

امنیت سایبری ۱۰۱ ویژه فعالان حقوق بشر،  
فعالان مدنی، فعالان سیاسی، روزنامه  
نگاران و براندآزان: آیا تلگرام امن است؟ و آیا  
امکان جاسوسی و شنود داده های کاربران  
تلگرام توسط نهادهای امنیتی رژیم جمهوری  
اسلامی وجود دارد؟

پست شده در July 4, 2019  87 دقیقه  مددوو بابائی 



از زمان عرضه تلگرام در سال ۲۰۱۳ تا کنون، این پیام رسان دائما در حال رشد و افزودن قابلیت های جدید بوده است تا آنجا که سازندگان تلگرام در مارس ۲۰۱۸ تعداد کاربران فعال این پیام رسان را ۲۰۰ میلیون نفر اعلام نمودند. ممکن است شما هم یکی از کاربران این پیام رسان باشید. چنان چه شما یک فعال حقوق بشر، فعال مدنی، فعال سیاسی، روزنامه نگار، و یا برانداز هستید و یا فعالیت هایی انجام می دهید که ممکن است شما را در صف مخالفان رژیم جمهوری اسلامی قرار دهد، احتمالا بهتر است که هر چه زودتر استفاده از این پیام رسان را متوقف نمایید!

ظاهرا در میان عموم مردم پیام رسان تلگرام به عنوان یکی از امن ترین پیام رسان های موجود شناخته می شود. اما حقیقت تلخ در مورد تلگرام این است که: تلگرام به آن اندازه که کمپین های بازاریابی این شرکت ممکن است شما را متلاعنه نموده باشند، امن نیست. امیدوارم مرا به خاطر اسپویل نمودن ادامه مقاله بدون هشدار قبلی بخشیده باشید! برخلاف ادعای سازندگان پیام رسان تلگرام، از نظر متخصصین شناخته شده حوزه امنیت، این پیام رسان نه تنها امن نیست بلکه یکی از نامن ترین پیام رسان های موجود و بسیار مورد علاقه آژانس های اطلاعاتی و نهادهای امنیتی جمهوری اسلامی می باشد.

در ادامه این نوشتار که اولین مقاله از مجموعه مقالات [#امنیت\\_سایبری\\_۱۰۱](#) می باشد به چگونگی و چرایی نامن بودن تلگرام خواهیم پرداخت. از آنجایی که این مقاله شامل

مقدمه سری امنیت سایبری ۱۵۱ نیز می باشد و به دلیل ماهیت و حساسیت اجتناب ناپذیر موضوع تلگرام، توجه داشته باشید که مدت زمان مطالعه این نوشتار حدودا به اندازه یک مسابقه فوتبال زمان می برد. البته قول می دهم که مقالات آتی از این سری، تا حد ممکن بسیار کوتاه باشند.

پیشنهاد می کنم قبل از شروع مطالعه مقاله، یک فنجان چایی، قهوه، یا نوشیدنی مورد علاقه خود را تهیه نمایید؛ به من اعتماد کنید، به آن نیاز خواهید داشت ؛)

تقدیم به تو دوست شجاع و آزادی خواه، برادر عزیزم [علی اشرف دارابی](#)، که به نام آزادی و برای ایران عزیzman، ۵۹۱ شبانه روز حبس در زندان های [#فرقه\\_تبهکار](#) را به جان خریدی.

بی گمان با وجود انسان هایی چون تو، دنیا جای زیباتری است.

## فهرست مطالب

در این نوشتار چه چیزی خواهیم آموخت  
من کی هستم و آیا صلاحیت اظهار نظر در این باره را دارم؟  
چرا تصمیم به انتشار این مجموعه از مقالات گرفتم؟

## سلب مسئولیت

آیا تلگرام به عنوان یک پیام رسان، امن است؟

جوری توضیح بده که انگار من ۵ ساله هستم

- رمزگاری یا Cryptography

- الگوریتم کلید متقارن یا Symmetric-key Algorithm

- رمزگاری کلید عمومی یا Public-key Cryptography و یا رمزگاری نامتقارن یا

- Asymmetric Cryptography

- ترکیب رمزگاری متقارن و نامتقارن

- رمزگذاری سر تا سر یا End-to-end Encryption

- متادیتا

مشکل تلگرام دقیقا چیست؟

- عدم رمزگذاری سر تا سر بصورت پیش فرض

- عدم پشتیبانی از رمزگذاری سر تا سر در چت های گروهی

- عدم رمزگذاری سر تا سر در نسخ دسکتاب و وب

- عدم ارائه حق انتخاب به کاربران جهت خروج از کlad تلگرام

- انتقال داده های لیست تماس تلفن همراه به کlad تلگرام

- نیاز به شماره تلفن جهت ثبت نام

- عدم پشتیبانی از رمز یکبار مصرف آفلاین

- عدم توانایی تایید هویت طرفین در چت های مخفی

- شبکه های تحويل محتوا یا CDN تلگرام در ایران

- نشت متادیتا

- مشکلات پروتکل MTProto

- ابهام در مدل درآمدزایی تلگرام

- تحويل داده های کاربران به مقامات قضایی در صورت دریافت دستور دادگاه

- موضوع پرداخت رشوه یا اعمال فشار

- اما تلگرام متن باز است و هر کسی می تواند کد منبع آن را مشاهده نماید

- اما تلگرام به دستور مقامات قضایی جمهوری اسلامی فیلتر شده است

- پس چرا جمهوری اسلامی اقدام به عرضه طلاگرام (تلگرام طلایی) و هاتگرام نموده است؟

## جایگزین ها

- لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط Prism Break
- لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط privacytools.io
- لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط ThinkPrivacy
- مقایسه امنیت پیام رسان ها توسط ThinkPrivacy
- مقایسه امنیت پیام رسان ها بر اساس استانداردهای Electronic Frontier Foundation
- مقایسه امنیت پیام رسان ها توسط Secure Messaging Apps
- Signal
- Wickr
- Riot.im
- Wire
- Jami
- Keybase
- Rocket.Chat
- Tox
- Briar
- RetroShare
- Ricochet
- Silence
- Status
- کلاینت های مبتنی بر XMPP
- Aenigma
- کلاینت های مبتنی بر XMPP با پشتیبانی از OMEO
- Conversations

Gajim •

Monal •

+Psi •

ChatSecure •

Kontalk •

سایرین •

• پیام رسان ویژه قطعی احتمالی اینترنت: Manyverse

سخن پایانی

## در این نوشتار چه چیزی خواهیم آموخت

مباحثی که در این نوشتار خواهیم آموخت به شرح ذیل می باشد:

- برخی از مفاهیم امنیت سایبری
- مفاهیم مربوط به رمزگاری
- درک ماهیت متادیتا و اهمیت آن در شنودهای ابیوه
- مشکلات و نقصان های امنیتی تلگرام
- آشنایی با جایگزین های بسیار امن تر از تلگرام
- آشنایی با یک شبکه اجتماعی ویژه و امن که در صورت قطعی اینترنت می توان بدون نیاز به اینترنت از آن جهت پیام رسانی فوری استفاده نمود

## من کی هستم و آیا صلاحیت اظهار نظر در این باره را دارم؟

با وجود گذشت بیست و اندی سال از روزگاری که کار با کامپیوترهای مبتنی بر MS-DOS و به طبع برنامه نویسی آن ها را آغاز نمودم تا به امروز که حرفه ام بازی سازی است،

کامپیوترها زرق و برق سحرآمیز و جادوئی خود را برایم از دست نداده اند.

از همان ابتدا به دلیل شیوع ویروس های کامپیوتری در محیط سیستم عامل داس، علاقه شدیدی به مقوله امنیت پیدا کردم تا آنجا که با انگیزه نوشتن یک ویروس کامپیوتری در دوران راهنمایی، برنامه نویسی [زبان اسمبیل](#) را یاد گرفتم. هر چند که کد اولین ویروسی که نوشتم را با از دست رفتن هارديسکم از دست دادم، ولی هنوز هم [کد برنامه کوچکی](#) که برای شکستن قفل یک نرم افزار آموزشی نوشته بودم را می توان در [گیت هاب](#) یا [گیت لب](#) پیدا نمود. در نهایت، به عنوان یک نوجوان مشتاق در زمینه امنیت کامپیوتری، سال PC Intern: System Programming: The خواندن کتاب [Encyclopedia of DOS Programming Know-how](#) فارسی، به کسب دانش در گروه ها و انجمن های خصوصی و خارج از دسترس عموم، یا در اصطلاح عامه، هکری گذشت.



من در کنار میکوهایپونن کاشف اولین ویروس کامپیوتری و مدیر ارشد تحقیق شرکت  
ضدovirus اف سکیور - اسلاشن ۲۰۱۴، هلسینکی، فنلاند

قدیمی های وب فارسی، [اولین مجله تخصصی امنیت اطلاعات](#) در ایران به نام اسنوب در زمینه امنیت دیجیتال را به خوبی به خاطر می آورند. هنوز هم [با کمی جستجو](#) می توان

شماره های مختلف این مجله را در گوشه و کنار وب فارسی یافت. به عنوان هیات تحریریه در شماره های ۲ و ۲.۵ این مجله، مقالاتی در زمینه امنیت تحت عنوان [مبهم سازی کد در .NET و Java و توزیع شما نا امن است: اوبونتو منتشر نمودم](#). لازم به ذکر است که انتشار و بازخورد موفقیت آمیز این مجله، باعث معرفی آن در برنامه کلیک بی بی سی فارسی نیز شد.

علاوه بر این ها، علاقه به مباحث امنیت در نوجوانی باعث جذب من به سیستم عامل های یونیکسی مانند [گنو/لینوکس](#) و بعدها سیستم عامل [فری بی اس دی](#) (رجوع شود به مقالات نوشته شده توسط نگارنده: [تاریخچه FreeBSD و FreeBSD چیست؟ یک نمای کلی از سیستم عامل Linux و FreeBSD یا FreeBSD مسئله این است؟](#)) شد.



من در کنار ریچارد استالمن بنیانگذار بنیاد نرم افزارهای آزاد و پروژه گنو - اسلامش ۲۰۱۴، هلسینکی، فنلاند

با توجه به این که در حال حاضر یکی از طرفداران پر و پا قرص تکنولوژی های [متن باز](#) و یونیکسی می باشم، از طریق توسعه، پورت، و نگهداری چندین نرم افزار به عنوان بخشی از مجموعه پورت های رسمی FreeBSD در پروژه FreeBSD مشارکت نموده ام. افرادی

که با تیم توسعه FreeBSD و دستورالعمل های امنیتی این سیستم عامل ایمن آشنایی دارند، خوب می دانند که به دلیل استفاده عمده این سیستم عامل در سرور (برای مثال پلتفرم محصولات شرکت های واتس اپ و نت فلیکس و ... بر پایه این سیستم عامل طراحی شده اند، جهت کسب اطلاعات بیشتر رجوع شود به مقالات فوق)، چنان چه پورت های شما از حداقل استانداردهای امنیتی برخوردار نباشند، توسط این پروژه پذیرفته نخواهند شد.

لازم به ذکر است که سابقه ساخت دیسترو یا سیستم عامل مبتنی بر لینوکس سفارشی از طریق پروژه های Funtoo و LFS, Gentoo را دارم. در این نوع سیستم عامل های مبتنی بر سورس، به جای نصب سیستم عامل، شما کامپوننت های سیستم عامل را خودتان از صفر کامپایل و به شکل دستی در جای خود قرار می دهید که بسته به تجربه از چندین ساعت تا چندین روز زمان می برد و پس از اجرای موفقیت آمیز، درک بسیار عمیقی از مبانی سیستم عامل و امنیت را در شما ایجاد می نماید. در واقع سیستم عاملی که این پست را در آن نوشته ام یا وب سایتی که این سایت بر روی آن قرار دارد، به همین شکل برپا شده است. در نهایت، یک Overlay غیررسمی برای سیستم عامل Gentoo (کد منبع در گیت هاب یا گیت لب) را توسعه داده و نگهداری می نمایم.

## چرا تصمیم به انتشار این مجموعه از مقالات

### گرفتم؟

راستش را بخواهید علاوه بر تجربه در زمینه امنیت، زمانی که در ایران زندگی می کردم، به دلیل سرکش بودن و عدم برتابیدن گفتگو این دیکتاتور مآبانه، همیشه می دانستم که بلاخره روزی گذرم به نهادهای امنیتی جمهوری اسلامی خواهد افتاد. بازداشت دوست بسیار نزدیکم علی (که این نوشتار به او تقدیم شده است) در جریان قضایای ۸۹ / ۸۸ در منزل و ضبط کلیه دستگاه های دیجیتالی، اعم از کامپیوتر، هارد دیسک، گوشی و ... را هم زنگ خطری برای خود می دانستم تا روش ها و عملکرد دیجیتالی خود را مورد بازنگری قرار

دهم. ظاهرا جرم او ایمیل نمودن تصاویری از اعتراضات بود که با دوربین شخصی اش گرفته بود. این عکس ها دستمایه اتهاماتی نظیر توهین به رهبری، تبلیغ عیله نظام و ... قرار گرفت که منجر به ۵۹۱ شبانه روز حبس شد.

موضوع بازداشت و حبس غیرمنصفانه علی به کنار، اگر موضوع [بازداشت و خودکشانی](#) فعال محیط زیست و جانباز جنگ ایران و عراق، دکتر کاووس سیدامامی را دنبال نموده یا به خاطر داشته باشد، پس از به قتل رسیدن کاووس سیدامامی توسط نهادهای امنیتی، مستندی از صدا و سیمای میلی جمهوری اسلامی پخش شده بود که به شکلی مضحك با استناد به عکس های خصوصی کاووس سیدامامی در استخر یا مهمانی، کاووس سیدامامی را متهم به جاسوسی برای دوکل غربی نموده بود. نمونه دیگر، بازداشت و محکومیت [گلرخ ایرایی](#) می باشد که با کشف داستان منتشر نشده ای در دفترچه شخصی اش به ترتیب به ۵ سال حبس و ۱ سال حبس، به دلایل توهین به مقدسات و تبلیغ علیه نظام متهم شده بود. شک نداشته باشد داده هایی که از نظر شما ممکن است بی ارزش به نظر برسد، برای نهادهای امنیتی جمهوری اسلامی بسیار بالارزش تر از آن چیزی است که تصور می نمایید.

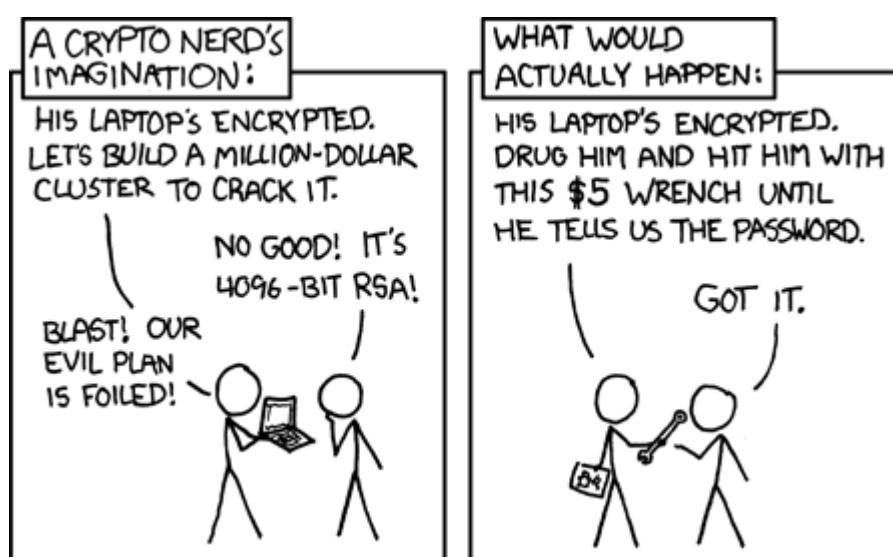
اینجا بود که دیدگاهم نسبت به مسایل و مشکلات حریم خصوصی و امنیت در اثر استفاده از تکنولوژی کاملاً متحول شد و دریافتمن زمانی که شما به هر دلیلی توسط نهادهای امنیتی رژیم دستگیر می شوید، هر نوع داده ای که از شما کشف شود بر علیه شما استفاده خواهد شد، حتی اگر شما کار بدی نمی کنید یا چیزی خاصی برای مخفی نمودن ندارید. شک ندارم هر شهروند ایرانی حداقل یک فرد بی گناه را سراغ دارد که تنها به دلیل بدینی نهادهای امنیتی یا نیاز به سناریویی خاص برای پیشبرد اهداف رژیم، به تحمل مجازات های سنگین و غیرقابل جبران و یا حتی از دست دادن جانشان مواجه شده اند.

چیزی که آن را بدتر می نماید، در زمان دستگیری در نهادهای امنیتی در ایران نه تنها شما حق دسترسی به وکیل را نخواهید داشت بلکه اگر دستگاهی نظیر کامپیوتر، لپ تاپ، گوشی تلفن همراه، هارد درایو، و یا حتی اکانت ایمیل یا شبکه های اجتماعی از شما

کشف شود، تفاوتی نخواهد داشت اگر پسورد شما باشد یا

799Nk209I90;y046mT23y7H.\0LB5|6362=288wA^y76180S84q260!995\$3o&H

هیچ چیز شما را نجات نخواهد داد:



امنیت - xkcd شماره ۵۳۱

تصورات یک خوره رمزگاری:

- لپ تاپش رمز نگاری شده. بباید یه خوشه کامپیووتری یک میلیون دلاری برای شکستن بشناسیم.

- خوب نیست! این [الگوریتم] آراس ای ۴۰۹۶ بیتی هستش!

- پووووو! نقشه شیطانیمون نقش برآب شد!

اتفاقی که در واقعیت می‌افتد:

- لپ تاپش رمز نگاری شده. نعشه اش کن و با این آچار ۵ دلاری تا زمانی که پسورد رو بهمون بگه کتکش بزن.

محتوای کامیک فوق، به مفهومی آشنا برای متخصصین حوزه رمزنگاری تحت عنوان اشاره دارد. در واقع اهمیتی ندارد که الگوریتم رمز نگاری [Rubber-hose cryptanalysis](#) یا پسورد شما چقدر قوی باشد؛ استخراج کلمات عبور از یک انسان با متوجه شدن به تهدید یا شکنجه، بسیار ساده‌تر و کم هزینه‌تر از حملات رمزنگاری است که نیازمند صرف دانش فنی، امکانات و هزینه‌ی می باشد. علاوه بر آن به راحتی توسط هر فردی قابل انجام است.

بلاخره روز موعود فرا رسید و اتفاقی که انتظارش را داشتم پیش آمد. در تظاهرات دیماه ۹۶، ظرف مدت ۳ روز، ۲ مرتبه در حوالی میدان انقلاب دستگیر شدم. [مرتبه اول](#) با مقداری خوش شانسی آزاد شدم، اما [مرتبه دوم](#) برای حدود ۹ روز با نقض حق دسترسی به وکیل، فقط به دلیل رنگ مو، پوست و شکل و شمایل غربی، با اتهامات امنیتی / سیاسی، از جمله جاسوسی برای آژانس‌های امنیتی اسرائیل، انگلیس و آمریکا؛ اقدام علیه امنیت ملی، و اخلال در نظم و آسایش عمومی بازداشت شدم. بر کسی پوشیده نسیت که اتهام جاسوسی، به خصوص اگر شواهدی علیه شما کشف شود، به منظور پیش برد مقاصد شوم رژیم، به راحتی می تواند صدور حکم غیرانسانی اعدام را در پی داشته باشد.

خوبی‌ترین شیوه هایی که در طول سالیان سال برایم به عادت تبدیل شده بود، به همراه آشنایی با تکنیک‌ها، مفاهیم، روش‌ها و ابزارهایی مانند رمزنگاری با استفاده از [Plausible Deniability](#)، [احراز هویت دو عاملی](#) با استفاده از [رمز یکبار مصرف](#) آفلاین یا [U2F](#) به جای استفاده از SMS (به این دلیل که نهادهای امنیتی می توانند فقط با داشتن شماره تلفن شما، کد تایید هویت مورد نظر در پیامک ارسالی از [گوگل](#)، [توییتر](#)، و ... را حتی بدون در دسترس بودن تلفن همراه، پیش از رسیدن

به شماره شما بخوانند)، علیرغم اجبار به افشاری کلمات عبور، به دلیل عدم کشف هر گونه شواهدی، فقط به دلیل حضور در تظاهرات با اتهام مبنی اساس اخلال در نظم و آسایش عمومی به **۸ ماه حبس تعزیری و تحمل ۳۰ ضربه شلاق** محکوم شدم، که با **رافت و عطوفت اسلامی** به مدت ۳ سال تعلیق شد. شک ندارم که اگر به محتویات ایمیل، چت ها، پیام های توییتر، یا اطلاعات رمزگاری شده داخل هارد درایو و کامپیوترم که با تکنیک خاصی مخفی سازی شده بود، دسترسی پیدا می کردند، با توجه به اتهامات اولیه مطرح شده، نه تنها امکان آزادی من وجود نداشت و با حکم غیرانسانی تری مواجه می شدم، بلکه ممکن بود برای سایر افراد در ارتباط با من نیز مشکل ساز شود. فی الواقع، در طول بازجویی ها، جمله ای که توسط بازجوها مداما تکرار میشد این جمله بود که: "تو آموزش دیده ای!"

البته حق هم با آن ها بود، من نه توسط آژانس های اطلاعاتی دول غربی، بلکه به شکل خود ساخته، آموزش دیده بودم. راستش را بخواهید تا پیش از این اتفاق، هرگز به ذهنم خطور نمی کرد در شرایط غیر انسانی و افتضاح بندهای سپاه (وقتی به اوین رسیدم، در مقایسه، اوین برایم مانند بهشت بود) با وجود فشار بازجویی، نه تنها زیر آن فشار دوام بیاورم، بلکه علاوه بر حفظ روحیه خود، نقطه اتکای افراد دیگر هم باشم. افراد بی گناهی که به دلیل شکسته شدن زیر فشار بازجویی و اعتراف اجباری، با وثیقه های بسیار سنگین تری آزاد شدند. سعی ام بر این بود که بازجویی ها را بازی شطرنج ببینم تا از میزان فشار و استرس بازجویی بکاهم. با وجود این که تجربه بازداشت و زندان رفتن بدون آمادگی قبلی، برایم تجربه بسیار سختی بود (البته می دانم به شخصه از بسیاری از زندانیان عقیدتی، امنیتی و سیاسی خوش شانس تر بوده ام)، در حال حاضر که این تجربه را پشت سر گذاشته ام، اگر بدانم مسیرم بازهم ختم به زندان خواهد شد، باز هم همان مسیر را در پیش خواهم گرفت.

دلیلش؟ تجربه خودشناسی! هر چه قدر هم دیگران از تجربه بازداشت خود در نهادهای امنیتی و زندان های رژیم برای شما بگویند، تا آن را تجربه نکنید، به هیچ وجه درد و رنج حاصل از آن را احساس و یا لمس نخواهید نمود. در آن شرایط با خود واقعی تان طرف

می شوید و خودتان و آموخته هایتان را محک خواهید زد. شما باید و یک سیستم طویل و عریض که از به کار بردن هر گونه شیوه غیرانسانی برای شکستن شما، ابائی ندارد. خوب یا بد، راه این تجربه فقط از زندان می گذشت و باید بگوییم که مرا برای همیشه تغییر داد.

اما چرا تصمیم به نوشتن این سری مقالات گرفتم و اولین مقاله از این سری را به تلگرام اختصاص دادم؟

از آنجایی که همیشه معتقد بوده ام با وجود تمام ضعف های جمهوری اسلامی، **رژیم هم در پروپاگاندای داخلی و هم خارجی همیشه موفق عمل کرده است** (بزوی بیشتر در این زمینه خواهم نوشت)، به منظور ایجاد یک صدای مستقل، پس از آزادی از زندان، ماموریت ساخت و عرضه یک بازی تحت عنوان **Gods Of Deceit** یا **خدایان فریب** را اولویت اول ساعات فراغت خود قرار دادم. البته توسعه ایده اولیه مدتی طول کشید تا این که بالاخره در **سال روز مرگ دجال قرن و بنیانگذار فرقه تبهکار** با صرف هزینه های شخصی اقدام به کلیدزن آغاز این پروژه در قالب یک برنده ناشناس تحت عنوان **Seditious Games** یا **کمپانی بازی های فتنه گر** نمودم. هر چند این نام ممکن است برای افراد دیگر بی معنی باشد، اما این نام برای من یادآور لقبی است که بازجوها به من تخصیص داده بودند. به دلیل مدل ریش دوران ویکتوریایی انتخابی و مورد علاقه ام، آن ها مرا تحت عنوان "انگلیسی فتنه گر" صدا می زدند. مطمئن نیستم که به عنوان یک سندروم آیا نامی برای آن ابداع شده است یا نه؛ واقعیت امر این نام را دوست داشتم و به نظرم برای یک کمپانی بازی سازی که ماموریت خنثی نمودن پروپاگاندای رژیم را سرلوحه کار خود قرار داده است نام بسیار مناسب و به جایی است.



ممدوو بابائی

با وجود این که اولویت اولم به پایان رساندن این پروژه بود، و با وجود آگاهی از نامن بودن تلگرام، تا پیش از این هیچ وقت به ذهنم خطور نکرده بود که با توجه به شرایط بسیار بد فعلی، که سایه جنگ، فروپاشی داخلی و فقر کشور را تهدید می نماید، آموزش صحیح نکات پیشگیرانه در زمینه امنیت سایبری تا چه حد می تواند در حفظ حریم خصوصی و امنیت جانی سایر فعالان و براندازان اهمیت داشته باشد. شک ندارم با کوچکترین قیام و حرکت مردمی، بگیر و ببند های دسته جمعی فعالان حقوق بشر، مدنی، سیاسی، روزنامه نگاران و براندازان آغاز خواهد شد. به خصوص پس از **گفت و گوی اخیر ایران وایر با دو عضو بسیج در رابطه با اعدام آنی شهروندان به رسم دادگاهای صحرایی، در صورت آغاز قیام های مردمی:**

...

او گفته است: «یکی از وظایف اصلی ما این است که به کانال های تلگرامی گروه های مختلف در هر منطقه نفوذ کرده و حساب های کاربری اینستاگرام را زیر نظر بگیریم تا

بیینیم فعال‌ترین افراد چه کسانی هستند و درباره چه بحث و گفت‌وگو می‌کنند.»

...

«همین دو روز پیش فرمانده بسیج به ما گفت اگر امریکایی‌ها حمله کنند و ما در هر گونه تظاهراتی شرکت کنیم، در جا و به صورت صحرایی اعدام می‌شویم.»

به گفته این عضو بسیج در شمال ایران، فرمانده بسیج تاکید کرده است: «در دوران صلح، ما با شما به عنوان مجرم برخورد می‌کنیم و مثل حالا از رافت اسلامی بهره‌مند می‌شویم اما در دوران جنگ هر نوع تظاهراتی خیانت و کمک به دشمن است و شما مثل منافقین، سریع و در دادگاه صحرایی به اعدام محکوم می‌شویم.»

— ایران وایرگفت‌وگو با دو بسیجی: برای مقابله با شورش‌های شهری آموزش می‌بینیم

به خاطر دارم که در گیر و دار نوروز ۹۸، به صورت کاملاً اتفاقی در توییتر بحثی فی‌مایین چند کاربر را مشاهده نمودم مبنی بر ایجاد یا وجود گروه یا کانالی براندازانه در تلگرام که دیگران را تشویق به عضویت در آن می‌نمود. باید بگوییم با توجه به تجربیات شخصی و آگاهی از ناامنی بی‌حد این پیام رسان تا حدود زیادی نگران شدم. به دلیل صرف یکسال اوقات فراغت و هزینه شخصی، متوقف نمودن پروژه بازی که در دست توسعه داشتم بسیار سخت می‌نمود. اما پس از مدتی کلنجر رفتن با خود، به دلیل خلا آموزشی موجود در زمینه امنیت سایبری برای فعالان حقوق بشر، مدنی، سیاسی، روزنامه نگاران و براندازان، و به خصوص کابوس قربانی شدن هر روزه فرزندان پاک و دلیر ایران زمین، نظیر جاویدنامان [ستاربیهشتی](#)، [سیناقدیری](#)، [سارو قهرمانی](#)، [وحید صیادی نصیری](#)، و اخیرا جاویدنام [علیرضا شیرمحمدعلی](#) که با اتهامات سیاسی - امنیتی بازداشت، شکنجه و به دست نیروهای امنیتی در زندان‌های فرقه تبهکار به قتل رسیده اند، تصمیم به تغییر اولویت و تهیه و عرضه مفصل یک سری آموزشی امنیت سایبری گرفتم.

اگر من توانستم با ترکیبی از بخت و اقبال، دانش، و استراتژی زیرکانه، با پرداخت حداقل بهای ممکن در دام این سیستم غیرانسانی گرفتار نشوم، چرا دیگران نتوانند؟ حتی اگر مطالب عرضه شده در این مقالات باعث رهایی یا حفظ جان یک نفر از چنگال فرقه تبهکار شود، این مجموعه نوشتار به مقصود خود رسیده است.

از آنجایی که اولین مقاله از این سری، در مورد تلگرام می‌باشد، گفتگو راجع به سایر شیوه‌ها، تکنیک‌ها، و راهکارهای امنیتی مطرح شده را به مقالات بعدی از این مجموعه موكول می‌نماییم.

## سلب مسئولیت

در پایان این مقدمه نسبتاً طولانی اما ضروری، بایستی مجددًا خاطرنشان شوم که نگارنده خود را متخصص بی‌چون و چرای حوزه امنیت نمی‌داند؛ اما به دلیل تجربیات قبلی در حوزه امنیت، درک صحیح از اصول، مبانی و حداقل‌های حوزه امنیت سایبری، و همچنین تجربه بازداشت توسط نهادهای امنیتی جمهوری اسلامی، از شناخت موردنیاز و کافی جهت اظهارنظر در این زمینه برخوردار می‌باشد. این مطالب به همراه رعایت نکات و راهکارهای ارائه شده در آن‌ها، به وضوح برای شخص نگارنده در زمان بازداشت در نهادهای امنیتی جمهوری اسلامی مسمرثمر بوده است. این در حالی است، که به کار بستن محتویات این مقالات، بسته به شرایط، ممکن است برای شما سودمند یا زیان بار باشد. لذا، هیچ یک از عواقب استفاده از این مطالب و راهکارهای ارائه شده متوجه شخص نگارنده نمی‌باشد. بنابراین، با آگاهی کامل از تمامی عواقب و خطرات به کاربستان این مطالب و راهکارهای ارائه شده، مسئولیت کامل آن، فقط و فقط بر عهده استفاده کننده می‌باشد.

یادآور می‌شوم که مقاله حاضر و مقالات آتی در حوزه امنیت سایبری، علاوه بر توافق نامه فوق، از لیسانس مطالب منشر شده در این وب سایت (در انتهای تمامی صفحات)،

پیروی می نمایند. شما با ادامه مطالعه این مطلب و مطالب آتی، موافقت کامل خود با این توافق نامه را اعلام می نمایید:

تمامی محتویات این وب سایت تحت مجوز [CC BY-SA 3.0\) Creative Commons Attribution-ShareAlike 3.0 Unported License](#) منتشر شده است. همچنین، تمامی سورس کدهای منتشر شده در این وب سایت تحت لیسانس [MIT License](#) منتشر شده است، مگر آن که به صراحة ذکر شده باشد. تمامی محتویات ارائه شده صرفا جنبه آموزشی و اطلاعاتی داشته و قادر هرگونه ضمانت، تعهد یا شرایطی از هر نوع می باشد. بایستی توجه نمود که اطلاعات عرضه شده حتی ممکن است دقیق و یا بروز نباشد. هرگونه اطمینان به و یا استفاده از محتویات یا منابع منتشر شده در این وب سایت با مسئولیت مخاطب بوده و نگارنده یا نگارنده‌گان هیچ‌گونه مسئولیتی در مورد عواقب آن را نخواهند پذیرفت.

— ممدوو بابائی لیسانس مطالب منتشر شده در وب سایت

## آیا تلگرام به عنوان یک پیام رسان، امن است؟

آشنایی من با پیام رسان تلگرام به روزهای اولیه انتشار آن یعنی چندین ماه پیش از شنیده شدن زمزمه های اولیه فیلترینگ [پیام رسان واپر](#) در ایران و یک پیشنهاد کاری خارج از ایران در رابطه با توسعه یک نرم افزار پیام رسان امن، باز می گردد. دوستی که مطرح کننده پیشنهاد بود، نرم افزار تلگرام را به دلایل ذیل به عنوان الگوی توسعه معرفی نمود:

۱. متن باز بودن کلاینت تلگرام

۲. مستندات عالی [پروتکل](#) و [API](#) تلگرام

### ۳. قابلیت رمزگذاری سر تا سر یا End-to-end encryption

۴. جایزه سیصد هزار دلاری تعیین شده از سوی سازندگان تلگرام برای افرادی که موفق به شکستن الگوریتم رمزگاری تلگرام یعنی MTProto شوند

پس از نصب اولیه این پیام رسان، بایستی اعتراف کنم که با توجه به محدودیت های وایبر از جمله، نمایش شماره تلفن به سایر کاربران در گروه ها، محدودیت حجم ویدیوی آپلودی تا سقف ۱۰ مگابایت، و رابط گرافیکی نه چندان دلچسب آن، شدیدا عاشق تلگرام شدم. تلگرام از لحاظ تجربه کاربری فرسنگ ها از نرم افزارهای مشابه مانند وایبر، واتس اپ، لاین، وی چت و ... جلوتر بود. قابلیت ارسال فایل به تعداد نامحدود تا حجم ۱.۵ گیگابایت و ویژگی Broadcast که بعدها به کanal های تلگرام تغییر شکل یافت از دیگر ویژگی های منحصر به فرد آن بود که مرا هر چه بیشتر شیفته این پیام رسان نمود. این باعث شد که اطرافیان خود را تشویق به مهاجرت به تلگرام نمایم که به دلیل محبوبیت آن روزهای وایبر، در این امر تا حدود زیادی ناموفق بودم. تا آن که بلاخره وایبر به بهانه توسعه توسط یک شرکت اسرائیلی با همین نام، و اتهام شنود و جاسوسی، در ایران فیلتر شد و خیل عظیم کاربران ایرانی آن به سوی سایر پیام رسان ها از جمله تلگرام سرازیر شدند، تا آنجا که کاربران ایرانی، اکثریت قریب به اتفاق کاربران این پیام رسان نوظهور را تشکیل می دادند. هر چند که وایبر بعدها توسط شرکت ژاپنی راکوتون خریداری شد اما در ایران هرگز از فیلترینگ خارج نشد. به دلیل مارکتینگ بسیار قوی تلگرام به عنوان یک نرم افزار ایمن و متن باز، تا مدت ها با وجود عرضه پیام رسان های کاملا متن باز و ایمن تر مانند سیگنال، تلگرام همچنان پیام رسان شماره یک در تمامی دستگاه های دیجیتالی من بود. حتی فیلترینگ موقت تلگرام در اعتراضات گسترده دیماه ۹۶ و فیلترینگ قطعی تلگرام در اردیبهشت ماه ۱۳۹۷ مانع از استفاده کاربران از این پیام رسان محظوظ در ایران نشد. لازم به ذکر است که به شخصه، مدت بسیار کوتاهی پس از فیلترینگ قطعی آن در ایران، با استفاده از بات های تلگرام و API آن، راهکار خاص خود جهت ارسال و دریافت فایل و اطلاعات به / از تلگرام بدون نیاز به فیلترشکن را نیز توسعه دادم.

فارق از خیمه شب بازی های سال های اخیر مسئولان جمهوری اسلامی در قبال مسئله پیام رسان ها، ترجیح می دهم هر چه زودتر به سوالات اصلی و پاسخ آن ها بپردازیم.

- آیا تلگرام امن است؟

- متخصصین حوزه امنیت معتقدند که پاسخ به این سوال منفی است.

- آیا امکان جاسوسی و شنود داده های کاربران تلگرام توسط نهادهای امنیتی رژیم جمهوری اسلامی وجود دارد؟

- ظاهرا بله!

- اگر امکان دسترسی به داده های کاربران تلگرام توسط نهادهای امنیتی جمهوری اسلامی میسر شده است، این دسترسی چگونه فراهم شده؟ آیا ممکن است [معماری نرم افزاری](#) معیوب یا [اشکالات نرم افزاری](#) و یا حتی شیوه های غلط پیش گرفته شده توسط این پیام رسان مسبب اصلی این موضوع می باشد؟ آیا اصولا سازندگان تلگرام از این موضوع باخبرند؟

- همهممممممم، راستش را بخواهید پاسخ به این سوال بسیار سخت است. بایستی ابتدا به چیزهای دیگری بپردازیم.

## جوری توضیح بدہ که انگار من ۵ ساله

### هستم

پیش از پرداختن به مقوله امنیت تلگرام نیازمند آشنایی با یک سری مفاهیم حوزه امنیت، از جمله رمزگاری خواهیم بود که یقین دارم برای مخاطب عادی به سرعت پیچیده خواهد شد. لذا، اجازه دهید به منظور حفظ سادگی مطلب، به مد [EL15](#) یا [جوری توضیح بدہ که انگار من ۵ ساله هستم](#)، سویچ نماییم.

# Cryptography یا رمزگاری

تصور نمایید دو شخص ممدوو و فلور قرار است با هم چند پیام مخفی را رد و بدل کنند. آن ها فقط می توانند از طریق پست که بسیار نا امن است این کار را انجام دهند. چرا که هر فردی (مثلًا اداره پست، مامور پست، و یا حتی نهادهای امنیتی) می تواند پیام را در میانه راه بخواند، یا حتی متن پیام را دستکاری نموده و دوباره مهر و موم کند. جهت جلوگیری از این امر، ممدوو و فلور می توانند بر سر روشی مشترک (الگوریتم یا Algorithm) به منظور مبهم سازی (رمزگاری یا Cryptography) متن پیام استفاده نمایند. این پروسه مبهم سازی را رمزگاری می نامند. برای رمزگاری روش های متعدد ریاضیاتی وجود دارد که الگوریتم نامیده می شود. یکی از الگوریتم های بسیار ساده رمزگاری، الگوریتم روت ۱۳ یا ROT13 است که خود گونه ای از الگوریتم ساده تر رمز سزار یا Caesar cipher می باشد و در روم باستان توسعه داده شده است. جهت اعمال نمودن الگوریتم روت ۱۳ بر روی یک متن به زبان انگلیسی (عمل رمزگذاری یا Ciphering یا Encryption)، هر حرف از متن، با سیزدهمین حرف ما بعد از خود در جدول حروف الفبای انگلیسی جایگزین می شود. برای مثال، حرف A به حرف N، حرف B به حرف O، و ... تبدیل می شود. با توجه به این که زبان انگلیسی ۲۶ حرف دارد، اگر شما الگوریتم روت ۱۳ را مجددا بر روی متن رمزگذاری شده اعمال نمایید، به متن اصلی پیام خواهید رسید (عمل رمزگشایی یا Deciphering یا Decryption). فی الواقع، بر خلاف سایر الگوریتم ها، عمل رمزگذاری و رمزگشایی در روت ۱۳ یکی است. در رمزگاری، متن اصلی پیش از رمزگذاری را متن ساده یا Plaintext و متن پس از رمزگذاری را متن رمز یا Ciphertext می نامند. برای مثال، نمونه متن ذیل توسط الگوریتم روت ۱۳ رمزگذاری شده است (می توانید با یکی از ابزارهای [cryptii.com](http://cryptii.com) و یا [rot13.com](http://rot13.com) اقدام به رمزگذاری مton خود نمایید):

نمونه الگوریتم رمزگاری جانشینی روت ۱۳

Plaintext: The quick brown fox jumps over 13 lazy dogs.

Ciphertext: Gur dhvpx oebja sbk whzcf bire 13 ynm1 qbtf.

پیش از آنکه توسط متخصصین حوزه رمزگاری مورد حمله واقع شوم، توجه داشته باشد که روت ۱۳ در واقع یک **الگوریتم رمزگاری جانشینی** یا Substitution cipher می باشد. در این روش متن پیام با اعمال Encoding و به طبع آن Decoding (ایده ای ندارم مناسب ترین واژه جایگزین در زبان فارسی برای این دو چه می باشد) مبهم سازی می شود. در نتیجه، استفاده از واژه های Encryption/Decryption برای روت ۱۳ کاملاً اشتباه می باشد. تنها به دلیل حفظ سادگی مطلب برای مخاطب عادی، تصمیم به استفاده از این واژه ها گرفته ام. در واقع این متد یک راز نیست و هرگزی با دانستن نحوه کارکرد آن قادر به رمزگشایی متن پیام خواهد بود. بنابراین، امروزه برای محافظت از پیام های خصوصی کاربردی ندارد. الگوریتم های واقعی و صنعتی رمزگاری برای رمزگذاری و رمزگشایی (Encryption and Decryption) از چیزی تحت عنوان **کلید** یا Key استفاده می نمایند و بسیار پیچیده تر از روت ۱۳ می باشند.

## الگوریتم کلید متقارن یا Symmetric-key Algorithm

فلور تصمیم می گیرد که یک جعبه دارای قفل با دو کلید همسان (آن را جعبه متقارن خواهیم نامید) که فقط این دو کلید توانایی باز کردن آن را دارند، خریداری نماید. پس از آن پیام خود را جهت ارسال درون جعبه گذاشته، اما پس از قفل نمودن آن متوجه می شود که هیچ راه امنی برای رد و بدل نمودن کلید به همراه جعبه وجود ندارد؛ چرا که اگر کلید را به مامور پست بسپارد همیشه این احتمال وجود دارد که یک، مامور پست جعبه را باز نموده و داخل آن را مشاهد کند؛ و دو، این که می تواند یک کپی از کلید را جهت استفاده در دفعات بعدی ایجاد نماید. به عنوان تنها راه امن، اما نه چندان متقاعدة کننده، فلور تصمیم می گیرد که در یک کافه یا بار نزدیک با ممدوو قرار بگذارد و شخصاً یکی از کلید ها را به او بسپارد. هر چند این کار متقاعدة کننده به نظر نمی رسد و اسباب زحمت است، اما فلور تنها یکبار نیازمند انجام این کار می باشد.

از چه جهت می‌گوییم این روش امن است اما اسباب زحمت است یا متقادع کننده نیست؟

۱. این روش امن است به این دلیل که مامور پست نمی‌تواند جعبه را باز نماید. او امکان خواندن پیام را ندارد. بله، مامور پست حتی می‌تواند جعبه را دور بیاندازد اما به هیچ وجه امکان خواندن آن را ندارد.

۲. حالا فرض کنید فلور و ممدوو در دو سمت اقیانوس باشند. دیدار حضوری این دو بسیار سخت تر، پر زحمت تر، و هزینه برتر خواهد بود. که استفاده از این روش را در پاره‌ای از موقع نامناسب و غیر متقادع کننده می‌سازد.

حالا این سوال پیش می‌آید که در دنیای واقعی، مامور پست ممکن است با استفاده از هر وسیله ممکن، از جمله پتک، دریل، ... اقدام به باز نمودن جعبه نماید. یا مثلاً برخی جعبه‌ها ممکن است دارای شاه کلید باشند که امکان بازکردن تمامی جعبه‌ها از آن مدل خاص را دارد. آیا در رمزگاری چنین چیزی امکان پذیر است؟ باید بگوییم که تصور شما کاملاً درست و سوال به جایی است. هر نوع جعبه (الگوریتم رمزگاری)، نقاط ضعف و قوت خود را دارد، همین طور هر الگوریتم رمزگاری. برخی جعبه‌ها یا الگوریتم‌ها ضعف‌های شناخته شده ای دارند و در مقابل برخی حملات (پتک، دریل، ...) آسیب پذیر می‌باشند. برخی الگوریتم‌ها (جعبه‌ها) در حال حاضر امن هستند، یا آسیب پذیری و حملات به آن‌ها در حد تئوری باقی مانده است. اما ممکن است در آینده به دلیل کارآمدی بهتر ابزارها (کامپیوترها) و یا ارائه ابزارهای جدید (کامپیوتراهای کوانتمی) به سادگی شکسته شوند مگر آنکه از اساس به شکل مقاوم در برابر کوانتم طراحی شده باشند. مثلاً الگوریتم استاندارد و بسیار موفق "استاندارد رمزگاری پیشرفته" یا AES (سرنام Advanced Encryption Standard) که - به افتخار توسعه دهنگان بلژیکی آن - تحت عنوان رینداو یا Rijndael هم شناخته می‌شود در برخی از گونه‌های خود مانند AES-128 و AES-192 داری حملات شناخته شده در برابر کوانتم هستند. اما، اوضاع برای AES-256 در میان مدت مقداری بهتر است.

به عنوان یک مثال واقعی، آن هایی که با خصوصیات فنی بیت کوین آشنا هستند به خوبی می دانند که الگوریتم رمزنگاری آن یعنی [ECDSA 256](#)، به احتمال قریب به یقین با تجارتی سازی کامپیوترهای کوانتومی حداکثر ظرف یک دهه آینده شکسته خواهد شد که به دلیل نقصان امنیتی باعث بی ارزش شدن کامل بیت کوین خواهد شد. به همین دلیل ارزهای دیجیتال جایگزین مانند [The Quantum Resistant Ledger](#) یا [QRL](#) که از اساس به منظور مقاومت در برابر حملات کوانتومی طراحی شده اند، ابداع شده است.

نکته دیگر مقوله شاه کلید می باشد که نه تنها در مورد جعبه ها صدق می نماید بلکه در برخی از الگوریتم های رمزنگاری، تعمدا از سوی توسعه دهنده و یا پیشنهاد دهنده آن، یا حتی به درخواست آژانس های اطلاعاتی با اعمال فشار یا پرداخت رشوه، در اصطلاح رمزنگاری آن [درب پشتی](#) (معادل شاه کلید)، گنجانده می شود. اگر فکر می کنید که این مورد از حس تئوری توطئه من یا دیگران برخواسته است، باید نامیدتان کنم. به عنوان نمونه، [ظاهرها](#) [RSA](#) پرداخت ۱۰ میلیون دلار رشوه به شرکت [RSA](#) (گزارش تکمیلی بر اساس تحقیقات یکساله گروهی از اساتید دانشگاه جان هاپکینز)، تولید کننده الگوریتم نامتقارن [RSA](#) (جلوتر به این نوع از الگوریتم ها خواهیم پرداخت) را متقادع می سازد تا در کتابخانه [BSafe](#) از محصولات این شرکت، الگوریتم داری آسیب پذیری [Dual\\_EC\\_DRBG](#) را به عنوان الگوریتم تولید اعداد تصادفی پیش فرض قرار دهد (دقیقت داشته باشید که بر خلاف انسان ها، کامپیوترها در تولید اعداد تصادفی که اساس رمزنگاری می باشد بسیار بد عمل می کنند؛ این موضع از آن جهت حائز اهمیت است که احتمال حدس زدن و شکسته شدن یک الگوریتم رمزنگاری را بسیار بالا می برد) که باعث آسیب پذیر شدن بخش عمده ای از سرورها و دستگاه های متصل به اینترنت شده است. در این مورد، موضوع پرداخت رشوه، توسط کارمندان سابق [RSA](#) تایید شده است.

**رمزنگاری** **Cryptography** **و** **نامتقارن** **یا** **رمزنگاری** **کلید** **عمومی** **یا** **Public-key**

# Asymmetric Cryptography

این بار به دنبال راه حلی منطقی تر، فرض را بر این بگذاریم که فلور و ممدوو هرگز نیازی به ملاقات نداشته باشند. ممدوو یک قفل به همراه کلید مطابق با آن را خریداری می نماید. پس از آن، ممدوو کلید را نزد خود نگاه داشته، اما قفل را در حالت باز به وسیله پست برای فلور ارسال می نماید. فلور یک جعبه ساده بدون قفل را که توانایی قفل شدن با یک قفل دلخواه را داشته باشد (آن را جعبه نامتقارن می نامیم) خریداری نموده و پیام خود را درون آن قرار می دهد. سپس، جعبه را با قفلی که ممدوو برایش ارسال کرده قفل نموده و از طریق پست جعبه را برای ممدوو ارسال می نماید. حالا به این دلیل که راهی جهت گشودن قفل وجود نخواهد داشت، فلور می تواند خاطر جمع باشد که مامور پست توانایی خواندن پیام را نخواهد داشت. زمانی که جعبه به دست ممدوو برسد، او می تواند با کلیدی که در اختیار دارد جعبه امن را باز نموده و پیام را بخواند.

توجه داشته باشید که این روش تنها برای فرستادن پیام های یک طرفه کاربرد خواهد داشت. البته به عنوان یک راه حل احتمالی، فلور هم می تواند درست مانند ممدوو، قفل و کلید خود را خریداری نموده، سپس، با حفظ کلید خود، قفل خریداری شده را برای ممدوو ارسال نماید. با این روش، هر دو طرف، امکان ارسال پیام با قفل فرد دیگر را به صورت دو طرفه خواهند داشت.

## ترکیب رمزنگاری متقارن و نامتقارن

راه حل دیگر، ترکیب دو روش فوق به منظور ارسال پیام خواهد بود. به جای فرستادن پیام در جعبه نامتقارن با قفل ارسال شده توسط ممدوو، فلور می تواند یکی از کلیدهای جعبه متقارن را درون جعبه نامتقارن قرار داده، با قفل ارسالی ممدوو آن را قفل نموده و برای ممدوو ارسال نماید. از این به بعد چون طرفین، هر کدام مالک یکی از کلیدها هست، رد و بدل پیام ها می توانند فقط توسط جعبه متقارن انجام شود.

در مثال فوق، قفل ها نقش کلیدهای عمومی را دارند؛ کلیدهای قفل های عمومی، به دلیل آن که در نزد هر شخص باقی می ماند، نقش کلیدهای خصوصی در رمزنگاری را خواهند داشت. جعبه ها هم نقش الگوریتم های رمزگذاری را ایفا می نمایند.

در دنیای واقعی، رمزنگاری با کلید عمومی یا نامتقارن به دلیل محاسبات بسیار پیچیده تر، به حد غیر قابل تصوری پرهزینه تر از رمزنگاری متقارن می باشد. درست مانند راه حل مثال آخر، از این نوع رمزگذاری فقط برای ارسال کلید رمزنگاری متقارن، به منظور آغاز تماس استفاده می شود. پس از آن، جهت ارتباط و ارسال و دریافت پیام از رمزنگاری متقارن که بهینه تر می باشد استفاده می شود. جهت جا افتادن موضوع و راضی نگه داشتن متخصصین امر در حوزه رمزنگاری، اجازه دهید به مثال فوق بازگردیم و تصویر را به شکل دقیق تری ترسیم نماییم تا از لحاظ فنی هم معنادارتر شود.

ممدوو، یک جفت کلید شامل کلید عمومی خود (قفل قرمز) و یک کلید خصوصی (کلید قرمز) را ایجاد می نماید. پس از آن، ممدوو کلید عمومی خود (قفل قرمز) را منتشر می نماید و فلور آن را بدست می آورد (ممدوو قفل خود را از طریق پست برای فلور ارسال می نماید). سپس، فلور یک کلید متقارن موقتی (یک جفت کلید نارنجی) را ایجاد نموده و با استفاده از کلید عمومی ممدوو (قفل قرمز) آن (یکی از کلیدهای نارنجی) را به روشی ایمن (جعبه نامتقارن) برای ممدوو ارسال می نماید. در این مرحله، ممدوو با استفاده از کلید خصوصی خود (کلید قرمز)، کلید متقارن ارتباطات آتی (کلیدهای نارنجی) را بدست می آورد. از این به بعد ممدوو و فلور می توانند با استفاده از کلیدهای متقارن (نارنجی)، بدون نگرانی از افشاری پیام های خصوصی، اقدام به ارسال و دریافت پیام (با جعبه متقارن) نمایند.

در واقع هر بار که شما از یک وب سایت یا سرور ایمیل، یا یک پیام رسان امن با پشتیبانی از پروتکل [SSL/TLS](#) استفاده می نمایید، داستان ممدوو و فلور تکرار می شود. برنامه مرورگر، ایمیل خوان، یا پیام رسان شما نقش فلور را بازی می کند و سروری که به آن متصل می شوید نقش ممدوو را.

# رمزگذاری سر تا سر یا End-to-end Encryption

اجازه دهید مقداری به روز تر فکر کنیم. فلور و ممدوو قصد دارند پیام های خود را به جای یک جعبه با استفاده از یک پیام رسان رد و بدل کنند. اگر پیام رسان قابلیت پشتیبانی از رمزگذاری را نداشته باشد پیام ها را به اصطلاح به شکل Cleartext یا متن واضح ارسال می نماید که مطلوب نیست؛ چرا که هر کسی در هر یک از نقاط اتصال فی مابین ممدوو و فلور، از جمله افراد حاضر در شبکه داخلی، شرکت سرویس دهنده اینترنت، هکرها، آژانس های اطلاعاتی و ... می توانند متن، صدا یا تصاویر ارسالی از طریق اینترنت را، در میانه راه مشاهده نمایند.

حالا فرض کنیم که این دو، از یک پیام رسان با پشتیبانی از قابلیت رمزگذاری جهت رد و بدل نمودن پیام استفاده می نمایند. تا حدود زیادی مشکلات امنیتی مربوط به شنود توسط افراد یا سازمان های ثالث کاهش می یابد. هر چند که این احتمال هنوز صفر نیست!

چرا این احتمال صفر نیست؟ سوال خوبی است. چون برنامه پیام رسان فقط داده را مابین دستگاه کامپیوتر ممدوو و سرور برنامه پیام رسان رمزگذاری می نماید. درون سرور پس از رمز گشایی، مجدداً پیام رمزگذاری شده و به دستگاه تلفن همراه فلور ارسال می شود. در این بین شرکت عرضه کننده برنامه پیام رسان توانایی خواندن پیام موردنظر و حتی تهیه کپی از آن درون یک پایگاه داده را خواهد داشت. حتی اگر شرکت سازنده برنامه پیام رسان نخواهد از داده شما کپی تهیه نماید یا آن را شنود کند، ممکن است نهادهای امنیتی و اطلاعاتی به دلیل قدرتی که دارند به شکل قانونی یا غیرقانونی شرکت سازنده پیام رسان را مجبور به ارائه ابزار شنود یا تهیه کپی از چت های شما نمایند. برای نمونه این اتفاق در مورد [لوابیت](#)، یکی از سرویس دهنگان ایمیل در آمریکا افتاد که با وجود رای دادگاه، لدار لویسون بنیانگذار شرکت، حاضر به تسليم نمودن اطلاعات ایمیل [ادوارد اسنودن](#) به دولت آمریکا نشد و در نتیجه آن، کسب و کارش را از دست داد. البته بر اساس قوانین برخی کشورها مانند آمریکا، سوئد و ... هنگامی که داده های شما از داخل

خاک آن ها می گزدد، آژانس های اطلاعاتی به شکل قانونی توانایی و حق رهگیری آن داده را دارند. حتی قانون به آن ها حق مطالبه کلیدهای خصوصی رمزگاری یا کلیدهای متقارن را داده است. بنابراین، بسیاری از شرکت های تکنولوژیک مجبور به همکاری با نهادهای امنیتی و اطلاعاتی در کشورهای مورد فعالیتشان هستند، در غیر اینصورت ممکن است مانند لاوابیت کسب و کار خود را از دست دهند. در واقع در این روش، شرکت سرویس دهنده پیام رسان، مانند مامور پستی است که کلید جعبه ای که حمل می کند را در اختیار دارد. اگر رئیس او بخواهد محتوای جعبه ارسالی فی مایبن فلور و مدمدو را مشاهده نماید و مامور پست از در اختیار گذاشتن کلید و محتویات آن طفره رود، به احتمال زیاد او اخراج خواهد شد.

پس از این وقایع، به جهت دور زدن این مشکل و حفظ حریم خصوصی کاربران، برخی سرویس دهنده ها اقدام به ارائه قابلیت رمزگذاری سرتا سر نمودند. در این روش، در هر یک از دستگاه های مدمدو و فلور، یک جفت کلید رمزگاری نامتقارن (کلید و قفل قرمز برای مدمدو؛ کلید و قفل آبی برای فلور) ایجاد می شود. دقت داشته باشید که به جز کلیدهای عمومی (قفل های آبی و قرمز)، کلیدهای خصوصی (کلیدهای آبی و قرمز) هیچ وقت به سرور ارسال نخواهند شد و فقط بر روی دستگاه های مدمدو و فلور باقی خواهند ماند (مگر آن که شیطنتی از سوی شرکت سازنده پیام رسان صورت گرفته باشد و مخفیانه در کنار داده های رمزگذاری شده، کلیدها را به سرور ارسال نماید). کلید رمزگاری متقارن (کلید نارنجی) در دستگاه طرف آغاز کننده تماس ایجاد شده و با استفاده از کلیدهای نامتقارن (آبی و قرمز) یکبار برای همیشه با استفاده از رمزگاری نامتقارن جابجا شده و پس از آن این کلید فقط در دستگاه های فلور و مدمدو وجود خواهد داشت. از این به بعد فلور و مدمدو قادر به ارسال و دریافت پیام های کاملاً امن از دستگاه مبدا به دستگاه مقصد، بدون نگرانی از خوانده شدن آن ها خواهند بود. چرا که حتی اگر آژانس های اطلاعاتی از شرکت سرویس دهنده، کپی داده های این دو یا شنود آن را درخواست کنند با داده های رمزگاری شده مواجه خواهند شد که بدون حضور کلید رمزگشایی، کاملاً بلا استفاده خواهد بود (حداقل تا زمانی که امکان شکستن الگوریتم رمزگاری استفاده شده فراهم شود). درست مانند مامور پستی که جعبه قفل شده را در اختیار دارد، اما چون

کلید آن را ندارد حتی اگر رئیس او درخواست کلید را داشته باشد به این دلیل که کپی کلید را در اختیار ندارد، رئیس او بهانه‌ای جهت توبیخ او نخواهد یافت.

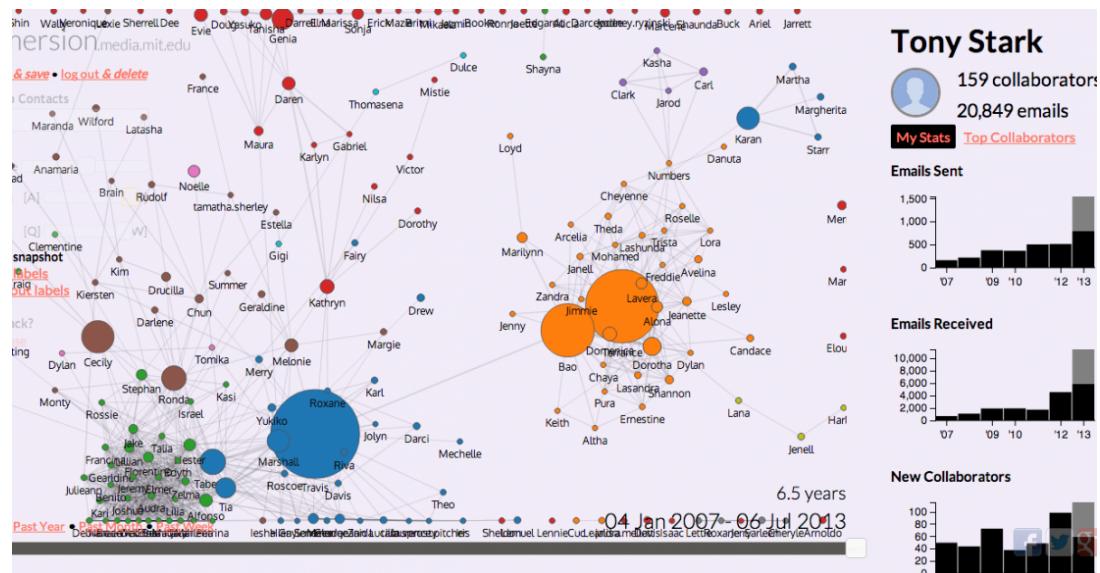
به دلیل انجام عمل رمزگذاری و رمزگشایی داده‌ها در مبدا و مقصد، این روش را رمزگذاری سر تا سر می‌نامند.

## متادیتا

**متادیتا یا فراداده** به داده‌هایی اطلاق می‌شود که داده‌های دیگر را توصیف یا تشریح می‌نماید. به عبارت دیگر، داده‌هایی هستند درباره داده‌های دیگر. برای مثال در یک تماس تلفنی، داده‌ها، خود مکالمه و کلمات رد و بدل شده میان طرفین می‌باشد. اما متادیتها، شماره تلفن‌های طرفین، طول زمان مکالمه، چه کسی تماس گیرنده بوده، نام اپراتورهای تلفن همراه یا ثابت درگیر تماس، موقعیت جغرافیایی طرفین تماس و ... می‌باشد. در واقع در بسیاری از مواقع ارزش متادیتها از خود داده‌های اصلی بیشتر می‌باشد. باور کنید یا نه، متادیتها در همه جا حضور دارند، اما ممکن است تا به حال متوجه آن‌ها و اهمیت شان نشده باشید؛ حتی در دنیای واقعی. به عنوان یک مثال پیش‌پا افتاده، زمانی که از یک مقاله چاپ شده در روزنامه صحبت می‌کنیم، متادیتها، نام روزنامه، صفحه روزنامه، تاریخ چاپ، نویسنده، تعداد کلمات و ... می‌باشد.

کاربرد اصلی متادیتا، کاوش، بازیابی، دسترسی، کشف، مستندسازی، ارزیابی و انتخاب می‌باشد. برای مثال زمانی که شما یک فایل ویدیویی را در کامپیوتر، تلویزیون هوشمند، یا گوشی خود پخش می‌نمایید، نرم افزار پخش فایل ویدیویی، بدون اسکن کردن تمام فریم‌های داخل فایل ویدیویی از طریق متادیتها به حجم فایل ویدیویی، طول زمان پخش، سایز تصویر، کیفیت تصویر و صدا، زبان زیرنویس پیش‌فرض داخل فایل و ... پی‌برده و بی‌درنگ با استفاده از این اطلاعات، بدون کاوش نمودن کل فایل، اقدام به پخش فایل و نمایش برخی داده‌ها در رابط کاربری خود می‌نماید.

اما برای درک بهتر مفهوم متادیتا در امنیت و ارتباطات دیجیتال، اجازه دهید **ابزار متن بازی تحت عنوان MIT Immersion** جهت به نمایش گذاشتن ارزش و خطر متادیتها در دانشگاه MIT توسعه داده شده و در اختیار عموم قرار گرفته است را معرفی نمایم. با صدور اجازه دسترسی توسط شما به صندوق پست الکترونیک تان، این ابزار بدون کاوش نمودن عنوان یا متن پیام ها، تنها با کاوش قسمت To, Cc و زمان دریافت یا ارسال آن ها، اقدام به ترسیم نقشه ارتباطات شما با دیگران می نماید:



نمونه ای از متادیتای استخراج شده توسط MIT Immersion از یک صندوق پست الکترونیکی

تصویر نمونه فوق که توسط این ابزار ترسیم شده است ممکن است برای بسیاری از افراد تداعی کننده چیز خاصی نباشد؛ اما، این تصویر حاصل کاوش و پردازش تعداد ۲۰,۸۴۹ پیام در صندوق پستی آقای تونی استارک و کشف روابط میان ۱۵۹ مشارکت کننده می باشد.

این ابزار اقدام به ترسیم ارتباطات آقای استارک با هر شخص به شکل یک دایره می نماید. میزان ارتباطات آقای استارک با اندازه دایره نسبت مستقیم دارد؛ به این معنی که هر چه دایره بزرگتر باشد یعنی تعداد پیام رد و بدل شده میان آقای استارک و آن شخص بیشتر می باشد و بالعکس؛ هر چه ارتباطات کمتر، دایره هم کوچک تر. سپس با جزیره بندی

ارتباطات مشترک، پی به روابط میان هر گروه می برد. هر کدام از دایره های هم رنگ یک جزیره می باشد که معمولا نزدیک به یکدیگر ترسیم می شود. حالا اگر دایره بزرگی با کمترین یا بدون یک خط اتصال به سایر دایره ها وجود داشته باشد، این احتمال قوی وجود دارد که یک ارتباط مشکوک میان آقای استارک و آن فرد، که به خوبی مخفی نگه داشته شده، کشف شده باشد. علاوه بر آن، در آنالیز تصویر فوق، برای مثال می توان پی برد که در جزیره یا تیم نارنجی، به ترتیب کاربران Laver, Jimmie و در نهایت Dorotha احتمالا مهم ترین افراد جزیره ارتباطی خود می باشند. در نتیجه اگر آقای تونی استارک فرد مظنون باشد و یک آژانس امنیتی پس از بررسی متادیتا اینباکس آقای استارک به تصویر فوق رسیده باشد، احتمال این که سه کاربر فوق نیز جزو مظنونین اصلی باشند بسیار زیاد است. بدین ترتیب با شناسایی تیم ها و رهبران آن ها، دایره مظنونین اصلی محدودتر، جستجو هدفمندتر و از نظر تخصیص منابع کم هزینه تر و به صرفه تر خواهد بود.

فی الواقع کلید اصلی تجسس های آژانس های امنیتی، متادیتا می باشد که با کمک آن، ابتدا تماس ها و الگوی فی مابین آن ها، و سپس روابط، به سادگی شناسایی و طبقه بندی می شود. پس از طی نمودن مرحله شناسایی در صورت نیاز بر روی استخراج داده اصلی (در این اینجا محتوای پیام های رد و بدل شده) تمرکز می شود. ذکر این نکته ضروری است که این مورد ساده ترین کاربرد متادیتا در امور تجسس می باشد، در واقع کسی نمی داند که نهادهای امنیتی دقیقا چه داده هایی را جمع آوری می نمایند و چه داده های دیگری با پردازش آن ها کشف می شود.

با توجه به حجم عظیم داده های روزانه ای که آژانس ها و نهادهای امنیتی با آن مواجه هستند، بدون حضور و بهره گیری از متادیتها و ویژگی های آن ها، کاوش، پردازش و یافتن و استخراج اطلاعات اصلی که این سازمان ها به دنبال آن هستند، به طرز دیوانه واری غیرقابل تصور خواهد بود.

اگر هنوز در مورد خطرات متادیتها و ارزش بسیار بالای آن ها مت怯اعد نشده اید، فرض کنید که شما یک تصویر به ظاهر بی خطر را با گوشی تلفن همراه خود ثبت نموده، سپس

آن را در یک شبکه اجتماعی ارسال نموده اید. باز هم فرض را بر این بگذاریم که افراد یا سازمان هایی به دنبال محل اختفای شما باشند. به یکباره این افراد در محل اختفای شما سبز می شوند. هاااا! شرط می بندم اصلاً انتظارش را نداشتید!

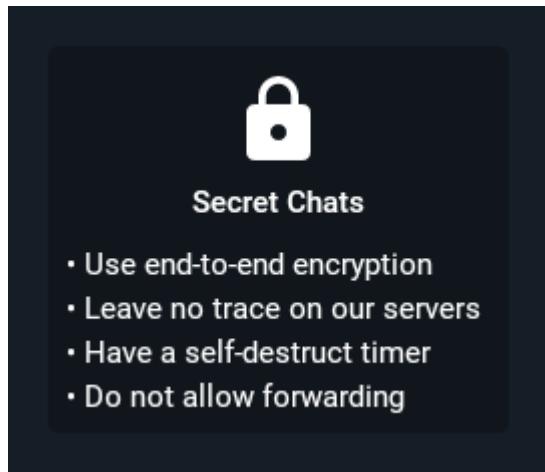
امروزه به طور معمول گوشی های تلفن همراه پس از ثبت عکس از طریق دوربین، متادیتاهای خاصی تحت عنوان [اکسیف](#) را در فایل تصویر ثبت می نمایند که بسیاری از کاربران تلفن های هوشمند از حضور این متادیتاهای در فایل های تصویرشان مطلع نیستند. یکی از متادیتاهای یاد شده مختصات جغرافیایی محل ثبت تصویر می باشد که با کمک تراشه [جی پی اس](#) موجود در تلفن همراه شما استخراج و در فایل عکس ثبت می شود. افراد یا سازمان هایی که به دنبال شما هستند به سادگی با نگاه انداختن به این قسمت از فایل تصویر موقعیت جغرافیایی ثبت تصویر - و به احتمال زیاد شما - را کشف می نمایند؛ مگر آنکه خودتان با واقف بودن به این موضوع با ابزارهای ویرایش تصویر اقدام به حذف یا تغییر این متادیتاهای نموده باشید. البته برخی از شبکه های اجتماعی با اطلاع از خطرات یاد شده، به شکل خودکار اقدام به حذف این متادیتاهای نمایند.

در نهایت در چنین مواقعي، به دليل سهل انگاری یا عدم آشنایي و شناخت کافي تکنولوژي، مقصراً اصلی شما خواهيد بود و نه کس دیگر! در واقع هیچ کس جز خود شما به امنيت شما اهميتي نخواهد داد، در غير اينصورت شركت هاي تکنولوژيک و به شكل سهل انگارانه و گستردگه اقدام به ثبت ردپا شما از طریق ثبت متادیتاهای نمودند.

## مشکل تلگرام دقیقاً چیست؟

بسیار خب، پس از آشنایی با مفاهیم اولیه رمزگذاری و متادیتا، قصد داریم مشکلات امنیتی تلگرام به عنوان یک پیام رسان را بررسی نماییم.

## عدم رمزگذاری سر تا سر بصورت پیش فرض



یک چت مخفی تلگرام که بصورت پیش فرض غیرفعال می باشد

یکی از قابلیت های بسیار خوب تلگرام در زمینه امنیت، [قابلیت Secret Chats](#) یا چت های مخفی می باشد. متاسفانه [با ارائه چندین دلیل غیرمتقاude کننده از سوی سازندگان تلگرام](#) این قابلیت به صورت پیش فرض غیرفعال می باشد. اجازه دهید جمله بندی ام را [تغییر دهم](#):

هیچ دلیل قانع کننده ای برای غیرفعال نمودن قابلیت رمزگذاری سر تا سر وجود ندارد؛ به خصوص توسط نرم افزاری که شعار و برنداش امنیت بوده و خود را یک برنامه پیام رسان آمن معرفی می نماید!

مشکل دقیقا همین جاست! بسیاری از کاربران تلگرام به دلیل تبلیغات اشتباه آن، تصور می کنند که ارتباطات و چت های آن ها کاملا رمزگذاری شده است، در حالی که این گونه نیست و آن ها نمی دانند برای این کار باید مراحل بیشتری را طی نموده و کارهای دیگری انجام دهند. در [صفحه آغازین وب سایت](#) آن ها با وجود اشاره به: "پیام های تلگرام به شدت رمزگذاری می شوند و می توانند خود را از بین ببرند." هیچ اشاره ای به چت های مخفی نشده است!



## Private

### Telegram messages are heavily encrypted and can self-destruct.

تبلیغات حریم خصوصی و رمزگذاری در صفحه آغازین تلگرام

این دقیقا همان چیزی است که آژانس و نهادهای های امنیتی و یا هکرها خواهند. در واقع امر، به دلیل عدم آشنایی عمده افراد به جزئیات فنی رمزگاری و تکنولوژی پیام رسانها، اکثریت کاربرانی که از این واقعیات و تنظیمات پیشگیرانه آگاهی ندارند - که تعدادشان ابدا هم کم نیست - آسیب پذیر خواهند بود. این برخلاف نظرات تقریبا تمامی متخصصان حوزه امنیت و رمزگاری است. این در حالی است که [قسمت سوالات متدائل](#) تلگرام خود را امن تر از واتس اپ می داند:

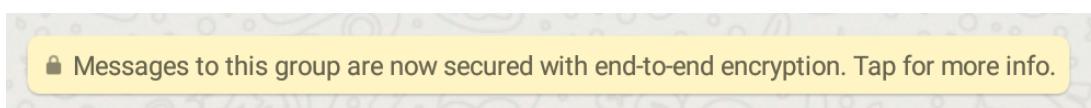
🔒 Messages to this chat and calls are now secured with end-to-end encryption. Tap for more info.

پشتیبانی از رمزگذاری سرتا سر و فعال بودن پیش فرض آن در چت های واتس اپ

راستش را بخواهید خیلی سعی کردم که مقایسه تلگرام و واتس اپ را با توجه به این نکته که تیم بازاریابی واتس اپ ابداً این محصول را به عنوان امن ترین پیام رسان ممکن تبلیغ نمی‌کنند، نادیده بگیریم. اما باید بگوییم که واتس اپ در این زمینه از تلگرام بهتر عمل نموده است. حتی [نرم افزار لاین هم در سال ۲۰۱۶ به صورت پیش فرض این قابلیت را فعال نموده است](#).

## عدم پشتیبانی از رمزگذاری سرتا در چت‌های گروهی

علاوه بر غیرفعال بودن پیش فرض قابلیت رمزگذاری سرتا در چت‌های فردی تلگرام، چت‌های گروهی تلگرام هیچ وقت از قابلیت رمزگذاری سرتا به امروز که حدوداً شش سال از عرضه آن می‌گذرد، پشتیبانی ننموده است. و به نظر نمی‌رسد که هیچ‌گاه این قابلیت به تلگرام اضافه شود. این در حالی است که واتس اپ نه تنها از قابلیت رمزگذاری سرتا در چت‌های گروهی پشتیبانی می‌نماید، بلکه این قابلیت به صورت پیش فرض نیز فعال می‌باشد:



پشتیبانی از رمزگذاری سرتا سر و فعال بودن پیش فرض آن در چت‌های گروهی  
واتس اپ

## عدم رمزگذاری سرتا در نسخه دسکتاپ و وب

اگر هنوز نالمید نشده‌اید، خبر بد دیگر این که، چنان‌چه از نسخه دسکتاپ این پیام رسان یا نسخه وب آن استفاده می‌نمایید، به هیچ وجه امکان استفاده از چت‌های مخفی حتی جهت ارسال پیام‌های فردی را به دلیل عدم پشتیبانی از این قابلیت،

نخواهید داشت. بازهم این در حالی است که پیام رسان واتس اپ علاوه بر نسخه موبایل، از این ویژگی هم در نسخه دسکتاپ و هم نسخه وب خود بهره می‌گیرد.

## عدم ارائه حق انتخاب به کاربران جهت خروج از کlad تلگرام

اگر از کنار تصمیم سهل انگارانه سازندگان تلگرام جهت غیرفعال نمودن پیش فرض رمزگذاری سر تا سر، و عدم پشتیبانی از آن در چت های گروهی و نسخ دسکتاپ و وب بگذریم، تحت هیچ عنوانی نمی توان از کنار عدم ارائه حق انتخاب به کاربران جهت خروج از کlad تلگرام، به سادگی گذشت. به صورت پیش فرض، تلگرام تمامی داده های شما شامل چت های انفرادی، چت های گروهی، فایل های عکس، صوتی، تصویری، و یا مستندات ارسال شده توسط شما را در کlad خود ذخیره می نماید. شاید از نقطه نظر بسیاری از کاربران این ویژگی بسیار سودمند به نظر برسد (به خصوص این که کاربر هر زمان که نیاز داشته باشد می تواند این داده ها را بازیابی نماید). اما، از نظر متخصصان حوزه امنیت این یک نقصان امنیتی بسیار بزرگ است.

چرا متخصصین امر تاکید دارند که این نه تنها یک ویژگی نیست، بلکه یک نقصان امنیتی بزرگ است؟ سوال خوبی است. اگر فراموش نموده اید یا هیچ وقت این خبر را نشنیده اید، بایستی هک آی کlad اپل توسط هکرها و در نتیجه انتشار گسترده تصاویر کاملاً برهنه و خصوصی بیش از ۵۰۰ فرد برجسته هنری و سینمایی (بیشتر بازیگران زن هالیوودی) در آخرین روز آگوست ۲۰۱۴ را به شما یاد آور شوم. این اتفاق بی سابقه در میان کاربران اینترنت با عنوان The Fappening که با ترکیب کلمات fap (اصطلاح عامیانه خوددارضائی) و فیلم The Happening محصول سال ۲۰۰۸ ابداع شده است، شناخته می شود.

در صورت هک احتمالی کlad تلگرام، به نظر شما بهترین راه حل پیشگیرانه جهت عدم انتشار داده های کاربرانی که اولویت آن ها امنیت است نه سادگی بازیابی، چیست؟

آفرین! مطمئنم که درست حدس زدید: عدم ذخیره داده های این دسته از کاربران در کلاد تلگرام یا ارائه قابلیتی جهت غیرفعال نمودن و خروج از آن!

بله سازندگان تلگرام ادعا می کنند که داده های نگهداری شده کاربران در کلاد این شرکت رمزگذاری می شود، اما همگی میدانیم که اگر هکرها توانسته اند به اطلاعات آی کلاد [اپل](#) دست بیابند، استخدام هکرهای این چنینی توسط دولت های ثروتمندی نظیر جمهوری اسلامی که هم اکنون ۹ درصد منابع طبیعی دنیا را در اختیار دارند، جهت هدف قراردادن کلاد کمپانی بسیار کوچک تر تلگرام، به هیچ وجه دور از ذهن نیست!

علاوه بر آن اگر امکان نفوذ به سرورهای تلگرام توسط هکرها فراهم شود، چه چیزی مانع دستیابی هکرها به کلیدهای رمزگاری ذخیره شده در این سرورها خواهد شد؟

اضافه کنم که در تلگرام اگر فرد یا سازمانی بتواند شبکه تلفن همراه را متقادع کند که شماره تلفن شما را در اختیار دارد (که توسط نهادهای امنیتی به سادگی قابل انجام است)، تلگرام تمامی داده های شما شامل پیام ها، فایل ها، مستندات، و لیست تماس ها را به دستگاه آن ها انتقال خواهد داد و آن ها توانایی دسترسی و خواندن همه چیز را خواهند داشت. این در حالی است که ممکن است شما هرگز از این موضوع باخبر نشوید. مزیت نرم افزارهایی مانند سیگنال و واتس آپ به دلیل عدم ذخیره این داده ها در کلاد در اینجا مشخص می شود. حتی اگر این نرم افزارها داده ها را به کلاد منتقل می نمودند به دلیل استفاده پیش فرض از رمزگذاری سر تا سر باز هم امکان رمزگشایی این داده ها در این پیام رسان ها وجود نخواهد داشت.

این یک خطر واقعی است! در ۹ ژوئن ۲۰۱۹، [اینترسپت](#) پیام های لو رفته تلگرامی مابین وزیر دادگستری برزیل و دادستان های برزیلی را منتشر نمود. فرضیه این بود که این نفوذ یا توسط [مبادله سیم کارت](#) و یا حمله کامپیوترا، انجام شده است. حمله تعویض سیم کارت با بهره برداری از قابلیت شبکه تلفن همراه جهت انتقال شماره تلفن به یک سیم کارت دیگر انجام می شود. این ویژگی به طور معمول زمانی استفاده می شود که مشتری سیم کارت یا تلفن خود را گم نموده است. البته با بهره گیری از احراز هویت دو

عاملی و اختصاص کلمه عبور برای کلاد در تلگرام تا حدودی می‌توان از چنین دسترسی‌های غیرمجازی جلوگیری نمود. اما، با توجه به مفهوم Rubber-hose cryptanalysis که پیش‌تر تشریح نمودیم، می‌دانیم در صورت در اختیار داشتن شخص شما، استخراج کلمه عبور از یک انسان کار چندان سختی نخواهد بود. حتی اگر گوشی تلفن همراه شما در دسترس نباشد، در چنین شرایطی دسترسی به داده‌های شما به سادگی محقق خواهد شد.

حالا سوال اساسی اینجاست که چرا سازندگان تلگرام اصرار بر ذخیره سازی داده‌های تمامی کاربران دارند و یا اجازه خروج از کلاد یا غیرفعال نمودن آن را نمی‌دهند؟ سوال خوبی است، اما من پاسخ دقیقی برای این سوال ندارم؛ تنها می‌توانیم بر سر آن گمانه زنی نماییم. پس ادامه مطلب را از دست ندهید!

## انتقال داده‌های لیست تماس تلفن همراه به کلاد

### تلگرام

پس از ثبت شماره تلفنتان در پیام رسان تلگرام، کافیست تنها یکبار به آن اجازه دسترسی به لیست تماس تلفن همراه خود را فراهم سازید. این اجازه می‌دهد تا تلگرام یک نقشه شبکه اجتماعی عظیم از همه کاربران و اینکه چگونه و تا چه حد یکدیگر را می‌شناسند، ایجاد نماید. حتی اگر شما اجازه دسترسی تلگرام به لیست تماس خود را فراهم نسازید، به این دلیل که شماره تلفن تماس شما به عنوان یک شناسه قابل ردیابی، در لیست تماس سایر افرادی که شما را می‌شناسند و به آن اجازه دسترسی داده‌اند، اطلاعات بسیار زیادی در مورد نحوه ارتباط شما با دوستانتان را بر ملا می‌سازد ([مبحث متادیتاها را به خاطر دارید؟](#)). در واقع ناشناس ماندن از دید شبکه تلگرام یا افرادی که ممکن است به شبکه آن‌ها نفوذ کنند، به دلیل آپلود لیست تماس سایر افرادی که شما را می‌شناسند تقریباً غیرممکن است. حتی اگر شما اکانت تلگرام ندارید و هیچ وقت عضو آن نبوده‌اید!

لیست های تماس بسیار ارزشمند هستند. ظاهرا آژانس های اطلاعاتی زحمات و هزینه هایی فراوانی را جهت به دست آوردن لیست های تماس از پیام رسان ها متحمل شده اند. در تلفن های همراه، لیست تماس ها حتی بسیار بالرتبه ترند، زیرا تطابق دادن آن ها با هویت آدم ها در دنیای واقعی و مجازی، به حد بسیار احتمانه ای ساده است.

## نیاز به شماره تلفن جهت ثبت نام

معمولًا دولت ها برای دنبال نمودن سوابق شهروندان به آن ها یک شماره اختصاصی نظیر کدملی را اختصاص می دهند. کدملی یک شناسه یا کلید جهت تگ کردن داده های یک فرد در ادارات و ارگان های مختلف خواهد بود که کار ذخیره، بازیابی، و پردازش داده ها را ساده تر می نماید. یک شماره تلفن نه تنها یک شناسه بسیار قوی جهت [رهگیری](#) داده های افراد و ارتباطات آن ها خواهد بود، بلکه هر فردی با دسترسی به [دکل های بی](#) تی اس قادر به یافتن موقعیت جغرافیایی و فیزیکی شخص مرتبط با آن شماره خواهد بود. اگر باور نمی کنید، کافیست [اپلیکیشن OpenSignal](#) یا یک برنامه مشابه را برای [اندروید](#) یا [آی اواس](#) نصب نمایید. این اپلیکیشن ها به شما اجازه یافتن محل دکل بی تی اس را خواهند داد. مشخصا عکس این عمل و رهگیری دستگاه موبایل با شماره تلفن موردنظر، توسط نهادهای امنیتی که ابزارهای بهتری از یک اپلیکیشن موبایل را در اختیار دارند، کار چندان سختی به نظر نمی رسد.

پرسیدن این سوال ضروری به نظر می رسد؛ تلگرام که ادعا می کند، احترام به حریم خصوصی و امنیت را سرلوحه کار خود قرار داده است، چرا مانند به عنوان مثال برنامه [اسکاپ](#)، به جای شماره تلفن قابلیت ثبت نام با یک آدرس ایمیل [یا حتی بدون آن](#) را به شما نمی دهد؟

## عدم پشتیبانی از رمز یکبار مصرف آفلاین

به طور معمول سرویس های آنلاین، جهت استفاده از احراز هویت دو عاملی، از پیامک یا تماس تلفنی جهت ارسال کد یکبار مصرف استفاده می نماید. با توجه به خطرات استفاده

از پیامک یا تماس تلفنی به دلایلی که پیش تر ذکر شد، بسیاری از سرویس های آنلاین اجازه استفاده از رمز یکبار مصرف آفلاین از طریق یک اپلیکیشن که بر روی یک گوشی یا دستگاه خاص نصب می شود را فراهم نموده اند. مزیت این مدل رمز یکبار مصرف این است که آسیب پذیری های روش ارسال از طریق پیامک در مورد آن ها صدق نمی کند. حتی به دلیل عدم نیاز به اتصال و ارسال و دریافت اطلاعات از / به سرور یا اینترنت، امنیت بسیار قابل قبول تری را فراهم می نمایند.

در مورد شخص من در زمان بازداشت، زمانی که آن ها قصد ورود به اکانت [جی میلم](#) را داشتند، با خیال راحت پسورد جی میل خود را در اختیار آن ها قرار دادم (البته آن ها اطلاعی هم نداشتند که من به جای استفاده از سرویس های ایمیل عمومی نظیر جی میل، میل سرور شخصی خود را راه اندازی نموده و نگهداری می نمایم). آن ها ابتدا ادعا کردند که به ایمیل من وارد شده اند و داده های زیادی در مورد من کشف نموده اند. اما، در بازجویی های بعدی گفتند که چرا رمز یکبار مصرف را توسط پیامک دریافت نمی کنیم؟ در واقع آن ها نمی دانستند که گوگل این رمز را هیچ وقت ارسال نخواهد نمود و من از رمز یکبار مصرف آفلاین استفاده می نمایم. من هم ادعا می نمودم که نمی دانم مشکل از کجاست.

در مقالات بعدی، به تفصیل راجع به این تکنولوژی صحبت خواهیم نمود. فقط به خاطر داشته باشید که تلگرام از این قابلیت پیش پا افتاده که توسط اکثر سرویس ها و نرم افزارهای آنلاین مانند توییتر، [فیسبوک](#)، گوگل، [ایнстاگرام](#) و ... پشتیبانی می شود، پشتیبانی نمی نماید.

## عدم توانایی تایید هویت طرفین در چت های مخفی

سناریویی را فرض کنید که یکی از طرفین توسط نهادهای امنیتی دستگیر شده یا توسط افرادی ربوده شده باشد، یا این که آن افراد مطابق آن چه قبلا گفته شد توانایی متقادع نمودن شبکه تلفن همراه را برای جاذب خود به جای یکی از طرفین مکالمه داشته باشند.

شما چگونه می توانید مطمئن باشید که طرف یا طرفین دیگر مکالمه واقعا افراد مورد نظر شما هستند؟

متاسفانه چنین ویژگی در تلگرام وجود ندارد. این در حالی است که سیگنال و واتس اپ مدت هاست که قابلیت تایید هویت طرفین مکالمه با استفاده از اعداد امن یا کیوآر کد را در رابط کاربری خود جای داده اند.

شاید این ویژگی برای بسیاری از کاربران پر اهمیت نباشد، اما افرادی که نیاز به امنیت حداقلی در ارتباطات خود داشته باشند می توانند یکبار یکدیگر را ملاقات نموده و پس از تبادل کلیدها، مطمئن باشند که شیطنتی در ارتباطات آن ها صورت نخواهد گرفت. در سیگنال، کاربران حتی قابلیت چرخش و تعویض کلیدها، بدون از دست دادن پیام ها را خواهند داشت.

## شبکه های تحويل محتوا یا CDN تلگرام در ایران

چنان چه به قسمت سوالات متداول برای کاربران فنی تر در وب سایت تلگرام (که کاملا به زبان انگلیسی است) مراجعه نمائید، در میان متن پرسش و پاسخ های این صفحه بسیار بلند، یک لینک فارسی در قسمت شبکه های تحويل محتوا (CDN) رمزگاری شده خودنمایی می کند:

### Encrypted CDNs

As of Telegram 4.2, we support encrypted CDNs for caching media from public channels with over 100.000 members. The CDN caching nodes are located in regions with significant Telegram traffic where we wouldn't want to place Telegram servers for various reasons.

For technical details of the implementation, encryption and verification of data, [see the CDN manual](#).

See [this document](#) for a Persian version of this FAQ.

بخش فارسی

لینک فارسی در قسمت شبکه های تحويل محتوا (CDN) رمزگاری شده در وب سایت پیام رسان تلگرام

وجود تنها یک صفحه مستندات فارسی در وب سایت تلگرام به همراه یک پست به زبان فارسی از آقای پاول دورف کمی عجیب به نظر می رسد. چرا فقط زبان فارسی و نه زبان دیگر؟ چرا فقط مستندات مربوط به "شبکه های تحويل محتوا رمزنگاری شده"؟

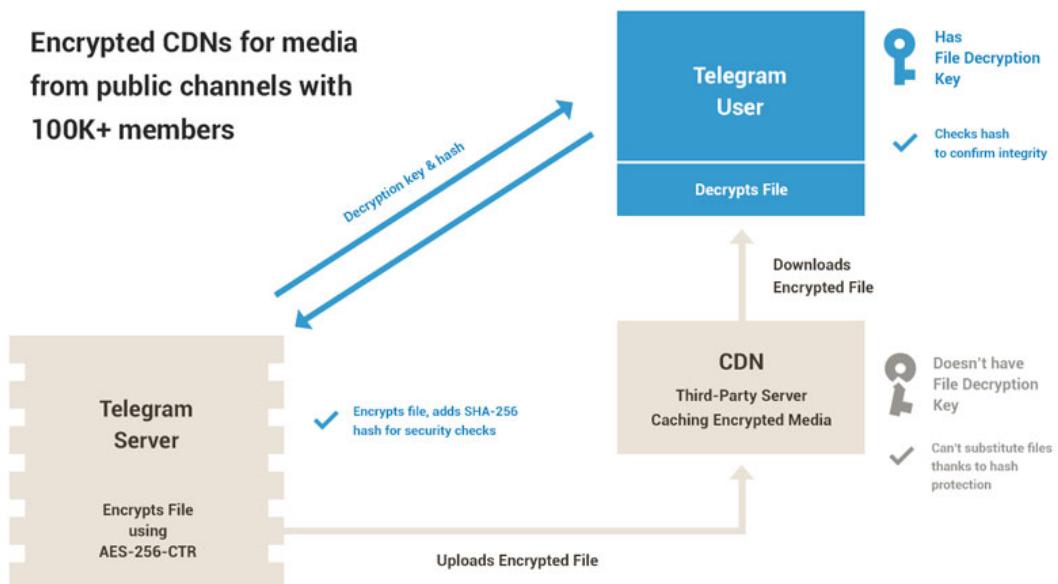
احتمالا دلیل ارائه این بخش از مستندات به زبان فارسی و تاکید پاول دورف در پست فارسی مبنی بر این بودن شبکه های تحويل محتوا تلگرام، به تنش های متعدد ایجاد شده میان مسئولان جمهوری اسلامی در زمان وزارت محمود واعظی در سمت وزیر ارتباطات و فناوری اطلاعات باز می گردد، که برای مدتی در سر تیتر خبرها بود. یکی از تنش های ایجاد شده بر سر [انتقال سرور تلگرام به ایران](#) بود، که در نهایت با توافق های صورت گرفته منجر به برپایی شبکه های تحويل محتوا تلگرام (نه سرور) در ایران شد. تا این که در نهایت [پاول دورف با توبیت نمودن یک پست در توبیت اقدام به شفاف سازی](#)

در این زمینه نمود:

اگر تاکنون با یک تله کلیک با عنوان "تلگرام سرورهای خود را به ایران / کره شمالی / موردور منتقل نموده" مواجه شده اید، این را بخوانید

با وجود این که سرور های تلگرام به ایران منتقل نشد، موضوع انتقال شبکه های توزیع محتوا، کماکان مایه نگرانی فعالان حوزه اینترنت بوده است. برای مثال توجه شما را به **NetFreedom** مهندی یحیی نژاد موسس بالاترین و **Pioneers** در این رابطه در وب سایت **AzerNews** جلب می نمایم.

به شخصه کد منبع کلاینت های تلگرام را مطالعه ننموده ام. اما بر اساس دیاگرام رسمی نحوه کارکرد شبکه های تحویل محتوای تلگرام، این پیام رسان از شبکه های تحویل محتوا تنها به منظور ذخیره سازی فایل های کanal های عمومی با بیش از یک صد هزار عضو و دسترسی سریع تر کاربران به این فایل ها، استفاده می نماید. بر اساس این دیاگرام، هیچ گونه داده خصوصی بر روی شبکه های توزیع محتوا ذخیره نخواهد شد. همچنین این شبکه ها به کلیدهای رمزگشایی دسترسی ندارند. و در نهایت از تابع **Hash** به منظور تایید اصالت فایل ها استفاده می نمایند که امنیت قابل قبولی را مهیا می نماید:



نحوه کارکرد شبکه های توزیع محتوای رمزگذاری شده تلگرام برای فایل های چندرسانه ای به اشتراک گذاشته شده در کanal های عمومی با بیش از یک صد هزار عضو

علیرغم تمامی تمهیدات امنیتی اندیشیده شده برای شبکه های تحویل محتوای تلگرام، هنوز یک **پاشنه آشیل** و آسیب پذیری جدی وجود دارد. مطابق با نمودار فوق، نرم افزار

تلگرام نصب شده در دستگاه کاربران، اقدام به دریافت مستقیم فایل ها از شبکه های توزیع محتوا می نماید که باعث به جای ماندن رد پای کاربر در شبکه های توزیع محتوا خواهد شد. هر فرد یا سازمانی که به شبکه های توزیع محتوا دسترسی فیزیکی داشته باشد می تواند با استفاده از متادیتای [نشانی آی پی](#)، اقدام به شناسایی مختصات جغرافیایی کاربران نماید. علاوه بر آن پس از مرتبه ساختن نشانی های آی پی به کاربران، آن ها دقیقاً متوجه می شوند که کدام فایل های صوتی - تصویری، عکس ها و یا مستندات، توسط کدام کاربر با نشانی آی پی مشخص شده دیده شده است.

حساسیت این موضوع بدین جهت است که برای مثال، کanal عمومی آمدنیوز که توسط نهادهای امنیتی حکومت ایران مسبب اصلی شعله ور شدن تظاهرات بی سابقه دیماه ۹۶ شناخته می شود، در زمان اعتراضات دیماه ۹۶ بیش از یک میلیون و دویست هزار عضو داشته است. بر اساس شرایط منتشر شده توسط تلگرام برای میزبانی فایل های کanal های عمومی در شبکه های تحويل محتوا، یعنی داشتن بیش از یک صد هزار عضو، آمدنیوز کاندید قطعی میزبانی بر روی شبکه های توزیع محتوا بوده است. این بدان معنی است که احتمالاً قابلیت رصد دسترسی کاربران به داده های به اشتراک گذاری شده در این کanal، در آن زمان برای نهادهای امنیتی در ایران مهیا بوده است.

در صورت استفاده شما از اینترنت ADSL، نقطه به نقطه، اینترنت تلفن های همراه، معمولاً در [خدمات دهنده اینترنت](#) یا اپراتور تلفن همراه مورد استفاده شما، یک اکانت با نام کاربری و پسورد، و یا شماره تلفن مختص شما ثبت شده است. چنان چه در چنین شرایطی دستگیر شوید، با کشف نحوه دسترسی شما به اینترنت و درخواست نهادهای امنیتی، این شرکت ها موظف به در اختیار گذاشتن تاریخچه دسترسی اینترنتی شما خواهند بود، که مطابقت دادن این تاریخچه با درخواست های ارسال شده شما جهت مشاهده فایل های میزبانی شده کanal های عمومی مانند آمدنیوز چندان دشوار به نظر نمی رسد. البته تمامی این ها به شرطی است که شما اقدام به دریافت نشانی آی پی اختصاصی از سرویس دهنده اینترنت خود ننموده باشید، در غیر اینصورت به دلیل

اختصاص مستقیم آن نشانی آی پی به شما، حتی نیازی به درخواست داده ها و متادیتاهای شما از این شرکت ها نیز نمی باشد.

حتی در سناریوی دیگر، آن ها می توانند کار ردیابی و تفکیک کاربران با استفاده از طبقه بندی آی پی ها را انجام داده، سپس برای درخواست های خاص به شبکه های تحويل محتوا، اطلاعات کاربر مرتبط با آن درخواست ها را مطالبه نماید. این از آن جهت بد است که ممکن است فردی از اطرافیان شما سابقه فعالیت های سیاسی یا حقوق بشری را داشته باشد. با استفاده از این اهرم جهت اعمال فشار به آن شخص، آن ها شواهد مورد نیاز جهت نشانه رفتن انگشت اتهام به سوی شما را خواهند داشت.

البته اگر از یک فیلترشکن امن جهت دسترسی به تلگرام استفاده نمایید (برخی از فیلترشکن های عمومی یا خصوصی خریداری شده به هیچ وجه امن نمی باشند، به همین دلیل از واژه امن استفاده می نمایم؛ در مقالات آتی به این دسته از فیلترشکن ها خواهیم پرداخت)، این آسیب پذیری بر استفاده شما از تلگرام و کanal های عمومی اثر گذار نخواهد بود و با خاطر جمع می توانید این کanal ها را دنبال نمایید. به خصوص این که در حال حاضر تلگرام در ایران فیلتر می باشد، در نهایت کاربران مجبور به استفاده از فیلترشکن می باشند که در این حالت شبکه های توزیع محتوا اثری بر امنیت کاربران نخواهند داشت.

## نشت متادیتا

متاسفانه یکی از نقصان های جدی امنیتی در پیام رسان تلگرام، نشت متادیتا می باشد. به عنوان یک مثال، در سال ۲۰۱۶ میلادی یک محقق امنیتی متوجه شد که یک هکر به راحتی می تواند زمان آنلاین یا آفلاین بودن یک کاربر خاص در تلگرام را به راحتی تشخیص دهد. این آسیب پذیری به هکر اجازه خواهد داد که متوجه شود شما با چه کسی در یک لحظه خاص در حال گفتگو هستید. این موضوع زمانی بدتر می شود که هکر حتی نیازی به شنود ۲۴/۷ شما نخواهد داشت، بلکه از طریق اعلان فراهم شده توسط تلگرام، از زمان آنلاین شدن شما با خبر خواهد شد.

```
User [REDACTED] online (was online [2015/11/27 22:28:54])
User [REDACTED] offline (was online [2015/11/27 22:24:22])
User [REDACTED] online (was online [2015/11/27 22:29:27])
User [REDACTED] offline (was online [2015/11/27 22:24:31])
User [REDACTED] online (was online [2015/11/27 22:29:38])
User [REDACTED] offline (was online [2015/11/27 22:24:45])
User [REDACTED] online (was online [2015/11/27 22:29:51])
User [REDACTED] offline (was online [2015/11/27 22:24:58])
```

نشت متادیتا در تلگرام

نکته تاسف بار این است که با انجام یک تنظیم ساده در این پیام رسان کاربران قادر به جلوگیری از این آسیب پذیری و عواقب آن خواهند بود. که به دلیل عدم نمایش این متادیتاها غیرضروری در رابط کاربری، آن ها هرگز متوجه آن نشده و بازهم قربانی تنظیمات پیش فرض تلگرام می شوند. جالب تر این که برای دسترسی به این متادیتاها نیاز به ابزار چندان عجیب و غریبی نیز نمی باشد؛ بلکه با ابزار متن باز و رایگان [vysheng/tg](#) خودتان قادر به آزمایش صحت این موضوع می باشد.

## مشکلات پروتکل MTProto

با توجه به برندینگ بسیار عالی تیم مارکتینگ تلگرام، تقریبا اکثر کاربران این پیام رسان نام پروتکل MTProto را شنیده و به خوبی می دانند که امنیت تلگرام بر روی این پروتکل متمرکز است. ابتدائی ترین و مهم ترین قانونی که تمامی متخصصین حوزه امنیت بر سر آن توافق دارند و به تمامی افراد تازه وارد در این زمینه به شکل پی در پی گوشزد می شود، قانون مهمی است تحت عنوان “[Never Roll Your Own Crypto](#)“، به این معنی که “هرگز الگوریتم رمزنگاری خود را نپیچید“؛ به خصوص این که اگر شما یک متخصص حوزه رمزنگاری آموزش دیده و متبحر نیستید. این اولین درس دوره های امنیت کامپیوتر ۱۵۱ در دوره های تخصصی امنیت است.

بنابر اذعان [اکانت رسمی تلگرام در هکر نیوز](#)، مشخصا آن ها متخصص حوزه رمزنگاری نیستند:

*The team behind Telegram, led by Nikolai Durov, consists of six ACM champions, half of them Ph.Ds in math. It took them about two years to roll out the current version of MTProto. Names and degrees may indeed not mean as much in some fields as they do in others, but this protocol is the result of thoughtful and prolonged work of professionals.*

تیم پشت تلگرام به رهبری نیکولاوی Durov، متشکل از شش قهرمان مسابقات بین‌الملی برنامه نویسی دانشجویی است، که نیمی از آنها دکترای ریاضیات هستند. برای آن‌ها حدود دو سال طول کشید تا نسخه فعلی MTProto را منتشر کنند. نام و مدرک تحصیلی در واقع ممکن است در برخی از زمینه‌ها به همان اندازه که در سایر زمینه‌ها اهمیت دارد، معنی نداشته باشد، اما این پروتکل نتیجه کار طولانی و متکرانه حرفه‌ای هاست.

*TelegramApp Telegram - secure, free messaging –*

وات د فاز! دکترهای ریاضیات متخصص حوزه رمزگاری نیستند! پروتکلی که آن‌ها ابداع کرده اند به حتم یقین ناقص و آسیب پذیر است. اگر باور نمی‌کنید شما را به مقاله تخصصی نوشته شده توسط Geoffroy Couprie متخصص و مشاور حوزه امنیت و معماری نرم افزار، تحت عنوان: تلگرام، با نام مستعار "عقب باستید، ما دکترهای ریاضیات داریم!" ارجاع می‌دهم، که اتفاقاً در بخش کامنت‌های آن، مناظره اکانت رسمی توییتر تلگرام و نویسنده مقاله بیش از پیش خواندنی می‌نماید. در واقع آن‌ها یک پروتکل سرهم کرده اند. از نظر یک متخصص حوزه رمزگاری این دیوانه وارترین کار ممکن است.

مشکل دیگر پروتکل MTProto چیزی است که در میان متخصصین حوزه رمزگاری تحت عنوان Security through obscurity (امنیت از طریق ابهام) شناخته می‌شود. در واقع

به این دلیل که سایرین از جزئیات پروتکل MTProto خبردار نیستند، این پروتکل اصل Kerckhoffs's principle یا کرکهوفس را زیر پا گذاشته است که هر چه بیشتر این پروتکل را از منظر امنیتی غیرقابل اتکا می‌سازد.

علاوه بر این‌ها، تلگرام یک چالش نسبتاً مضحك را با تعیین جایزه سیصدهزار دلاری برای شکستن پروتکل MTProto برگزار کرده است. از این‌جهت مضحك که شرایطی که آن‌ها برای این چالش تعیین نموده‌اند، حتی شکستن ضعیف‌ترین پروتکل‌های رمزنگاری را غیرممکن می‌سازد. مکسی مارلینسپایک، کارآفرین، متخصص حوزه رمزنگاری، محقق امنیت کامپیوترا، رئیس سابق تیم امنیتی توییتر، بنیان‌گذار اوپن‌ویسپر سیستمز، موسس و مدیرعامل سیگنال، و درنهایت یکی از خالقان پروتکل رمزنگاری سیگنال که توسط تمامی کارشناسان خبره حوزه رمزنگاری مورد ستایش قرار گرفته و در پیام‌رسان‌های سیگنال، واتس‌اپ، پیام‌رسان فیسبوک، اسکایپ، و گوگل ال‌او در جهت رمزگذاری سر تا سر به کار گرفته شده است، در مقاله‌ای در وبلاگ خود به تفصیل به شرح مغلطه‌ای که اساس این مسابقه بوده، پرداخته است.

اگر هنوز هم در نامن بودن پروتکل MTProto شک دارید، در تاریخ نهم ژانویه ۲۰۱۵ یک حمله و آسیب پذیری برای MTProto در تلگرام معرفی شد که حتی چت‌های مخفی را هم تحت تاثیر قرار می‌دهد.

علاوه بر آسیب پذیری فوق، یک Paper جدید نشان می‌دهد که MTProto به دلیل عدم رعایت IND-CCA امن نیست.

تمامی این‌ها به کنار، نه فقط هکرهای حرفه‌ای، آژانس‌های اطلاعاتی، و ... بلکه حتی دانشجویان فارغ التحصیل نشده دانشگاه MIT هم قدرت به چالش کشیدن امنیت آن را دارند. جهت اطلاعات بیشتر این پرسش و پاسخ در سایت Quora مبنی بر ایرادات نسخه دوم پروتکل MTProto را مشاهده نمایید.

## ابهام در مدل درآمدزاپی تلگرام

یکی از قابلیت های تلگرام که آن را به خط شکن در زمینه ارسال و دریافت فایل ها تبدیل کرد، اجازه آپلود فایل تا حجم ۱.۵ گیگابایت به دفعات نامحدود، جهت به اشتراک گذاری در چت ها، گروه ها و کanal ها می باشد. این فایل ها هیچ وقت از کlad تلگرام حذف نمی شوند، حتی فایل هائی که چند سال پیش آپلود شده اند. قطعاً این فضای نامحدود نیازمند تامین هزینه هارد دیسک های فیزیکی، سرور، الکترونیکی و جهت روشن نگه داشتن سرور و در نتیجه در دسترس بودن فایل ها می باشد.

با توجه به تعداد بیش از **۲۰۰ میلیون کاربر فعال در مارس ۲۰۱۸** و رشد سالانه بیش از **۵۰ درصد در آگوست ۲۰۱۷** باقیمانده این سرویس در انتهای ماه مارس ۲۰۱۹، به حداقل **۳۰۰ میلیون کاربر فعال رسیده باشد** که با توجه به اعلام مدیر عامل این شرکت مبنی بر ثبت نام **۳ میلیون کاربر تنها در ۲۴ ساعت در ۱۴ مارس ۲۰۱۹**، به هیچ وجه گمانه زنی غیر معقولی به نظر نمی رسد.

بدون در نظر گرفتن فایل های به اشتراک گذاشته شده در کanal ها، اگر هر کاربر به طور متوسط ماهیانه **۱۰ گیگابایت** داده را به اشتراک بگذارد (حدود **۳۴۱/۳۳ مگابایت** داده در روز برای هر کاربر که به عنوان متوسط آپلود با در نظر گرفتن سلیقه ها و کاربری های متفاوت کاربران این سرویس، تخمین معقولی می باشد)، میزان فضای ذخیره سازی مورد نیاز جدید در هر ماه به شرح ذیل می باشد:

**۱۰ گیگابایت داده برای هر کاربر در ماه  $\times$  **۳۰۰ میلیون کاربر = ۳,۰۰۰,۰۰۰,۰۰۰** گیگابایت  
داده جدید در هر ماه**

یا به عبارتی **۳,۰۰۰,۰۰۰ ترابایت داده جدید در هر ماه**

یا به عبارتی **۳,۵۰۰ پتابایت داده جدید در هر ماه**

یا به عبارتی **۳ اگزابایت داده جدید در هر ماه**

با توجه به هزینه های تهیه و نگهداری سرور، شامل الکتریسیته، سخت افزار سرور، RAID به منظور **تحمل پذیری خطا**، مشخصا هزینه ساخت و برقی دیتا سنتر مقرن به صرفه نخواهد بود. از طرفی پس از برنامه فیلترينگ تلگرام در روسیه [۱][۲] مشخص شد که سرویس تلگرام بر روی **سرویس های وب آمازون** و **گوگل کلاد** میزبانی می شود. به منظور سادگی محاسبات و پرهیز از گمانه زنی بیشتر، با توجه به حجم داده های ماهانه پیام رسان تلگرام، و واقع شدن مقر اصلی این شرکت در برلین آلمان، **قیمت ۰/۰۲۲۵ دلار در هر گیگابایت داده در شهر فرانکفورت برای AWS** را در نظر خواهیم گرفت:

### Storage pricing

Region: EU (Frankfurt) ▾

#### Pricing

##### S3 Standard Storage

First 50 TB / Month	\$0.0245 per GB
Next 450 TB / Month	\$0.0235 per GB
Over 500 TB / Month	\$0.0225 per GB

تعرفه فضای ذخیره سازی استاندارد S3 بر روی سرویس های وب آمازون

در نتیجه، با فرض عدم افزایش کاربران پیام رسان تلگرام، فقط هزینه فضای ذخیره سازی جدید در هر ماه به شرح ذیل خواهد بود:

۳,۰۰۰,۰۰۰,۰۰۰ گیگابایت داده افزوده شده در هر ماه  $\times ۰/۰۲۲۵$  دلار در هر یک گیگابایت = ۶۷,۵۰۰,۰۰۰ دلار هزینه جدید در ماه

این هزینه در ماه اول ۶۷,۵۰۰,۰۰۰ دلار، در ماه دوم ۱۳۵,۰۰۰,۰۰۰ دلار، در ماه سوم ۲۰۲,۰۰۰,۰۰۰ دلار و ... تا این که در ماه دوازدهم به مبلغ ۸۱۰,۰۰۰,۰۰۰ دلار می رسیم. این یعنی این که این شرکت با فرض ثابت ماندن تعداد کاربران تلگرام و عدم رشد آن در هرسال، علاوه بر هزینه سال های قبل بایستی هشتصد و ده میلیون دلار هزینه جدید برای تامین فضای ذخیره سازی خود صرف نماید.

بنابر پرسش و پاسخ مطرح شده در قسمت سوالات متدالو تلگرام:

*.We believe in fast and secure messaging that is also 100% free*

*Pavel Durov, who shares our vision, supplied Telegram with a generous donation, so we have quite enough money for the time being. If Telegram runs out, we will introduce non-essential paid options to support the infrastructure and finance developer salaries. But making profits will never be an end-goal for Telegram*

ما به پیام رسانی سریع و ایمن اعتقاد داریم که ۱۰۰٪ رایگان نیز باشد.

**پاول دورف**، که چشم انداز ما را به اشتراک می‌گذارد، تلگرام را با کمک مالی سخاوتمندانه خود تامین نموده است، بنابراین در حال حاضر به اندازه کافی پول داریم. اگر تلگرام کم بیاورد، ما گزینه‌های پرداخت غیر ضروری را جهت حمایت از زیرساخت‌ها و حقوق و دستمزد‌های توسعه دهنده‌گان معرفی خواهیم نمود. اما سوددهی هرگز یک هدف غایی برای تلگرام نخواهد بود.

?telegram.org Q: How are you going to make money out of this –

با توجه به محاسبات فوق و اظهارات سازندگان تلگرام، به علاوه **ارزش خالص اعلام شده برای پاول دورف** توسط **فوربز** یعنی مبلغ ۲.۷ بیلیون دلار در لحظه فعلی، چگونه ایشان توانایی تامین هزینه‌های فوق را خواهند داشت؟

البته اگر میزان متوسط فایل‌های آپلود شده در هر ماه برای هر کاربر را به یک دهم یعنی ۱ گیگابایت در ماه یا معادل ۳۴.۱۳ مگابایت در روز کاهش دهیم، که بسیار غیرمعقول به

نظر می رسد، آن وقت به مبلغ ۸۱,۰۰۰,۰۰۰ دلار هزینه جدید ذخیره سازی در هر سال می رسمیم که احتمالاً توسط پاول دورف قابل تامین می باشد.

گمانه زنی در مورد فضای ذخیره سازی تلگرام و اظهارات سازندگان آن، این احتمال سوال را در ذهن تداعی می کند که آیا تلگرام در حال حاضر با بهره گیری از یک منبع مالی بی پایان، مانند برخی از استارتاپ‌ها یا کمپانی‌های حوزه تکنولوژی در حال زیان دهی صرف است؟

## تحویل داده‌های کاربران به مقامات قضایی در صورت دریافت دستور دادگاه

پس از فیلترینگ گسترده تلگرام در روسیه، این کمپانی در آگوست ۲۰۱۸ اعلام نمود که تغییراتی را در سیاست حفظ حریم خصوصی خود اعمال نموده است:

*If Telegram receives a court order that confirms you're a terror suspect, we may disclose your IP address and phone number to the relevant authorities. So far, this has never happened. When it does, we will include it in a semiannual transparency report published at:*

[.https://t.me/transparency](https://t.me/transparency)

اگر تلگرام یک حکم دادگاه دریافت کند که تأیید می نماید شما یک مظنون تروریست هستید، ممکن است ما آدرس آی پی و شماره تلفن شما را به مقامات مربوطه افشا نماییم. تا کنون این هرگز رخ نداده است. هنگامی که رخ دهد، ما آن را در یک گزارش شفاف سازی نیم سالانه منتشر شده در <https://t.me/transparency> قرار خواهیم داد.

خب؛ واقعیت امر گمان نمی کنم ارتباط دادن فعالیت های براندازنه یا حتی مذهبی، سیاسی و عقیدتی در جمهوری اسلامی به تروریسم برای مقامات و نهادهای قضایی یا امنیتی جمهوری اسلامی چندان کار دشواری باشد. باید منتظر ماند و نحوه واکنش تلگرام به درخواست های آتی مقامات جمهوری اسلامی از طریق دستور دادگاه در آینده را مشاهده نمود.

## موضوع پرداخت رشوه یا اعمال فشار

در ماه ژوئن ۲۰۱۷، پاول دورف ادعا نمود که در زمان بازدید توسعه دهنگان این شرکت از آمریکا در سال ۲۰۱۶، آژانس های اطلاعاتی ایالات متحده دو بار تلاش نموده اند تا با پرداخت رشوه به آن ها اقدام به تضعیف رمزگذاری این پیام رسان نمایند. پاول دورف حتی ادعا نمود که [اداره تحقیقات فدرال \(FBI\)](#) شخص وی را تحت فشار قرار داده است:



Pavel Durov ✅  
@durov

Replying to @yashalevine

During our team's 1-week visit to the US last year we had two attempts to bribe our devs by US agencies + pressure on me from the FBI.

4:15 PM - 11 Jun 2017

469 Retweets 446 Likes

25 469 446

در مدت زمان بازدید تیم ما از ایالات متحده در سال گذشته ما با دو تلاش جهت پرداخت رشوه به توسعه دهنگانمان از سوی آژانس های [اطلاعاتی] ایالات متحده به علاوه فشار بر [شخص] خودم از سوی اداره تحقیقات فدرال مواجه شدیم.

پیش تر از آن، در تاریخ ۲۰ اکتبر ۲۰۱۵، پاول دوروف با فاصله زمانی کوتاه در اکانت رسمی توییت خود در دو توییت ([توییت اول](#); [توییت دوم](#)) اذعان نموده که مقامات ایرانی خواستار جاسوسی از شهروندان خود شده اند:



Pavel Durov   
@durov

Replying to @youyeganeh

@youyeganeh Iranian officials want to use  
@telegram to spy on their citizens. We can  
not and will not help them with that.

10:23 PM - 20 Oct 2015

298 Retweets 366 Likes

53 298 366

مقامات ایرانی می خواهند از تلگرام برای جاسوسی از شهروندان خود استفاده کنند. ما نمی توانیم و نمی خواهیم به آنها کمک کنیم.



Pavel Durov   
@durov

Replying to @CDA

@CDA Iranian ministry of ICT demanded  
that @telegram provided them with spying  
and censorship tools. We ignored the  
demand, they blocked us.

10:56 PM - 20 Oct 2015

501 Retweets 581 Likes

64 501 581

وزارت ارتباطات و فناوری اطلاعات ایران خواستار این شد که تلگرام برای آن ها ابزار جاسوسی و سانسور فراهم نماید. آن تقاضا را نادیده گرفتیم، آن ها را مسدود نمودند.

شکی در این نکته که مقامات ایرانی به دفعات درخواست دسترسی به داده های کاربران ایرانی و جاسوسی از آن ها را داشته اند وجود ندارد. اما این حقیقت که تلگرام با آن ها همکاری داشته یا نداشته و یا اگر داشته تا چه حد بوده است، فقط از سوی سازندگان تلگرام قابل رد یا تایید می باشد.



ذکر این نکته ضروری است که سابقا (به خصوص در روزهای آغازین تلگرام)، تلگرام با مقامات جمهوری اسلامی در رابطه با بستن کانال های پورن، حذف برخی بات ها، و یا استیکرهای ناپسند همکاری نموده است. با وجود این که ممکن است این همکاری ها جزئی به نظر برسند، [مهندسا علیمردانی](#)، در پستی در وب سایت [Global Voices](#)، به خوبی در تشریح [نگرانی های کاربران](#) در رابطه با همکاری های احتمالی آتی تلگرام با درخواست های مقامات یا نهادهای قضایی و امنیتی جمهوری اسلامی، قلم زده است.

نهایتا باید ذکر کنم که، چون من یک برنامه نویس و توسعه دهنده بازی می باشم، طبعاً بخشی از افراد فعال در صنعت بازی در داخل یا خارج ایران را می شناسم و فعالان حوزه صنعت ساخت بازی های کامپیوترا بخشی از شبکه ارتباطی من می باشند. با توجه به سابقه توسعه و طراحی وب هم، بخش دیگری از شبکه من را طراحان و توسعه دهندهان وب تشکیل می دهند. در زمینه فعالیت سیاسی و مدنی هم، این چنین است. در نتیجه، با توجه به سابقه فعالیت تحقیقاتی و نوشتن در زمینه امنیت در سال های دور، هنوز هم بخشی از شبکه ارتباطی من را افراد فعال در حوزه امنیت تشکیل می دهند. از طرفی این افراد در شرکت های خصوصی کار می نمایند که پروژه های نهادهای امنیتی به دلیل کمبود نیروی متخصص به آن شرکت ها برون سپاری می شود. با توجه به این که قصد

ندارم امنیت جانی این افراد را تحت الشعاع قرار دهم، و این که امکان تایید ادعاهای آن ها را ندارم، به طور مختصر اشاره ای به گفته های آن ها می نمایم.

براساس ادعاهای مطرح شده از سوی این منابع که ابداً توانایی تایید آن ها را ندارم، به طرقی خاص - که بازهم تأکید می نمایم، به دلیل حفظ امنیت جانی و رعایت اخلاق امکان بازگو نمودن آن وجود ندارد - نهادهای امنیتی موفق به بدست آوردن کلیدهای رمزگاری تلگرام شده اند. از آنجایی که تلگرام به صورت پیش فرض از رمزگاری سر تا سر استفاده نمی نمایند و این قابلیت در گروه ها و نسخه های وب و دسکتاپ غیر فعال می باشد، اگر این ادعا صحت داشته باشد، این به آن معنی است که بخش عمده ای از کاربران تلگرام با استفاده از [حملات مرد میانی](#) آسیب پذیر می باشند. البته ذکر این نکته ضروری است که به دلیل حجم بالای داده، و نیاز به توان پردازشی بسیار بالا جهت رمزگشایی، احتمالاً امکان استفاده گسترده وجود نخواهد داشت. اما در موارد خاص و دست چین، یقیناً در صورت صحت موضوع امکان پذیر است.

پیش از آن که کسی انگشت اتهام را تماماً به سوی تلگرام نشانه رود، توجه داشته باشید که این دسترسی برای سایر اپلیکیشن ها، سرویس ها و پلتفرم های پیام رسانی هم محتمل است. اگر با [اقتصاد و نحوه درآمد هکرهای آشنا](#)ی داشته باشید، به طور معمول آن ها وقت خود را صرف یافتن آسیب پذیری در این سرویس ها می نمایند. ذکر این نکته ضروری است که [هکرهای در انواع و اقسام و گونه های مختلف وجود دارند](#). برای یک [هکر کلاه سیاه](#) گزارش یک آسیب پذیری به شرکت سازنده محصول یا ارائه دهنده سرویس به دلیل دریافت تنها چندهزار دلار، چندان مقرر نمی باشد. آن ها ترجیح می دهند با عرضه این آسیب پذیری ها به مشتریان خاص در [وب تاریک](#)، نظیر آزانس های اطلاعاتی و امنیتی، درآمدهای چندصد هزار دلاری یا گاها میلیون دلاری داشته باشند. طبعاً فروشنده و خریدار به دلیل حفظ منافع خود، سعی می کنند از افشای آن ها خودداری نمایند.

بر اساس ادعاهای این منابع، برای مثال ظاهراً با توجه به یک آسیب پذیری خریداری شده از سوی نهادهای امنیتی ایران، آن ها به محتوای اکانت های خصوصی اینستاگرام و چت

های اینستاگرام دسترسی دارند. تلگرام هم به نوبه خود، از این نوع آسیب پذیری ها، چندان مبرا به نظر نمی رسد (پاراگراف آخر مقاله که به اظهارات شناخته شده مقامات جمهوری اسلامی در رابطه با مرگ تصادفی یا خودکشانی زندانیان عقیدتی، سیاسی و امنیتی اشاره دارد را از دست ندهید).

باز هم تاکید می نمایم که امکان تایید صحت هیچ یک از ادعاهای فوق را ندارم! تنها دلیل بازگو نمودن شنیده هایم، نشان دادن خطرات مربوط به تصمیمات پیش فرض تحمیلی به کاربران توسط تلگرام، نظیر عدم رمزگذاری سر تا سر می باشد.

## اما تلگرام متن باز است و هر کسی می تواند کد منبع آن را مشاهده نماید

خیر! تلگرام متن باز نیست! تنها کد بخشی از آن یعنی [کلاینت های](#) سمت کاربر متن باز است. از مارس ۲۰۱۴ تا کنون، آن ها قول داده اند که:

*All code will be released eventually. We started with the most useful parts – a well-documented API that allows developers to build new Telegram apps, and open source clients that can be verified by security specialists*

تمام کد در نهایت منتشر خواهد شد. ما با بخش های مفید تر آغاز نموده ایم - یک API به خوبی مستند شده که به توسعه دهنده‌گان اجازه می دهد تا برنامه های مبتنی بر تلگرام جدید بسازند، و کلاینت های متن باز که می توانند توسط متخصصین امنیتی تأیید شوند.

?telegram.org Q: Why not open source everything –

با گذشت بیش از ۵ سال، تلگرام هرگز کد منبع سمت [سور](#) خود را، که مهم ترین قسمت این سرویس است، منتشر ننموده است.

## اما تلگرام به دستور مقامات قضایی جمهوری اسلامی فیلتر شده است

باید بگوییم که هیچ توضیحی برای این مسئله ندارم [\(۷\)](#) جز این که حضرات به خوبی می دانند کاربران ایرانی، پا به پای فیلترینگ پیش آمده و هر کاربر ایرانی راهکار خاص خود برای دور زدن فیلترینگ را در اختیار دارد. در واقع فکر می کنم کاربران ایرانی در کنار کاربران چینی، از لحاظ تکنولوژیک، جزو با سوادترین کاربران اینترنت می باشند. علاوه بر آن [مسئولان امر خود اذعان داشته اند](#) که تنها ۲ درصد از کاربران ایرانی پس از اعمال [فیلترینگ قطعی و گسترده از این پیام رسان خارج شده اند](#). پس آن ها به خوبی می دانند که فیلترینگ تلگرام مانند توییتر، یوتوب، فیسبوک و ... تا حد بسیار زیادی بی اثر است.

حتی اگر نهادهای امنیتی جمهوری اسلامی به داده های کاربران دسترسی داشته باشند، فیلترینگ تلگرام نه تنها مانع دسترسی ۹۸ درصد از کاربران نشده است، بلکه کاربران را خاطرجمع می نماید که چون این نرم افزار امن بوده و داده ها در دسترس نهادهای امنیتی ایران قرار ندارد، کاربران با خیال راحت تری از این پیام رسان استفاده می نمایند. این سناریوی احتمالی، درست مانند خنجری از پشت سر، خطرناک ترین حالت ممکن است!

## پس چرا جمهوری اسلامی اقدام به عرضه طلاگرام (تلگرام طلایی) و هاتگرام نموده است؟

سوال بسیار خوبی است. [بنا بر اذعان مجتبی ذوالنوری](#)، نماینده اصولگرای مجلس شورای اسلامی پیام رسان های مبتنی بر پلتفرم تلگرام، یعنی طلاگرام (تلگرام طلایی) و هاتگرام

توسط نهادهای امنیتی جمهوری اسلامی راه اندازی و عرضه شده اند. سازندگان تلگرام با ماه ها تأخیر، بالاخره در اواخر سال ۲۰۱۸ واکنش نشان داده و با ارسال پیامی به کاربران این دو اپلیکیشن اظهار نموده اند که امنیت کاربران فقط در صورت استفاده از نسخه رسمی تلگرام تضمین خواهد شد:



اگر این فرضیه را در نظر بگیریم که نهادهای امنیتی، به هر طریقی، به داده های کاربران ایرانی تلگرام دسترسی داشته اند، به این دلیل که این دسترسی یقیناً نمی توانسته تا ابد ادامه داشته باشد، آن ها بایستی راهکارهای آتی برای دسترسی به این داده ها را توسعه می داده اند که به یکباره در دسترسی به داده ها و شنود کاربران دچار مشکل نشوند. حتی اگر هم آن ها هرگز به این داده ها دسترسی نداشته اند، اگر [ادعای ابوالفضل حسن بیگی](#)، [عضو کمیسیون امنیت ملی مبنی بر عضویت ۲۵ میلیون کاربر ایرانی در تلگرام طلایی](#) را در نظر بگیریم، استفاده از طلاگرام و هاتگرام فقط حریم خصوصی اعضای این پیام رسان ها را به خطر نمی اندازد، بلکه تمامی مخاطبین این افراد هم ناخواسته و ندانسته در معرض خطر قرار می گیرند؛ که با توجه به آمار ۲۵ میلیونی این کاربران،

یعنی این اتفاق برای هر کاربر ایرانی که عضو این پیام رسان های غیررسمی نیست هم به شدت خطرناک می باشد.

## جایگزین ها

از آنجایی که مسایل مربوط به شنود انبوه و جاسوسی تنها مختص ایران نیست، متخصصین امر و کاربران علاقمند به حفظ حریم خصوصی، به دنبال جایگزین برای پیام رسان هایی نظیر تلگرام، واتس اپ، وایبر، پیام رسان فیسبوک، اسکایپ، لاین، [Threema](#)، [اسلک](#)، [دیسکورد](#)، [فایرچت](#)، و سایر سرویس ها یا نرم افزارهایی که به دلیل بسته بدون کد منبع آن ها، توانایی مطاله و بررسی آن ها از منظر امنیتی وجود ندارد، اقدام به ایجاد وب سایت ها و انجمن های متعددی به منظور بررسی، معرفی، و یا توسعه نرم افزارهای متن باز که قابلیت بررسی، مطالعه، ایرادیابی، و حل اشکلات آن ها از این جهت امکان پذیر می باشد، نموده اند. از جمله این وب سایت ها می توان به سایر دیت های [ThinkPrivacy](#)، [PRISM Break](#)، [privacytools.io](#) و یا [r/degoogle](#) و [r/privacy](#) و [r/privacytoolsIO](#) در این زمینه ایجاد شده اند. به علاوه، لیست های مقایسه ای پیام رسان ها از نظر میزان امنیت و حفظ حریم خصوصی نظیر [Secure Messaging Apps Comparison](#)، [Practical Application of EFF's Guide to Choosing a Messenger](#)، [ThinkPrivacy Messenger Comparison Chart](#) ایجاد شده اند.

بر اساس لیست های منتشر شده در این وب سایت ها و انجمن ها، در ادامه به معرفی مختصر نرم افزارهای امن پیام رسان می پردازیم.

## لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط Prism Break

## لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط Prism Break به شرح ذیل می باشد:

		برنامه پیام رسان		مالکیت طلبانه*
	Briar Peer-to-peer messaging app Android		Aenigma Secure-by-default XMPP server installer Servers	Discord
	Conversations ...ber client for Android 4.0+ smart phones Android		ChatSecure .OMEMO or OTR encrypted IM for iOS	Facebook Messenger
	Jami .Distributed video chat application Windows macOS GNU/Linux Android Experimental		Gajim ...x and Windows—OTR support via plugin	Google Hangouts
	RetroShare سکوی اریباطی دوطرفه، امن و آزاد Windows macOS GNU/Linux BSD		+Psi ...for power users with built-in OTR support	ICQ
	Signal .Secure messenger for Android and iOS iOS Android		Riot ...n the decentralized Matrix ecosystem, p	iMessage
	Tox ...tated goal of the project is to provide sec macOS iOS GNU/Linux BSD Android Experimental Windows		Silence .A fork of TextSecure with SMS encryption Android	LINE
				Skype
				Snapchat
				Tencent QQ
				Trillian
				Viber Messenger
				WeChat
				WhatsApp

## لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط Prism Break

لازم به ذکر است که در جدول فوق، نرم افزارهای ستون [مالکیت طلبانه](#) نرم افزارهایی هستند که به اعتقاد Prism Break بایستی از آن ها حذر نمود. اما دو ستون بعدی (نرم افزارهای جایگزین می باشند.)

## لیست پیام رسان های مورد تایید و جایگزین تلگرام

**privacytools.io**

لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط [privacytools.io](#) به شرح ذیل می باشد:

## 🔗 Encrypted Instant Messenger

If you are currently using an Instant Messenger like WhatsApp, Viber, LINE, Telegram or Threema, you should pick an alternative here.

Mobile: Signal



Signal is a mobile app developed by Open Whisper Systems. The app provides instant messaging, as well as voice and video calling. All communications are end-to-end encrypted. Signal is free and open source.

[Website](#) [Forum](#)



Riot.im



Riot.im is a decentralized free-software chatting application based on the Matrix protocol, a recent open protocol for real-time communication offering E2E encryption. It can bridge other communications via other protocols such as IRC too. [beta](#)

[Website](#) [Forum](#)



Wire



A free software End-to-End Encrypted chatting application that supports instant messaging, voice, and video calls. Full source code is available. [experimental](#) [\(more info\)](#)

[Website](#) [Forum](#)



[Provider](#) [Browser](#) [Software](#) [OS](#) [Participate](#)

[Language](#) [Services](#) [Donate](#)

### Complete Comparison

- [securechatguide.org](#) - Guide to Choosing a Messenger.
- [securemessagingapps.com](#) - Secure Messaging Apps Comparison.
- [thinkprivacy.io](#) - Simple Secure Messaging Apps Comparison.

### Worth Mentioning

- [Ricochet](#) - Ricochet uses the [Tor network](#) to reach your contacts without relying on messaging servers. It creates a hidden service, which is used to rendezvous with your contacts without revealing your location or IP address. [Experimental](#) [Danger](#) [Keep Tor up to date](#)
- [RetroShare](#) - An E2E encrypted instant messaging and voice/video call client. RetroShare supports both TOR and I2P.
- XMPP federated clients with OMEMO support:
  - [Monal](#) (iOS, MacOS) - An XMPP client in active development.
  - [Conversations](#) (Android) - An open source Jabber/XMPP client for Android 4.4+ smartphones. Supports end-to-end encryption with either OMEMO or OpenPGP.
  - [Gajim](#) (Linux) - An open source fully featured XMPP client.
  - [List of OMEMO ready clients](#)
- [Kontalk](#) - A community-driven instant messaging network. Supports end-to-end encryption. Both client-to-server and server-to-server channels are fully encrypted.
- [Status](#) - [Experimental](#) A free and open-source, peer-to-peer, encrypted instant messenger with support for DAPPS.

لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط [privacytools.io](#)

# لیست پیام رسان های مورد تایید و جایگزین تلگرام

## ThinkPrivacy توسط

لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط [ThinkPrivacy](#) به شرح ذیل

می باشد:

# Messaging

Use Instead Of: WhatsApp, Facebook Messenger, Telegram, Text Messaging, Snapchat, Slack.

COMPARE MESSENGER APPS

EDITOR'S CHOICE

Product	Description	Skill Level
Signal	Signal is a mobile app developed by Open Whisper Systems. The app provides instant messaging, as well as voice and video calling. All communications are end-to-end encrypted.	Beginner

Product	Description	Skill Level
Wire	A free software End-to-End Encrypted chatting application that supports instant messaging, voice, and video calls.	Beginner
Riot	Riot.im is a decentralized free-software chatting application based on the Matrix protocol, a recent open protocol for real-time communication offering E2E encryption.	Intermediate
Jami	One of the closest Skype replacements out there. Encrypted text and video chats. Great for podcasters.	Beginner
Keybase	A great messenger for more technical users, Keybase's integrated file sharing is robust and convenient for sharing files across the web.	Intermediate
Rocket.Chat	A self-hosted team chat solution for those who want to keep files and conversations safely on their own servers.	Advanced

لیست پیام رسان های مورد تایید و جایگزین تلگرام توسط ThinkPrivacy

## مقایسه امنیت پیام رسان ها توسط ThinkPrivacy

نتایج مقایسه امنیت پیام رسان ها توسط ThinkPrivacy، به شرح ذیل می باشد:



How do these commonly used messenger apps stack up against each other? Use this handy chart to compare them.

Comparison	Signal	Wire	Wickr	Telegram	Whatsapp	iMessage	Facebook Messenger
Refused to cooperate with government agencies?	✓	✓	✓	✓	✗	✗	✗
Transparency reports available?	✓	✓	✓	✗	✓	✓	✓
Does <u>not</u> collect user data	✓	✓*	✓	✗	✗	✗	✗
Default encryption	✓	✓*	✓	✗	✓	✓	✗
Open source?	✓	✓	✓	✗	✗	✗	✗
Encrypts metadata?	✓	✗	✓	✗	✗	✗	✗
Does <u>not</u> log IP address	✓	?	✓	✗	✗	✗	✗

[BACK TO MESSAGING APPS](#)

\*When using Wire, metadata -- the fact that you communicated with -- is not encrypted. [Here are instructions](#) on how to stay more anonymous when using Wire.

مقایسه امنیت پیام رسان ها توسط ThinkPrivacy

## مقایسه امنیت پیام رسان ها بر اساس استانداردهای

## Electronic Frontier Foundation

این مقایسه با توجه به مقاله ای تحت عنوان فکر کردن درباره چیزی که در یک پیام رسان آمن نیاز دارد، که در وب سایت بنیاد [Electronic Frontier Foundation](#) منتشر شده، توسط [SecureChatGuide.org](#) تهیه شده است:

Name	Platforms	Country of Origin	Ephemeral Messages	ID contains personal info	Foolproof (All Messages Encrypted)	Puddle Test	Hammer Test	Has Contact Verification
✗ Adamant	iOS, Web	Republic of Ireland	No	No	Yes	Data recoverable	Data recoverable	No
✗ Antox	Android	No centralized servers	No	No	Yes	Data not recoverable	Data recoverable	No
✓ Babelfish	Android, iOS, MacOS, Windows	Czech Republic	Yes	No	Yes	Data not recoverable	Data not recoverable	Yes
✓ BlackBerry Messenger	Android, iOS, MacOS, Windows, BlackBerry	Canada	Yes	No	Yes	Data recoverable	Data not recoverable	No
✓ Briar Project	Android (via Google Play, F-Droid repo or APK)	None	No	No	Yes	Data not recoverable	Data not recoverable	Yes
✓ Brosix	Android, iOS, MacOS, Windows, Linux (many)	Bulgaria	No	No	Yes	Data not recoverable	Data not recoverable	No
✗ Cashew	Android, iOS	USA	Yes	No	Yes	Data recoverable	Data recoverable	No
✗ Confide	Android, iOS, MacOS, Windows	USA	Yes	Email	Yes	Data not recoverable	Data not recoverable	No
✓ Conversations (XMPP)	Android	Germany	No	No	No (Unless OMEMO Encryption is set to Always)	Data recoverable	Data recoverable	Yes
✗ Crypto	Android, iOS, Mac, Windows, Web	Norway	No	Email	Yes	Data recoverable	Data recoverable	Yes
✗ Crypvisor	Android, iOS	Germany	Yes	No	Yes	Data recoverable	Data not recoverable	No
✗ Cwtch	Android, Windows, Linux	Canada	Yes	No	Yes	Data not recoverable	Data not recoverable	?
✗ Elect	Android (direct APK download), iOS, MacOS, Windows, Linux (Applimage), Web	UK	Yes	No	Yes	Data not recoverable	Data not recoverable	No
✗ FireChat	Android, iOS	USA	No	No	No	Data not recoverable	Data not recoverable	No
✗ foilChat	Android, iOS, Web	Finland	Yes	Email	Yes	Data recoverable	Data recoverable	No
✗ FortKnozter	Android, iOS, Web	UK	No	No	Yes	Data recoverable	Data recoverable	No
✗ get2Clouds	Android, iOS, Windows	UK	Yes	No	No	?	Data recoverable	No
✓ Giro	Android, iOS	Germany	Yes	Phone	Yes	Data not recoverable	Data not recoverable	Yes
✗ Hoccer	Android, iOS	Germany	No	No	Yes	Data not recoverable	Data recoverable	Yes
✗ HoopMessenger	Android	Canada	Yes	No	No	Data recoverable	Data recoverable	No
✗ Janji	Android, iOS, Linux, MacOS, Windows	Canada	No	No	Yes	Data not recoverable	Data recoverable	No
✓ Keybase	Android, iOS, MacOS, Windows, Linux (many)	USA	Yes	No	Yes	Data recoverable	Data not recoverable	No
✗ Kortalk	Android (on F-Droid), Java client	None	No	Phone	Yes	?	Data recoverable	Yes
✗ Krister	Android	UK	Yes	No	Yes	Data not recoverable	Data recoverable	Yes
✗ KryptoChat	Android, iOS	United Arab Emirates	No	No	Yes	Data not recoverable	Data recoverable	No
✗ LinkCast	Android, iOS	Japan	Yes	No	Yes	Data not recoverable	Data recoverable	No
✓ MySudo	iOS	USA	Yes	No	No	Data recoverable	Data not recoverable	No
✓ Patchwork	Linux (Applimage), MacOS, Windows	None	No	No	No	Data recoverable	Data recoverable	No
✗ Pinnacle	Android, iOS	Latvia	No	Phone	Yes	Data not recoverable	Data recoverable	No
✓ Pix-Art (XMPP)	Android	Germany	No	No	No (Unless OMEMO Encryption is set to Always)	Data recoverable	Data recoverable	Yes
✓ Quicksy (XMPP)	Android	Germany	No	Phone	No (Unless OMEMO Encryption is set to Always)	Data recoverable	Data recoverable	Yes
✗ Ravn	Android, iOS	Dominican Republic	No	No	Yes	Data not recoverable	Data not recoverable	No
✓ RetroShare	Windows, MacOS, Linux (many), FreeBSD	None	No	No	Yes	Recoverable?	Recoverable?	No
✗ Ricochet	Windows, MacOS, Linux (many)	No centralized servers	Yes	No	Yes	Data not recoverable	Data not recoverable	No
✓ Riot	Android (on F-Droid), iOS, Mac OS, Windows, Linux (Debian, Ubuntu), Web	UK	No	No	No	Data not recoverable	Data not recoverable	Yes
✓ SafeSwiss	Android, iOS, Windows	Switzerland	Yes	No	Yes	Data not recoverable	Data not recoverable	Yes
✓ SafeText	Android, iOS, Web	UK	Yes	No	Yes	Data recoverable	Data not recoverable	No
✗ SeeEMS	Android, iOS (MacOS and Windows coming soon)	China	Yes	No	Yes	Data not recoverable	Data not recoverable	No
✗ Sid	Android, iOS, MacOS, Windows, Linux (Ubuntu)	Germany	No	No	Yes	Data not recoverable	Data recoverable	No
✓ Signal	Android (Direct APK download), iOS, MacOS, Windows, Linux (Debian)	USA	Yes	Phone	No	Data not recoverable	Data not recoverable	Yes
✓ Silence	Android	No centralized servers	No	Phone	No	Data not recoverable	Data not recoverable	Yes
✓ Skred	Android, iOS	France	No	No	Yes	Data not recoverable	Data not recoverable	No
✗ Soma	Android, iOS, Web	USA	No	Phone	Yes	Data not recoverable	Data not recoverable	No
SecureChatGuide.org	STEP-BY-STEP GUIDES ▾	CHARTS AND LISTS ▾	APP REVIEWS ▾	MORE ▾				
✗ StealthChat	Linux	USA	Yes	Phone	Yes	Data not recoverable	Data not recoverable	Yes
✗ Surespot	Android, iOS	USA	Yes	No	Yes	?	Data recoverable	No
✗ Telegram	Android, iOS, Windows, MacOS, Web	UK	Yes	Optional aliases	No	Data recoverable	Data recoverable	Yes
✓ Threema	Android (Threema Shop), iOS, Windows Phone, Web	Switzerland	No	No	Yes	Data not recoverable	Data not recoverable	Yes
✗ Together	Android, iOS	USA	No	No	No	?	?	No
✗ Tok	Android, iOS	None	No	Yes	Yes	Data not recoverable	Data not recoverable	No
✓ Tungsten	Android, iOS (MacOS/Windows/Linux coming soon)	Germany	No	No	Yes	Data not recoverable	Data not recoverable	No
✗ Twice	Android, iOS	Canada	Yes	No	?	?	?	?
✓ TwinMe	Android, iOS	France	No	No	Yes	Data not recoverable	Data not recoverable	No
✗ Varish Messenger	Android, iOS	Canada	No	No	Yes	Data not recoverable	Data not recoverable	No
✗ Vega	Android, iOS	Belgium	Yes	Phone	Yes	Data not recoverable	Data recoverable	No
✗ Viber	Android, iOS, MacOS, Windows, Linux	Japan	Yes	Phone	Yes	Data not recoverable	Data recoverable	Yes
✗ ViPole (Free version)	Android, iOS, MacOS, Windows, Linux	UK	No	No	Yes	Data recoverable	Data recoverable	No
✗ ViPole (Pro version)	Android, iOS, MacOS, Windows, Linux	UK	Yes	No	Yes	Data recoverable	Data recoverable	No
✓ Whisperer	Android, iOS, Web	Germany	No	No	Yes	Data recoverable	Data not recoverable	Yes
✓ WickrMe	Android, iOS, MacOS, Windows, Linux (Ubuntu 16.04)	USA	Yes	No	Yes	Data not recoverable	Data not recoverable	Yes
✓ Wire	Android (Direct APK), iOS, MacOS, Windows, Linux (Ubuntu, Debian, Applimage), Web	Switzerland	Yes	No	Yes	Data recoverable	Data not recoverable	Yes
✗ Zangi	Android, iOS, MacOS, Windows and web coming soon	USA	No	Phone	Yes	Data not recoverable	Data recoverable	No
✓ Zom	Android, iOS	USA	No	No	Yes	Data recoverable	Data recoverable	Yes

مقایسه امنیت پیام رسان ها توسط

# Secure Messaging Apps Comparison

Messaging Apps

نتایج مقایسه امنیت پیام رسان ها توسط Secure Messaging Apps که با کوشش آقای مارک ویلیامز میسر شده است، به شرح ذیل می باشد:

# SECURE MESSAGING APPS COMPARISON

BECAUSE PRIVACY MATTERS

Due to Patreon's banning of Sargon of Akkad, I have closed my Patreon account.

Comparison	Allo	iMessage	Messenger	Riot	Signal	Skype	Telegram	Threema	Viber	Whatsapp	Wickr	Wire
TL;DR: Does the app secure my messages and attachments?	No	No	No	No	Yes	No	No	Yes	No	No	No	Yes
Company jurisdiction	USA	USA	USA	UK	USA	USA	USA / UK / Belize	Switzerland	Luxembourg / Japan	USA	USA	Switzerland
Infrastructure jurisdiction	USA, Belgium, Finland, Ireland, the Netherlands, Chile, Taiwan, and Singapore	USA (Ireland and Denmark planned); iMessage runs on AWS and Google Cloud	USA, Sweden (Ireland planned)	UK (and potentially all jurisdictions, given it's a decentralised messaging platform)	USA	USA, the Netherlands, Australia, Brazil, China, Ireland, Hong Kong, and Japan	UK, Singapore, USA, and Finland	Switzerland	USA	USA (unlike other locations)	USA (unlike other locations)	Germany / Ireland
Implicated in giving customers' data to intelligence agencies?	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	No
Surveillance capability built into the app?	No	No	No	No	No	Yes	No	No	No	No	No	No
Does the company provide a transparency report?	Yes	Yes	Yes	No	Yes	Yes	No	Yes	No	Yes	Yes	Yes
Company's general stance on customers' privacy	Poor	Poor	Poor	Good	Good	Poor	Poor	Good	Poor	Poor	Good	Good
Funding	Google	Apple	Facebook	New Vector Limited	Freedom of the Press Foundation, the Knight Foundation, the Shuttleworth Foundation, and the Open Technology Fund, Signal Foundation (Brian Acton)	Microsoft	Pavel Durov	User pays	Rakuten, friends and family of Salmon Marco (it's very unclear)	Facebook	Gilman Louie, Juniper Networks, the Knight Foundation, Breyer Capital, CME Group, and Wargaming	Janus Friis, Iconical, Zeta Holdings Luxembourg
Company collects customers' data?	Yes	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes	No	No
App collects customers' data?	Yes	Yes	Yes	Minimal	Minimal	Yes	Yes	No	Yes	Yes	No	Minimal
Is encryption turned on by default?	No	Yes	No	No	Yes	Yes	No	Yes	Yes (if device supports it)	Yes (if device supports it)	Yes	Yes
Cryptographic primitives	RSA-1280 (encryption), ECDSA 256 (signing) / AES 128 / SHA-1	Curve25519 / AES-256 / HMAC-SHA256	Curve25519 / AES-256 / HMAC-SHA256	Curve25519 / AES-256 / HMAC-SHA256	RSA-1536 & 2048 / AES 256 / 256 / SHA-1	RSA 2048 / AES 256 / 256 / SHA-256	Curve25519 256 / Xsalsa20 256 / Poly1305-AES 128	Curve25519 256 / Salsa20 128 / HMAC-SHA256	Curve25519 256 / AES-256 / HMAC-SHA256	ECDH512 / AES-256 / HMAC-SHA256	Curve25519 / ChaCha20 / HMAC-SHA256	
Are the app and server completely open source?	No	No	No	Yes	Yes	No	No (clients and API only)	No	No	No	No	Yes
Can you sign up to the app anonymously?	No	No	No	Yes	No	No	No	Yes	No	No	Yes	No
Can you add a contact without needing to trust a directory server?	No	No	No	No	No	No	No	Yes	Yes	No	No	No
Can you manually verify contacts' fingerprints?	No	No	Yes	Yes	Yes	No	No (session only, does not provide users' fingerprint information)	Yes	Yes	Yes	Yes	Yes
Directory service could be modified to enable a MITM attack?	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Do you get notified if a contact's fingerprint changes?	No	No		Yes	Yes	No	No (session only, does not provide users' fingerprint information)	Yes	Yes	No (setting turned off by default)	No	If contact was previously verified
Is personal information (mobile number, contact list, etc.) hashed?	No	No	No		Mostly	No	No	Yes	No	No	Yes	Mostly
Does the app generate & keep a private key on the device itself?		Yes	Yes	Yes	Yes		Yes	Yes	Yes	Yes	Yes	Yes

Can messages be read by the company?	Yes	No	Yes	No	No	Yes	Yes	No	No	No	No	No
Does the app enforce perfect forward secrecy?		No	Yes	Yes	Yes			No (session keys do change after being used 100 times)	No	Yes	Yes	Yes
Does the app encrypt metadata?		No	No		Yes		No	Yes		No	Yes	Mostly
Does the app use TLS/Noise to encrypt network traffic?	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Does the app use certificate pinning?		Yes (>= iOS 9.3)			Yes		Yes					Yes
Does the app encrypt data on the device? (iOS and Android only)		Yes (if passphrase enabled)			Yes (if passphrase enabled)		iOS: Yes (if passphrase enabled); Android: Yes (if			iOS: Yes (if passphrase enabled); Android: Yes	Yes	Yes
Comparison	All	iMessage	Messenger	Riot	Signal	Skype	Telegram	Threema	Viber	Whatsapp	Wickr	Wire
Does the app allow a secondary factor of authentication?	No	No	No	No	No	No	Yes	Yes	No	Yes	Yes (password for account used)	Yes
Are messages encrypted when backed up to the cloud?		No			N/A, Signal is excluded from iCloud/iTunes & Android backups		Yes			iOS: Yes Android: No		N/A, Wire is excluded from iCloud/iTunes & Android backups
Does the company log timestamps/IP addresses?	Yes	Yes	Yes		No	Yes	Yes	No	Yes	Yes	No	Some
Have there been a recent code audit and an independent security analysis?	No	No	No	No	Yes (October, 2014)	No	Yes (November, 2015)	Yes (November, 2015)	No	No	Yes (August, 2014)	Yes (March, 2018)
Is the design well documented?	No	Somewhat	Somewhat	Somewhat	Somewhat	No	Somewhat	Somewhat	Somewhat	Somewhat	Somewhat	Somewhat
Does the app have self-destructing messages?	Yes	No	Yes	No	Yes	No	Yes	No	No	No	Yes	Yes

Red = Something of major concern.

Yellow = Something of concern.

Green = Nothing of concern.

Blank = I couldn't find any information about it.

## مقایسه امنیت پیام رسان ها توسط Secure Messaging Apps

# Signal

در تمامی لیست های مرتبط با پیام رسان های امن، [سیگنال](#) یکی از ایمن ترین گزینه های موجود می باشد، که همانطور که قبل ذکر شد، پروتکل رمزگاری آن مورد ستایش اکثربت قریب به اتفاق متخصصین حوزه رمزگاری می باشد. سیگنال که توسط [Whisper Systems](#) توسعه داده است، قابلیت ارسال و دریافت پیام های فوری، همچنین تماس صوتی و تصویری را فراهم می نماید. به صورت پیش فرض، تمامی ارتباطات در این نرم افزار از رمزگذاری سر تا سر استفاده می نماید. همچنین این پیام

رسان متن باز و کاملا رایگان بوده و برای پلتفرم های اندروید، آی اواس، لینوکس، ویندوز، و در نهایت مک قابل دریافت می باشد.

ذکر نکته مهمی در مورد سیگنال لازم به نظر می رسد. متاسفانه در سیگنال امکان مخفی نمودن شماره تلفن یا ثبت نام بدون شماره تلفن یا ایمیل موجود نمی باشد. این نرم افزار برای ارتباط میان افرادی که یکدیگر را می شناسد و نیازی به مخفی نمودن هویت خود ندارند از نظر امنیت ارتباطات بسیار عالی است. اما در مواردی که نیاز به مخفی نمودن هویت می باشد استفاده از [Wire](#) یا [Wickr](#) منطقی تر به نظر می رسد.

## Wickr

پیام رسان فوری رایگان و متن باز [Wickr](#)، اجازه ارتباطات با استفاده از رمزگذاری سر تا سر شامل ارسال پیام، فایل های عکس، صوتی و تصویری، تماس صوتی یا کنفرانس ویدیویی را می دهد. این نرم افزار برای پلتفرم های اندروید، آی اواس، لینوکس، ویندوز، و مک قابل دریافت می باشد.

مزیت بزرگ پیام رسان [Wickr](#) ناشناس ماندن کامل کاربر می باشد. این پیام رسان حتی نیاز به دانستن شماره تلفن یا ایمیل شما در زمان ثبت نام ندارد. در این نرم افزار یک شناسه که فقط شما از آن با خبرید به شما اختصاص داده شده که به شکل برگشت ناپذیر از طریق افزودن نمک، این شناسه چندین دور رمزنگاری می شود. به این ترتیب حتی سازندگان این پیام رسان قادر به ردیابی اطلاعات مربوط به شما نمی باشند.

لازم به ذکر است که در گزارش رعایت حریم خصوصی کاربران، منتشر شده توسط [Wickr](#)، در سال ۲۰۱۵ و متعاقب آن ۲۰۱۷ شرکت [Electronic Frontier Foundation](#) جزو ۹ کمپانی بوده است که در تمامی زمینه ها به خود یک ستاره را اختصاص داده است.

پس می توانید با استفاده از [Wickr](#) تا حد بسیار بسیار زیادی از مخفی ماندن هویت خود مطمئن باشید.

## Riot.im

پیام رسان Riot.im یک نرم افزار چت غیرمتمرکز متن باز و کاملا رایگان مبتنی بر پروتکل ماتریکس، یک پروتکل باز جدید برای ارتباطات با استفاده از قابلیت رمزگذاری سر تا سر می باشد. این پیام رسان علاوه بر پروتکل ماتریکس قابلیت اتصال به پروتکل های دیگر نظیر آی آر سی، اسلک، Gitter، تلگرام، و ادغام آن ها را نیز دارد.

از دیگر مزایای این نرم افزار قابلیت نصب اختصاصی آن بر روی سرور خودتان می باشد که می توانید با استفاده از این ویژگی صد درصد مطمئن باشید که داده های شما تنها در اختیار خودتان خواهد بود. این پیام رسان برای پلتفرم های اندروید، آی اواس، لینوکس، ویندوز، مک و حتی اجرا در مرورگرهای وب در دسترس بوده و رابط کاربری آن به ۲۵ زبان مختلف ترجمه شده است.

لازم به ذکر می باشد که تمرکز این پیام رسان بر روی کار و ارتباطات گروهی می باشد که آن را به جایگزین مناسبی برای نرم افزار اسلک مبدل می سازد.

## Wire

پیام رسان کاملا رایگان و متن باز Wire با پشتیبانی از قابلیت رمزگذاری سر تا سر در پیام های فوری، و تماس های صوتی و ویدیویی است که کد منبع آن به شکل کامل در دسترس می باشد. این پیام رسان برای پلتفرم های اندروید، آی اواس، لینوکس، ویندوز، مک و حتی اجرا در مرورگرهای وب در دسترس می باشد. در این نرم افزار شما می توانید به جای استفاده از شماره تلفن، از ایمیل جهت ثبت نام در نسخه دسکتاپ استفاده نمایید. البته در صورت استفاده از شماره تلفن یا ایمیل این اطلاعات به شکل خصوصی باقی مانده و کاربران امکان جستجو و یافتن شما با استفاده از این اطلاعات را نخواهند داشت.

جهت محافظت حداکثری از حریم خصوصی خود در Wire، مطالعه این نکات از بلاگ رسمی Medium Wire شدیدا توصیه می شود.

ذکر این نکته ضروری است که قبل از مشکلات متعدد امنیتی در این نرم افزار کشف شده است که امروزه عمدۀ این مسایل حل شده اند، هر چند که پروتکل مورد استفاده در این پیام رسان از نظر برخی متخصصین در مقایسه با Signal ضعیف تر می باشد.

## Jami

پیام رسان متن باز و رایگان Jami یکی از نزدیک ترین جایگزین های موجود برای اسکایپ می باشد. پیام ها، و حتی تماس های صوتی و تصویری در این نرم افزار رمزگذاری می شوند.

این پیام رسان برای پلتفرم های اندروید، آی اواس، فری بی اس دی، لینوکس، ویندوز، و مک در دسترس می باشد.

## Keybase

پیام رسان متن باز و رایگان Keybase یک گزینه عالی برای کاربران فنی تر می باشد که به عنوان یک جایگزین برای اسلک بر فعالیت های گروهی تمرکز نموده است. جهت به اشتراک گذاری فایل بر روی اینترنت این نرم افزار یک گزینه عالی می باشد. این پیام رسان برای پلتفرم های اندروید، آی اواس، لینوکس، ویندوز، و مک عرضه شده است.

## Rocket.Chat

پیام رسان متن باز و رایگان Rocket.Chat، یک راهکار چت گروهی برای افرادی است که می خواهند پیام ها، فایل ها و مکالمات خود را به شکلی امن بر روی سرورهای خود میزبانی نمایند. این پیام رسان برای پلتفرم های اندروید، آی اواس، لینوکس، ویندوز، و مک در دسترس می باشد.

## Tox

پروتکل و پیام رسان متن باز و رایگان [Tox](#) به منظور دریافت و ارسال پیام فوری و تماس های صوتی و تصویری کاربرد دارد. هدف اعلام شده این پروژه ارائه ارتباطات امن و در عین حال آسان برای همه است. این پروتکل بر پایه کتابخانه شبکه و رمزگاری شناخته شده [NaCl](#) پایه ریزی شده است. اما، هنوز توسط متخصصان امنیتی مورد بازرگانی قرار نگرفته است. لذا مسئولیت استفاده از آن تنها متوجه شخص خودتان خواهد بود.

این پیام رسان برای پلتفرم های اندروید، آی اواس، سیلفیش اواس، فری بی اس دی، لینوکس، ویندوز، مک، و اوپن ایندیانا عرضه شده است.

## Briar

پیام رسان متن باز و رایگان [Briar](#) یک پیام رسان [همتا به همتا](#) با قابلیت رمزگذاری پیام ها و تشکیل انجمن می باشد. حتی به کمک آن، مانند نرم افزار فایرچت، بدون نیاز به اتصال به اینترنت اقدام به ایجاد شبکه محلی از کاربران نمود. این نرم افزار فقط [برای سیستم عامل اندروید در دسترس می باشد](#).

## RetroShare

پیام رسان متن باز و رایگان [RetroShare](#) جهت ارسال پیام فوری و تماس های صوتی یا تصویری می باشد. این پیام رسان از پروتکل های متعدد به اشتراک گذاری فایل همتا به همتا از قبیل [بیت تورنت](#)، [eDonkey](#)، [ناتلا](#) و ... پشتیبانی می نماید. علاوه بر آن جهت عدم افشاری هویت کاربر، شبکه های [تور](#) و [پروژه اینترنت مخفی](#) را بکار می گیرد.

این پیام رسان برای پلتفرم های فری بی اس دی، اوپن بی اس دی، نت بی اس دی، اندروید، لینوکس، ویندوز، مک، و هایکو در دسترس می باشد.

برای افرادی که توانایی راه اندازی سرور را ندارند، احتمالاً ساده ترین راه جهت راه اندازی یک شبکه اجتماعی رمزگذاری شده استفاده از RetroShare می باشد. توجه داشته باشید که امنیت RetroShare توسط کارشناسان امنیتی جهت شناسایی آسیب پذیری های احتمالی، مورد ارزیابی قرار نگرفته است. بنابراین مسئولیت استفاده از آن تنها متوجه شخص خودتان خواهد بود.

## Ricochet

پیام رسان متن باز و رایگان Ricochet با استفاده از شبکه تور و بدون اتکا به سرورهای مرکزی، به مخاطبین شما دسترسی پیدا می نماید. این پیام رسان، این کار را از طریق ایجاد یک سرویس مخفی برای ارتباط با مخاطبین شما بدون نشان دادن موقعیت مکانی یا آدرس آی پی شما انجام می دهد. توجه داشته باشید که این نرم افزار آزمایشی است. همچنین جهت جلوگیری از آسیب پذیری های جدی [نیاز به به روز رسانی نسخه تور عرضه شده به همراه Ricochet می باشد](#).

این پیام رسان برای پلتفرم های فری بی اس دی، لینوکس، ویندوز، و مک عرضه شده است.

## Silence

پیام رسان متن باز و رایگان Silence که خود از نرم افزار تکست سکیور منشعب شده است، جهت رمزگذاری و ارسال پیامک یا [خدمات پیام چندرسانه ای](#) به شکل ایمن از طریق شبکه های تلفن همراه کاربرد دارد.

این پیام رسان برای پلتفرم اندروید عرضه شده است.

## Status

پیام رسان متن باز و رایگان **Status** یک پیام رسان فوری همتا به همتا با پشتیبانی از **DApp** می باشد. **DApp** بر اساس تکنولوژی  **بلاکچین** به منظور پردازش های غیرمتمرکز بنا شده است. این پیام رسان متکی بر شبکه **اتریم** می باشد.

این پیام رسان برای پلتفرم های اندروید، آی اواس، لینوکس، ویندوز، و مک در دسترس می باشد.

## کلاینت های مبتنی بر XMPP

برخی از پیام رسان های متن باز و رایگانی که به حریم خصوصی کاربران احترام می گذارند بر اساس **پروتکل اکس ام پی پی** توسعه یافته اند که در ادامه به اختصار به معرفی آن ها خواهیم پرداخت. لازم به ذکر است که این پروتکل در اصل به نام Jabber شناخته می شد و گاهها این واژه ها به جای یکدیگر به کار می روند.

### Aenigma

سرور رایگان و متن باز **Aenigma** که به صورت پیش فرض بسیار امن می باشد، به شما اجازه راه اندازی سرور شخصی جهت پیام رسانی فوری را خواهد داد. به دلیل پیاده نمودن استاندارد اکس ام پی پی، پس از راه اندازی می توان با نرم افزارهای متن باز، ایمن و رایگان نظیر **Conversations**, **Gajim**, **Monal**, **ChatSecure**, **بیجین**, **کوپته**, **جیتسی**, **Adium**, بر روی پلتفرم های مختلف، به سرور راه اندازی شده جهت ارتباطات امن متصل شد.

## کلاینت های مبتنی بر XMPP با پشتیبانی از OMEMO

پروتکل **OMEMO** بر روی XMPP به منظور رمزگذاری سر تا سر چند مخاطبه توسعه یافته است. فی الواقع با استفاده از الگوریتم **Double Ratchet** رمزگذاری چندسر به چندسر را فراهم می نماید. در ادامه به اختصار به معرفی برخی از پیام رسان هایی که از این ویژگی پشتیبانی می نمایند خواهیم پرداخت.

## Conversations

پیام رسان متن باز و رایگان [Conversations](#) به منظور ارسال و دریافت متن یا تصاویر کاربرد دارد. این پیام رسان برای پلتفرم اندروید عرضه شده است و عمدتاً بر پایه استانداردهای باز پذیرفته شده نظیر اکس ام پی پی و اس اس ال / تی ال اس بنا شده است. همچنین، رمزگذاری سر تا سر در این نرم افزار می‌تواند با استفاده از پروتکل OMEMO و یا [پی جی پی](#) با استفاده از [OpenPGP](#) انجام می‌شود.

## Gajim

پیام رسان متن باز و رایگان [Gajim](#) که برای پلتفرم‌های بی اس دی، لینوکس، و ویندوز عرضه شده است، یک پیام رسان سبک و سریع با پشتیبانی از پروتکل‌های GPG، XMPP، OMEMO، OTR، SSL/TLS می‌باشد.

## Monal

پیام رسان متن باز و رایگان [Monal](#) که بر مبنای پروتکل XMPP برای پلتفرم‌های آی او اس و مک عرضه شده است، جهت رمزگذاری سر تا سر از پروتکل OMEMO استفاده می‌نماید.

## +Psi

پیام رسان متن باز و رایگان [+Psi](#) که بر مبنای پروتکل XMPP برای پلتفرم‌های لینوکس، ویندوز، مک و هایکو توسعه یافته است، جهت رمزگذاری سر تا سر توانایی به کارگیری پروتکل‌های OMEMO، GPG و OTR را دارد.

## ChatSecure

پیام رسان متن باز و رایگان [ChatSecure](#) که بر مبنای پروتکل XMPP برای پلتفرم آی او اس عرضه شده است، جهت رمزگذاری سر تا سر از پروتکل‌های OTR و OMEMO و پشتیبانی می‌نماید.

## Kontalk

پیام رسان متن باز و رایگان [Kontalk](#) که بر مبنای پروتکل XMPP برای پلتفرم های اندروید، لینوکس، ویندوز، و مک توسعه یافته است، جهت رمزگذاری سر تا سر از پروتکل OMEMO پشتیبانی می نماید.

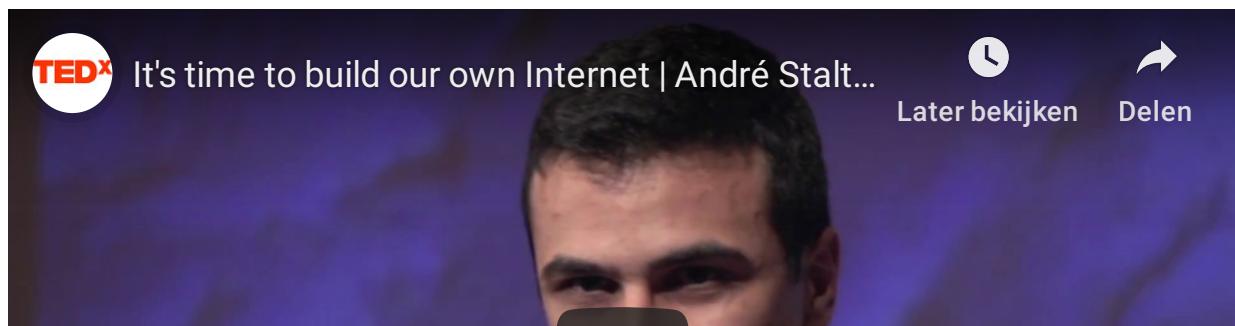
سایرین

به منظور اطلاع از آخرین وضعیت پشتیبانی از پروتکل OMEMO در سایر پیام رسان ها به [این لیست مراجعه نمایید.](#)

## پیام رسان ویژه قطعی احتمالی اینترنت: Manyverse

با توجه به این نکته که پیام رسان نو رسیده [Manyverse](#)، توسط هیچ یک از لیست های فوق معرفی نشده است، تصمیم گرفتم که این مورد را در انتهای مطلب معرفی نمایم.

از آنجایی که با دعوت استارتاپ [HackYourFuture](#) که در چهارکشور هلند، بلژیک، دانمارک و سوئد فعالیت می نماید اولین ورکشاپ این استارتاپ در زمینه [چگونگی ورود به عرصه تولید بازی های کامپیوتری با استفاده از Unreal Engine 4](#) (امکان دریافت اسلایدها در پست) را برگزار نموده ام، به شکل افتخاری در ورک اسپیس اسلک این استارتاپ حضور دارم و آن را دنبال می نمایم. در تاریخ ۲۰ مارس ۲۰۱۹ در کanal فارغ التحصیلان این استارتاپ اعلام شد که شخصی به نام [André Staltz](#) در اولین کنفرانس فارغ التحصیلان این استارتاپ در تاریخ ۸ ژوئن ۲۰۱۹ سخنرانی خواهد داشت. پس از گوگل نمودن نام آندره استالتز و یافتن [این سخنرانی در مجموعه همایش های جهانی تدکس](#)، با پلتفرم Manyverse که توسط آندره استالتز پایه ریزی شده است، آشنا شدم:





نرم افزار Manyverse بر اساس یک ایده آشنا، اما در عین حال کاملاً جدید توسعه یافته است. Manyverse یک برنامه تلفن همراه شبکه اجتماعی با ویژگی هایی است که شما انتظار دارید: پست ها، موضوعات، دوست، پروفایل ها، و غیره؛ اما در کلاد متعلق به یک شرکت اجرا نمی شود، بلکه پست های دوستان شما و تمام داده های اجتماعی شما به طور کامل در تلفن شما نگهداری می شوند. به این ترتیب، حتی زمانی که شما آفلاین هستید، می توانید اسکرول کنید، هر چیزی را بخوانید و حتی پست هایتان را بنویسید و مطالب مورد علاقه تان را لایک نمایید! هنگامی که تلفن شما مجدداً آنلاین می شود، آخرين به روز رسانی ها را مستقیماً با تلفن همراه دوستانتان همگام سازی می نماید. این عملیات می تواند از طریق اینترنت، وایفای مشترک محلی، و یا حتی بلوتوث اتفاق بیافتد.

این پروژه به شکل کاملاً متن باز و رایگان با تلاش علاقمندان توسعه داده می شود چرا که این افراد به ارتباطات تلفن همراه غیر تجاری، بی طرف و منصفانه برای همه اعتقاد دارند.

پیام رسان Manyverse در حال حاضر در [مرحله بتا](#) می باشد. البته این نرم افزار در حال حاضر تا حدود بسیار زیادی به خوبی کار می کند و از ویژگی های ذیل بهره می برد:

- کارایی بدون نیاز به اینترنت
- همگام سازی با استفاده از بلوتوث، شبکه محلی، و یا اینترنت
- پست ها و کامنت ها
- ویژگی بلاک و یا میوت نمودن
- پروفایل

در حال حاضر نسخه اندروید از F-Droid و یا گوگل پلی قابل دریافت است. با وجود این، نسخه آی اواس این پیام رسان هنوز در دست توسعه می باشد.

## سخن پایانی

به دلیل تحمیل تصمیم های امنیتی غلط به کاربران و انتخاب های پیش فرض امنیتی نادرست، مانند چت بدون رمزگذاری سر تا سر و یا سرهم نمودن یک پروتکل که منجر به یک محصول معیوب از نقطه نظر امنیت و حریم خصوصی می شود، تلگرام بهشت موعود برای هکرها و برنامه های نظارتی و جاسوسی جمهوری اسلامی و نهادهای امنیتی آن است.

فی الواقع آنچه که آژانس های اطلاعاتی آرزو دارند، تلگرام یکجا دارد.

بدترین حالت ممکن این است که یک نرم افزار ادعا کند که امن است، در حالی که کاربران آن ممکن است هرگز متوجه این مسئله نشوند که به دلیل عدم فعال بودن پیش فرض رمزگذاری سر تا سر، اطلاعات آن ها در سرور قابلیت رمزگشایی را دارد، و آن ها ممکن است قربانی حملات مرد میانی شوند. تلگرام به عنوان یک پیام رسان امن بازاریابی می شود در حالی که رمزگذاری سر تا سر به صورت پیش فرض غیرفعال است و در صورت فعال نمودن آن شما ویژگی چت های گروهی، نسخه دسکتاپ و یا وب را از دست می دهید. حتی برای کار کردن این قابلیت مخاطب شما بایستی آنلاین باشد.

علیرغم تاکید تمامی کارشناسان حوزه امنیت که معتقدند ابداع و استفاده از رمزنگاری خانگی یک ایده بسیار بد است، آن ها تمامی این هشدارها را نادیده گرفته اند؛ متخصصان حوزه امنیت، آن را خطرناک و نامن نامیده و به شما اطمینان می دهند که اگر حریم خصوصی برای شما مهم است، از آن اجتناب کنید. من و شما و حتی سازندگان

تلگرام متخصص رمزگاری نیستیم. قوانین و نظرات متخصصین حوزه رمزگاری، حاصل دهه ها کار و تحقیق در حوزه امنیت می باشد.

توسعه دهندهان تلگرام تاکید می کنند که با ذخیره داده های شما در کlad تلگرام، می توانید چت های خود را در صورت گم شدن گوشی یا از طریق دستگاه های دیگر بازیابی نمایید. اما چرا آن ها به شما اجازه خروج از کlad تلگرام را نمی دهند؟ و چرا رمزگذاری سرتا سر جهت احترام به حریم خصوصی شما به صورت پیش فرض فعال نیست؟ مسلما نگه داشتن اطلاعات چت شما در این سرورها، باعث ایجاد هزینه های گزارف برای شرکت ناسودبر آن ها می باشد.

علاوه بر این ها، مسایل دیگر مانند نشت متادیتا، عدم پشتیبانی از رمز یکبار مصرف آفلاین، عدم توانایی تایید هویت طرفین در چت های مخفی، نیاز به شماره تلفن جهت ثبت نام، انتقال داده های لیست تماس تلفن همراه به کlad تلگرام و ... خلاف چیزهایی است که در زمینه احترام به رعایت حریم خصوصی آموخته ایم.

تلگرام بسیار شبیه تغییرات آب و هوای است. یک توافق گستردگ در میان آگاهان وجود دارد (بخوانید: رمزگاران آکادمیک و حرفه ای) که نقصان های امنیتی تلگرام حقیقت دارند، و این نقصان ها به شکل تجربی قابل اثبات است. هم‌زمان، اختلافاتی وجود دارد که تقریبا به طور کامل توسط افراد بی اطلاع به وجود آمده است (بخوانید: غیررمزگارها) که نقصان های امنیتی تلگرام را انکار می کنند و تلاش های صورت گرفته جهت نمایش آن ها را از طریق ایجاد انحراف تضعیف می نماید.

اجازه دهید به شکل مختصر و مفید اینگونه بیان کنم: از منظر [تحلیل رمز](#) و بهترین شیوه های طراحی رمزگاری هیچ استدلالی معتبری وجود ندارد که تلگرام دارای یک مدل امنیتی مطلوب باشد.

فراموش نفرمایید که موضوع حریم خصوصی برای فعالان حقوق بشر، فعالان مدنی، فعالان سیاسی، روزنامه نگاران و برندازان در برابر رژیم تمامیت خواهی نظیر جمهوری

اسلامی، غیر قابل چانه زنی است! این امر بایستی به شکل پیش فرض در تمامی سیستم هایی که توسط این افراد مورد استفاده قرار می گیرد رعایت شود.

*aenigma allo android apple assembly barandazan briar :تگ ها  
bsd c c++ cdn censorship chatsecure cia citizenfour  
conversations crypto cryptography cybersecurity dos e2e edward  
snowden facebook facebook messenger fbi five eyes floss foss  
freebsd funtoo fvey gajim gentoo github gitlab gnu google  
guardian haiku instant messaging ios iran islamic republic of iran  
jami keybase kontalk lavabit lfs line linux manyverse metadata  
microsoft mikko hyppönen monal ms-dos mtproto netbsd netflix  
nsa omemo open source open whisper systems openbsd otr prism  
privacy psi+ retroshare richard stallman ricochet riot.im rocket.chat  
reuters security signal silence skype social media status telegram  
tox twitter unix whatsapp wickr windows wire xmpp*



### بیشتر بخوانید

- چرا عرازش و سایبری ها با پروپاگاندای هدایت شده، هم در داخل هم خارج از ایران، از براندازان جلوتر هستند؟
- سری آموزشی توسعه بازی های کامپیوتری و C++
- حملات ریودن هشتگ یا Hashtag Hijacking Attacks چیست و چگونه از آن جلوگیری نماییم؟
- Linux یا FreeBSD مسئله این است؟



© ۲۰۰۶ - ۲۰۱۹ تمامی حقوق برای مددو بابائی محفوظ است.

تمامی محتویات این وب سایت تحت مجوز CC BY-SA 3.0) Creative Commons Attribution-( ShareAlike 3.0 Unported License منتشر شده است. همچنین، تمامی سورس کدهای منتشر شده در این وب سایت تحت لیسانس MIT License منتشر شده است، مگر آن که به صراحت ذکر شده باشد. تمامی محتویات ارائه شده صرفا جنبه آموزشی و اطلاعاتی داشته و قادر هرگونه ضمانت، تعهد یا شرایطی از هر نوع می باشد. بایستی توجه نمود که اطلاعات عرضه شده حتی ممکن است دقیق و یا بروز نباشد. هرگونه اطمینان به و یا استفاده از محتویات یا منابع منتشر شده در این وب سایت با مسئولیت مخاطب بوده و نگارنده یا نگارندگان هیچ گونه مسئولیتی در مورد عواقب آن را نخواهند پذیرفت.

با افتخار نیرو گرفته از FreeBSD | nginx | Hugo v0.55.6  
پوسته توسط Beautiful Hugo تغییر یافته به Beautiful Jekyll  
نسخه d69c4ed