولانی‌ان، و امکان خوندن یا وارد کردن اون‌ها به صورت دستی وجود نداره. از این رو، برای پیدا کردن و همچنین احراز هویت افراد اثرانگشت کلید عمومی اون‌ها رو بررسی می‌کنیم.

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

توجه کنید که شناسه بلند کلید (long key ID) و شناسه کوچک کلید (short key ID) به ترتیب شونزده و هشت رقم آخر اثرانگشتن. شما با داشتن هر کدوم از این‌ها می‌تونید کلید عمومی من رو پیدا و وارد کنید.

احراز هویت کلید عمومی با اثرانگشت

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



با راست کلیک روی کلید و انتخاب گزینه 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]
```

```
gpg --fingerprint mcsaeid
```

مثال:

توجه کنید، صرفِ قراردادادن اثرانگشت در پروفایل توئیتر، امضای ایمیل، تلگرام، و جاهای دیگر چیزی رو اثبات نمی‌کنه. در بهترین حالت، وقتی شخص رو چهره‌به‌چهره دیدید، کلید عمومی‌اش رو احراز کنید، و آگه 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 مکالمه صوتی بتونن اثرانگشت خود رو با هم مقایسه و احراز کنن—مشابه الفبای آوایی ناتو (NATO phonetic alphabet) اما با کلمات بیشتر.

آگه 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 خوانده می‌شه، طوری که چپ‌ترین بایت معادل کلمه زوج و راست‌ترین بایت معادل کلمه فرد. برای مثال، در A6FF، کلمه منصوب به A6 زوج و FF فرد.

A PGP public key fingerprint that displayed in hexadecimal as

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

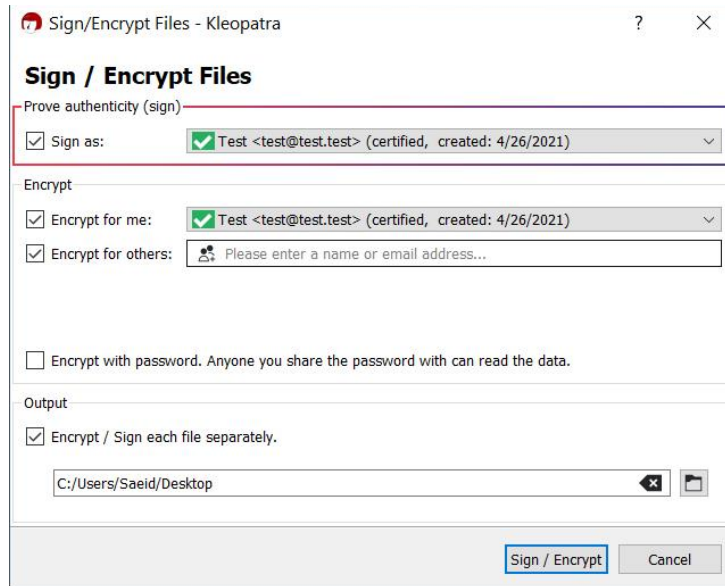
would display in PGP Words (the "biometric" fingerprint) as

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.

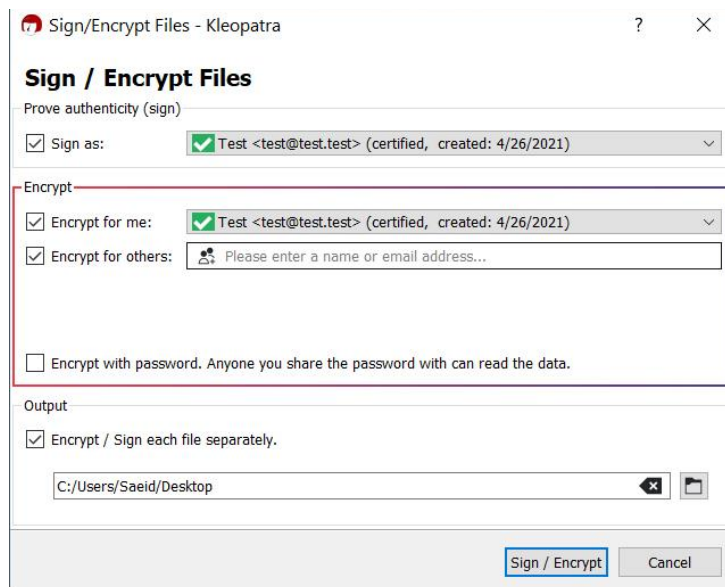
در نرم‌افزار Kleopatra به دو روش می‌تونید رمزنگاری کنید: متن و فایل. برای رمزنگاری فایل‌ها کافیه گزینه Sign/Encrypt رو بزینید، فایل رو انتخاب کرده، و در پنجره‌ای که باز می‌شه گیرنده یا گیرندگان رو مشخص کنید. به تصاویر صفحه بعد توجه کنید.



می‌تونید انتخاب کنید فایل رو با کلید خودتون امضا کنید

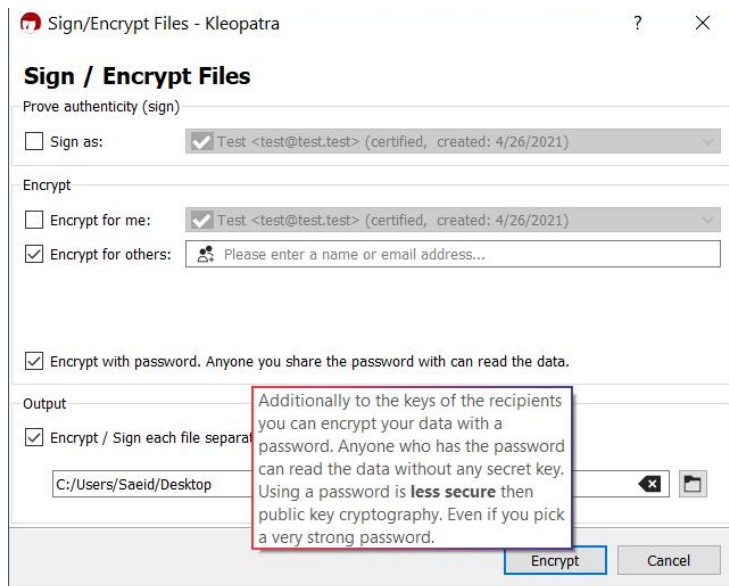
اینجا می‌تونید فایل رو امضا کنید. جلوتر بیشتر بهش خواهیم پرداخت. کسی که فایل رو رمزگشایی می‌کنه می‌بینه که شما اون رو امضا کرده‌اید، و می‌تونه اطمینان داشته باشه محتوا توسط شخص دیگه‌ای دست کاری نشده. هیچ‌کسی جز شما، بدون داشتن کلید خصوصی شما، قادر به ارائه اون امضای منحصر به فرد نیست.

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 به طور پیش فرض برای شما هم رمزنگاری می‌شه، مگه اینکه تیک Encrypt for me رو بردارید. (شاید نخواهید فایل رو در آینده باز کنید، یا شاید اطلاعات حساسیه و نخواهید 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 گزینه 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.

```

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

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

PS C:\Users\Saeid> gpg --encrypt Example.txt
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID. End with an empty line: mcsaeid

Current recipients:
rsa4096/F310A708cd808112 2021-04-26 "Test <test@test.test>"

Enter the user ID. End with an empty line:
PS C:\Users\Saeid> gpg --encrypt --sign -r test@test.test Example.txt
PS C:\Users\Saeid>
    
```


ساده‌ترین دستور اینه:

`gpg --encrypt [نام فایل]`

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

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

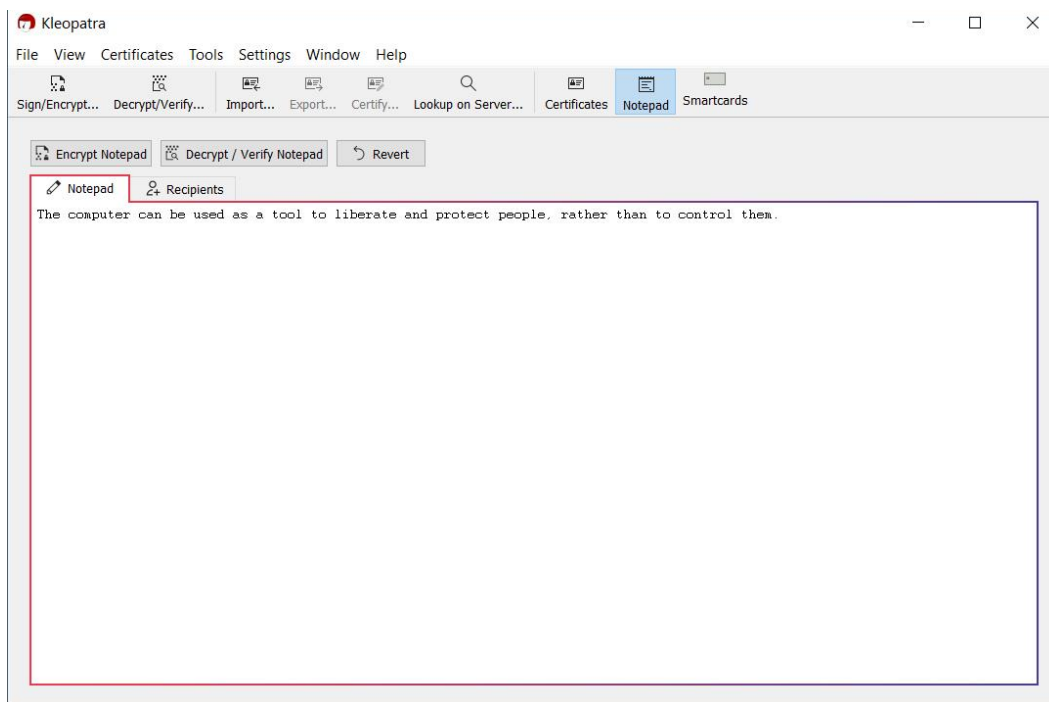
اینجا به توضیح کوتاهی در مورد پارامترها بسنده می‌کنم، که ممکنه جالب توجه باشه:

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

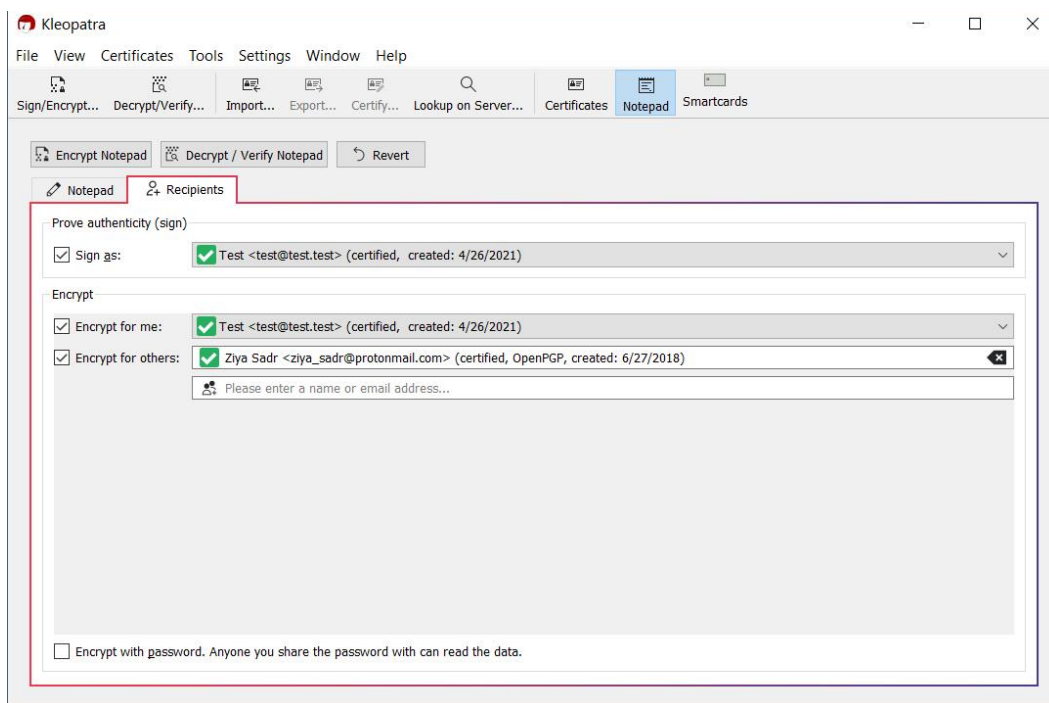
توجه مهم: اگه می‌خواید بتونید فایل رو رمزگشایی کنید، حتماً باید خودتون رو هم جزو گیرنده‌ها قرار بدید. درضمن، می‌تونید چند گیرنده داشته باشید؛ در این صورت، چند مورد `-r` خواهید داشت.

توجه مهم: بعد از اینکه GPG فایل رو رمزنگاری کرد، فایل اصلی رو دست‌نخورده نگه می‌داره. حواستون باشه اون رو حذف کنید، چه بسا به‌شکلی امن و غیرقابل برگشت. (اگه کاربر ویندوز هستید، در مورد [SDelete](#) بخونید.)

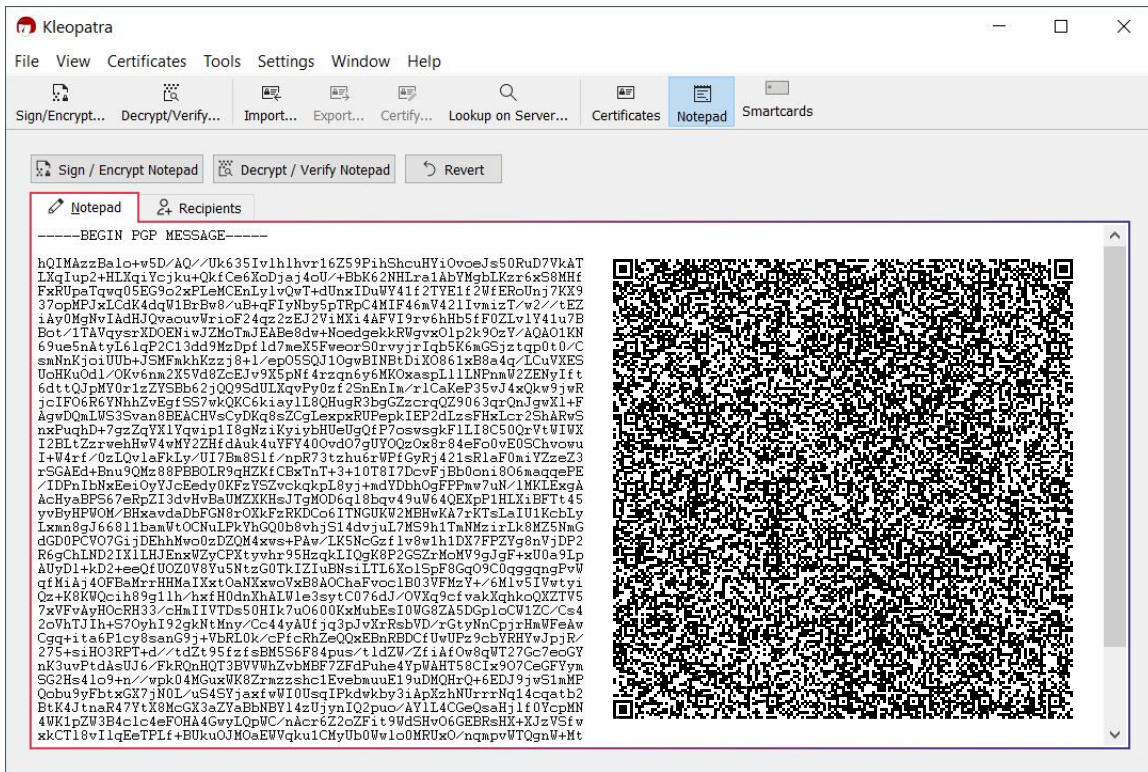
تا اینجا به رمزنگاری فایل‌ها پرداختیم، اما چطور یک متن رو رمزنگاری کنیم؟ خیلی ساده. از ابزار Notepad استفاده کنید.



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

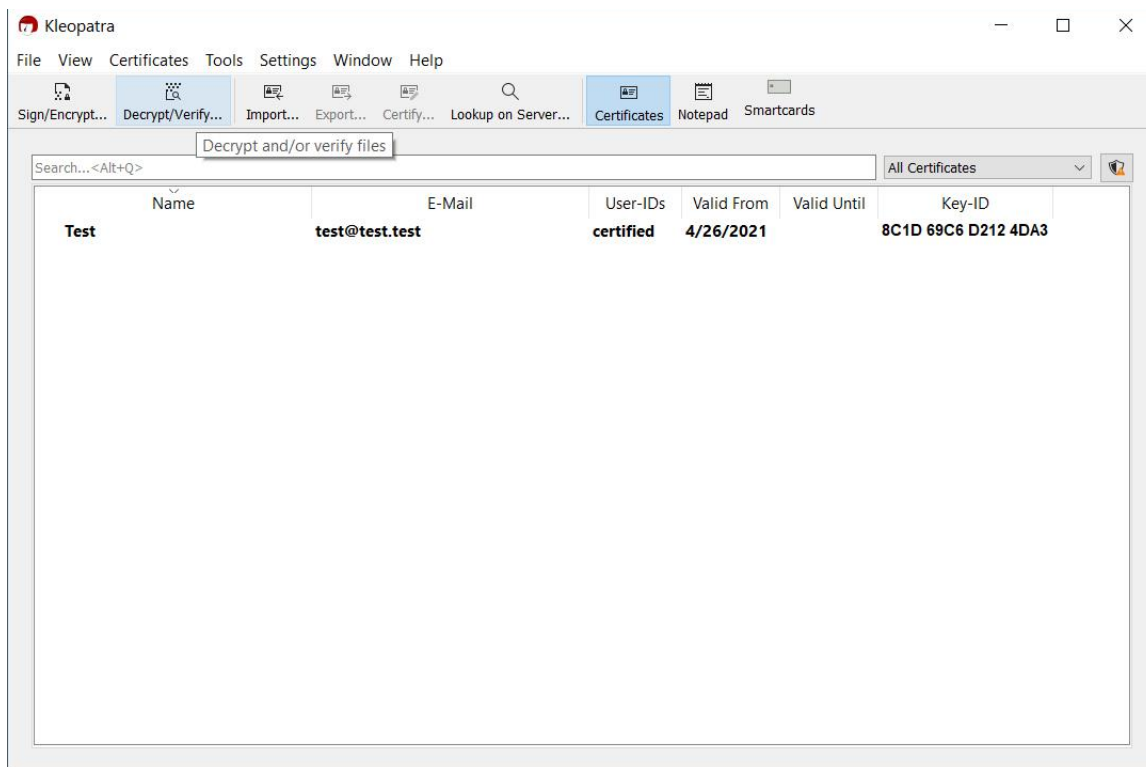


پس از نوشتن متن و تعیین گیرنده(ها)، با زدن گزینه Sign / Encrypt Notepad متن رمزنگاری شده رو تحویل خواهید گرفت

برای مثال، اینجا پیامی رو برای خودم و ضیاء رمزنگاری کردم. او می تونه تصویر با کیفیتی رو از کد QR بالا ذخیره کنه (برای مثال، با زوم کردن و گرفتن یک اسکرین شات)، با ابزار [QR Decoder](#) اون رو decode کنه، و محتوای پیام رو بخونه. شما هم می تونید 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 آسانی رمزنگاری کردن اون‌هاست. برای فایل‌ها می‌تونید از گزینه Decrypt/Verify استفاده کنید (یا روی فایل راست کلیک کرده و Decrypt and verify رو انتخاب کنید).



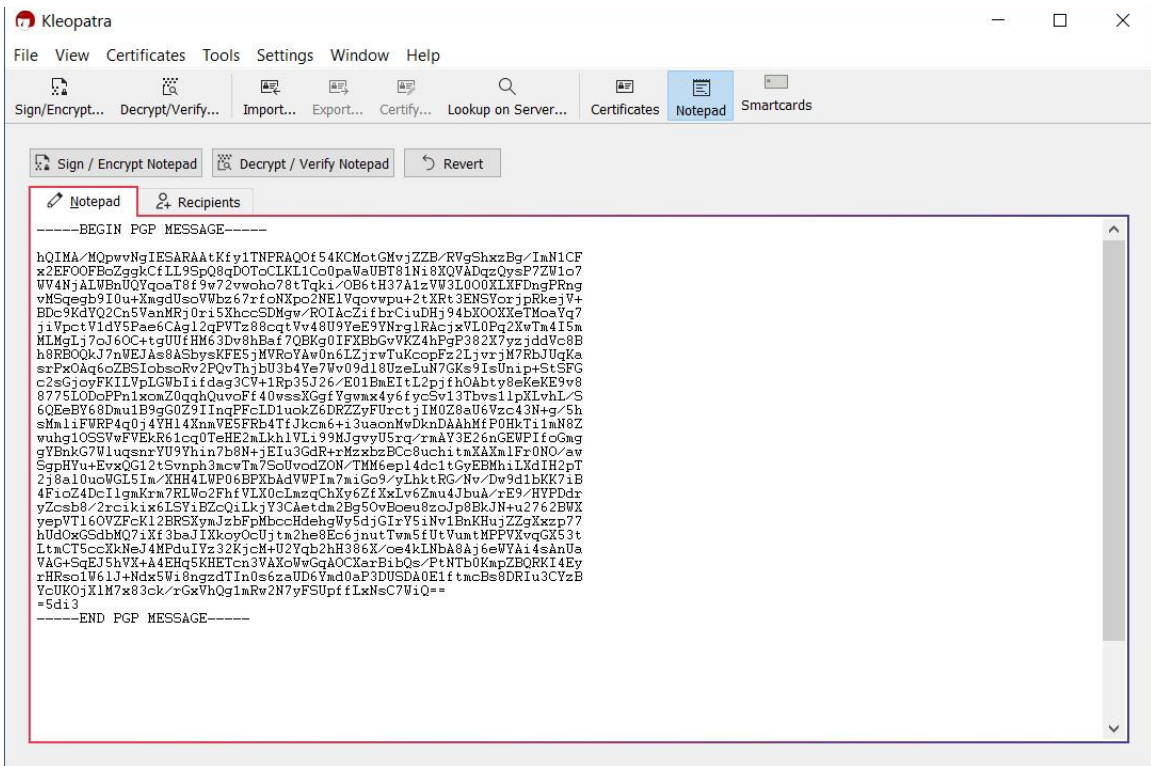
رمزگشایی فایل‌ها با گزینه Decrypt/Verify...

همچنین، می‌تونید از دستور زیر استفاده کنید:

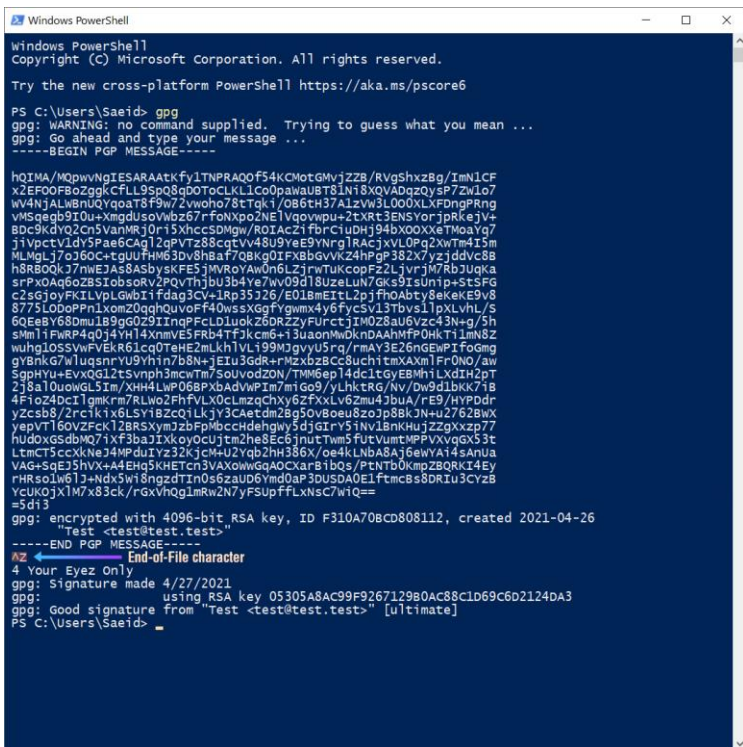
`gpg --decrypt [نام فایل]`

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

`gpg -d [نام فایل]`



رمزگشایی متون با Notepad



درضمن، اگر متن رمزنگاری شده دارید، می‌تونید اون رو در Notepad قرار بدید.

همچنین، اگر دوست دارید اون رو در

ترمینال رمزگشایی کنید، ابتدا بنویسید

gpg و enter بزنید، سپس پیام رو

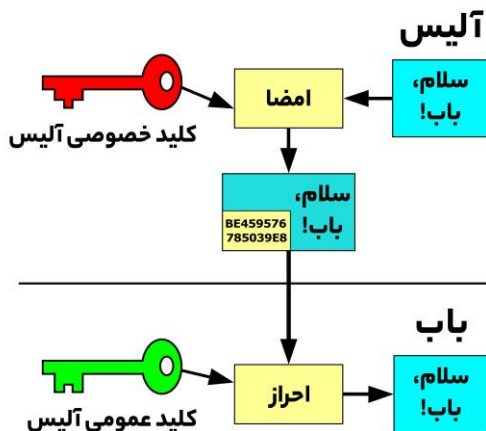
paste کنید، و در انتها برای پایان Ctrl

+ Z رو زده (کاراکتر End-of-File):

Ctrl-D (در Unix) و enter بزنید.

امضای دیجیتال

به مقوله مهم امضا کردن (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 منحصر به فرد نیست، و این، اطمینان می‌ده محتوا حین ارسال دست‌کاری نشده.

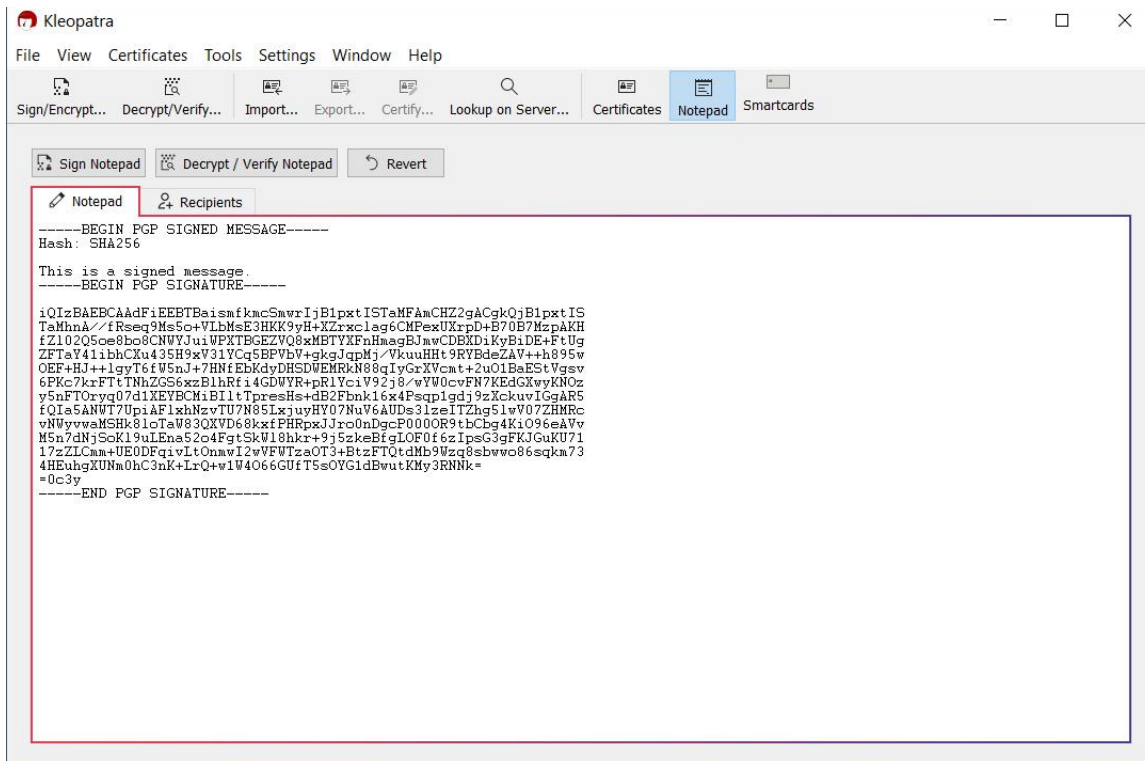


همچنین شخص مقابل، با داشتن کلید عمومی شما، می‌تونه امضای دیجیتال شما رو احراز (verify) کنه و مطمئن باشه از سمت شما اومده. اگه پیامی رو رمزنگاری می‌کنید، بهتره همیشه اون رو امضا کنید.

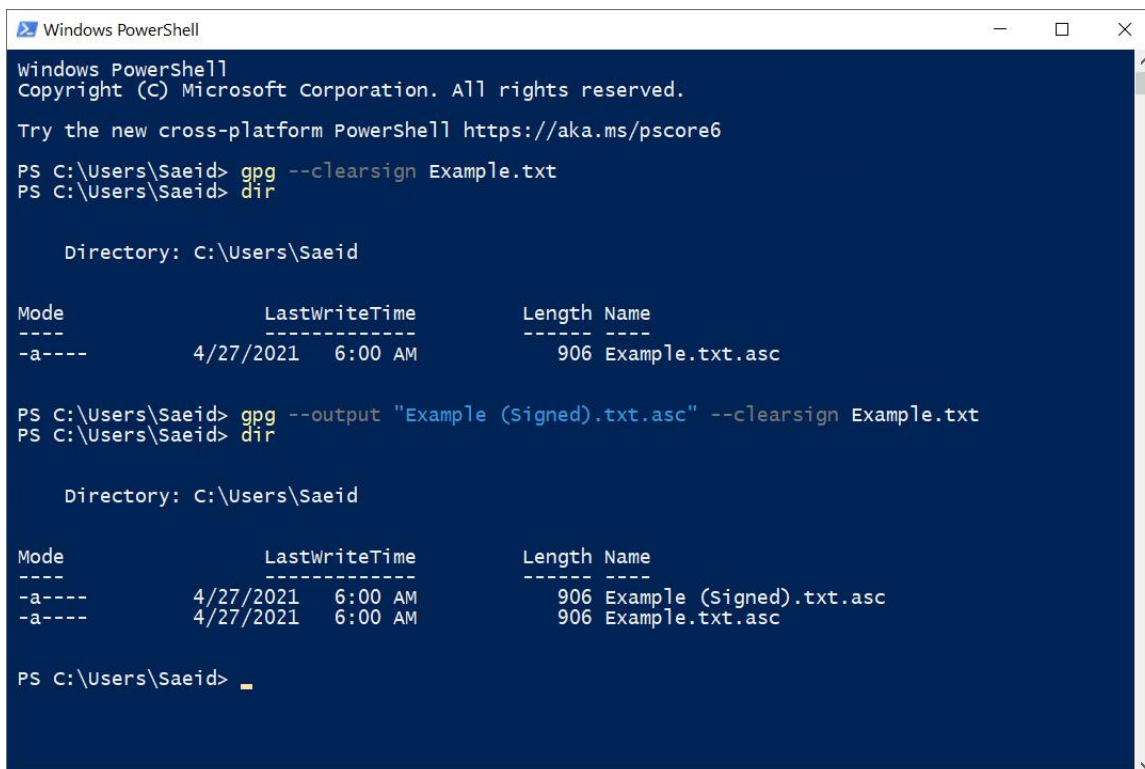
امضا می‌تونه کاربردهای متعددی داشته باشه، از جمله:

- وقتی پیام مهمی ارسال می‌کنید؛ حین یک مکالمه 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، امضا کردن نباید کار سختی باشه، چه با نرم‌افزار و چه در محیط ترمینال. به نمونه‌های صفحه بعد توجه کنید.



متن امضا شده در محیط نرم افزار



امضای فایل Example.txt با استفاده از ترمینال

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

```

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

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

PS C:\Users\Saeid> gpg --detach-sign Example.txt
PS C:\Users\Saeid> dir

    Directory: C:\Users\Saeid\New

Mode                LastWriteTime         Length Name
----                -
-a----             4/27/2021   6:00 AM           566 Example.txt.sig

PS C:\Users\Saeid> gpg --verify Example.txt.sig
gpg: assuming signed data in 'Example.txt'
gpg: Signature made 4/27/2021
gpg:                using RSA key 05305A8AC99F9267129B0AC88C1D69C6D2124DA3
gpg: Good signature from "Test <test@test.test>" [ultimate]
PS C:\Users\Saeid>
    
```

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.

 Python (3.6.1 and higher)	Electrum-4.1.2.tar.gz	signature
 Linux	Appimage	signature
 Windows (7 and higher)	Standalone Executable	signature
	Windows Installer	signature
	Portable version (security advice)	signature
 OSX (10.13 and higher)	Executable for OS X	signature
 Android (5.0 and higher) (available on Google Play)	64 bit	signature
	32 bit	signature

امضاهاى فایل‌هاى نصب كيف پول الكترام


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

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

PS C:\Users\Saeid> gpg --verify electrum-4.1.2-setup.exe.asc
gpg: assuming signed data in 'electrum-4.1.2-setup.exe'
gpg: Signature made 4/8/2021
gpg:                using RSA key 6694D8DE7BE8EE5631BE D9502BD5824B7F9470E6
gpg: Good signature from "Thomas Voegtlin (https://electrum.org) <thomasv@electrum.org>"
[unknown]
gpg:                aka "ThomasV <thomasv1@gmx.de>" [unknown]
gpg:                aka "Thomas Voegtlin <thomasv1@gmx.de>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:                There is no indication that the signature belongs to the owner.
Primary key fingerprint: 6694 D8DE 7BE8 EE56 31BE D950 2BD5 824B 7F94 70E6
PS C:\Users\Saeid>
```

احراز امضای توسعه‌دهنده 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. جمله زیر در ابتدا برام عجیب بود، اما هرچی بیشتر بهش فکر کردم، معنانش برام قابل لمس تر شد. کنجکاو باشید، درمورد چیزهایی که علاقه دارید مطالعه کنید، و لذت ببرید.



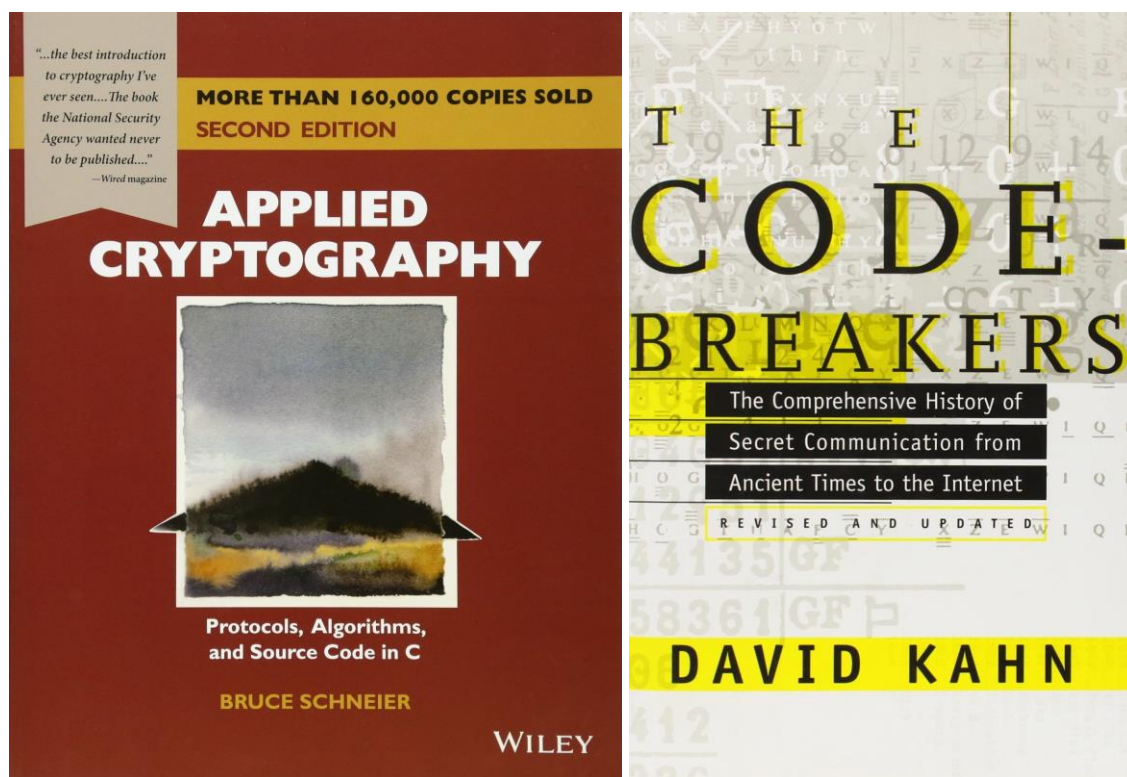
منابعی که در ادامه می‌ذارم برای اون یک نفریه که مثل من دوست داره همه چیز رو بدون و مسیر یادگیری‌اش اینجا تموم نمی‌شه. (برای مقایسه، مسیر اصلی یادگیری من تازه از اینجا شروع شده.)

از اونجایی که 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 سر می‌زنم، [راهنمای GPG آلن ایلیاسون \(Alan Eliassen\)](#) است. اگه دوست دارید آشنایی خوبی نسبت به GPG پیدا کنید، نباید از دستش بدید. الهام‌بخش نوشتن این مقاله‌ها بود. اگه کنجکاوید راجع به نحوه آشنایی من با این شخص و انگیزه نوشتن این مطالب بدونید، [این رشته‌توییت](#) رو بخونید.

جزئیات زیادی درمورد داستان زیمرمن و سایفرپانک‌ها هست که از حوصله این مطلب خارجه اما دوستانتون به شما کمک می‌کنه تصویر دقیق‌تری از اون روزها به دست بیارید. دو مقاله عالی از Wired هستن که خوندنشون ضروریه: [Crypto Rebels](#) و [Cypher Wars](#).

سایت شخصی زیرمن به تنهایی منبع بسیار خوبی برای شروع. 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 هیچ‌جا دیگه‌ای پیدا شون نکنید. صحبت‌های زیرمن در دف کان یازده شنیدنیه. حضور و صحبت‌هاش در Bitcoin Wednesday هم جالب و دیدنیه. وقتی یکی ازش می‌پرسه با توجه به سختی‌هایی که در چند دهه اخیر متحمل شده‌ای، آیا باز هم این کارها رو انجام می‌دادی، می‌گه، «آره، ولی احتمالاً از الگوریتم‌های بهتری در نسخه اصلی PGP استفاده می‌کردم!»

برای پایان، دو کتاب معرفی می‌کنم، که خودم هنوز شروع نکردم اما به شدت جذاب به نظر میان: رمزنگاری کاربردی (Applied Cryptography) از بروس اشتاینر و رمزگشایان (The Codebreakers) از دیوید کان.



این راهنما توسط **ام‌سی سعید** گردآوری شده است. برای دریافت مطالب آموزشی مرتبط با بیت کوین و حریم خصوصی می‌توانید به کانال تلگرام او به آدرس t.me/dieascm مراجعه کنید.

این راهنما تحت مجوز «مالکیت عمومی» منتشر می‌شود و بازنشر آن به هر شکل آزاد است.



bitcoind.me

منابع فارسی بیت کوین

معرفی کتاب‌ها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت‌کوین، اقتصاد، و حریم خصوصی که توسط علاقه‌مندان و فعالان جامعه فارسی‌زبان بیت‌کوین تالیف یا ترجمه شده‌اند