



رمزنگاری کلید عمومی RSA

سیستم رمزنگاری کلید عمومی RSA (آراس‌ای) یکی از قدیمی‌ترین و جذاب‌ترین‌هاست، و در این مطلب می‌خوایم 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.

به طورکلی، دو نوع رمزنگاری داریم: [متقارن \(asymmetric\)](#) و [نامتقارن \(symmetric\)](#). در رمزنگاری متقارن، از یه کلید هم برای رمزنگاری و هم برای رمزگشایی استفاده می‌شه، به این معنا که فرستنده و گیرنده هر دو به یه کلید مشترک دسترسی دارن، و این، در بعضی موارد استفاده، می‌تونه ضعف محسوب بشه.

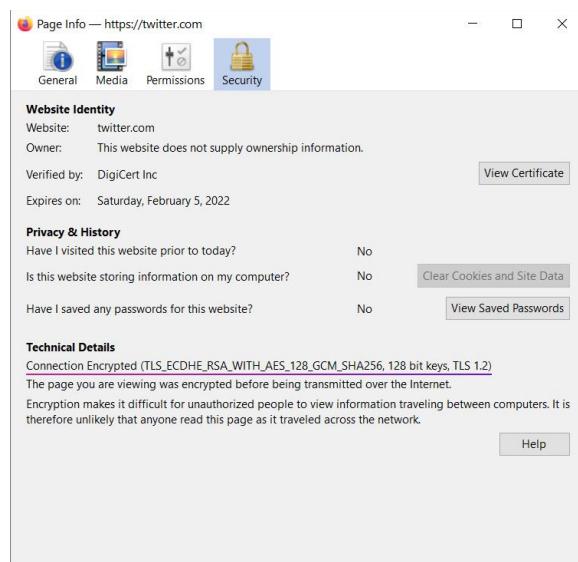


رمزنگاری نامتقارن فرآیند پیچیده‌تری داره: دو کلید دارید، یکی عمومی و دیگری خصوصی.

رمزنگاری کلید عمومی

در این روش، شما با استفاده از کلید عمومی خودتون چیزی رو رمزنگاری می‌کنید، و اون پیام یا داده تنها با کلید خصوصی مرتبط قابل رمزگشاییه. درحالی‌که 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 می‌ده، از این جهت که رسیدن به رابطه بین دو کلید و پیدا کردن کلید خصوصی دشواره—به لطف [تابع یه طفه‌ای](#) که جلوتر بهش می‌پردازیم. از طرفی، رمزنگاری نامتقارن روش کندتری در مقایسه با رمزنگاری متقارن به حساب می‌آد.



یکی از رایج‌ترین الگوریتم‌های رمزنگاری متقارن [AES](#) (استاندارد رمزنگاری پیشرفته) است. همین‌الآن مرورگر شما برای اتصال امن به تؤییر از این نوع رمزنگاری استفاده می‌کنه.



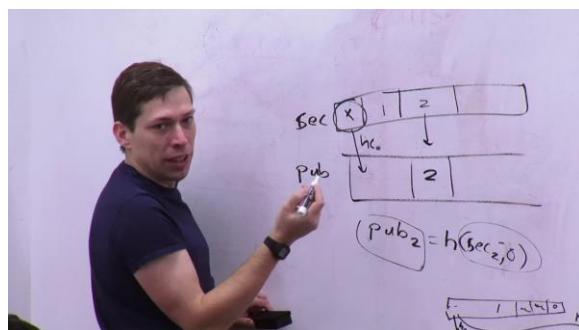
«۱۲۸ بیتی یا ۲۵۶ بیتی؟» تفاوت امنیت کلیدها در یوتیوب

معرفی AES در یوتیوب

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

طول کلیدها در رمزنگاری کلید عمومی بسیار بلندتره (۲۰۴۸ بیت به بالا)، اما روش سنجش امنیتش از رمزنگاری متقارن متفاوت‌هه. برای مثال، یه کلید عمومی ۳۰۷۲ بیتی از نظر امنیت کم‌ویش با یه کلید ۱۲۸ بیت AES برابره. در مرور دش بخونید. (کلیدواژه‌ها: طول کلید ([key size](#))، سطح امنیت ([security level](#)))

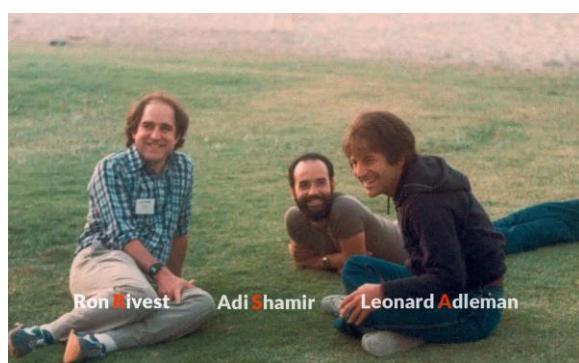
دو نمونه از سیستم‌های نامتقارن RSA و ECC (رمزنگاری منحنی بیضوی) هستن. اولی موضوع صحبت ماست، و دومی سیستمیه که در [بیت‌کوین](#) به کار رفته و کلیدهای عمومی و خصوصی شما بر پایه‌ش ساخته می‌شن.



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 راه حل عملی‌ای برای ارائه ندادند.

ریوست، شامیر، و آدلمن هر سه در ام آی تی تدریس می‌کردند، و ارتباط نزدیکی با هم داشتند. روزی یکی از شاگردان 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 داشتند، تصمیم می‌گیرند روی این مسئله کار کنند.

این دو ماه‌ها تلاش می‌کنند تابع یه طرفه‌ای رو پیدا کنند که محاسبه‌ش از یه سمت سریع اما از سمت دیگه بسیار سخت باشد، و در عین حال ضعف امنیتی‌ای نداشته باشد که برگشت‌پذیری‌اش رو ساده کنند. آدلمن، که ریاضی دان بود، مسئولیت این رو داشت که توابع پیشنهادی رو بشکند و نقاط ضعف‌شون رو پیدا کنند.

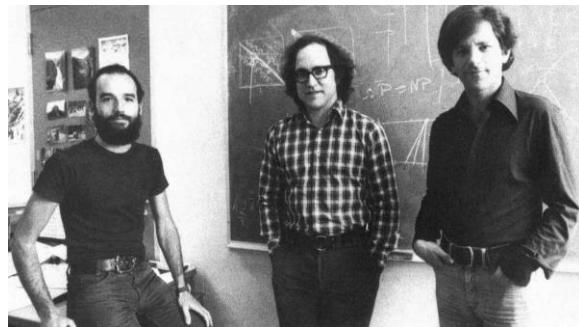


مرور تاریخچه RSA با لئونارد آدلمن در [یوتیوب](#)

شبی در آوریل ۱۹۷۷، این سه توسط یکی از دانشجوها به مهمونی پسح (عیدی یهودی) دعوت می‌شون. بعد از برگشتن به خونه‌هایشون، ریوست، که خواشش نمی‌برد، شروع می‌کند به کار روی مسئله و بالاخره تابع یه طرفه رو پیدا می‌کند. به آدلمن زنگ می‌زنند، مطرحش می‌کنند، و آدلمن همونجا بهش تبریک می‌گیرد. ریوست تمام شب رو بیدار می‌ماند و تا صبح مقاله‌ش رو می‌نویسد.

دانستان انتخاب اسم RSA هم یکی از اون چیزهاییه که شانسی اما فوق العاده اتفاق می‌افتد. ریوست ابتدا قصد داشت نویسنده‌های مقاله رو به ترتیب معمول «آدلمن، ریوست، شامیر» بنویسند، اما آدلمن، که حس می‌کرد بیشتر کار رو اونها انجام دادن، موافق نبود اسمش لحاظ بشد. درنهایت، بعد از کلی صحبت و فکر، قبول می‌کند اما می‌گه اسم من رو آخر بذارید، و این طوری RSA خلق می‌شود.

ریوست، شامیر، و آدلمن سال ۲۰۰۲ جایزه تورینگ (بالاترین جایزه در حوزه کامپیوتر و به نوعی نوبل علوم کامپیوتر) را 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 انپی بخونید). اگه علاقه مندید با ریوست و کارهاش آشنا بشید، «تاریخ شفاهی رونالد ریوست» رو ببینید. به طبع، مصاحبه کامل آدلمن با ACM (انجمن اعطائکننده جایزه تورینگ) رو هم پیشنهاد می کنم.

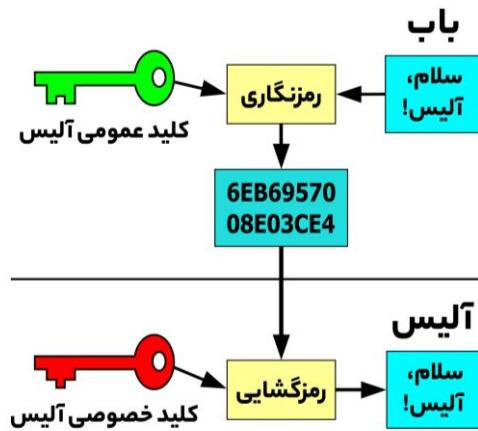
عملکرد RSA

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.

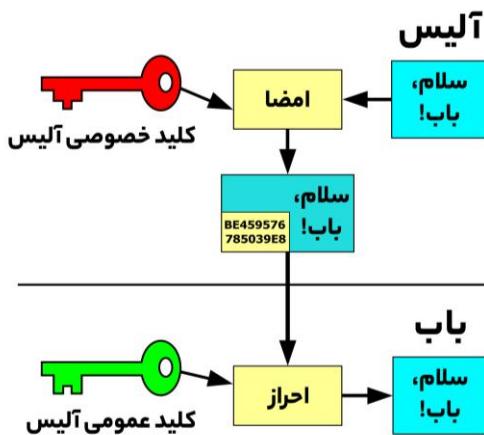
افراد می تونن از کلید عمومی شما برای ارسال پیامی محترمانه استفاده کنن، و اون شخص و شما می تونید مطمئن باشید کسی جز شما (دارنده کلید خصوصی مرتبط با اون کلید عمومی) قادر به خوندن پیام نیست.

رمزگاری و رمزگشایی



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

اصالت‌سنجی/احراز هویت



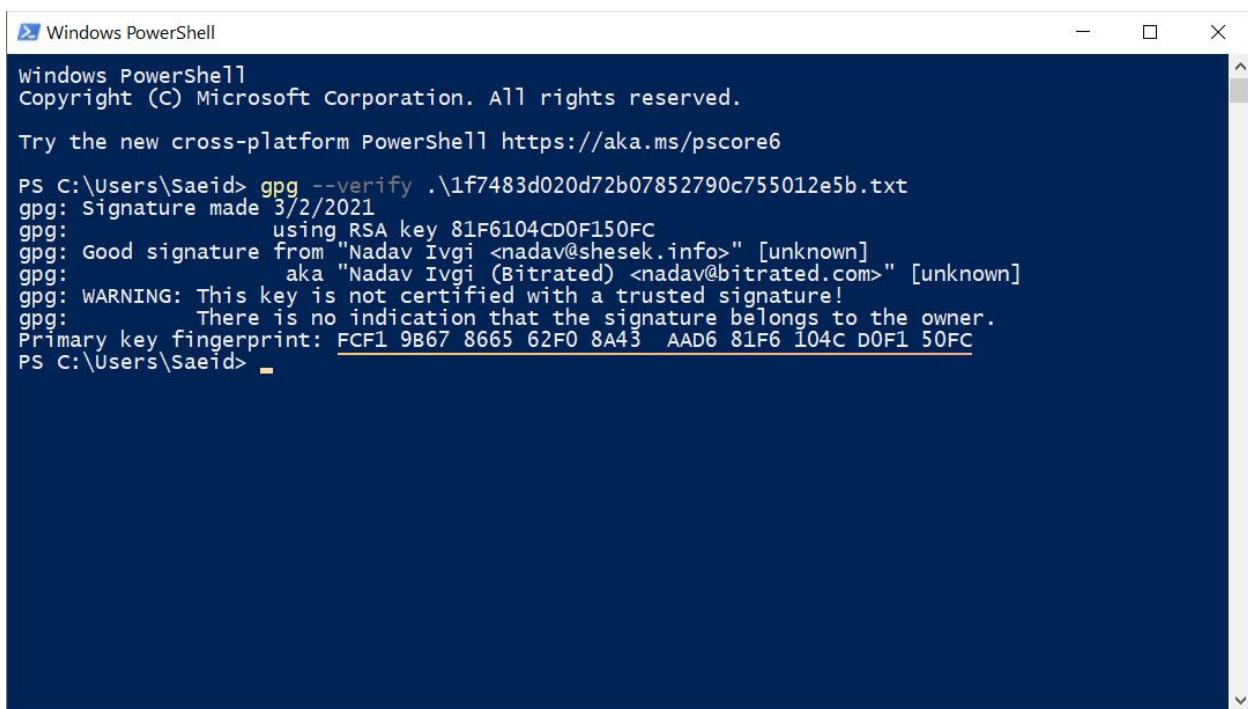
رمزگاری کلید عمومی همچنین امکان اصالت‌سنجی/احراز هویت (authentication) را به ما می‌دهد، و این در بعضی شرایط می‌توانه حیاتی باشه، مثل زمانی که می‌خوايد هویت شخصی ناشناس را احراز کنید.

شخص پیامی رو با کلید خصوصی اش «امضا» می‌کنه، و شما با داشتن کلید عمومی اش قادر به احرازش هستید. در اینجا کمی وارد موضوع PGP می‌شیم—که جلوتر مفصل درموردش صحبت خواهیم کرد—اما قبل از اینکه من و [ناداو ایوگی](#)، از توسعه‌دهنده‌های قدیمی حوزه بیت‌کوین، [شروع به همکاری کنیم](#)، نیاز بود هويت 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.

```
gitfile1.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 D0Ty2cq7wV27SBgQP0o5pREYHVzvV0ka/9260pJXMCTbfyVpvA3zoNc1fRcdWBA
11 xu89fDa+y/SOEMQ5IH1/poI2REEwEQcBjBU/1WLAstyGsrkZ2uR3o/dwjTOb9VdfG
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 واردکردن کلید عمومی اش و (import) صحبت‌سنگی این پیام موفق به احراز هویتش برای خودم شدم.

بهتر می‌بود اگه زمان رو هم لحظه می‌کرد، 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> -
```

اثرانگشت کلید عمومی ناداو ایوگی

اصالت سنجی فایل‌ها، بهویژه در دنیای نرم‌افزار آزاد، بسیار مهمه. شما می‌خوايد 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 امضا دیجیتال ممکنه.

نکته: کلیدهای عمومی به طور معمول بسیار بلندن، و این، کار رو برای انتقال و وارد کردن شون سخت می‌کنه. از این‌رو، از اثرانگشت کلید عمومی استفاده می‌کنیم. ما می‌توانیم 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.

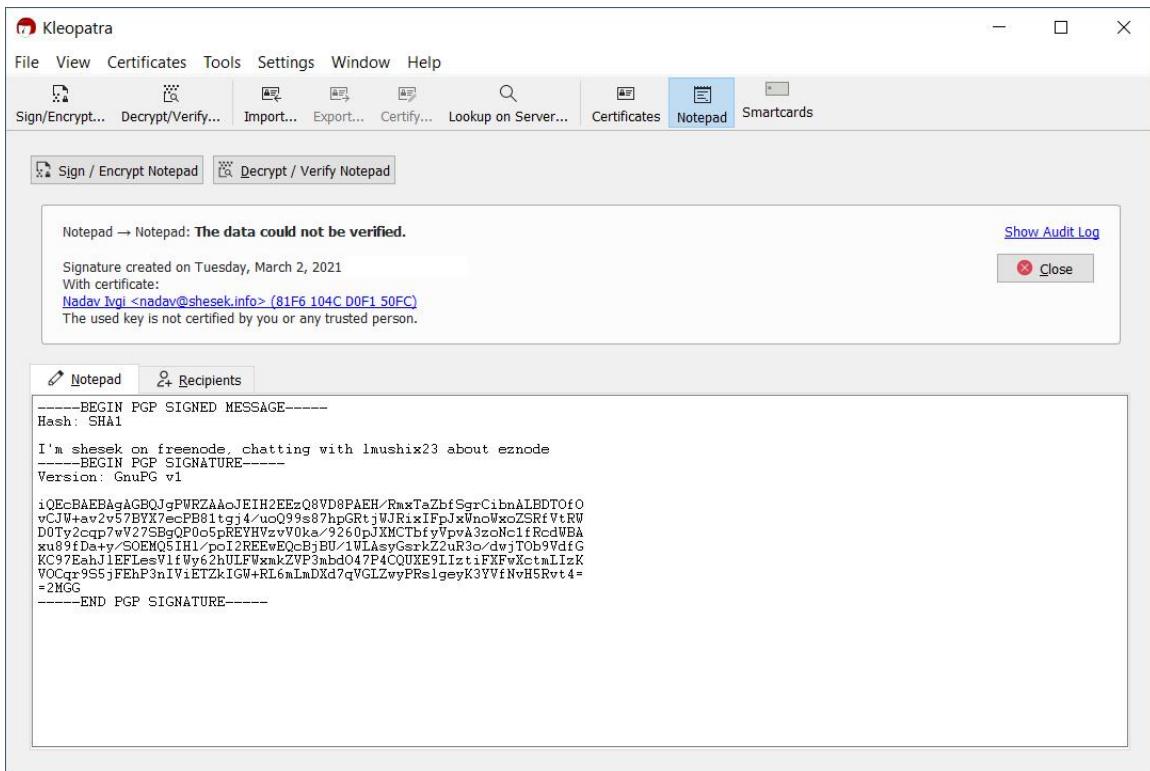
ممکنه اثرانگشت PGP بعضی رو در وبسایت یا پروفایل توئیترشون باشد. شما با داشتن این اثرانگشت می‌توانید به کلید عمومی شون برسید.

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) به ترتیب شونزده و هشت رقم آخر اثرانگشت‌شن. با داشتن هرکدام از این‌ها می‌توانید کلید عمومی من رو پیدا و وارد کنید.

تولید کلید عمومی و خصوصی

یکی از رایج‌ترین نرم‌افزارها GPG یا GNU Privacy Guard است. اگه کاربر ویندوز هستید، از Gpg4win استفاده کنید. لینک‌های دانلود بر حسب سیستم عامل در سایت رسمی [GnuPG](#) قرار داده شدن.



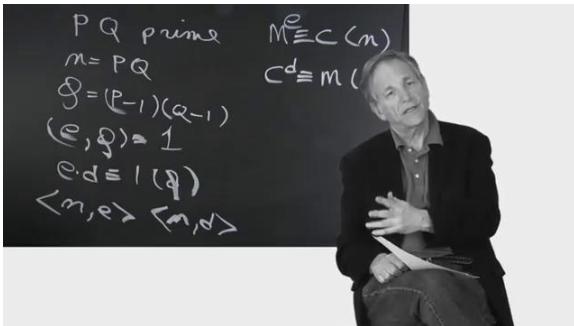
نرم‌افزار کلئوپاترا

سخن پایانی

ریاضی پشت کلید عمومی RSA بسیار جذابه اگه علاقه‌مند و کنجکاو به دونستنش هستید. توضیحش در قالب این مطلب کمی سخته، اما [ویدئویی](#) رو پیشنهاد می‌کنم که قدم به قدم توضیح می‌ده، و حتی اگه فکر می‌کنید در ریاضی قوی نیستید، می‌تونید نحوه کارش رو درک کنید.



دانستان ریوست-شامیر-آدلمن در یوتیوب



شرح RSA از زبان سازندگان اوون 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 تلاش‌هاشون، ما امروز فضای اینترنت و ارتباطات امن‌تری داریم. شما این طور فکر نمی‌کنید؟

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



تاریخچه و راهنمای PGP: مقدمه

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

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

644 1976 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 card 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

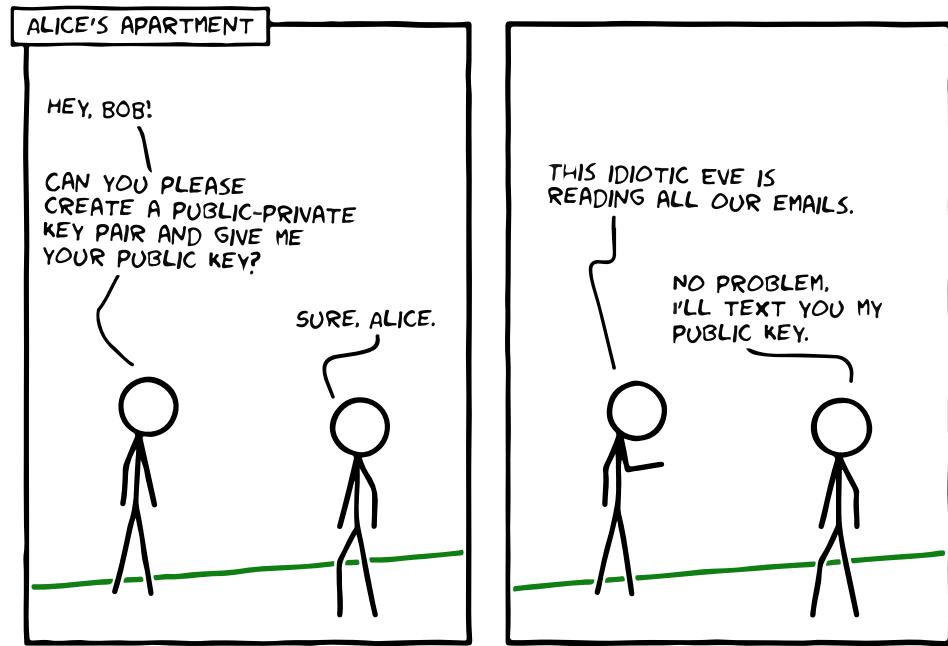
از راست به چپ، ویتفیلد دیفی، مارتین هلمن، و رالف مرکل

وقتی راجع به رمزنگاری مدرن صحبت می‌کنیم، باید به دهه ۱۹۷۰ برگردیم، زمانی که ویتفیلد دیفی، مارتین هلمن، و رالف مرکل پایه رمزنگاری کلید عمومی را بنا نهادند.

مرکل را، که الهام‌بخش دیفی و هلمن در رسیدن به ایده رمزنگاری نامتقارن بود، ممکن است با طرح درخت مرکل (Merkle tree) بشناسیم.

ظہور 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.



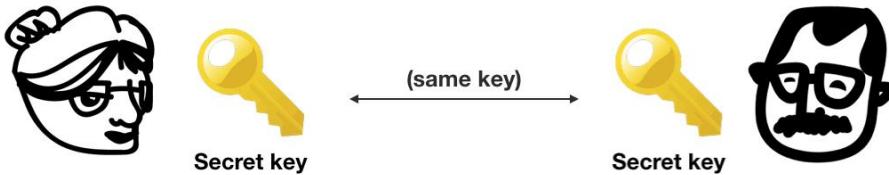
هرچیزی که با یکی از کلیدها رمز بشه، با کلید دوم گشوده می‌شه.

در اینجا، از دو اصطلاح متن آشکار (plaintext) و متن رمزنگاری شده (ciphertext) استفاده می‌کنیم. اگه من بخواهم 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 رمزگاری متقارن، از یک کلید هم برای رمزگاری 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، می‌تواند ضعف محسوب بشود.

تا قبل از این، افراد از رمزگاری متقارن استفاده می‌کردند. در این سیستم، دو طرف به یک کلید خصوصی مشترک دسترسی دارند، و ارسال کلید به رو شی امن کار رو دشوار می‌کند.

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 رمزگاری](#) (Crypto Wars) معروف شد. جنگ جهانی دوم نشون داد رمزگاری چقدر می‌تواند در استفاده‌های نظامی مهم باشد، و همین باعث شد این تکنولوژی در دسته تسلیحات نظامی (munition) قرار بگیره.

باورش امروز ممکنه سخت باشد، اما تا ۱۹۹۲، رمزگاری به عنوان تجهیزات نظامی کمکی (Auxiliary Military Equipment) در لیست تسلیحات ایالات متحده شناخته می‌شد، و صادر کردن هر نوع رمزگاری‌ای—از روش‌ها گرفته تا حتی شرح اون‌ها—به شدت سخت گیرانه و نیازمند مجوز بود.



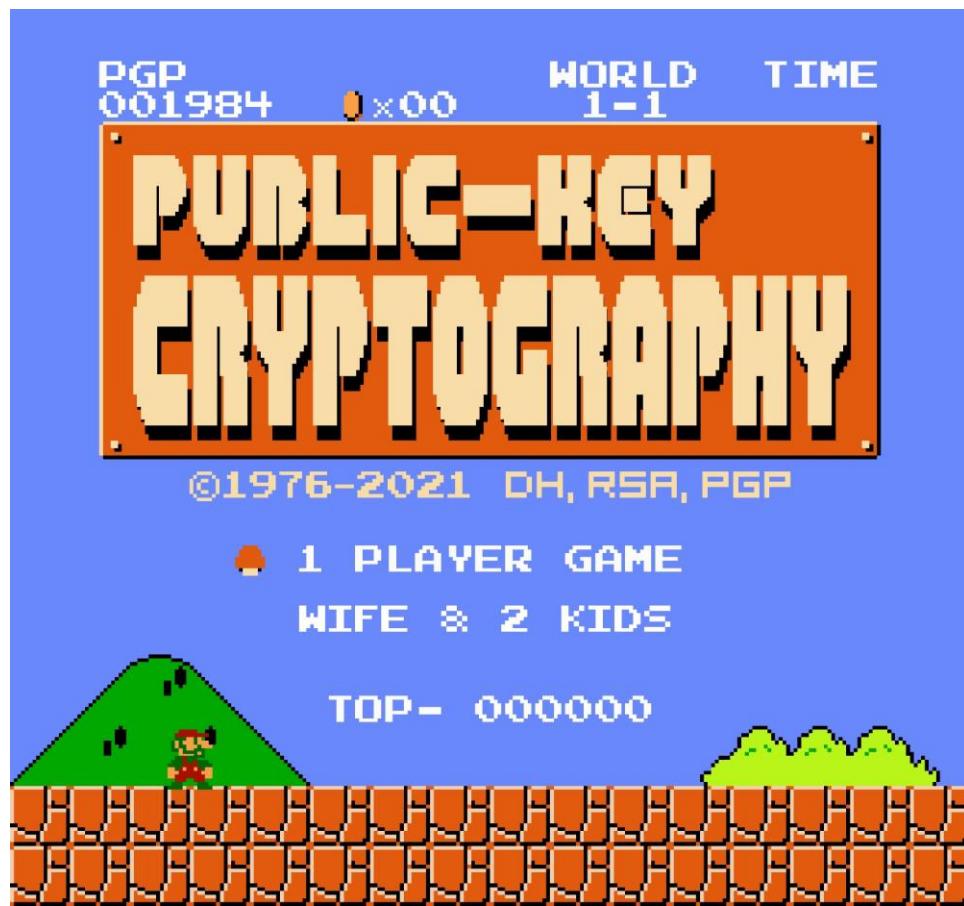
فیلیپ زیمرمن، خالق PGP

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 رسیک محاکمه شدن)، راه برای برچیده شدن 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 می‌توانستن مکالمه‌های روزمره و حتی فایل‌هашون 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 بی می‌برد. زیمرمن بعدها در شرح نرم‌افزارش حرف‌های قابل تأملی می‌نویسه، بهویژه در انتهای پاراگراف اول.



تشبيه فليپ زيمermen به سوبر ماريو (تصويرسازی: [MC Saeid](#))

زيمermen، که تخصص ویژه‌ای در رمزنگاری نداشت، کند پیش می‌رفت. درحالی که شغل اصلی خودش رو داشت، دارای همسر و دو فرزند هم بود، و همین موضوع باعث می‌شد تا تنونه با اون سرعتی که می‌خواهد پروژه رو پیش ببره. باين حال، ازش دست نکشید. در ۱۹۸۶ موفق شد RSA رو پياده‌سازی کنه.

۱۹۹۱ رسيد، و زيمermen همچنان نرم‌افزار کاملی برای عرضه نداشت، تا اينکه بایدن (که در اون زمان سناتور بود) قدمی برداشت که باعث شد زيمermen چندين ماه بي وقهه روی پروژه کار کنه تا اون رو به پيان برسونه.

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

در ژانویه ۱۹۹۱، بایدن لایحه ۲۶۶ رو پیشنهاد داد. جايی در اين متن او مده که شركت‌ها موظفن در صورت ارائه درخواست قانوني، محتواي متنى، صوتى، و داده افراد رو دراختيار دولت قرار بدن. اين همون آينده [اورولى](#) اي بود که زيمermen تلاش می‌کرد ازش جلوگيری 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 شباهنگ روز 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 پر پیچ و خم که چندین سال از عمرش رو صرفش کرده بود، بالاخره نرمافزارش رو عمومی کرد و نام اون رو PGP گذاشت—کوتاه شده Pretty Good Privacy یا «حریم خصوصی بسیار خوب».

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

زیمرمن حتی تا مرز ازدستدادن خونه 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.

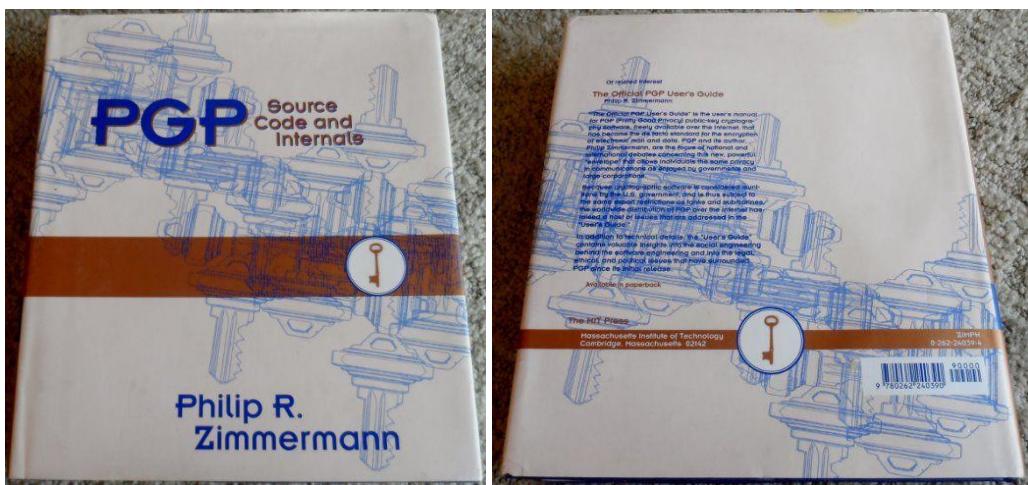
این، از دید من، نشون از فدایکاری بزرگش داره.

دردرس‌های حقوقی

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

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

در حالی که استفاده از PGP در ایالات متحده آزاد بود، وقتی در کشورهای دیگر پدیدار شد (و PGP در زمان کوتاهی به محبوبیت بسیار بالایی بین کاربرها رسید)، دردرس‌های قانونی‌ای برای زیمرمن دربی 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؟ 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 را در قالب کتاب منتشر کرد. براساس متمم اول (First Amendment) قانون اساسی ایالات متحده و زیرمجموعه قانون آزادی بیان، نشر و صادرات کتاب هیچ گونه 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](#).

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 می‌دهد.

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 dc.

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](#)

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

راهاندازی و استفاده از PGP

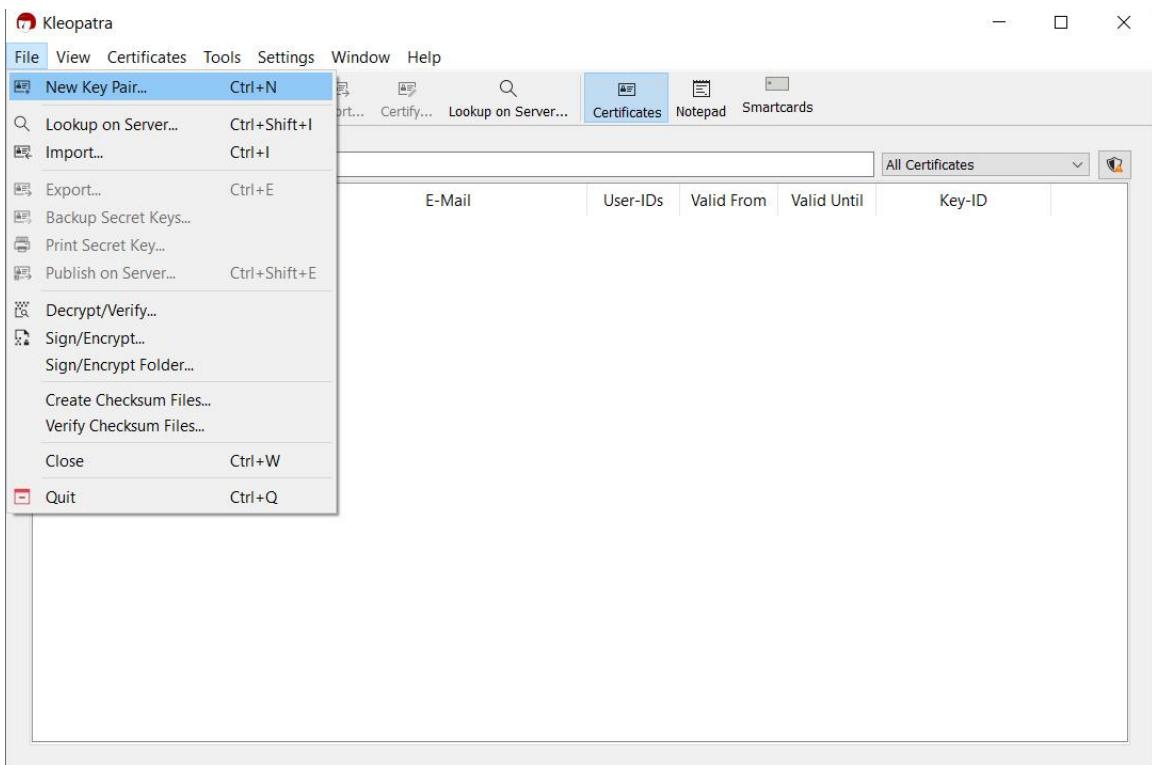
حالا که با تاریخچه PGP آشنا شدیم، می‌توانیم کمی درمورد کاربرد و عملکردش صحبت کنیم. اولین قدم اینه که نرم‌افزارش رو دانلود و نصب کنیم و کلید خودمون رو بسازیم.

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

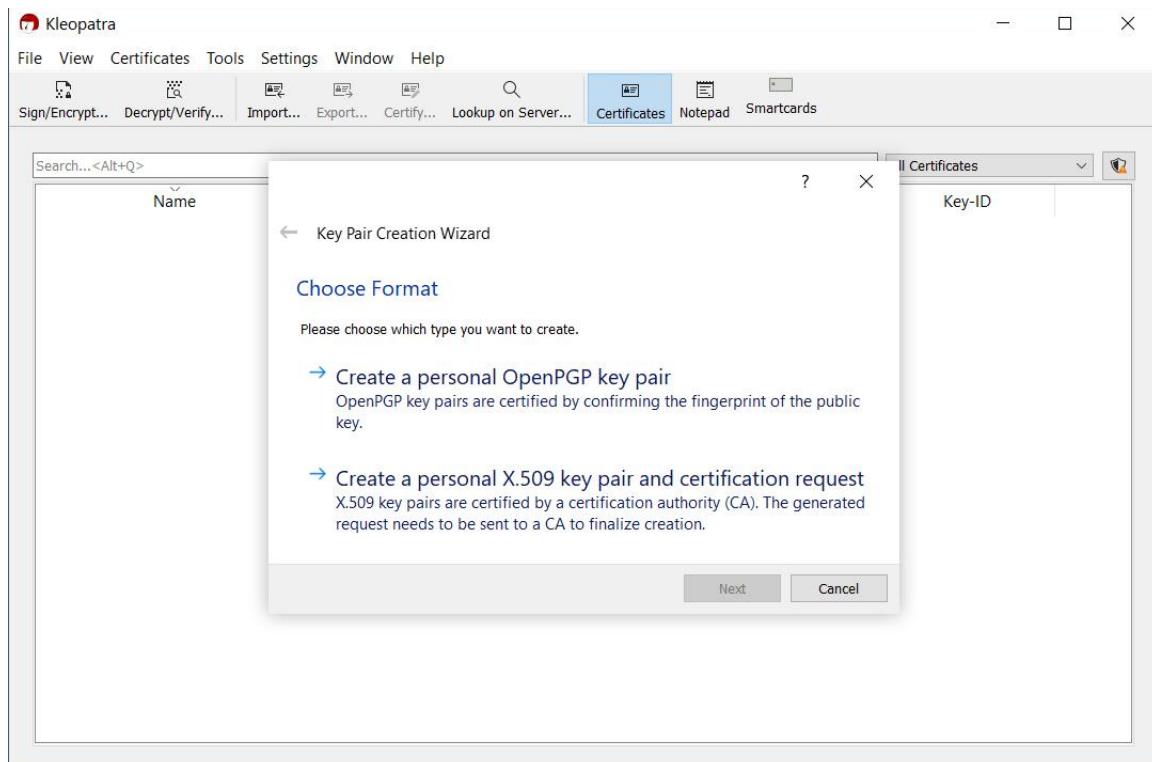
ساخت کلید

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

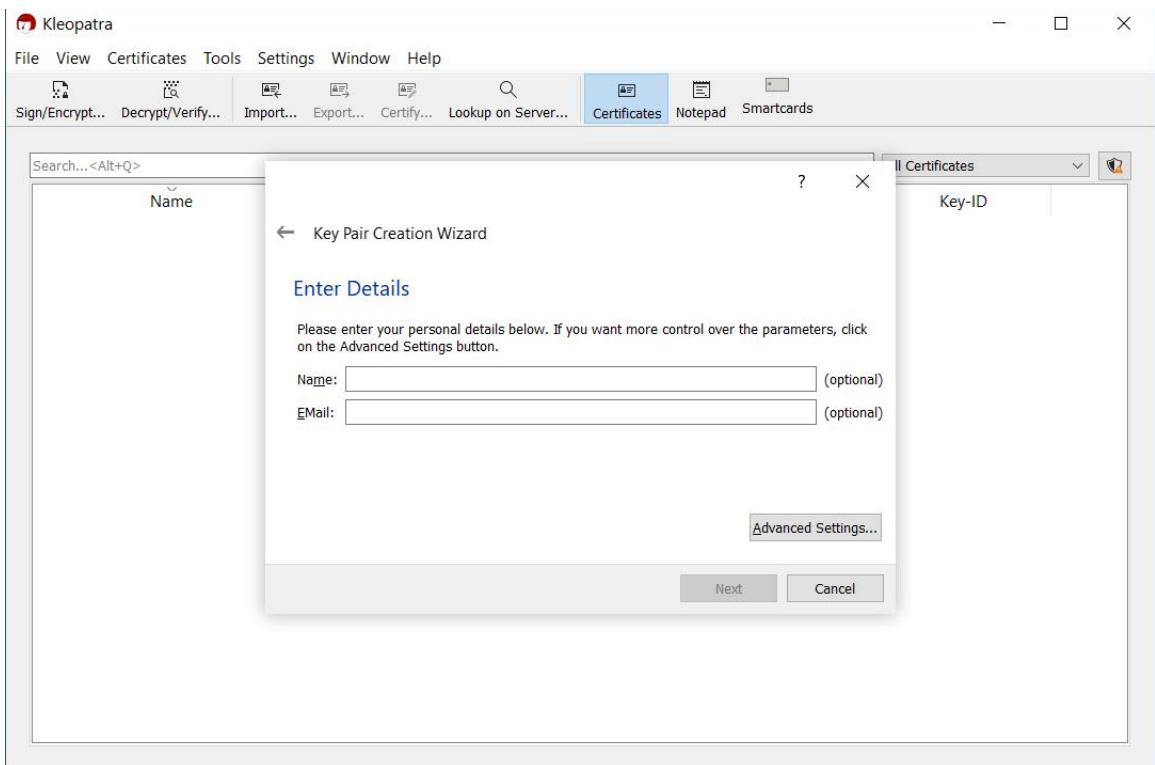
از نرم‌افزار Kleopatra برای تولید کلید شخصی، مدیریت کلیدها، رمزنگاری، و رمزگشایی استفاده می‌کنیم. به تصاویر صفحات بعد توجه کنید.



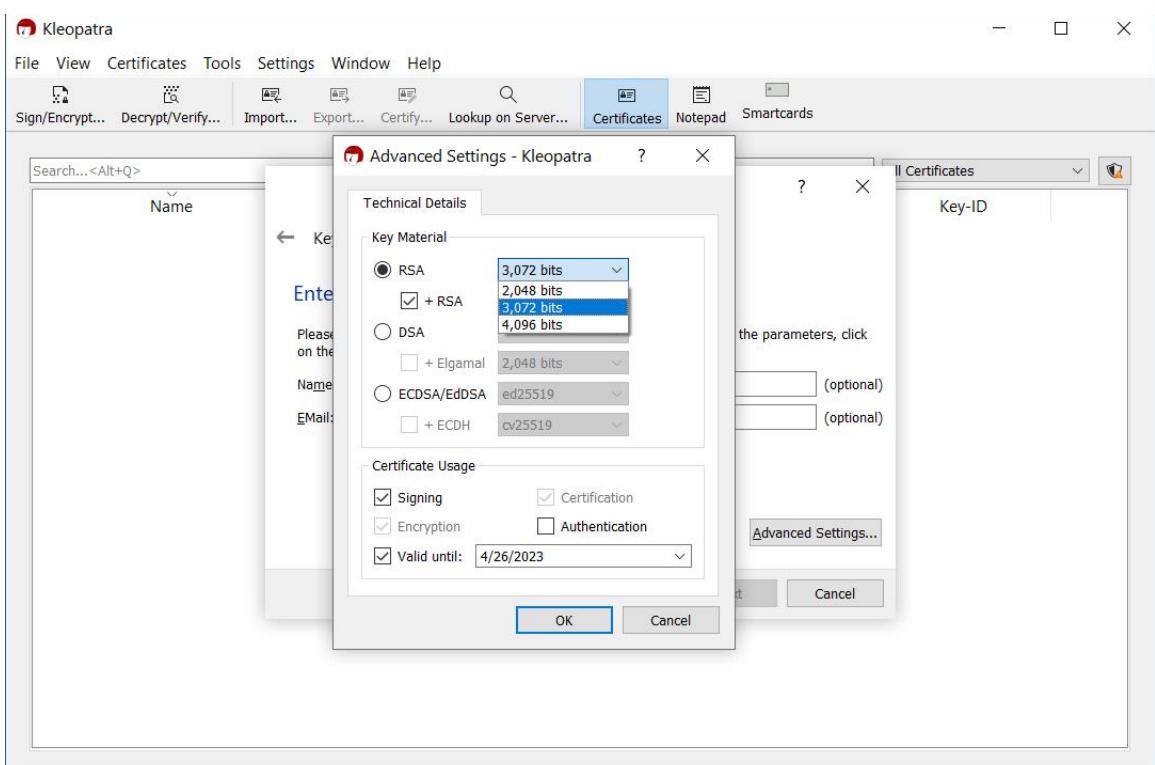
قدم اول در ساخت کلید: File → New Key Pair (یا استفاده از میانبر Ctrl + N)



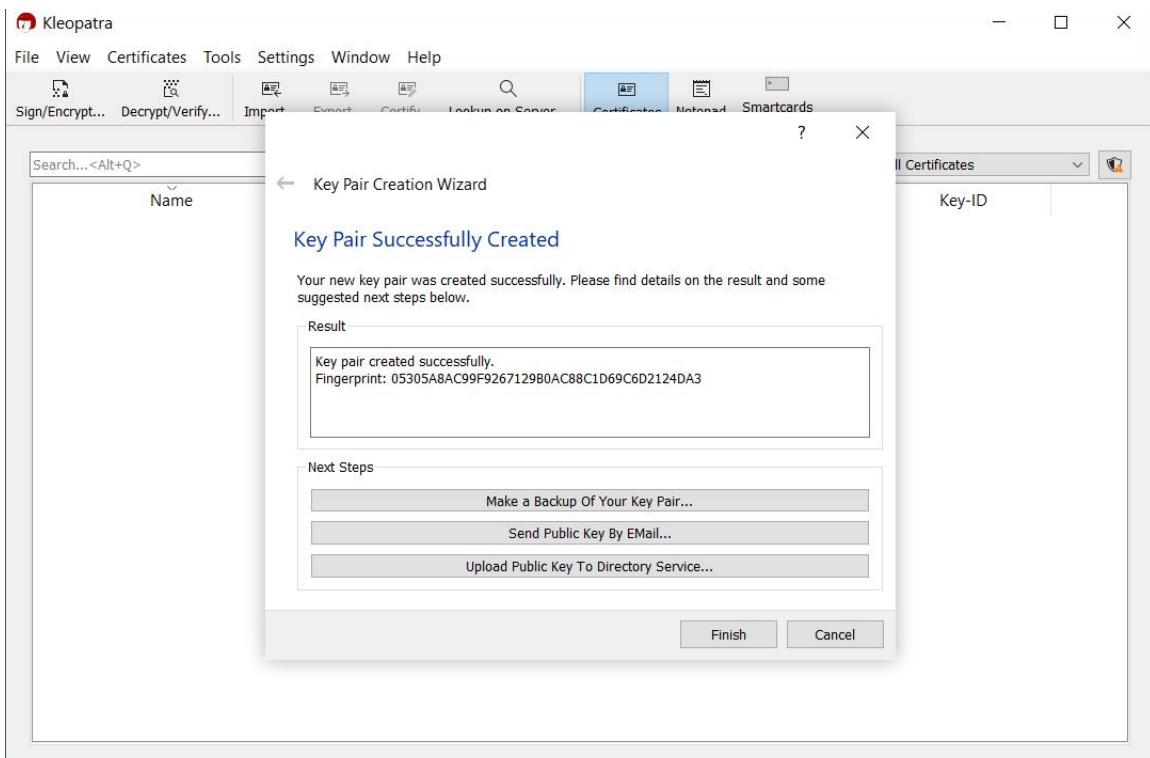
قدم دوم: انتخاب گزینه Create a personal OpenPGP key pair



قدم سوم: وارد کردن اطلاعات (اختیاری)



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



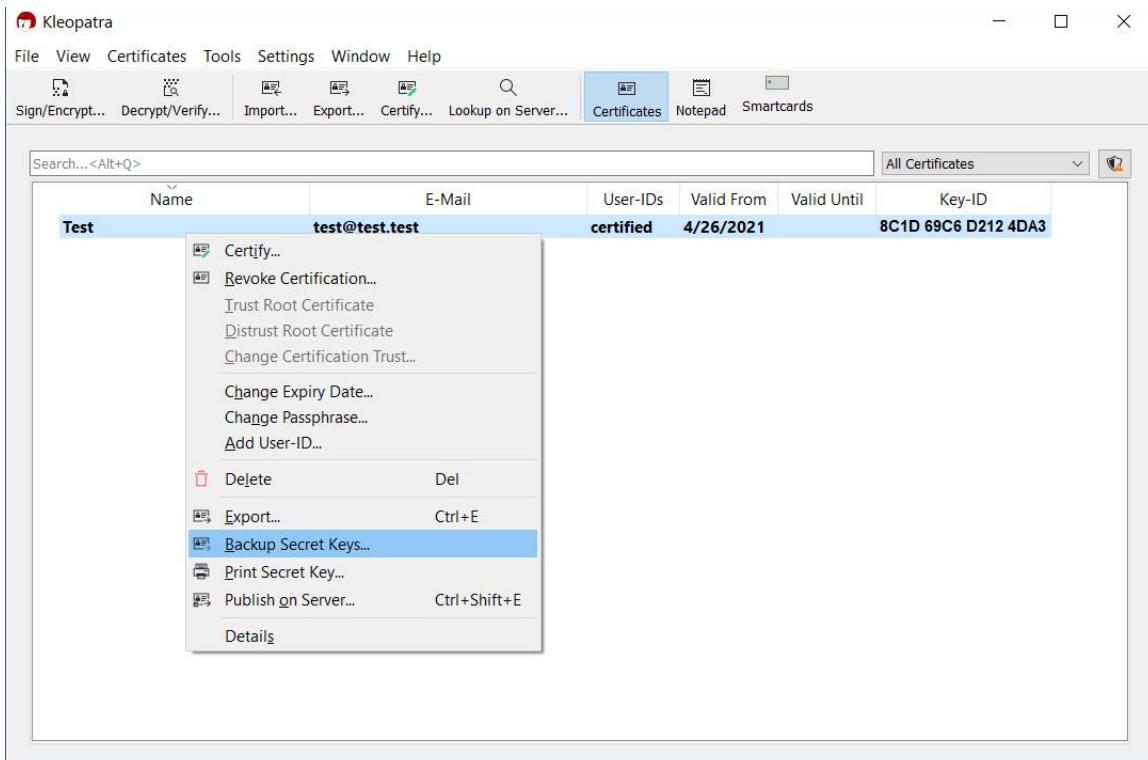
کلید شما با موفقیت ساخته شد.

اگه درمورد اجزای مختلف این پنجره کنجهکاوید، سایت GnuPG یکی از جامعترین و جذابترین سوالهای پر تکرار رو داره، که می تونید [اینجا](#) بخونید. درمورد امنیت و طول کلیدها کنجهکاوید؟ [این مقاله](#) رو در توئیتر دنبال کنید.

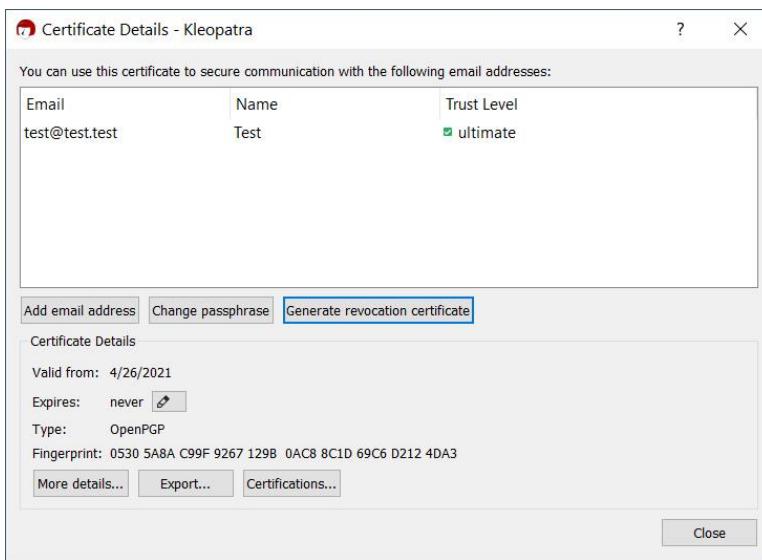
کلید خصوصی: تهیه نسخه پشتیبان و گواهی ابطال

به تصویر بالا و گزینه های نمایش داده شده در چهارچوب Next Steps توجه کنید. از کلید خصوصی تون بک آپ تهیه کرده و اوون رو در جایی امن نگه دارید. کل این فرآیند در امن نگهداشتن و محافظت از کلید خصوصی شما خلاصه می شه.

انجام این کار به روش های دیگه‌ای هم امکان پذیره، مثل تصویر زیر.



تهیه نسخه پشتیبان از کلید خصوصی (بسیار مهم)

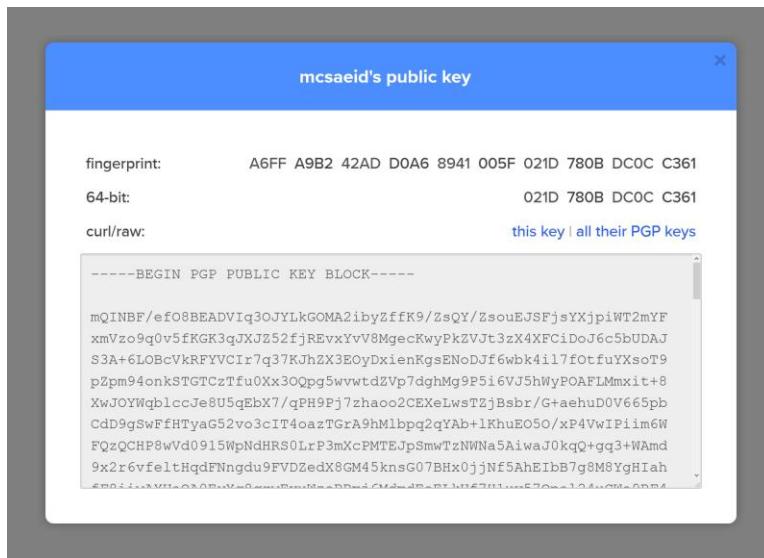


تولید گواهی ابطال

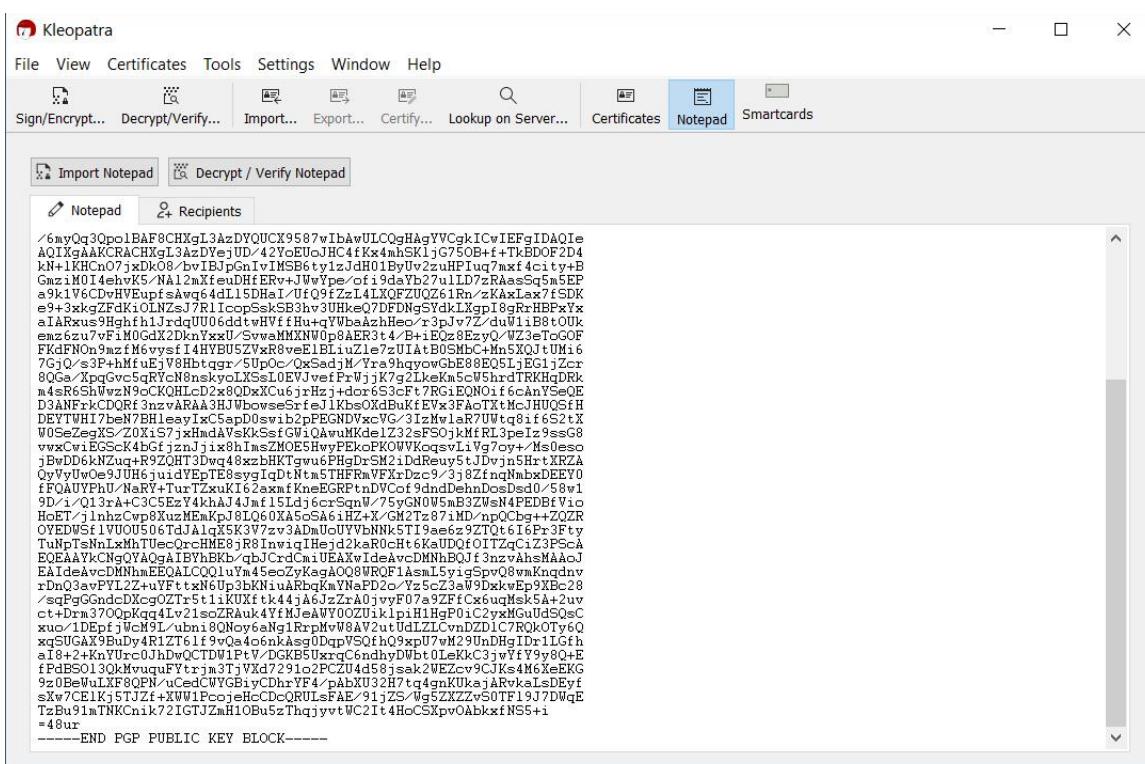
یکی از اولین کارهایی که انجام می‌دید باید تولید گواهی ابطال (revocation) باشد. اگه زمانی کلیدتون گم بشه یا لو بره، با استفاده از این گواهی و انتشارش می‌تونید کلید رو باطل کنید. در ساخت کلید و ابطالش دقت کافی رو به خرج بدید. داشتن چند کلید باطل شده نشوئه چندان جالبی نیست.

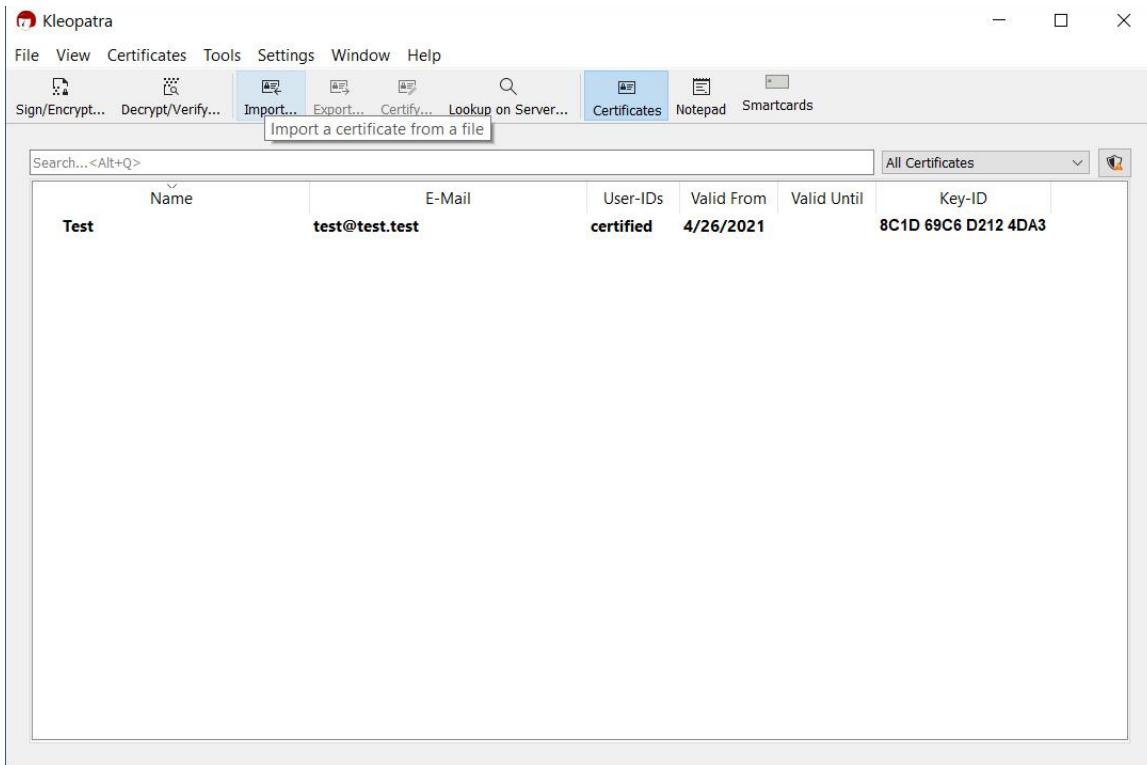
وارد کردن کلید عمومی دیگران

برای اینکه بتونید 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

اگه 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 pgp_keys.asc
gpg: key 021d780B0C0C361: "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 021d780B0C0C361, created: 2020-12-19, expires: 2030-12-20
Keys 1-1 of 1 for "mcsaeid@protonmail.com". Enter number(s), N(ext), or Q(uite) > 1
gpg: key 021d780B0C0C361: "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 021d780B0C0C361
gpg: key 021d780B0C0C361: "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 F97c47977F2EB716, created: 2018-06-27, expires: 2034-06-23
(2) Ziya Sadr <ziyamirisadr@gmail.com>
        2048 bit RSA key E28fc1f3DCBEFCC, created: 2018-03-13
Keys 1-2 of 2 for "ziya_sadr". Enter number(s), N(ext), or Q(uite) > 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_
```

gpg --import [نام فایل]

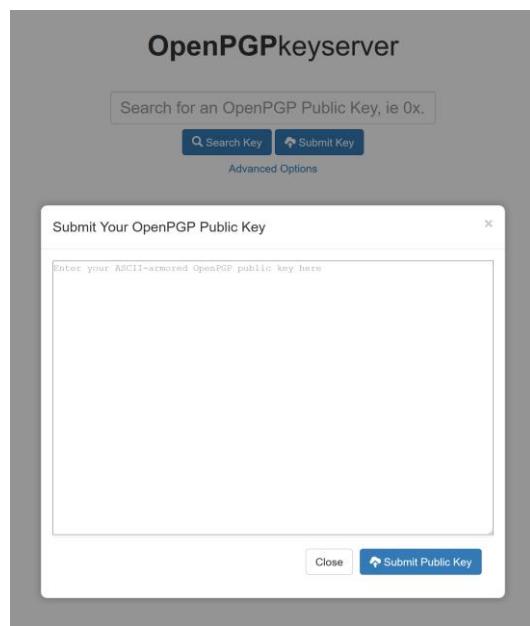
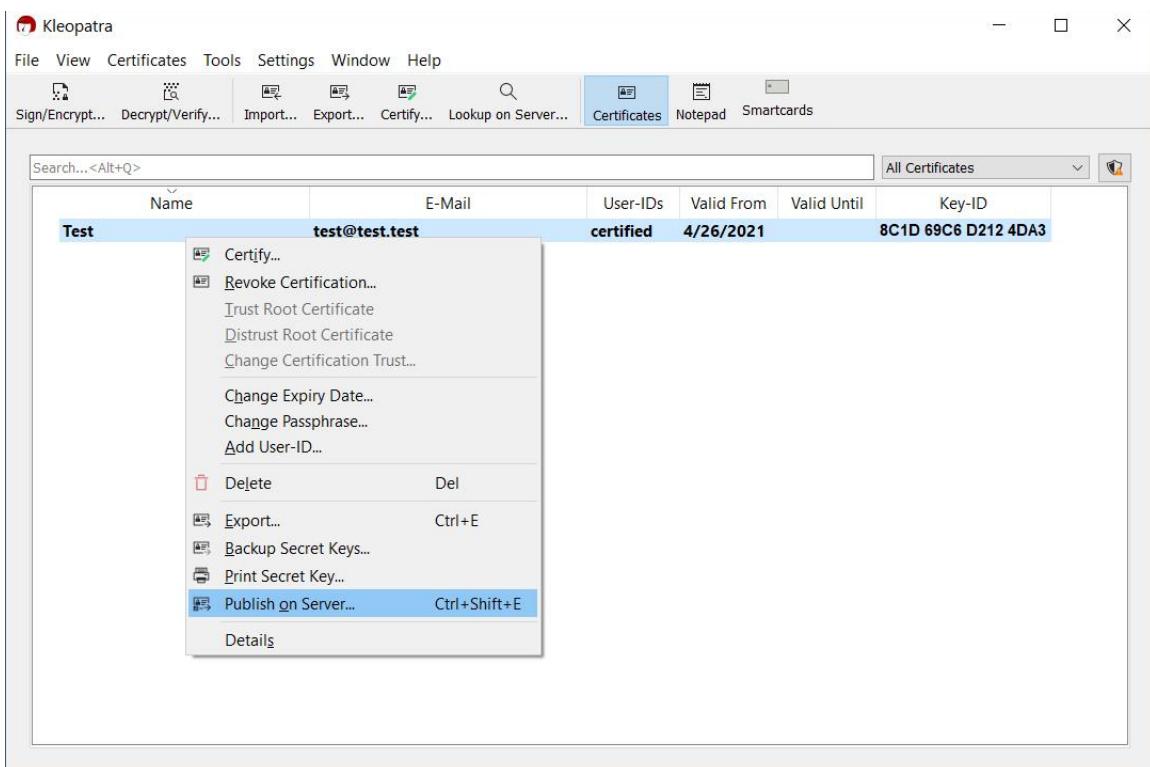
برای وارد کردن از فایل

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

جستجو در سرورهای کلید

gpg --keyserver keys.gnupg.net --recv-keys [اثرانگشت]

جستجو با اثranگشت



انتشار کلید عمومی در سرور کلید از طریق نرم افزار یا به صورت دستی

شما می تونید کلید عمومی من رو با جستجو در سرورهای کلید مختلف پیدا کنید، اما این کار خودکار صورت نمی گیره. من از قبل کلید عمومی خودم رو در یکی از این منابع منتشر کردهم، و از اونجا بیکار همیگه رو mirror می کنم، کلید عمومی من در جاهای دیگه هم قابل یافته.

اثرانگشت کلید عمومی

خب، حالا که کلید عمومی هم رو داریم، می‌توانیم به صورت امن مکالمه کنیم؟ نه، اصلاً. از کجا مطمئنیم این کلید به من تعلق دارد؟ شما ابتدا باید هویت من رو احراز کنید.

این خیلی مهمه. هر کسی می‌توانه با هر آدرس ایمیلی کلید بسازه. هر کسی می‌توانه اون کلید رو در هر سرووری منتشر کنه. تنها در صورتی که هویت شخص رو احراز و اطمینان حاصل کنید کلید واقعاً به او تعلق داره، امنیت خواهد داشت.

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



مشاهده در [یوتیوب](#)

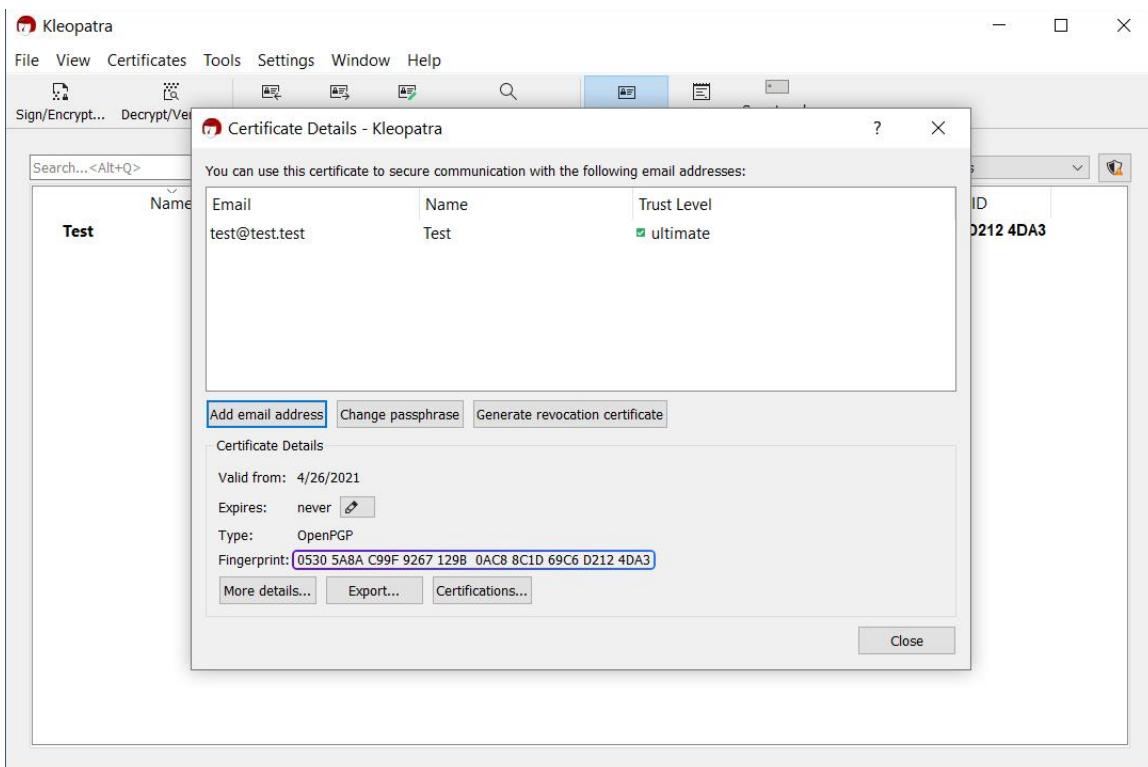
در مقاله پیشین در مورد اثرانگشت مختصر صحبت شد. همون طور که پیشتر دیدیم، کلیدهای عمومی بسیار طولانی‌ان، و امکان خوندن یا وارد کردن اون‌ها به صورت دستی وجود نداره. از این‌رو، برای پیدا کردن و همچنین احراز هویت افراد اثرانگشت کلید عمومی اون‌ها رو بررسی می‌کیم.

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 اثرانگشت‌شن. شما با داشتن هر کدام از این‌ها می‌توانید کلید عمومی من رو پیدا و وارد کنید.

احراز هویت کلید عمومی با اثرانگشت

یکی از راههای احراز هویت، مقایسه و تطابق دادن اثرانگشت شخصیه که قصد دارید با هاش ارتباط بگیرید. در این مورد حساسیت لازم رو به خرج بدید، مطالعه کنید، و دو نسخه های خودتون رو بالا بیرید.



با راست کلیک روی کلید و انتخاب گزینه Details می تونید جزئیات اون رو ببینید، از جمله اثرانگشت

احتمالاً اثرانگشت PGP افراد رو در وبسایت یا پروفایل توئیتر اونها دیده اید. 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، صریح قراردادن اثرانگشت در پروفایل توثیق، امضای ایمیل، تلگرام، و جاماهای دیگه چیزی رو اثبات نمی‌کنه. در بهترین حالت، وقتی شخص رو چهره به چهره دیدید، کلید عمومی اش 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 مکالمه صوتی بتوان 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 (odd) و فرد (even). کلمه‌های زوج دویخشی و فردنا سه‌بخشی‌ان. اثرانگشت از چپ به راست خونده 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

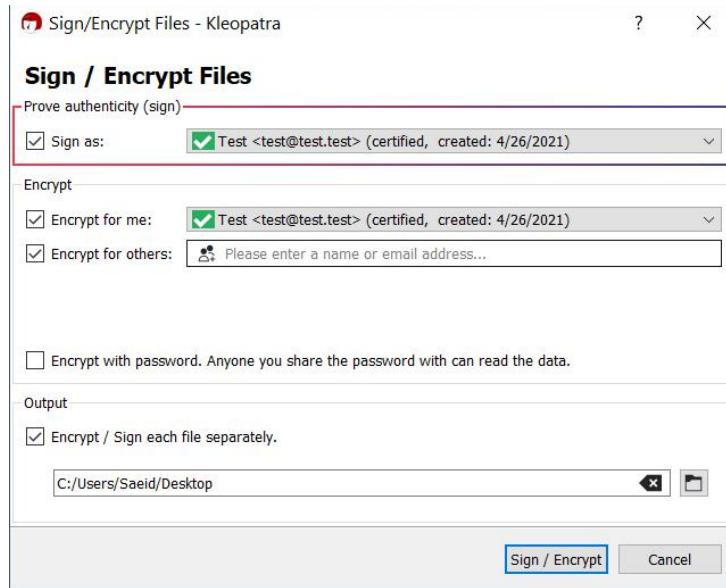
would display in PGP Words (the “biometric” fingerprint) as

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.

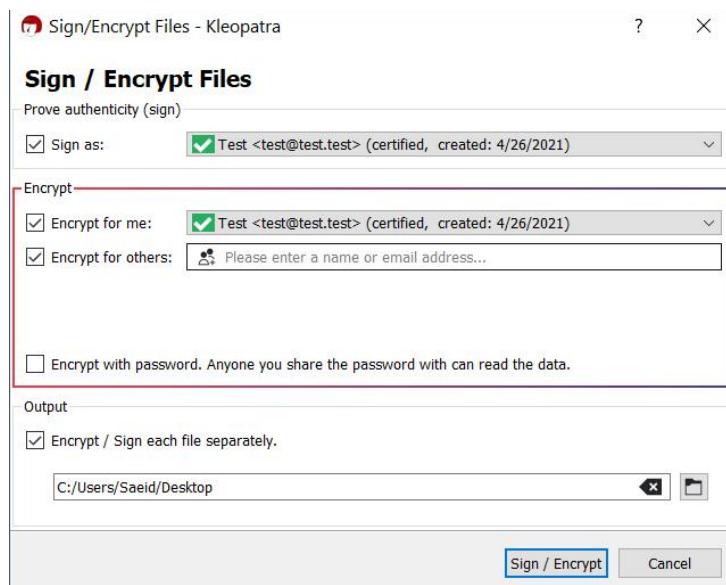
در نرم‌افزار Kleopatra به دو روش می‌توانید رمزنگاری کنید: متن و فایل. برای رمزنگاری فایل‌ها کافیه گزینه Sign/Encrypt رو بزنید، فایل رو انتخاب کرده، و در پنجره‌ای که باز می‌شه گیرنده یا گیرنده‌گان رو مشخص کنید. به تصاویر صفحه بعد توجه کنید.



می‌توانید انتخاب کنید فایل را با کلید خودتون امضا کنید

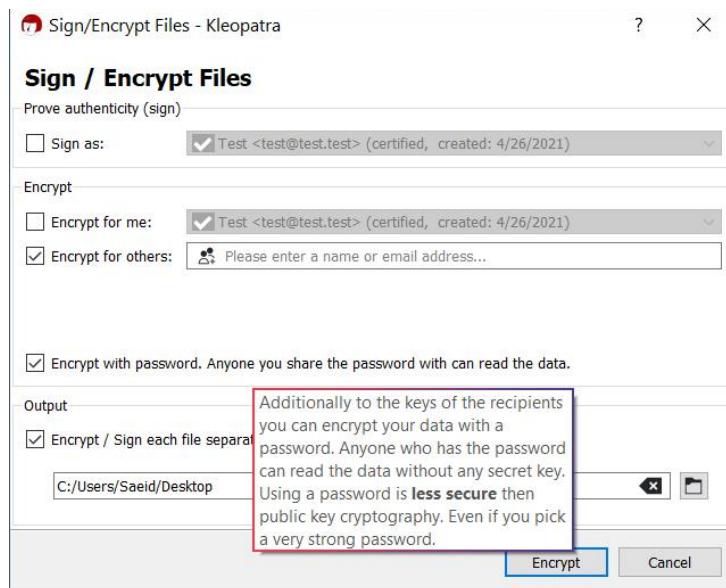
اینجا می‌توانید فایل را امضا کنید. جلوتر بیشتر بهش خواهیم پرداخت. کسی که فایل رو رمزگشایی می‌کنه می‌بینه که شما اون رو امضا کرده‌اید، و می‌تونه اطمینان داشته باشه محتوا توسط شخص دیگه‌ای دست‌کاری نشده. هیچ کسی جز شما، بدون داشتن کلید خصوصی شما، قادر به ارائه اون امضای منحصر به فرد نیست.

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



می‌توانید انتخاب کنید فایل را برای خودتون، شخص دیگه‌ای، یا هر دو رمزگاری کنید

در اینجا فایل به طور پیشفرض برای شما هم رمزنگاری می‌شه، مگه اینکه تیک Encrypt for me رو بدارید. (شاید نخواهد فایل رو در آینده باز کنید، یا شاید اطلاعات حساسیه و نخواهد 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 می‌خوايد برای چه کسی رمزگاری کنید. دستور کامل‌تر می‌توانه این باشه:

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

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

- رمزگاری: `--encrypt`

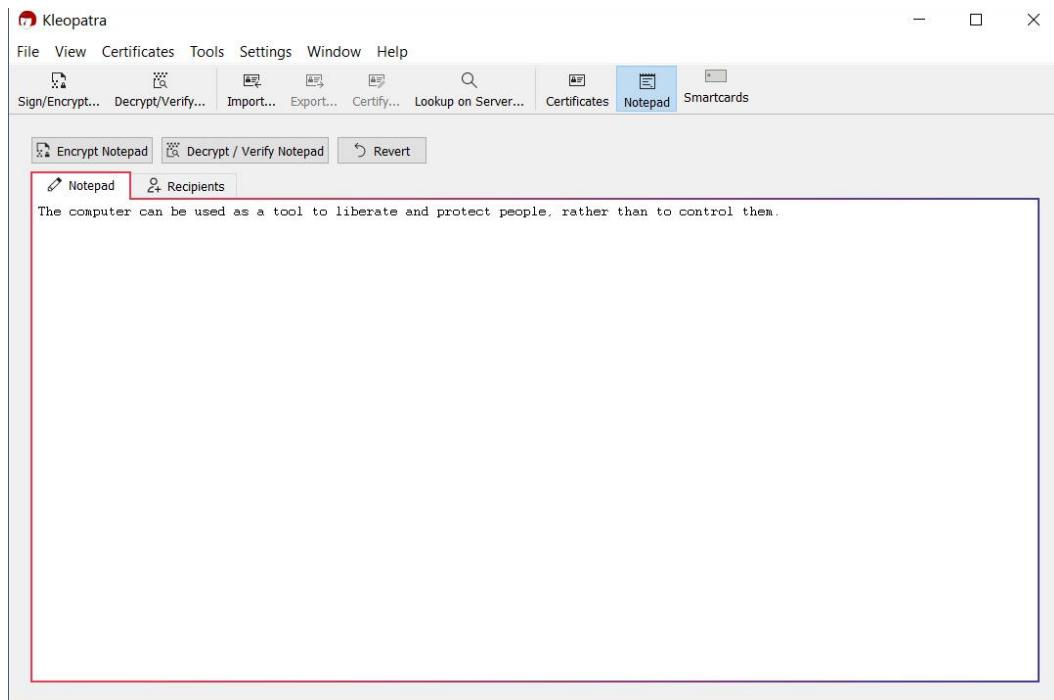
- امضاء: `--sign`

- افزودن گیرنده: `-r (همچنین recipient)`

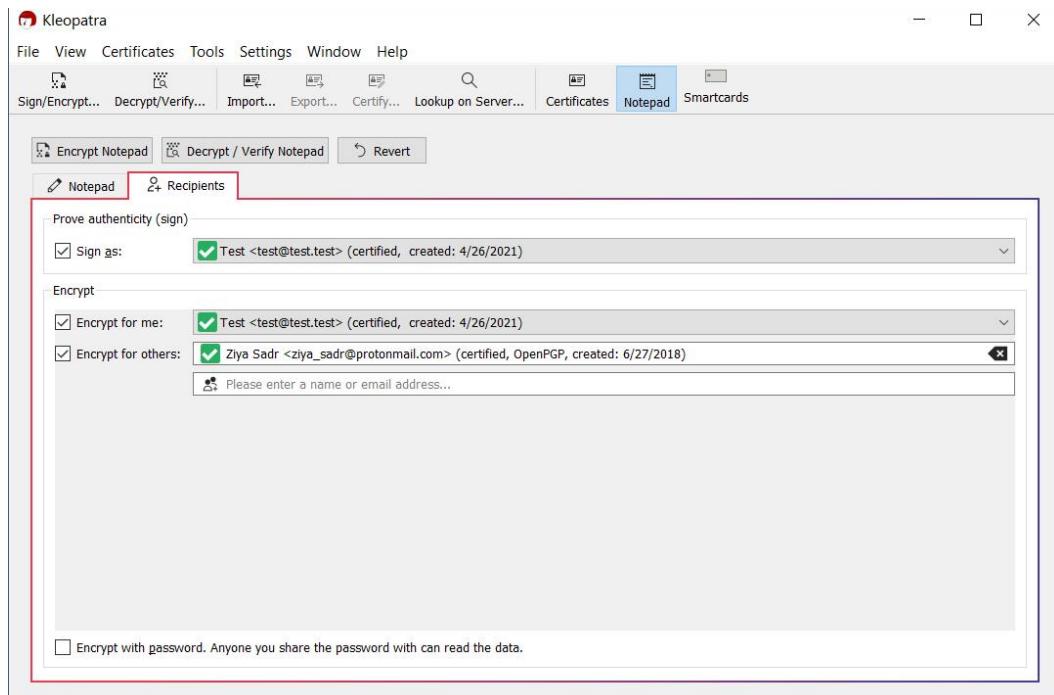
توجه مهم: اگه می‌خوايد بتونید فایل رو رمزگشایی کنید، حتماً باید خودتون رو هم جزو گیرنده‌ها قرار بدید. در ضمن، می‌تونید چند گیرنده داشته باشید؛ در این صورت، چند مورد `r`- خواهید داشت.

توجه مهم: بعد از اینکه GPG فایلی رو رمزگاری 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.)

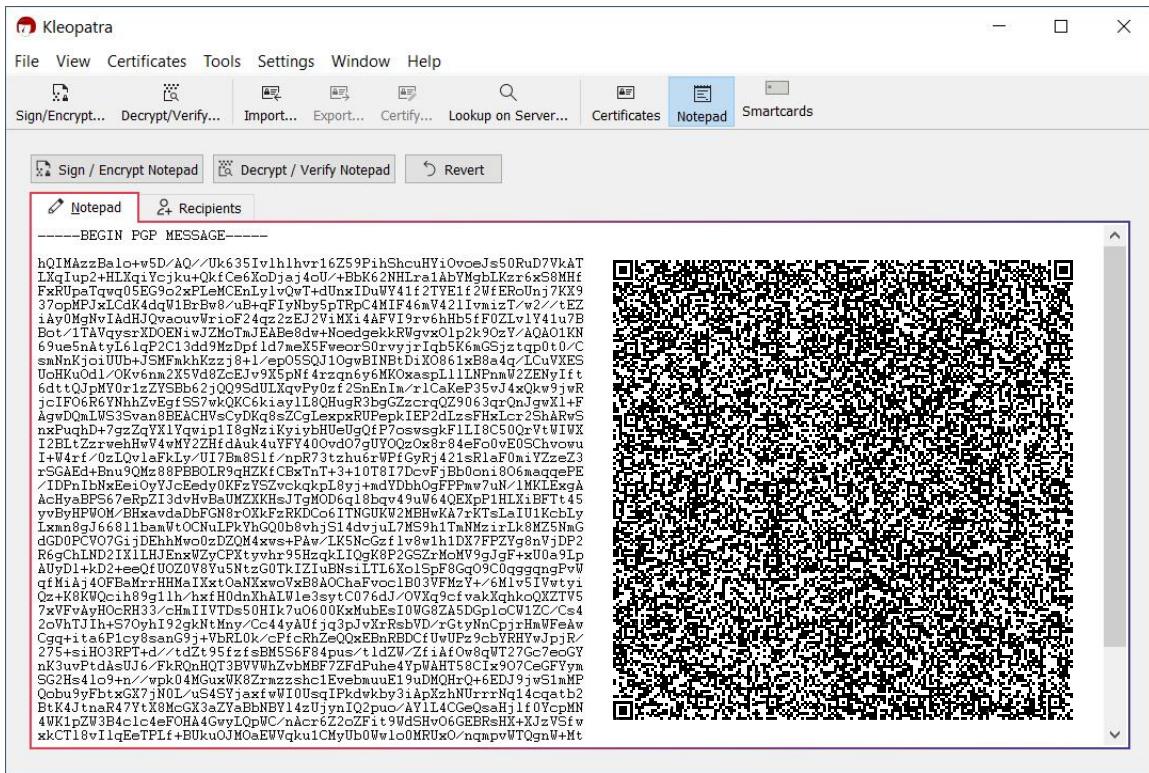
تا اینجا به رمزگاری فایل‌ها پرداختیم، اما چطور یک متن رو رمزگاری کنیم؟ خیلی ساده. از ابزار Notepad استفاده کنید.



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



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

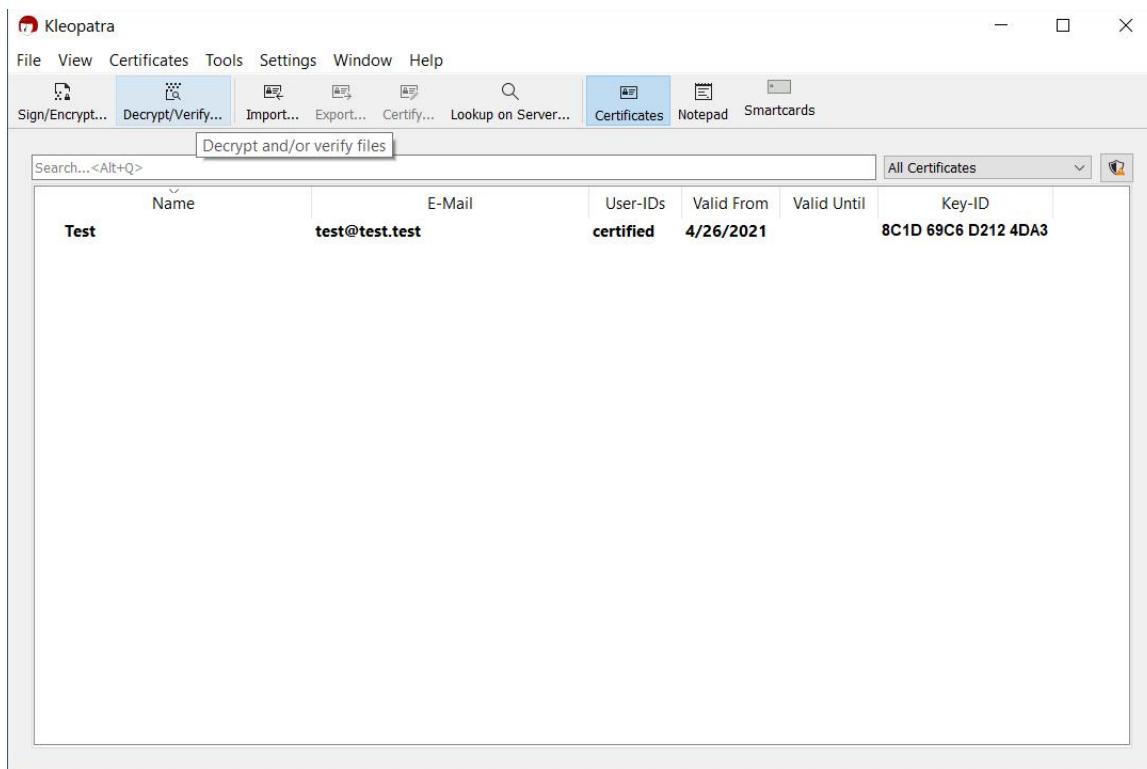


پس از نوشتن متن و تعیین گیرنده‌ها، با زدن گیرنده Sign / Encrypt Notepad متن رمزگاری شده رو تحویل خواهید گرفت

برای مثال، اینجا پیامی رو برای خودم و ضیاء رمزگاری کردم. او می‌تونه تصویر باکیفیتی رو از کد QR بالا ذخیره کنه (برای مثال، با زوم کردن 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 اما decode نه چون به کلید خصوصی من یا ضیاء دسترسی ندارید و این پیام برای شما رمزگاری نشه.

رمزگشایی

رمزگشایی پیامها و فایل‌ها هم به آسونی رمزنگاری کردن اون‌هاست. برای فایل‌ها می‌توانید از گزینه Decrypt/Verify رمزگشایی فایل راست کلیک کرده و Decrypt and verify را انتخاب کنید.



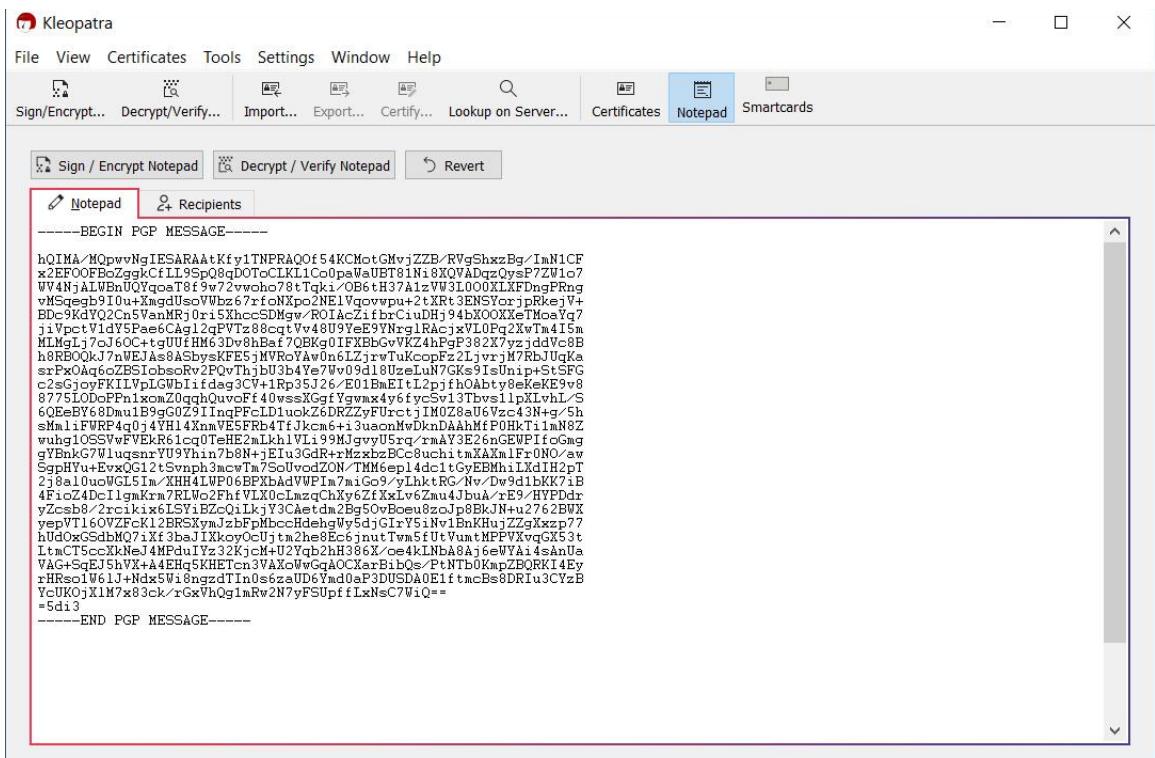
رمزگشایی فایل‌ها با گزینه... Decrypt/Verify...

همچنین، می‌توانید از دستور زیر استفاده کنید:

```
gpg --decrypt [نام فایل]
```

توجه مهم: بعد از اینکه GPG فایلی را رمزگشایی کرد، کاری با فایل رمزنگاری شده نداره. بعد از بازکردن فایل یادتون باشه فایل اصلی رو حذف کنید، ترجیحاً به روشی امن. در ضمن، اگه محتوای متى رمزنگاری شده دارید، می‌توانید بدون اینکه ذخیره ش کنید محتوای اون رو ببینید:

```
gpg -d [نام فایل]
```



رمزگشایی متنون با Notepad

The screenshot shows a Windows PowerShell window. The command entered is `gpg --decrypt <test>`. The output is as follows:

```

windows PowerShell
copyright (C) Microsoft corporation. All rights reserved.

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

PS C:\Users\Saeid> gpg
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: Go ahead and type your message ...
-----BEGIN PGP MESSAGE-----
hQIMA/MQpvvNgIESARAAtkFy1TNPRAQoF54KCMotGMvjZZB/RVgShxzBg/ImN1CF
x2EFOOFBoZggKcflLSp08gD0TcCLKL1CoOpawaUBT81N18XQVADqzQysP7zW1o7
wV4MjALBnUQyqaT8f3wvwoh78Tgk1/0B6tH37Alzvz3L000XLxFdngPrng
vMSqeqb9I0uXmgdusoVbz67rfNopo2NE1vgowpnu-2txrt3ENSYorjpkRejv+
Bdc9KdY02Cn5VanMR0i5KhcsSDMgw/ROIAc1zfbciuH94bXOKOXXeTMoqYq7
jiVpc1vdySpae6Ag12pVTz88cqtv48U9YeE9YNg1RacjxVL0Pq2xWtm415m
MLMglj7oJ6C-tgUHM63Dv8BaF0TBkg1UFKbcbvVKZ4hPgP38ZX7yzjddVc8B
h8RBQkJ7wEA8As8Asby5KFES5MVRoAvon6LZjrwTuycopfZ2lJvrjM7RbjUqka
srFxOaq6cZBS1chv2rFvThb13b4Ye7w9d180zeleUN7Gke91sUn+pScSFG
c2sGjoyPKILVpLGWblidag3CV+1Rp5j26/EU1BmElL2pjfh0Abty8ekE9v8
8775LDcPfN1x0Z0qhbwF40/vssXcgfYgwmxay6lycSw13Tbvs1lpxLvhL/S
6QEeBY6Dnu1B9gC0291InqPFcLd1uck26DRZZyFrctj1Mu28a06Vzc43N+g/5h
sm11FWRP4q04VH14XnwE5FBb4tJfkm6-i3uacnMwDknaAHMF0Hk1l1mN8Z
wuh610SSVvFVEkR61cq0teHE21kh1V119MjgyvU5rq/rmAy3E26nGEWPfGmg
gYBnhG7w1uqsmvYU9Yhin78Bn+jElu3GdrMzbzBcc8uchitmAxlFrNcAw
SgpHyt+bxvG12t5vnph3mcwTm7SoUvodZON/TM6ep14cltGyEBMh1Lxd12pT
2j8a10uoWGL51m/XHH4IWMP0EFXAdWPIm/mG9/yLhtkRG/Nv/D9d1bKK71B
4Fioz24D11gMkrhLRW5Fhf1x0cLmzQn9y5fzAxlv62m4Jdua-Ye9/HYDdn
yZcsb8/2rc1k1x6LS1vBzC1lkj73Caetdm2B50vBeou8zCjpBRJuN-u2762BWx
yepVt160VZFcR2BR5XwJzBfpMcccHdewy5djGixY51nEnKhuJZGxxzp7/
h0d0xGsdBmQ7jXt3bsj1XkoyOcUjma2he8E6jnntTw5fUtVuntMFPVXvgX53t
LtmCT5ccXRNc4NPhd1t7z2Kjcm4-U27q2h386X/ce4klNbA8aj6eWTA14sanUA
VAG+sQxE5hVX-A4He5SKHETcn3VAxw+eQACkarBtbo-/PNTb0KmpZBQRK14Ey
rhRsos1W61j+Ndx5W18ngzd1In0sezaD6ynd0aP3DUSDA0Ef1tmcBs8DRiu3CYzB
YcUK0jXLM7x83ck/rGxVhQg1mRw2N7yFSUpffLxNsC7W1o=
-----END PGP MESSAGE-----

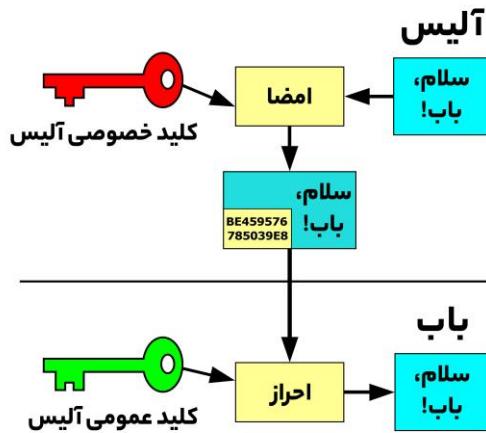
```

در ضمن، اگه متن رمزگاری شده دارید، می تونید اون رو در Notepad قرار بدید.

همچنین، اگه دوست دارید اون رو در ترمینال رمزگشایی کنید، ابتدا بنویسید `Ctrl+Enter` و `gpg` کنید، و در انتهای پایان `Ctrl+Z` + `Enter` (کاراکتر End-of-File) و `Ctrl-D` 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 دست کاری نشده.

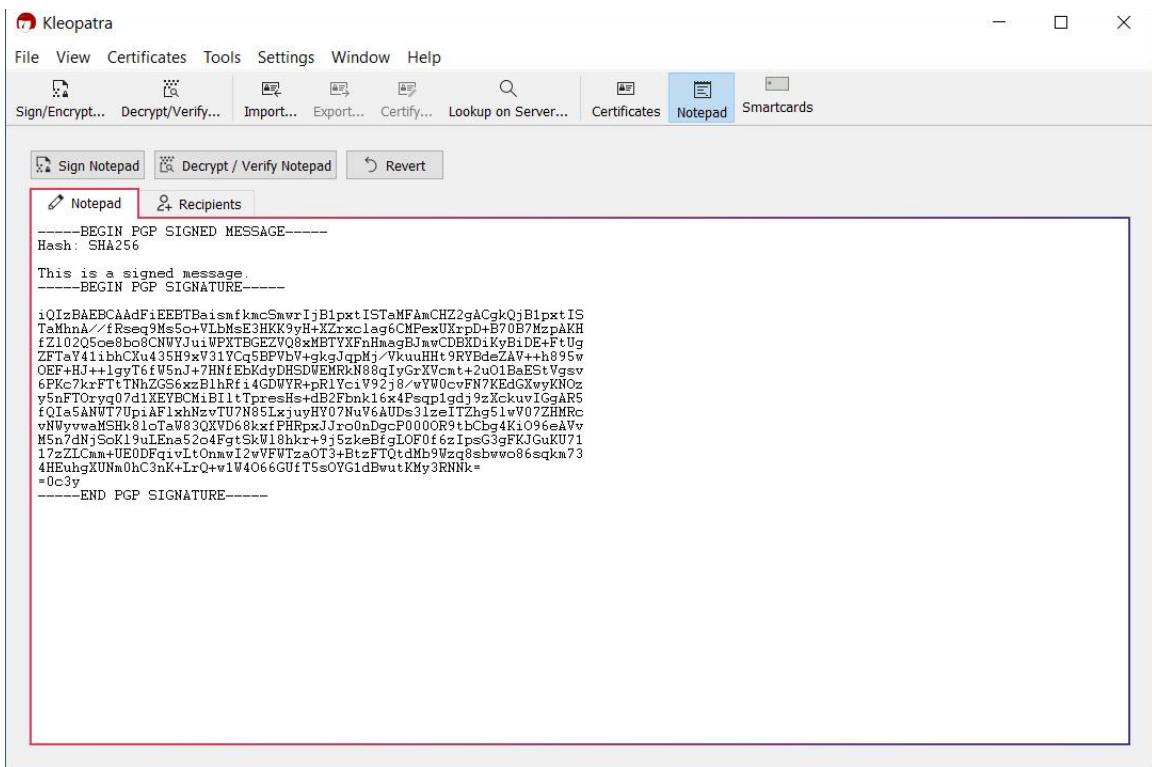


همچنین شخص مقابل، با داشتن کلید عمومی شما، می‌توانه امضای دیجیتال شما رو احراز (verify) کنه و مطمئن باشه از سمت شما او مده. اگه پیامی رو رمزگاری می‌کنید، بهتره همیشه اون رو امضا کنید.

امضا می‌توانه 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 او مده و دست کاری 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 صفحهٔ بعد توجه کنید.



متن امضا شده در محیط نرم افزار

The screenshot shows a Windows PowerShell window. The command history includes:

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

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

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

    Directory: C:\Users\Saeid

Mode           LastWriteTime         Length Name
----           -----          ----- 
-a---        4/27/2021   6:00 AM       906 Example.txt.asc

PS C:\Users\Saeid> gpg --output "Example (Signed).txt.asc" --clearsign Example.txt
PS C:\Users\Saeid> dir

    Directory: C:\Users\Saeid

Mode           LastwriteTime         Length Name
----           -----          ----- 
-a---        4/27/2021   6:00 AM       906 Example (signed).txt.asc
-a---        4/27/2021   6:00 AM       906 Example.txt.asc
```

امضای فایل Example.txt با استفاده از ترمینال

پارامتر clearsign -- چیزی رو به شما می ده که در تصویر صفحه قبل مشاهده کردید. درواقع، متن پیام درون امضا قرار می گیره. با دستور detach-sign -- می تونید فایل امضای مجرزا 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 سیس احراز اون

یکی از مهم‌ترین کاربردهای امضا در احراز و اصالت سنجی فایل‌هایی 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
	Standalone Executable	signature
 Windows (7 and higher)	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

امضاهای فایل‌های نصب کیف پول الکترونیک

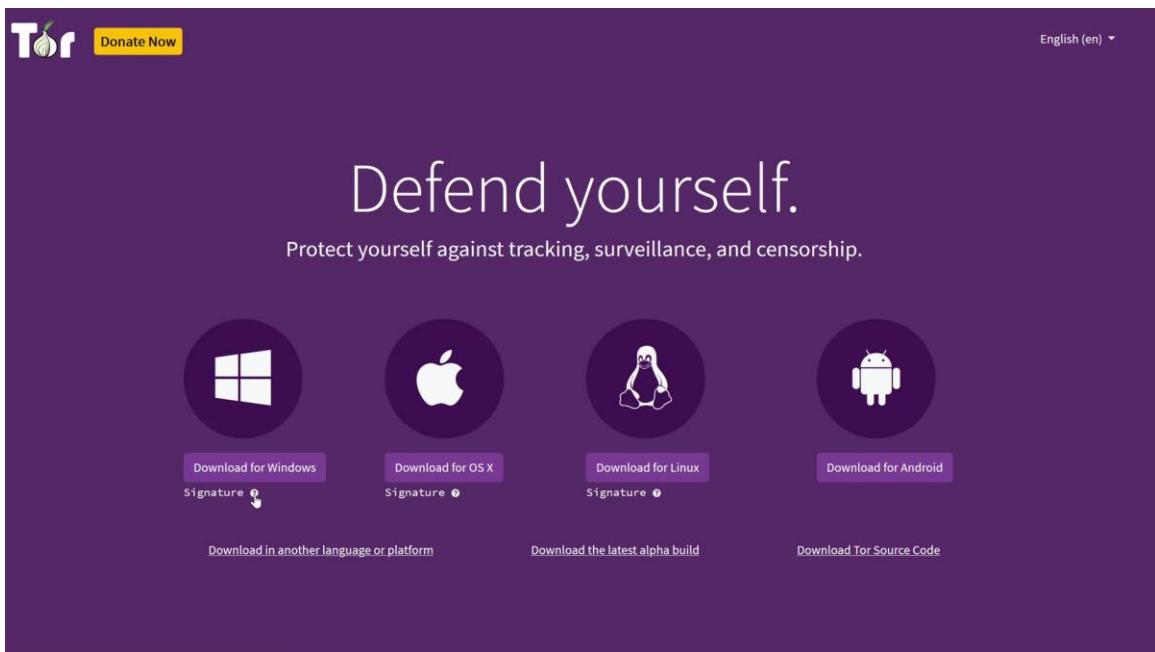
Windows PowerShell

```
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 6694D8DE7BE8EE5631BED9502BD5824B7F9470E6
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 توسعه‌دهندهٔ کیف پول الکترونیک



آموزش تصویری اصالتشناسی فایل‌ها در یوتیوب

سخن پایانی

اطلاعاتی که اینجا خوندید تنها بخش کوچکی از چیزهایی بودن که می‌توانید درمورد GPG یاد بگیرید، هرچند این‌ها نیاز کاربر عادی را برطرف می‌کنند. [راهنمای این نرم‌افزار](#) بیش از ۲۰۰ صفحه است، و حتی بعد از آشنایی کامل با عملکردش، همچنان نکات امنیتی زیادی هست که می‌شه یاد گرفت.

اگه تنها یک درس باشه که بخواه انتقال بدم اینه که به مقدار کمی دانش بسنده نکنید. جمله زیر در ابتدا برام عجیب بود، اما هرچی بیشتر بهش فکر کردم، معناش برام قابل‌لمس‌تر شد. کنجکاو باشدید، 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 تلوم نمی‌شه. (برای مقایسه، مسیر اصلی یادگیری من تازه از اینجا شروع شده.)

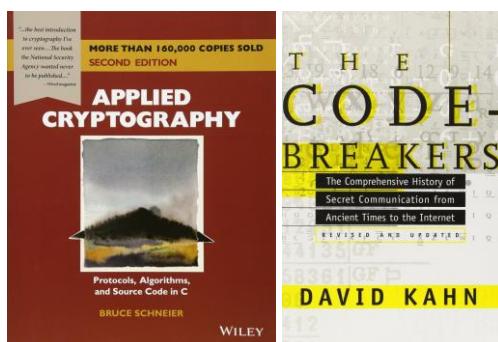
از اونجایی که سطح انتظار بالایی برای quality content دارم، کم پیش میاد که مطلبی من رو شگفت‌زده کنه. یکی از بهترین، جامع‌ترین، و لذت‌بخش‌ترین منابعی که خوندهم و حالا هرازگاهی بهش سرمی‌زنم، [راهنمای GPG آلن ایلیاسون \(Alan Eliasen\)](#) است. اگه دوست دارید آشنایی خوبی نسبت به GPG پیدا کنید، نباید ازدستش بگیرید. الهام‌بخش نوشتن این مقاله‌ها بود. اگه کنجکاوید راجع به نحوه آشنایی من با این شخص و انگیزه نوشتن این مطالب بدونیم، [این رشته‌تئیت](#) رو بخونید.

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

سایت شخصی زیمرمن به تهابی منبع بسیار خوبی برای شروعه. اونقدر لینک و مقاله داره که چند روزی شما رو سرگرم نگه داره. پیشنهاد می کنم با متن ده سالگی PGP شروع کنید. یکی از بهترین روش ها برای آشنایی با یک موضوع اینه که اون رو از زبون سازنده یا سازنده هاش بشنوید. وقتی پای حرفشون می شینید، نکاتی رو می فهمید که ممکنه هیچ جای دیگه ای پیدا شون نکنید. صحبت های زیمرمن در دف کان یازده شنیدنیه. حضور و صحبت هاش در Bitcoin

Wednesday هم جالب و دیدنیه. وقتی یکی ازش می پرسه با توجه به سختی هایی که در چند دهه اخیر متholm شده ای، آیا باز هم این کارها رو انجام می دادی، می گه، «آره، ولی احتمالاً از الگوریتم های بهتری در نسخه اصلی PGP استفاده می کردم!»

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



راهنماهای مرتبط



فایرفاکس: حریم خصوصی، ابزارها، و ترفندها



حریم خصوصی در عصر دیجیتال

