Dr. Alfonso Muñoz

alfonso@criptored.com

@mindcrypt

Privacidad en Telegram: Criptografía bajo estudio

Colabora

Una al día

Hispasec

uma.es

cajamar CAJA RURAL

UAD360

cajamar CAJA RURAL

Hispasec

uma.es

SLIMBOOK

SOFISTIC CYBERSECURITY

freepik

KOODOUS

BBVA

mdigital ESCUELA DE TALENTO DIGITAL

eset Digital Security Progress. Protected.

SMARTFENSE

ALL-PENTESTING

Málaga TechPark

My Public Inbox

Singularity Hackers

Bancard

0xWORD

UPPERY.CLUB

Vulseek By Securetia

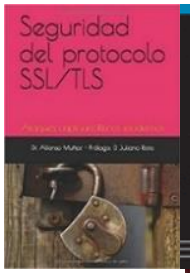
About.me

- **Leading Cybersecurity – SandboxAQ** (previously ***sandbox@alphabet /Google***)
- Doctor Ingeniero Telecomunicación (UPM)
- 18 años de “carretera”…
- Expert security member – Europol (EC3)
- Libros (5), patentes (2), certificaciones de seguridad (+10)…
- ***Investigador y ponente en conferencias de prestigio*** *(RootedCon (12), Ekoparty, Blackhat USA & Europe, 8.8, BSIDES, VirusBulletin, HackInTheBox (3), DeepSec, STIC CCN/CERT (4)…), tools, premios académicos e industriales (3 premios SIC, IDG 2020-Top 50 Blue Team, etc.), artículos científicos en revistas de impacto (+70), docente en másteres universitarios (4)….*
- **Bug hunter** - Security bulletins (Microsoft, Foxit, Google - Hall of fame, etc.).
- *Founder CriptoCert Certified Crypto Analyst & Criptored* https://www.criptocert.com

Perfil:

- Offensive security (sw/hw)
- Cryptography & covert channels/stego
- Cutting-edge research (defensive & offensive)

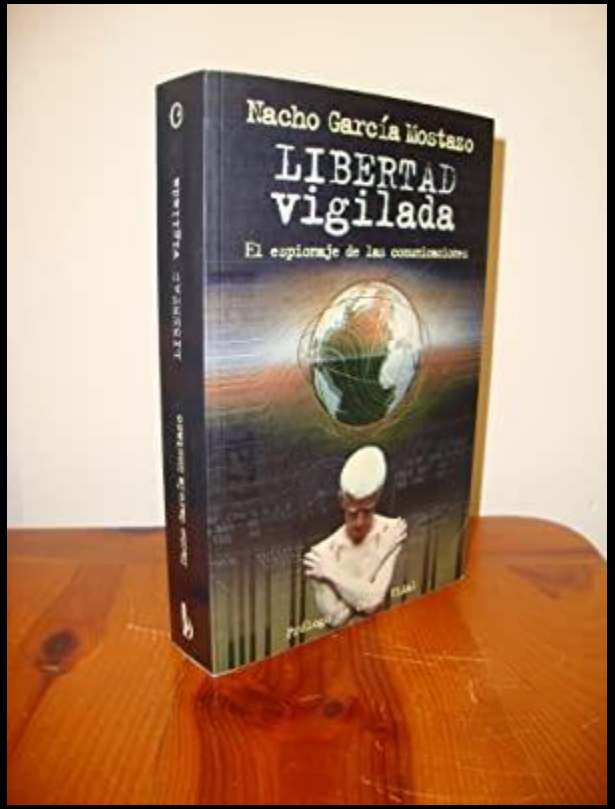
alfonso@criptored.com
t.me/criptored
http://github.com/mindcrypt
https://es.linkedin.com/in/alfonsomuñoz
@mindcrypt



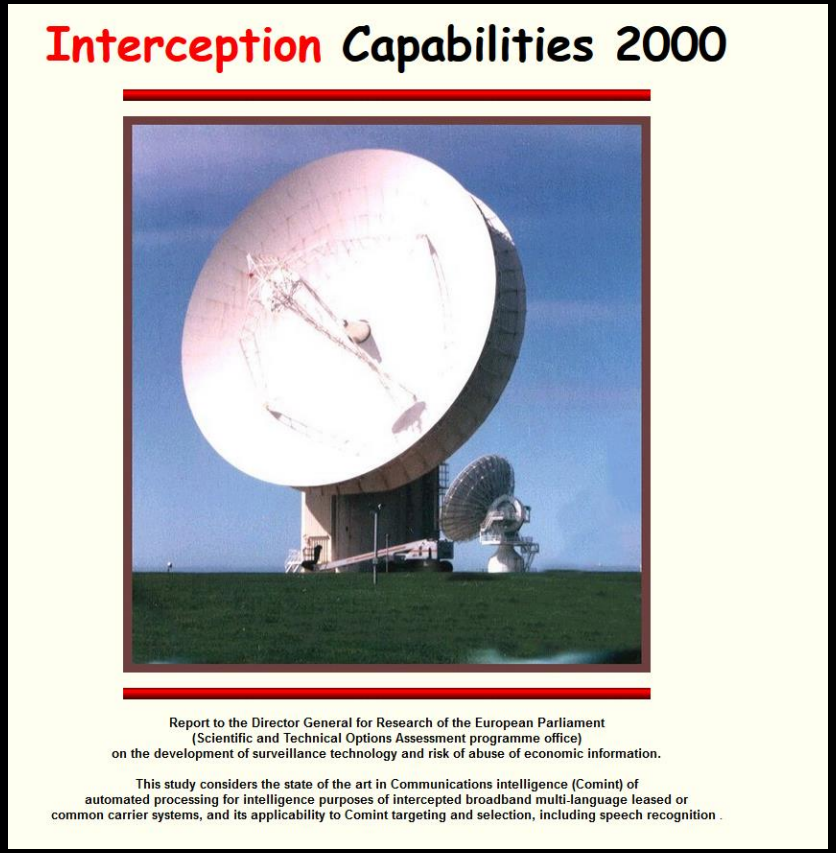
https://www.amazon.com/Criptografía-Ofensiva-Atacando-defendiendo-organizaciones/dp/B08RB6LGRK

UAD360

Toda historia… tiene un comienzo



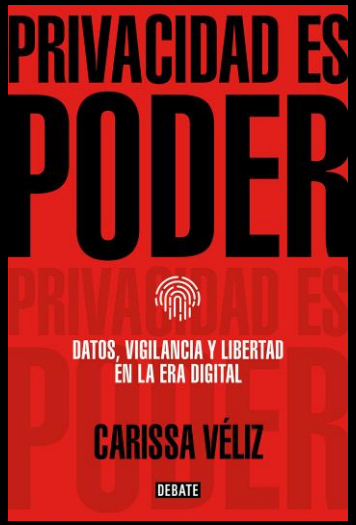
Oct, 2007 - https://www.amazon.es/Libertad-Vigilada-Espionaje-Comunicaciones-Cronica/dp/8466610995/



https://irp.fas.org/eprint/ic2000/ic2000.htm

https://en.wikipedia.org/wiki/Duncan_Campbell_%28journalist%29

UAD360



1. La privacidad no es sólo cosa tuya. La privacidad es algo relativo a la sociedad

Cuando se dice que tus datos son personales parece que se esté dando a entender que tu eres la única parte interesada en compartirlos. Pero eso es un error. La privacidad es tan colectiva como personal.

La privacidad se asemeja en ese sentido a los problemas ecológicos. Por mucho que te esfuerces en minimizar tu huella ecológica si otros no ponen de su parte, todos sufriremos las consecuencias del calentamiento global.

2. La privacidad es “subjetiva”. Soberanía digital

El problema es la asimetría en la privacidad (“Yo no tengo nada que ocultar”)

Lección aprendida - *La criptografía no se ataca… se esquiva*

Edward Snowden publicó documentos que afirman la existencia de programas clasificados con el interés de anular las protecciones criptográficas en comunicaciones y datos.

- Robo de contraseñas, infección de redes y terminales (VPNs), criptoanálisis, infección y colaboración de operadoras de telecomunicación, relaciones e influencias en los organismos de estandarización (Dual_EC_DRBG, SIMON-SPECK, etc.) e industrias principales criptográficas (RSA-EMC…), almacenamiento…

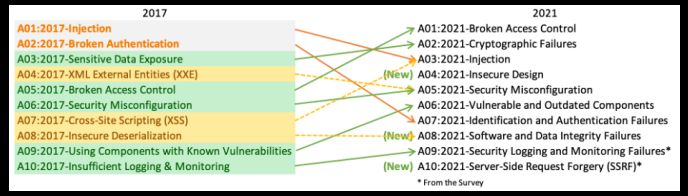
Life before June 2013 – Looking back at Snowden revelations – Matthew Green https://blog.cryptographyengineering.com/2019/09/24/looking-back-at-the-snowden-revelations/

Criptografía… Retos

- Crypto Agility & Criptografía transparente/rápida
  - Es el tiempo de “arquitectos” e “ingenieros”
  - Tamaño de la información (bloque), almacenamiento y velocidad
    - Cifrado de protocolos (redes inalámbricas)
    - Criptografía post-cuántica
    - Criptografía IoT y hardware
      - *Lightweight cryptography standardization*
    - *Full Homomorphic encryption, FPE, PET, MPC, differential privacy…*
    - Mensajería instantánea

Criptosistema	Categoría	Tamaño de clave	Parámetro de seguridad	Algoritmo cuántico estimado que rompa el criptosistema	Nº de qubits lógicos necesarios	Nº de qubits físicos necesarios	Tiempo necesario para romper el sistema
AES-GCM	Cifrado simétrico	128 192 256	128 192 256	Algoritmo de Grover	2.953 4.449 6.681	$4{,}61 \times 10^6$ $1{,}68 \times 10^7$ $3{,}36 \times 10^7$	$2{,}61 \times 10^{12}$ años $1{,}97 \times 10^{22}$ años $2{,}29 \times 10^{32}$ años
RSA	Cifrado asimétrico	1.024 2.048 4.096	80 112 128	Algoritmo de Shor	2.290 4.338 8.434	$2{,}56 \times 10^6$ $6{,}2 \times 10^6$ $1{,}47 \times 10^7$	3,58 horas 28,63 horas 229 horas
ECC Problema del logaritmo discreto	Cifrado asimétrico	256 386 512	128 192 256	Algoritmo de Shor	2.330 3.484 4.719	$3{,}21 \times 10^6$ $5{,}01 \times 10^6$ $7{,}81 \times 10^6$	10,5 horas 37,67 horas 95 horas
SHA256	Minado de Bitcoin	N/A	72	Algoritmo de Grover	2.403	2.23×10^6	$1{,}8 \times 10^4$ años
PBKDF2 con 10.000 iteraciones	Hashing de contraseñas	N/A	66	Algoritmo de Grover	2.403	2.23×10^6	2.3×10^7 años

Ilustración 31. Número de cúbits estimados para anular la criptografía actual. Datos basados en el informe Quantum Computing: Progress and Prospects (2019) y Capítulo 2 - Criptografía en el mundo real (Gonzalo Álvarez Marañón)

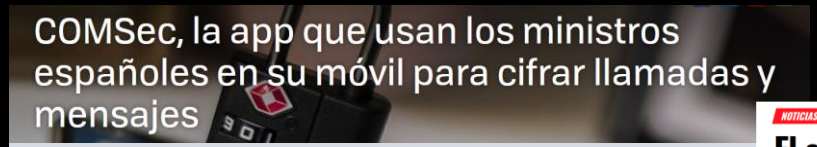


https://owasp.org/www-project-top-ten/

“A02:2021-Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise”

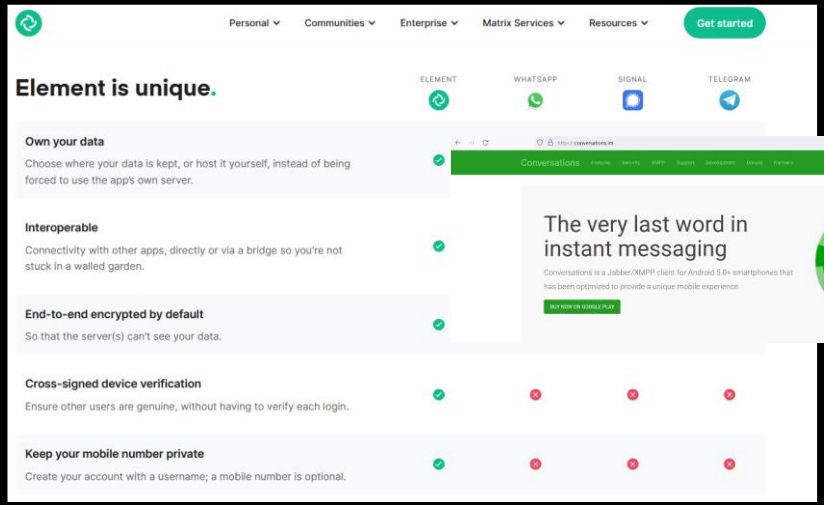
UAD360

¿Mi IM es segura?



(Ene, 2020) https://www.xataka.com/aplicaciones/comsec-app-que-usan-ministros-espanoles-su-movil-para-cifrar-llamadas-mensajes

FÄRIST MOBILE SYSTEM V3.1, ...



https://element.io/personal

NOTICIAS

El ejército suizo prohíbe el uso de WhatsApp, Telegram y Signal

Publicado el 10 enero, 2022 por Eduardo Malo

AN0M: How an app to decrypt criminal messages was born 'over a few beers' with FBI

https://www.rnz.co.nz/news/national/444358/an0m-how-an-app-to-decrypt-criminal-messages-was-born-over-a-few-beers-with-fbi

"Mueve el culo y ve a hablar en persona": por qué no es seguro ni el WhatsApp de los narcos

Policías de distintos países europeos se infiltraron en Encrochat, un sistema encriptado de mensajería muy usado en el mundo del crimen. La operación demuestra la enorme dificultad de crear modos de comunicación completamente seguros

https://elpais.com/tecnologia/2020-07-09/mueve-el-culo-y-ve-a-hablar-en-persona-por-que-no-es-seguro-ni-el-whatsapp-de-los-narcos.html

UAD360

Parámetros a considerar sobre la “seguridad” de mi IM

- ¿Quién está detrás? ¿Modelo de negocio?
- Privacidad de la información
  - Protección de la información (Criptografía) / Metadatos
    - Cliente-Servidor & Cliente-Cliente
  - Contactos y permisos
  - Duración de los mensajes
  - Almacenamiento local y remoto de la información
- Seguridad de la aplicación y actualizaciones
- Anonimato y rastreo de los comunicantes. Jurisdicción
- Autenticación y autorización
- Servidores
- Disponibilidad/Denegación de servicio (el gran olvidado) (¿centralizado?)
- …

¿Mi IM es segura?

	Google Messages	Apple iMessage	Facebook Messenger	Element / Riot	Signal	Microsoft Skype	Telegram	Threema	Viber	Facebook Whatsapp	Amazon Wickr Me	Wire	Session
Overview													
Is the app recommended to secure my messages and attachments?	No	No	No	No	Yes	No	No	Yes	No	No	No	Yes	Yes
Main reasons why the app isn't recommended **Improvements to apps that are recommended** More details	Named as NSA partner in Snowden revelations Makes money from personal data Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Named as NSA partner in Snowden revelations Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Named as NSA partner in Snowden revelations Encryption not enabled by default Makes money from personal data Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	No independent & recent code audit and security analysis	Remove the mandatory requirement for users to sign up with a mobile number Provide more comprehensive independent assessments of security/privacy	Named as NSA partner in Snowden revelations Encryption not enabled by default Makes money from personal data Data not protected, not all data protected Closed source	Bespoke cryptography Encryption not enabled by default Data not protected, not all data protected	Make APIs and server code open source Implement perfect forward secrecy at the end-to-end encryption layer Provide more comprehensive independent assessments of security/privacy	Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Named as NSA partner in Snowden revelations Messages can be read by Facebook if marked as "abusive" Makes money from personal data Data not protected, not all data protected No independent & recent code audit and security analysis Closed source	Former NSA chief Keith Alexander is on Amazon's board of directors Funded by the CIA Recent security audits are not public Closed source	Further limit metadata storage and logging Provide more comprehensive independent assessments of security/privacy	Implement perfect forward secrecy at the end-to-end encryption layer Provide more comprehensive independent assessments of security/privacy
Details													
Company jurisdiction	USA	USA	USA	UK	USA	USA	USA / UK / Belize / UAE	Switzerland	Luxembourg / Japan	USA	USA	USA / Switzerland	Australia
Infrastructure jurisdiction	Worldwide (rollout on-going, unsure of exact locations, most likely Google Cloud regions)	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 (unsure of other locations)	USA (unsure of other locations)	EU	Messages: Worldwide (uses de-centralised servers) Attachments: Centralised server in Canada
Implicated in giving	Yes	Yes	Yes	No	No	Yes	No	No	No	Yes	No	No	No

	Telegram
Is the app recommended to secure my messages and attachments?	No
Main reasons why the app isn't recommended **Improvements to apps that are recommended** More details	Bespoke cryptography Encryption not enabled by default Data not protected, not all data protected
Are reproducible builds used to verify apps against source code?	iOS and Android
Can you sign up to the app anonymously?	No
Can you add a contact without needing to trust a directory server?	No
Can you manually verify contacts' fingerprints?	No (session only, does not provide users' fingerprint information)
Directory service could be modified to enable a MITM attack?	Yes
Do you get notified if a contact's fingerprint changes?	No (session only, does not provide users' fingerprint information)
Is personal information (mobile number, contact list,	No

Company jurisdiction	USA / UK / Belize / UAE
Infrastructure jurisdiction	UK, Singapore, USA, and Finland
Implicated in giving customers' data to intelligence agencies?	No
Surveillance capability built into the app?	No
Does the company provide a transparency report?	No
Company's general stance on customers' privacy	Poor
Funding	Pavel Durov
Does the app generate & keep a private key on the device itself?	Yes
Can messages be read by the company?	Yes
Does the app enforce perfect forward secrecy?	No (session keys do change after being used 100 times)
Does the app encrypt metadata?	No
Does the app use TLS/Noise to encrypt network traffic?	No
Does the app use certificate pinning?	
Does the app encrypt data on the device? (iOS and Android only)	
Does the app allow a secondary factor of authentication?	Yes

Company collects customers' data?	Yes
App collects customers' data?	Contact info / contacts / identifiers
User data and/or metadata sent to parent company and/or third parties?	Yes
Is encryption turned on by default?	No
Cryptographic primitives	RSA 2048 / AES 256 / SHA-256
Are the app and server completely open source?	No (clients and API only)
Are messages encrypted when backed up to the cloud?	
Does the company log timestamps/IP addresses?	Yes
Have there been a recent code audit and an independent security analysis?	Yes (November, 2015)
Is the design well documented?	Somewhat
Does the app have self-destructing messages?	Yes

https://www.securemessagingapps.com/

Telegram
En detalle

UAD360

Historia - ¿Quién está detrás?

- Telegram es una plataforma de mensajería y VOIP, desarrollada por los hermanos Nikolái y Pável Dúrov.
- Se anuncia oficialmente 14 de agosto de 2013 [Signal 2010, Whatsapp: 2009 (creación), abril 2016 (E2E encryption), 2021 (backup Encryption)]

- Pável funda en 2006 la red social VK (Vkontakte) /be-con-tac/ (en contacto con). Red similar a Facebook con enfoque inicial en Rusia, Ucrania y Bielorrusia. En 2014 "deja" (vende sus acciones) la compañía ante la imposibilidad de evitar el control por parte del gobierno ruso / FSB.

+500 millones de usuarios activos/mes

Home › News › What is Telegram Premium? Everything You Need to Know

What is Telegram Premium? Everything You Need to Know

Subin B - Last Updated: June 8, 2022 3:48 pm

- "Opositores" a
  de Rusia. Pávе
  financiación y
  - Telegra
    desarrollo del servicio de mensajería
  - Telegram Group Inc (Islas Vírgenes Británicas) su matriz para operaciones tecnológicas

- Modelo de negocio (coste "*cientos*" de millones al año…)
  - Ofrecer nuevas características de pago para usuarios avanzados y empresas.
  - Generar beneficios económicos con stickers de artistas.
  - Colaborar con canales de alta demanda de usuarios con su plataforma de mensajes patrocinados.
  - https://www.france24.com/es/minuto-a-minuto/20210323-telegram-recauda-1-000-millones-de-dólares-en-una-emisión-de-bonos

Директору Федеральной
службы безопасности
России
Бортникову А.В.

Уважаемый Александр Васильевич!

Исполняя требования Федерального закона от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон „О противодействии терроризму“ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности», а также Федерального закона от 27 июля 2017 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», направляю вам ключи (2 шт.) от кроссплатформенного мессенджера Telegram со своими наилучшими пожеланиями.

Всего самого доброго

П.В.Дуров

Figure 1: A satirical letter from Pavel Durov to the FSB Director Alexander Bortnikov, and two accompanying metal keys. Published by the director of Agora, Pavel Chikov, on his personal Telegram channel on 10 April 2018, at https://t.me/pchikov/929.

The Telegram ban: How censorship "made in Russia" faces a global Internet
by Ksenia Ermoshina and Francesca Musiani

Abstract
When, in April 2018, the Russian Internet watchdog Roskomnadzor orders to block Telegram — the country's most popular messenger — Internet users in the country respond with a diverse set of digital resistance tactics, including obfuscation and circumvention protocols, proxies, virtual private networks, and full-fledged hacks. This article analyzes the "Telegram ban" and its ramifications, understanding it as a socio-technical controversy that unveils the tensions between the governmental narrative of a "sovereign Internet" and multiple infrastructure-based battles of resistance, critique and circumvention. We show how, in the context of a Russian Internet which is heavily entwined with and dependent from foreign and global infrastructures, a number of bottom-up, infrastructure-based digital resistances are able to emerge and thrive despite the strategy of effective centralised management that the Russian government seeks to present to the world as its own.

Contents
Introduction
The "Telegram ban"?
Methodology and theoretical framing

https://firstmonday.org/ojs/index.php/fm/article/view/11704/10130

https://www.usenix.org/conference/foci18/presentation/marechal

usenix ASSOCIATION Conferences Sign In

FOCI '18 ATTEND PROGRAM PARTICIPATE SPONSORSHIP ABOUT

From Russia With Crypto: A Political History of Telegram

Authors:
Nathalie Marechal, *University of Southern California*

Abstract:
This paper offers a political history of Telegram, a platform that combines aspects of social n
to user privacy and freedom of expression has brought it into open conflict with a number o
history traces Telegram's roots to Pavel Durov's ouster from Vkontakte, the social networking

April 22, 2018

Durov's Channel
For 7 days Russia has been trying to ban Telegram on its territory – with no luck so far. I'm thrilled we were able to survive under the most aggressive attempt of internet censorship in Russian history with almost 18 million IP addresses blocked.

If you live in Russia and support free internet, fly a paper plane from your window at 7 PM local time today. Please collect the airplanes in your neighborhood an hour later – remember, today is Earth Day.

My thanks to all the members of the #DigitalResistance movement. Keep up your great work setting up socks5-proxies and VPNs and spreading them among your Russian friends and relatives. They will be needed as the country descends into an era of full-scale internet censorship.

1.3M 15:16

Ukraine NOW [English]
63.155 subscribers
Previous message
Only up-to-date and verified information about events in Ukraine in different languages. ...

Ukraine NOW [English]
00:31
Husbands, fathers, sons and friends leaving Dublin airport to go and fight the war in Ukraine
#StandWithUkraine
Video: RTÉ News
702 320 60 12 3

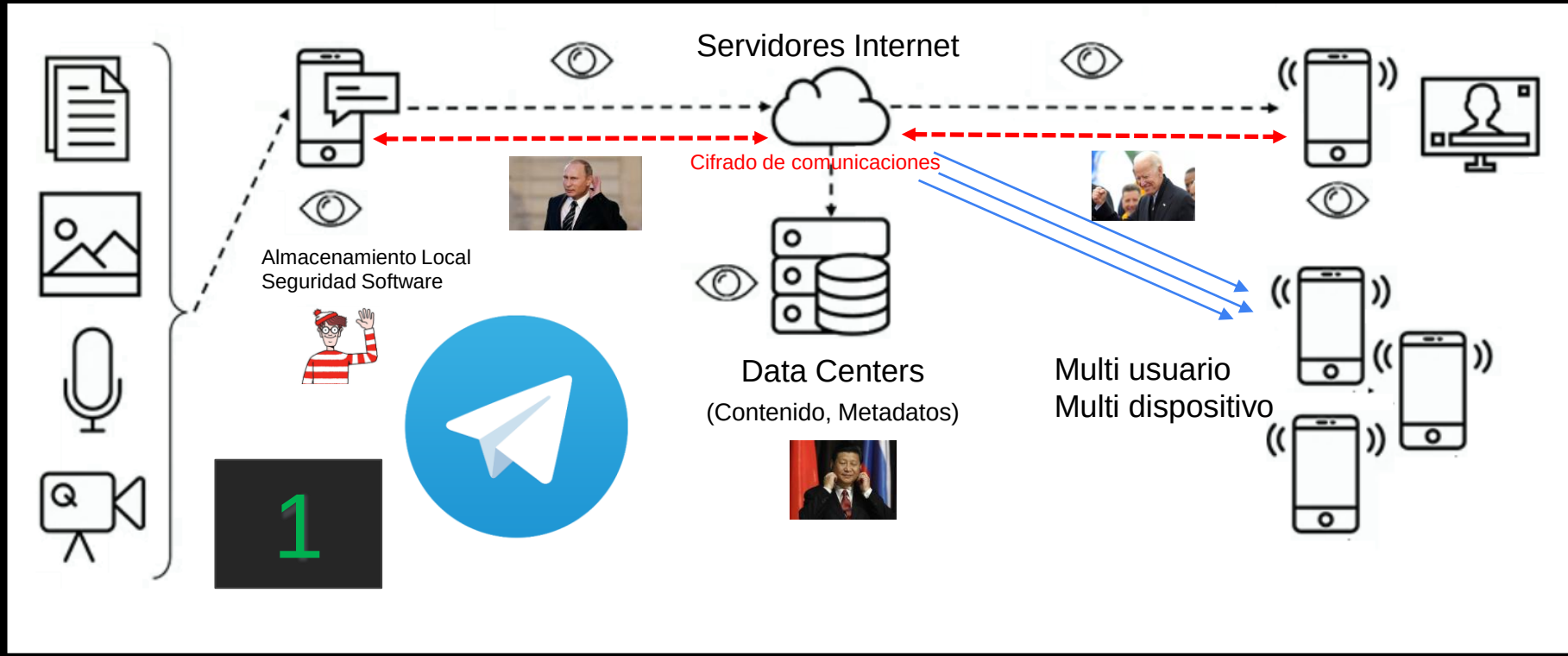
IT ARMY of Ukraine
275.176 subscribers

IT ARMY of Ukraine
Важливо максимально ускладнити роботу електронних підписів в росії. Ось перелік їх центрів видачі ключів:
—
Time to block electronic signature services in Russia. Find below:

https://iecp.ru/ep/ep-verification
https://iecp.ru/ep/uc-list
https://uc-osnovanie.ru/
http://www.nucrf.ru
http://www.belinfonalog.ru
http://www.roseltorg.ru
http://www.astralnalog.ru
http://www.nwudc.ru

UAD360

Privacidad – “Puntos de dolor”



Anonimato y rastreo de los comunicantes

¿Qué conocen los servidores?

Telegram – What personal Data We Use

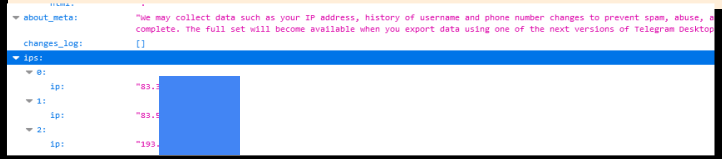
"To improve the security of your account, as well as to prevent spam, abuse, and other violations of our Terms of Service, we may collect metadata such as your IP address, devices and Telegram apps you've used, history of username changes, etc. If collected, this metadata can be kept for 12 months maximum."

We may share your personal data with: *(1)* our parent company, Telegram Group Inc, located in the British Virgin Islands; and *(2)* Telegram FZ-LLC, a group member located in Dubai, to help provide, improve and support our Services.

- **Basic account data** (mobile number, profile name-picture, e-mail) (tus dispositivos, versión del SO)
- **Grupos (altas/bajas), tus mensajes y ficheros/nombres de ficheros (cloud chats, public chats) en servidor Telegram**
- **Chat secretos E2E (Servidor Telegram y CDNs) – EL SERVIDOR ESTÁ EN MEDIO!!!!**

  ***Servidor almacena ficheros cifrados (E2E): sabe el nombre, sabe quién los recibe (sabe con quién te comunicas), "logs de conectividad"…**
- **Voz y videollamadas: con quién hablas…**
- **Contactos y Localización (si la compartes)**
- **Cookies**

https://telegram.org/privacy

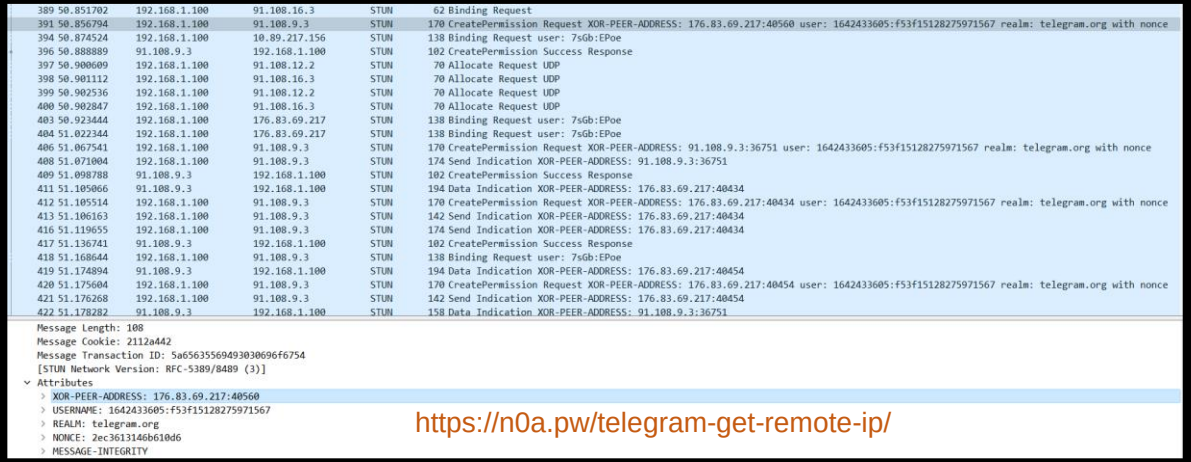


Settings->Advanced->Export Telegram data
(Account Information, contacts, chat, media, sessions, …)

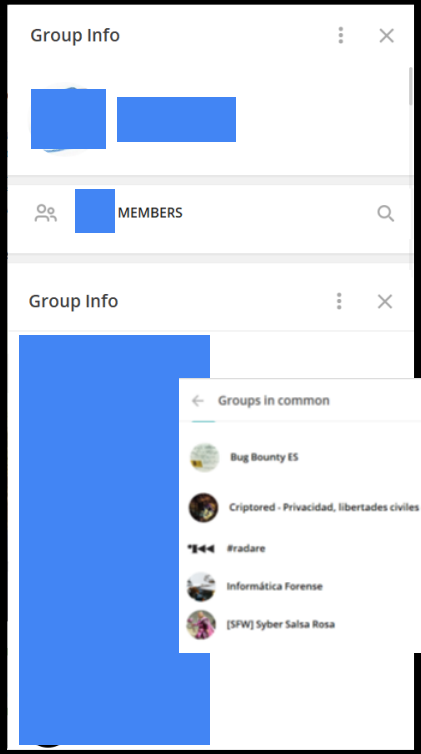
Anonimato y rastreo de los comunicantes

¿Qué puede conocer/hacer un usuario desde Telegram?

- *Datos públicos (nick, “telefono”, …)*
- *Enumeración de grupos/usuarios en canales/grupos públicos y mensajes*
- *Obtener la dirección IP de un destinatario o varios*
  - *(Chat Secret 1a1) - En una llamada (y localizarle)*
  - *…*



https://n0a.pw/telegram-get-remote-ip/



https://github.com/ItIsMeCall911/Awesome-Telegram-OSINT

Telegram, al hacer las llamadas, usa un protocolo llamado Stun. Este protocolo hace que los clientesNAT puedan encontrar su dirección IP pública.

UAD360

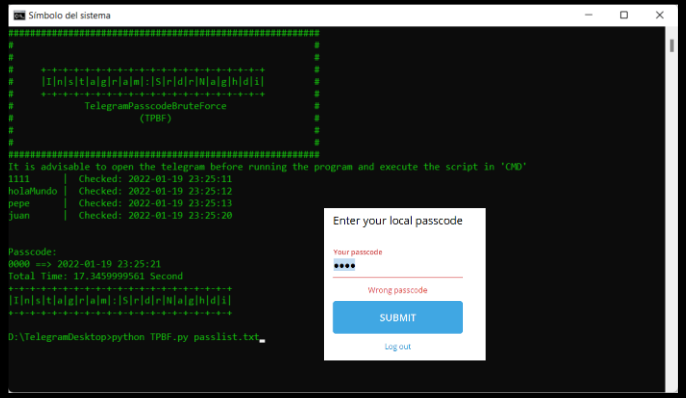
Seguridad del Endpoint – “Puntos de dolor”

Seguridad del cliente Telegram

https://en.wikipedia.org/wiki/Telegram_(software)#Architecture

These techniques permit the CIA to bypass the encryption of WhatsApp, Signal, Telegram, Wiebo, Confide and Cloackman by hacking the "smart" phones that they run on and collecting audio and message traffic before encryption is applied.

- Código fuente de clientes *DISPONIBLE* (GPLv3) (Telegram Desktop, Telegram X, …) y compilaciones reproducibles
  - https://telegram.org/apps#codigo-fuente
  - https://core.telegram.org/reproducible-builds
- Actualizaciones “periódicas” no “predecibles” (¿Riesgo?)
  - Ej., https://github.com/telegramdesktop/tdesktop/releases
  - Actualización cada 1, 2, 3, 4, 7, 16, 19 días…
- Funcionalidades de seguridad
  - Código de bloqueo (local) *(bypass!!!) (*)*
  - Verificación de dos pasos al registrarse en un nuevo dispositivo (password+SMS code),(recovery email)
  - Proxies, Eliminación de cuenta, temporizadores autodestrucción…
- Almacenamiento local de la información & backup *(*)*
  - Herramientas forenses (Ej, Oxygen forensic). Ej, localstorages, sqlite, tdata, caches
  - Settings->Advanced->Export Telegram data (Ej, Desktop)
- Riesgos (“la criptografía no se ataca se esquiva”)
  - Claves públicas, dirección IP, …, codificadas en el binario
  - “Malas” implementaciones de clientes, “modificación” del binario oficial, almacenamiento…

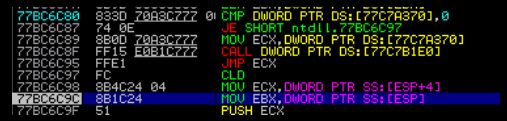


https://github.com/SrdrNaghdi/Telegram-Passcode-Brute-Force

Passcode: Telegram Desktop/tdata/ -> key_datas y maps

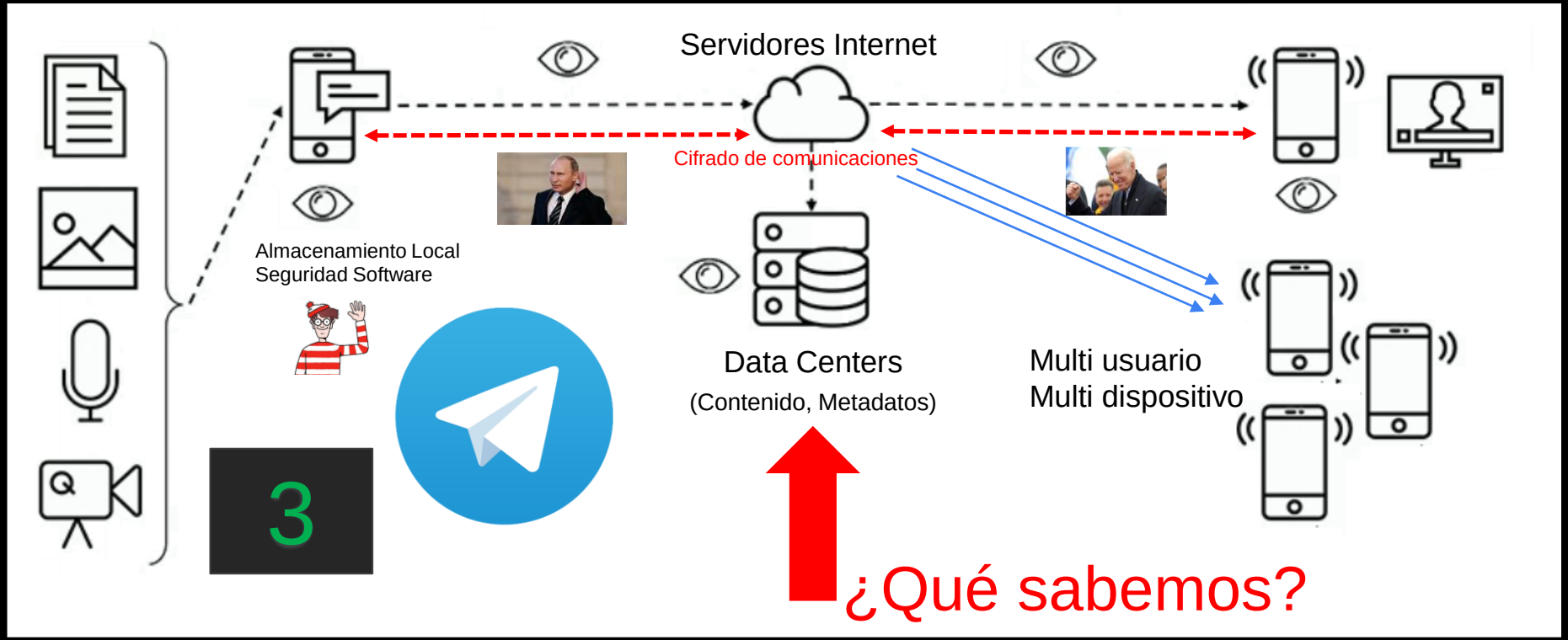
PKCS5_PBKDF2_HMAC, SHA512

https://en.wikipedia.org/wiki/Key_stretching



UAD360

Servidores Telegram – “Puntos de dolor”

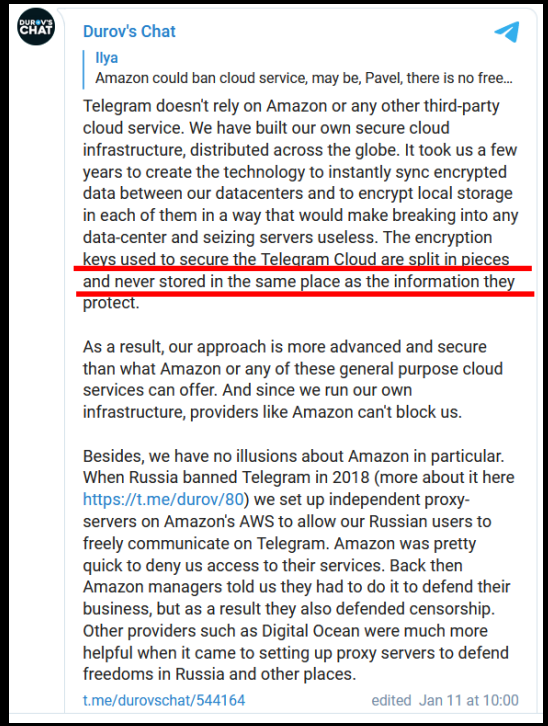


¿Qué sabemos de los servidores? ¿Dónde están?

https://telegram.org/evolution

- Código CERRADO ☹ - ¿Aunque fuera abierto no se puede verificar?
- ¿Qué almacenan? -> Ver la slide "Anonimato y rastreo"
  - Servidores almacenan información en claro y *cifrada* (fotos, videos y documentos), metadatos, *claves*…
- ¿Dónde están los servidores?¿Cómo almacenan la información?
  - OSINT (web, certificados, DNS, …)
    - Dominio web – https://web.telegram.org – 149.154.167.99 (London/UK)
    - Subdominios DNS (en IPs diferentes al dominio web)
    - Código Fuente de los clientes Telegram + Documentación official ☹
    - Proxy - Interceptación de tráfico (Telegram Desktop, Web, …)
    - Archive.org + Employee location: mail, google/bing dorks, pull requests,…
  - Ips: 149.154.{162, 163,164,167,170,171,175}.* 95.161.64.*, 18.194.34.*, 52.97.133.*, 142.250.200.*…
- "5 servidores + 3 servidores test (IPv4/IPv6)"

149.154.175.{50,100} (Antigua and Barbuda), 149.154.167.{51,91} (London/UK), 149.154.171.5 (Antigua and Barbuda), 149.154.175.{10,117,40} (Antigua and Barbuda)



Durov's Chat

Ilya
Amazon could ban cloud service, may be, Pavel, there is no free...

Telegram doesn't rely on Amazon or any other third-party cloud service. We have built our own secure cloud infrastructure, distributed across the globe. It took us a few years to create the technology to instantly sync encrypted data between our datacenters and to encrypt local storage in each of them in a way that would make breaking into any data-center and seizing servers useless. The encryption keys used to secure the Telegram Cloud are split in pieces and never stored in the same place as the information they protect.

As a result, our approach is more advanced and secure than what Amazon or any of these general purpose cloud services can offer. And since we run our own infrastructure, providers like Amazon can't block us.

Besides, we have no illusions about Amazon in particular. When Russia banned Telegram in 2018 (more about it here https://t.me/durov/80) we set up independent proxy-servers on Amazon's AWS to allow our Russian users to freely communicate on Telegram. Amazon was pretty quick to deny us access to their services. Back then Amazon managers told us they had to do it to defend their business, but as a result they also defended censorship. Other providers such as Digital Ocean were much more helpful when it came to setting up proxy servers to defend freedoms in Russia and other places.

t.me/durovschat/544164 edited Jan 11 at 10:00

If you live in a country in the European Economic Area (EEA), the Services are provided by Telegram, which for the purposes of applicable data protection legislation is the data controller responsible for your personal data when you use our Services. However, as Telegram is located outside the EEA, we have designated one of our EEA-based group companies, Telegram UK Holdings Ltd (71-75 Shelton Street, Covent Garden, London, England, WC2H 9JQ), as a representative to whom you may direct any issues you have relating to our processing of your personal data.

4.1. Storing Data

If you signed up for Telegram from the UK or the EEA, your data is stored in data centers in the Netherlands. These are third-party provided data centers in which Telegram rents a designated space. However, the servers and networks that sit inside these data centers and on which your personal data is stored are owned by Telegram. As such, we do not share your personal data with such data centers. All data is stored heavily encrypted so that local Telegram engineers or physical intruders cannot get access.

¿Qué sabemos de los servidores? ¿Dónde están?

https://telegram.org/evolution

Durov's Chat

Ilya

Amazon could ban cloud service, may be, Pavel, there is no free...

Telegram doesn't rely on Amazon or any other third-party cloud service. We have built our own secure cloud

Go to CIA.gov

THE WORLD FACTBOOK

led by Prime Minister Gaston Browne, continues to face significant fiscal challenges. The government places some hope in a new Citizenship by Investment Program, to both reduce public debt levels and spur growth, and a resolution o a WTO dispute with the US.

Contents

- Introduction
- Geography
- People and Society
- Environment
- Government
- Economy
- Energy
- Communications
- Transportation
- Military and Security
- Transnational Issues

Real GDP (purchasing power parity)

$1.76 billion note: data are in 2017 dollars (2020 est.)

$2.09 billion note: data are in 2017 dollars (2019 est.)

$2.02 billion note: data are in 2017 dollars (2018 est.)

note: data are in 2017 dollars

country comparison to the world: 198

Real GDP per capita

$18,000 note: data are in 2017 dollars (2020 est.)

$21,500 note: data are in 2017 dollars (2019 est.)

$21,000 note: data are in 2017 dollars (2018 est.)

note: data are in 2017 dollars

country comparison to the world: 94

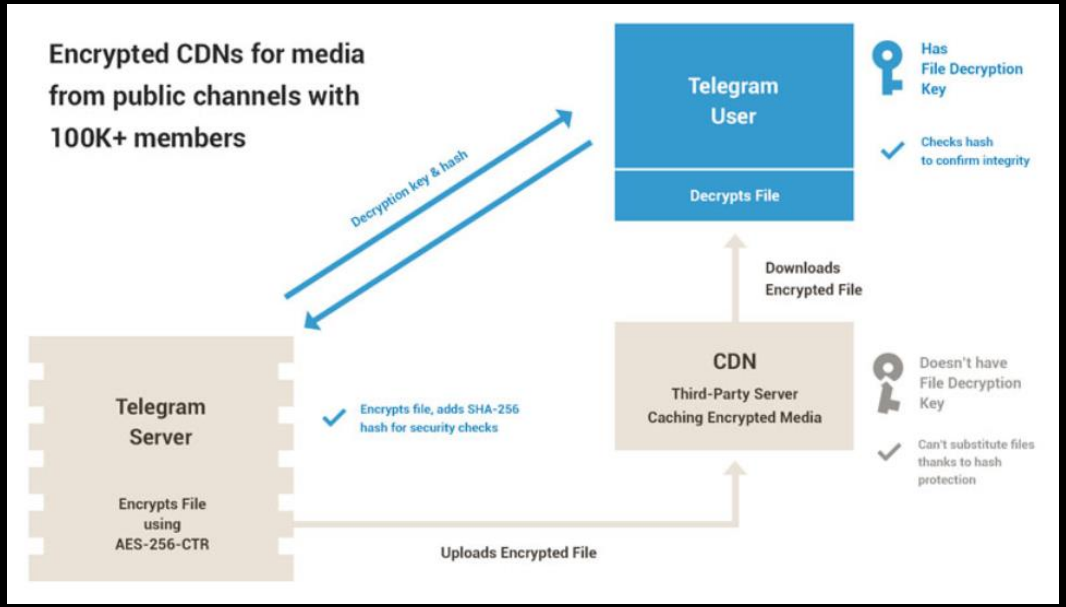
whom you may direct any issues you have relating to our processing of your personal data.

ta

or Telegram from the UK or the EEA, your data is stored in data centers in the Netherlands. These are third-party provided data centers in which Telegram rents a designated space. However, the servers and networks that sit inside these data centers and on which your personal data is stored are owned by Telegram. As such, we do not share your personal data with such data centers. All data is stored heavily encrypted so that local Telegram engineers or physical intruders cannot get access.

¿Qué sabemos de los servidores? ¿Dónde están?

https://core.telegram.org/cdn



"CDN DCs do not store files on hard disks – only in memory. When a CDN server runs out of memory, a simple LRU algorithm is used to replace the least popular files with new ones…"

https://core.telegram.org/techfaq#q-can-the-cdn-decipher-the-files
https://telegra.ph/On-Rumors-About-Telegram-Servers-in-Weird-Places-07-30

How this works

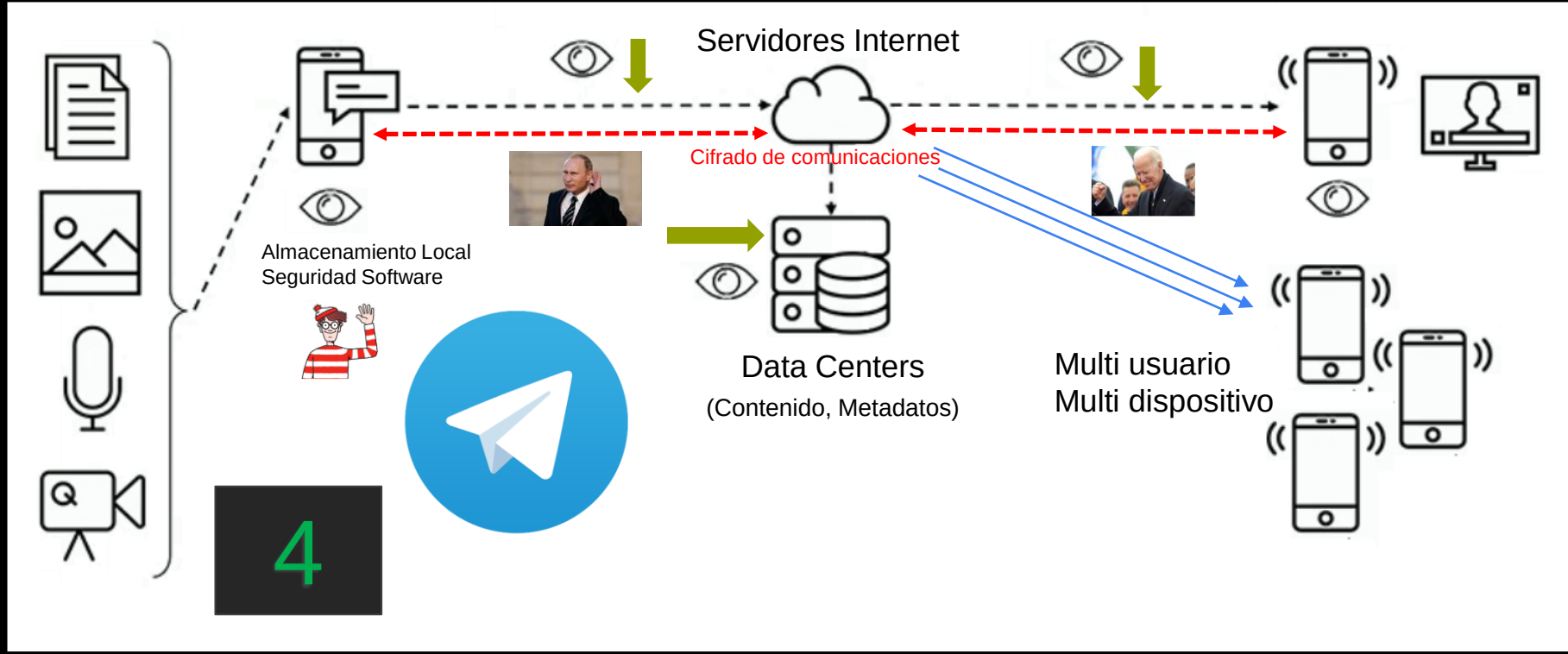
"When a file from a public channel with **~100,000** members becomes popular in a particular region, the Telegram server may encrypt this file with a unique AES-256-CTR key and send it to a relevant CDN DC for storage…

This is secure because CDN DCs are treated the same way as internet providers / random third parties:

- CDN DCs don't have the keys to decrypt files that are stored there, so they can't access the data even if a DC becomes compromised.
- Encrypted files fragments are protected from tampering by their SHA-256 hash which is checked on the client upon receipt.
- No private data is stored in or passed to the CDN DCs.
- The server only allows media from public channels with more than **100,000** subscribers to be cached in CDN DCs (this includes media forwarded from those channels and viral media that originated from other large public channels)"

Criptografía en tránsito / almacenamiento en servidor – “Puntos de dolor”

Protocolo de comunicación y protección de mensajes



https://core.telegram.org/mtproto | Código fuente clientes + Binarios Ej. Última versión Telegram Desktop (Windows, >3.4.X) y Telegram X (Android, > 8.5.X)

TDLIB (Telegram Database library) + Código fuente | Investigaciones académicas y terceros

Principios básicos de Criptografía (Telegram)

https://core.telegram.org/mtproto/description

- Mobile Transport Protocol - MTProto V2 (v2 2017-…, v1 2014-2017)
  - Protocolo diseñado desde cero. Decisiones criptográficas "controvertidas" y "actualizaciones oscuras"
  - MTProto v2 está enfocado en la multisesión (asíncrona), multiplataforma y el transporte de archivos sin importar su formato o capacidad desde varios dispositivos *(importante desde el punto de vista de la criptografía)*
  - Fases y modalidades
    - 1. Registro del dispositivo/sesión
    - 2. Cifrado y autenticación de la información
    - 3. Intercambio de claves
      Derivación de claves y PFS (Perfect Forward Secrecy)
    - Encryption client-server – Cloud chats (por defecto)
      - Public Channels & groups (Cloud chats)
    - Encryption client-client (E2E) – Secret chats
    - Video and voice calls
- Primitivas criptográficas: DH, RSA, SHA-1, SHA-256, AES, IGE, …

Q: Why are you mostly relying on classical crypto algorithms? We prefer to use well-known algorithms, created in the days when bandwidth and processing power were both a much rarer commodity. This has valuable side-effects for modern-day mobile development and sending large files, provided one takes care of the known drawbacks. *The weakspots of such algorithms are also well-known, and have been exploited for decades. We use these algorithms in such a combination that, to the best of our knowledge, prevents any known attacks.*

Q: Why are you not using X? (insert solution)
While other ways of achieving the same cryptographic goals, undoubtedly, exist, we feel that the present solution is both robust and also succeeds at our secondary task of beating unencrypted messengers in terms of delivery time and stability.

Criptografía Telegram for Dummies (Basics)

- **Hash criptográfico** – Calcula un resumen "comprimido" de un conjunto de bits (SHA-1, SHA-256) - Autenticación
- **Criptografía simétrica** – Emisor y receptor necesitan un/varias claves compartidas. Ej, algoritmo AES
- **Criptografía asimétrica** – Emisor y receptor tienen un par distinto de (clave pública, clave privada). Típicamente clave pública para CIFRAR, clave privada para DESCIFRAR o FIRMAR/AUTENTICAR -> Problema MitM.

Quiero TORTAS LOCAS!!!!

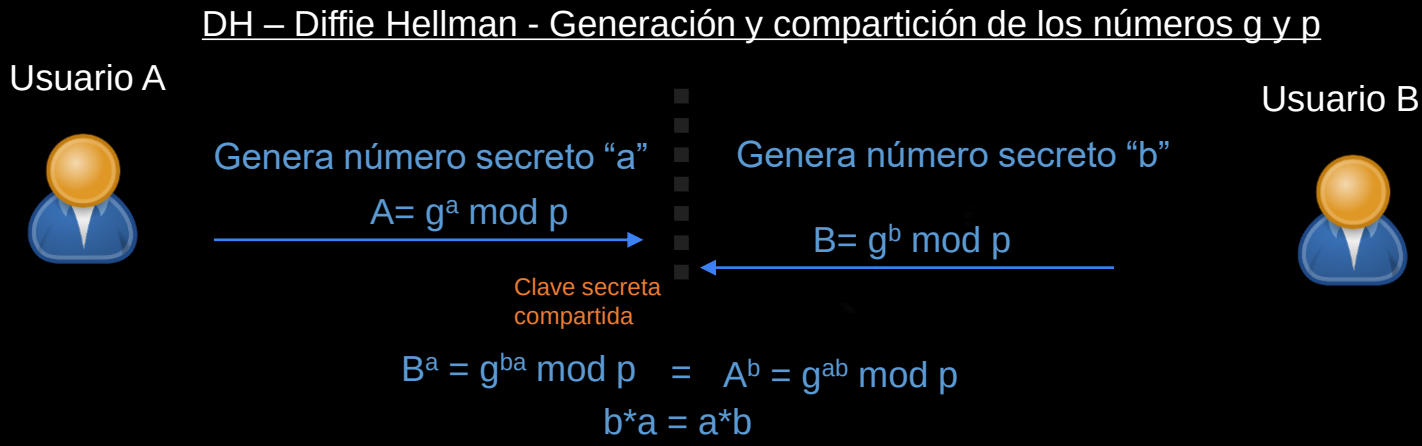
Side Channels – "El olor de la tortas…"

TTP

- NIST, PKI, …

Criptografía Telegram for Dummies (Basics)

- **Criptografía asimétrica** – Emisor y receptor tienen un par distinto de (clave pública, clave privada). Típicamente clave pública para CIFRAR, clave privada para DESCIFRAR o FIRMAR/AUTENTICAR -> Problema MitM.
  - RSA -> Clave pública son dos números (e,n) → cifrado = $mensaje^e \bmod n$ | $mensaje = cifrado^d \bmod n$
  - Diffie-Hellman -> Clave pública basada en dos valores g,p y clave privada dos números aleatorios a y b

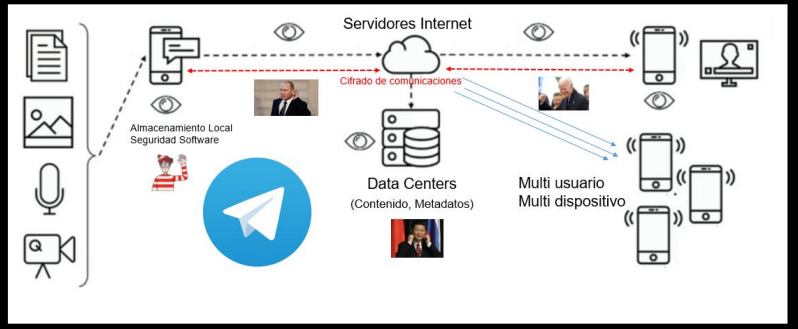


Dividendo = Divisor * Cociente + Resto
RSA => $Cifrado^d = n*cociente' + Mensaje$
DH => $g^a = p*cociente'' + A$

UAD360

1. Registro del dispositivo/sesión

Upon first installing the Telegram messaging application on a new device the user will be prompted to enter his/her phone number. This is used for authentication of the user for future logins as opposed to a username/email and password. After entering the phone number, the user will receive a five digit code by SMS in order to verify the number. Upon entering this code in the Telegram application, it will start the device authorization protocol.



Creating an Authorization Key

An authorization key is normally created once for every user during the application installation process immediately prior to registration. Registration itself, in actuality, occurs after the authorization key is created. However, a user may be prompted to complete the registration form while the authorization key is being generated in the background. Intervals between user key strokes may be used as a source of entropy in the generation of high-quality random numbers required for the creation of an authorization key.

See Creating an Authorization Key.

During the creation of the authorization key, the client obtains its server salt (to be used with the new key for all communication in the near future). The client then creates an encrypted session using the newly generated key, and subsequent communication occurs within that session (including the transmission of the user's registration information and phone number validation) unless the client creates a new session. The client is free to create new or additional sessions at any time by choosing a new random session_id.

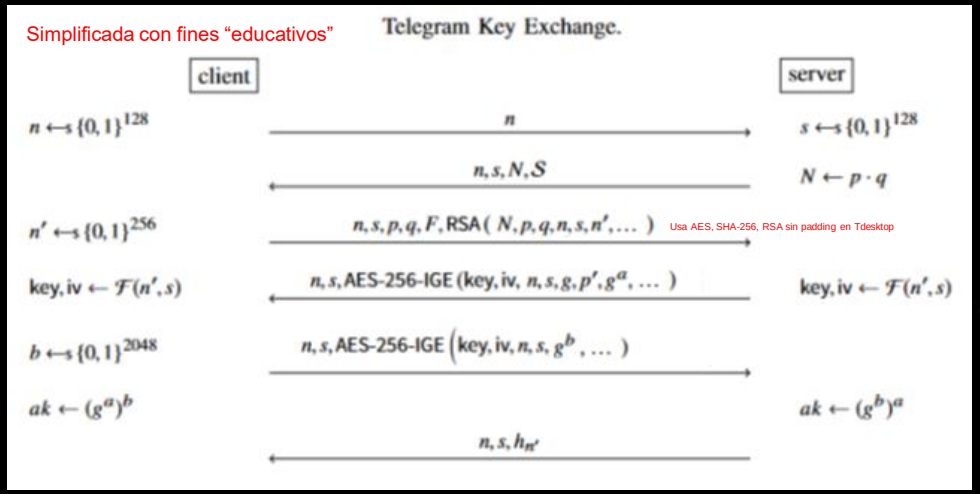
https://core.telegram.org/mtproto/description

Registro del dispositivo/sesión – Clave de autorización

https://core.telegram.org/mtproto/auth_key

- *Server authenticated - "The DH exchange is authenticated with the server's public RSA-key that is built into the client (the same RSA-key is also used for protection against MitM attacks)"*
- *Client authenticated – Various secrets (nonce, server_nonce, new_nonce) exchanged during key generation guarantee that the DH-key can only be obtained by the instance that initiated the exchange. Notice that new_nonce is transferred explicitly only once, inside an RSA-encrypted message from the client to the server.*

Simplificada con fines "educativos"



https://mtpsym.github.io/paper.pdf (Cloud chats)

https://core.telegram.org/mtproto/auth_key#dh-exchange-initiation | https://core.telegram.org/mtproto/samples-auth_key | mtproto_dc_key_creator.cpp | mtproto_rsa_public_key.cpp | mtproto_dh_utils.cpp

Números aleatorios (nonce)

n (cliente), s (servidor)

n' = número aleatorio importante 256 bits (no va en claro)

"Desafío criptográfico" (Proof of work)

N=p*q, valor menor 2^{63}-1

Fingerprints claves públicas

S = Fingerprints ofrecidas por el servidor

F = Fingerprint seleccionada por el cliente

F(n',s) Función para derivar claves basada en SHA-1

Padding, Timestamp, Hashes de payload (SHA-256 y SHA-1)

Diffie-Hellman (g,p',g^a,g^b) – g^{ab} mod p' (safe prime 2048 bits)

a y b = Numeros aleatorios de 2048 bits

ak = auth_key (2048 bits)

"Client and server now have a shared secret key which is used only for client-server communication and regular (not end-to-end encrypted) chats, and the client device is now registered and authorized. The Telegram application will upload the client's phone contacts to the server in order to check if any of them have already registered, and if so it automatically adds them as Telegram contacts…"

https://core.telegram.org/api/pfs

UAD360

Registro del dispositivo/sesión – Clave de autorización

Ej, Código fuente y binario – Claves públicas 2048 bits - Telegram Desktop (Windows) > 3.4.x) & Telegram X (Android) > 8.5.x)

mtproto_dc_options.cpp

const char ***kTestPublicRSAKeys**[] = { "\ (Desde 16 Jul 2021, v2.8.8) (En móvil – handshake.cpp)

-----BEGIN RSA PUBLIC KEY-----

MIIBCgKCAQEAyMEdY1aR+sCR3ZSJrtztKTKqigvO/vBfqACJLZtS7QMgCGXJ6XIRyy7mx66W0/sOFa7/1mAZtEoIokDP3ShoqF4fVNb6XeqgQf
aUHd8wJpDWHcR2OFwvplUUI1PLTktZ9uW2WE23b+ixNwJjJGwBDJPQEQFBE+vfmH0JP503wr5INS1poWg/j25slWeYPHYeOrFp/eXaqhISP6
G+q2IeTaWTXpwZj4LzXq5YOpk4bYEQ6mvRq7D1aHWfYmlEGepfaYR8Q0YqvvhYtMte3ITnuSJs171+GDqpdKcSwHnd6FudwGO4pcCOj4Wc
DuXc2CTHgH8gFTNhp/Y8/SpDOhvn9QIDAQAB

-----END RSA PUBLIC KEY----

const char ***kPublicRSAKeys**[] = { "\ (Desde 16 Jul 2021, v2.8.8) -> 8 meses (En móvil – handshake.cpp)

-----BEGIN RSA PUBLIC KEY-----

MIIBCgKCAQEA6LszBcC1LGzyr992NzE0ieY+BSaOW622Aa9Bd4ZHLl+TuFQ4lo4g5nKaMBwK/BIb9xUfg0Q29/2mgIR6Zr9krM7HjuIcCzFvDtr+
L0GQjae9H0pRB2OO62cECs5HKhT5DZ98K33vmWiLowc621dQuwKWSQKjWf50XYFw42h21P2KXUGyp2y/+aEyZ+uVgLLQbRA1dEjSDZ2iG
Ry12Mk5gpYc397aYp438fsJoHIgJ2lgMv5h7WY9t6N/byY9Nw9p21Og3AoXSL2q/2IJ1WRUhebgAdGVMlV1fkuOQoEzR7EdpqtQD9Cs5+bfo3N
hmcyvk5ftB0WkJ9z6bNZ7yxrP8wIDAQAB

-----END RSA PUBLIC KEY-----" };

Algo RSA - Format X.509

ASN1 Dump

RSA Public Key [42:f8:18:02:e4:7b:23:b7:5b:40:e0:a6:62:bb:8f:78:03:42:8a:02]

modulus:

e8bb3305c0b52c6cf2afdf7637313489e63e05268e5badb601af417786472e5f93b85438968e20e6729a301c0afc121bf7151f834436f7fda680847a66bf64accec78ee21
c0b316f0edafe2f41908da7bd1f4a5107638eeb67040ace472a14f90d9f7c2b7def99688ba3073adb5750bb02964902a359fe745d8170e36876d4fd8a5d41b2a76cbff9a
13267eb9580b2d06d10357448d20d9da2191cb5d8c93982961cdfdeda629e37f1fb09a0722027696032fe61ed663db7a37f6f263d370f69db53a0dc0a1748bdaaff6209
d5645485e6e001d1953255757e4b8e42813347b11da6ab500fd0ace7e6dfa3736199ccaf9397ed0745a427dcfa6cd67bcb1acff3

public exponent: 10001 -→ Número 4 de Fermat http://www.criptored.upm.es/crypt4you/temas/RSA/leccion2/leccion02.html#apartado2-3

UAD360

¿Cómo de viejas han sido?

Ej, Código fuente y binario – Claves públicas 2048 bits - Telegram Desktop (Windows) > 3.4.x) & Telegram X (Android) > 8.5.x)

mtproto_dc_options.cpp
(06 Jul 2021, v2.8.6)


const char *kPublicRSAKeys[] = {"\
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAwVACPi9w23mF3tBkdZz+zwrzKOaaQdr01vAbU4E1pvkfj4sqDsm6lyDONS789sVoD/xCS9Y0hkkC3gtL1tSfTlgCMOOul9lcixlEKzwKENj1Yz/s7daSan9tqw3bfUV/nqgbhGX81v/+7RFAEd+RwFnk7a+XYl9sluzHRyVVaTTveB2GazTwEfzk2DWgkBluml8OREmvfraX3bkHZJTKX4EQSjBbbdJ2ZXlsRrYOXfaA+xayEGB+8hdlLmAjbCVfaigX0CDqWeR1yFL9kwd9P0NsZRPsmoqVwMbMu7mStFai6alhc3nSlv8kg9qv1m6XHVQY3PnEw+QQtqSlXkIHwIDAQAB
-----END RSA PUBLIC KEY-----",
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAruw2yP/BCcsJliRoW5eBVBVle9dtjJw+OYED160Wybum9SXtBBLXriwt4rROd9csv0t0OHCaTmRqBcQ0J8fxhN6/cpR1GWgOZRUAiQxoMnlt0R93LCX/j1dnVa/gVbCjdSxpbrfY2g2L4frzjJvdI84Kd9ORYjDEAyFnEA7dD556OptgLQQ2e2iVNq8NZLYTzLp5YpOdO1doK+ttrltggTCy5SrKeLoCPPbOgGsdxJxyz5KKcZnSLj16yE5HvJQn0CNpRdENvRUXe6tBP78O39oJ8BTHp9oIjd6XWXAsp2CvK45Ol8wFXGF710w9lwCGNbmNxNYhtlkdqfsEcwR5JwIDAQAB
-----END PUBLIC KEY-----",
"\
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvfLHfYH2r9R70w8prHblWt/nDkh+XkgpflqQVcnAfSuTtO05lNPspQmL8Y2XjVT4tBcT6xAkdgfmmvnvRPOOKPi0OfJXoRVyIFzAQG/j83u5K3kRLbae7fLccVhKZhY46lvsuel1hQdLgNV9n1cQ3TDS2pQOCtovG4eDl9wacrXOJTG2990VjgnlKNA0UMoP+KF03qzryqIt3oTvZq03DyWdGK+AZjgBLaDKSnC6qD2cFY81UryRWOab8zKkWAnhw2kFpcqhI0jdV5QaSCExvnsjVaX0Y1N0870931/5Jb9ICe4nweZ9kSDF/gip3kWLG0o8XQ
-----END PUBLIC K
-----BEGIN PUBLIC K
MIIBIjANBgkqhkiG9
3UDJPGrzqTDHkO
voMrnt9MV1X92LG
Uk0xW14htcJrRrq+
mWtEYK6er8VqqW
-----END PUBLIC K
-----BEGIN PUBLIC K
MIIBIjANBgkqhkiG9
svIyvuDuGnP/RzPE
5UkO5hPhbb9mJpj
vuC+mQuJPyiHvSX
SMeRFvp3lWcmdJ
-----END PUBLIC K

dc_options.cpp (13 Jul 2018, v1.3.10) -> 3 años

```
const char *(PublicRSAKeys[]) = { "\
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAwVACPi9w23mF3tBkdZz+zwrzKOaaQdr01vAbU4E1pvkfj4sqDsm6lyDONS789sVoD/xCS9Y0hkkC
3gtL1tSfTlgCMOOul9lcixlEKzwKENj1Yz/s7daSan9tqw3bfUV/nqgbhGX81v/+7RFAEd+RwFnk7a+XYl9sluzHRyVVa
TTveB2GazTwEfzk2DWgkBluml8OREmvfraX3bkHZJTKX4EQSjBbbdJ2ZXlsRrYOXfaA+xayEGB+8hdlLmAjbCVfaig
xX0CDqWeR1yFL9kwd9P0NsZRPsmoqVwMbMu7mStFai6alhc3nSlv8kg9qv1m6XHVQY3PnEw+QQtqSlXkIHwIDA
QAB
-----END RSA PUBLIC KEY-----", "\
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAruw2yP/BCcsJliRoW5eBVBVle9dtjJw+OYED160Wybu
m9SXtBBLXriwt4rROd9csv0t0OHCaTmRqBcQ0J8fxhN6/cpR1GWgOZRUAiQxoMnlt0R93LCX/j1dnVa/gVbCjdSxpb
rfY2g2L4frzjJvdI84Kd9ORYjDEAyFnEA7dD556OptgLQQ2e2iVNq8NZLYTzLp5YpOdO1doK+ttrltggTCy5SrKeLoCP
PbOgGsdxJxyz5KKcZnSLj16yE5HvJQn0CNpRdENvRUXe6tBP78O39oJ8BTHp9oIjd6XWXAsp2CvK45Ol8wFXGF
710w9lwCGNbmNxNYhtlkdqfsEcwR5JwIDAQAB
-----END PUBLIC KEY-----", "\
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvfLHfYH2r9R70w8prHblWt/nDkh+XkgpflqQVcnAfSuTt
O05lNPspQmL8Y2XjVT4tBcT6xAkdgfmmvnvRPOOKPi0OfJXoRVyIFzAQG/j83u5K3kRLbae7fLccVhKZhY46lvsuel1
hQdLgNV9n1cQ3TDS2pQOCtovG4eDl9wacrXOJTG2990VjgnlKNA0UMoP+KF03qzryqIt3oTvZq03DyWdGK+AZjg
BLaDKSnC6qD2cFY81UryRWOab8zKkWAnhw2kFpcqhI0jdV5QaSCExvnsjVaX0Y1N0870931/5Jb9ICe4nweZ9kSD
F/gip3kWLG0o8XQ
-----END PUBLIC K
-----BEGIN PUBLIC K
MIIBIjANBgkqhkiG9
3UDJPGrzqTDHkO
voMrnt9MV1X92LG
Uk0xW14htcJrRrq+
mWtEYK6er8VqqW
-----END PUBLIC K
-----BEGIN PUBLIC K
MIIBIjANBgkqhkiG9
svIyvuDuGnP/RzPE
5UkO5hPhbb9mJpj
vuC+mQuJPyiHvSX
SMeRFvp3lWcmdJ
-----END PUBLIC K
```

Config.h (Primera Versión, v0.5.0 11 Mar 2017) → 4 años y 4 meses

```
inline const char **cPublicRSAKeys(uint32 &cnt) {
                static const char *(keys[]) = {"\
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAwVACPi9w23mF3tBkdZz+zwrzKOaaQdr01vAbU4E1pvkfj4sqDs
m6lyDONS789sVoD/xCS9Y0hkkC3gtL1tSfTlgCMOOul9lcixlEKzwKENj1Yz/s7da
S
an9tqw3bfUV/nqgbhGX81v/+7RFAEd+RwFnK7a+XYl9sluzHRyVVaTTveB2Gaz
TwEfzk2DWgkBluml8OREmvfraX3bkHZJTKX4EQSjBbbdJ2ZXlsRrYOXfaA+xay
EGB+8hdlLmAjbCVfaigX0CDqWeR1yFL9kwd9P0NsZRPsmoqVwMbMu7mStF
ai6alhc3nSlv8kg9qv1m6XHVQY3PnEw+QQtqSlXkIHwIDAQAB
-----END RSA PUBLIC KEY-----"};
```

special_config_request.cpp

```
constexpr auto kPublicKey = "\      (al menos desde v1.2.12, 11 Marzo 2018) -> 4 años      (En móvil – datacenter.cpp)
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAyr+18Rex2ohtVy8sroGPBwXD3DOoKCSpjDqYoXgCqB7ioln4eDCFfOBUlfXUEvM/fnKCpF46VkAftlb4VuPDeQSS/ZxZYEGqHay
wIroVnXHljgqoxiAd192xRGreuXIaUKmkwIM9JID9WS2jUsTpzQ91L8MEPLJ/4zrBwZua8W5fECwCCh2c9G5IzzBm+otMS/YKwmR1olzRCyEkyA
EjXWqBI9Ftv5eG8m0VkBzOG655WIYdyV0HfDK/NWcvGqa0w/nriMD6mDjKOryamw0OP9QuYgMN0C9xMW9y8SmP4h92OAWodTYgY1hZCxd
v6cs5UnW9+PWvS+WIbkh+GaWYxwIDAQAB
-----END RSA PUBLIC KEY-----\
```

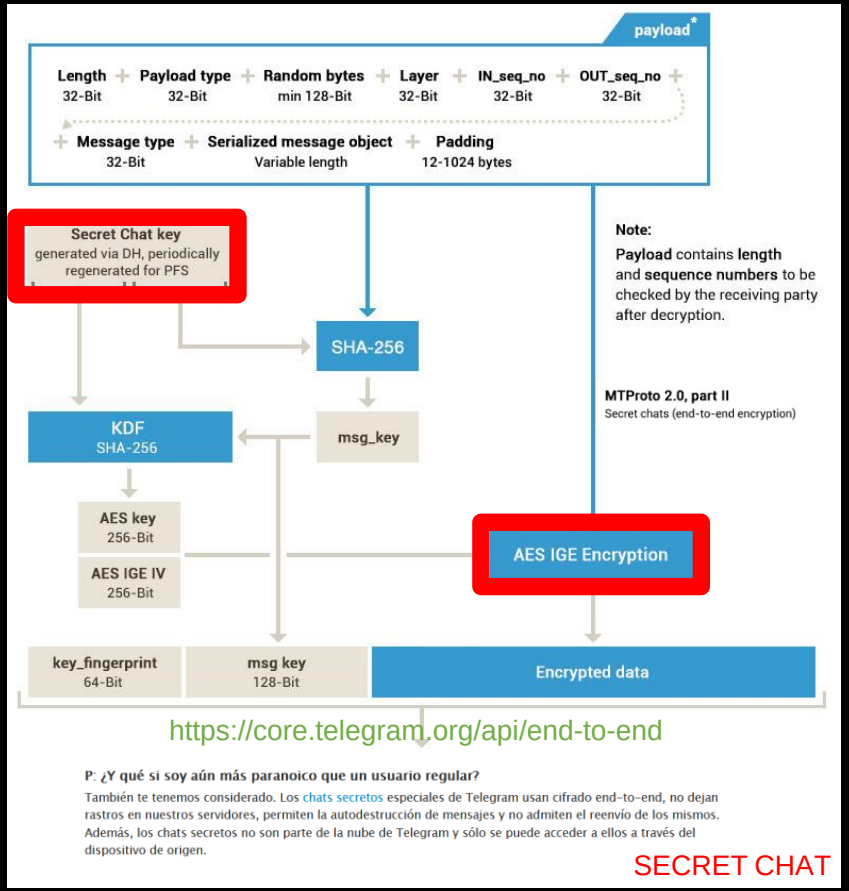
config.h

```
static const char *UpdatesPublicKey = "\   (desde la primera versión 0.5.0 – 11 Marzo 2017) -> 5 años
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMA4ViQrjkPZ9xj0lrer3r23JvxOnrtE8nI69XLGSr+sRERz9YnUptnUBZpkIfKaRcl6XzNJiN28cVwO1Ui5JSa814UAiDHzWUqCaXUiUEQ
6NmNTneiGx2sQ+9PKKlb8mmr3BB9A45ZNwLT6G9AK3+qkZLHojeSA+m84/a6GP4svAgMBAAE=
-----END RSA PUBLIC KEY-----\

static const char *UpdatesPublicBetaKey = "\   (al menos desde v1.2.12, 11 Marzo 2018) -> 4 años
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBALWu9GGs0HED7KG7BM73CFZ6o0xufKBRQsdnq3lwA8nFQEvmdu+g/I1j0LQ+0lQO7GW4jAgzF/4+soPDb6uHQeNFrlVx1JS9DZGh
hjZ5rf65yg11nTCIHZCGw/CVnbwQOw0g5GBwwFV3r0uTTvy44xx8XXxk+Qknu4eBCsmrAFNnAgMBAAE=
-----END RSA PUBLIC KEY-----\
";
```

2. Cifrado y autenticación de la información (Telegram)

Criptografía End2End (Chat secretos) vs Criptografía cliente-servidor (Chat clouds – POR DEFECTO)

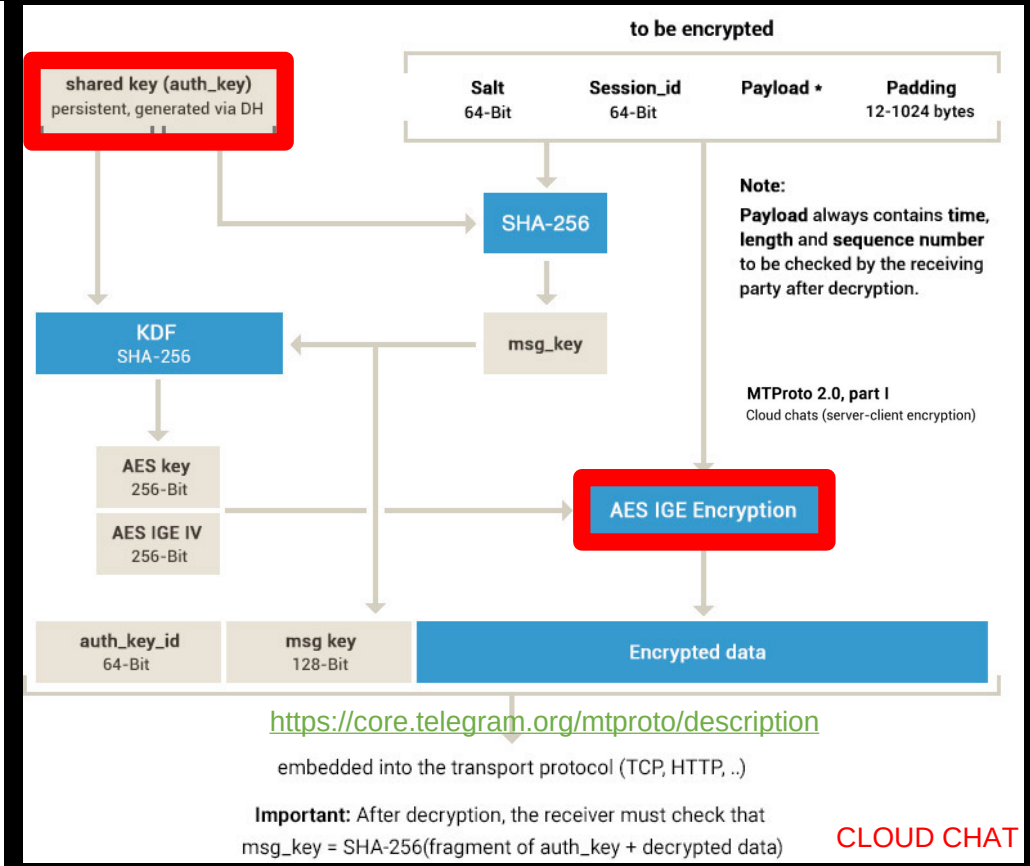


https://core.telegram.org/api/end-to-end

P: ¿Y qué si soy aún más paranoico que un usuario regular?

También te tenemos considerado. Los chats secretos especiales de Telegram usan cifrado end-to-end, no dejan rastros en nuestros servidores, permiten la autodestrucción de mensajes y no admiten el reenvío de los mismos. Además, los chats secretos no son parte de la nube de Telegram y sólo se puede acceder a ellos a través del dispositivo de origen.

SECRET CHAT



https://core.telegram.org/mtproto/description

embedded into the transport protocol (TCP, HTTP, ..)

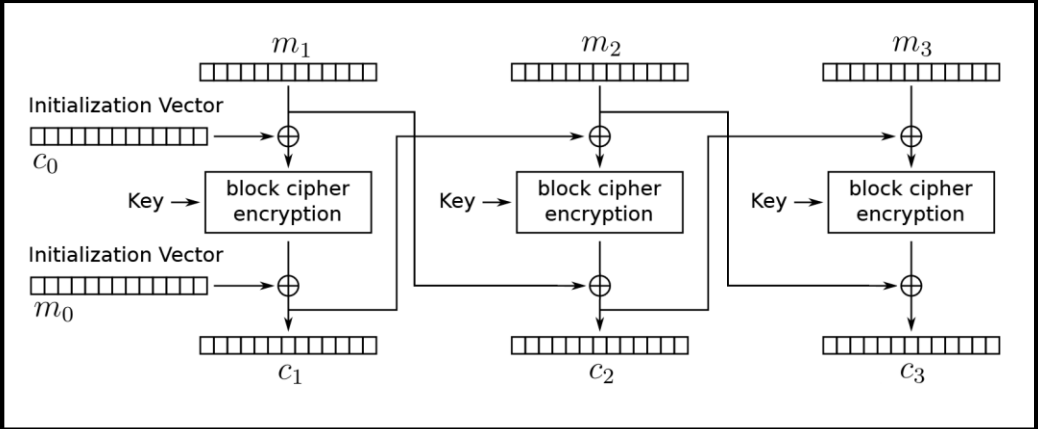
Important: After decryption, the receiver must check that msg_key = SHA-256(fragment of auth_key + decrypted data)

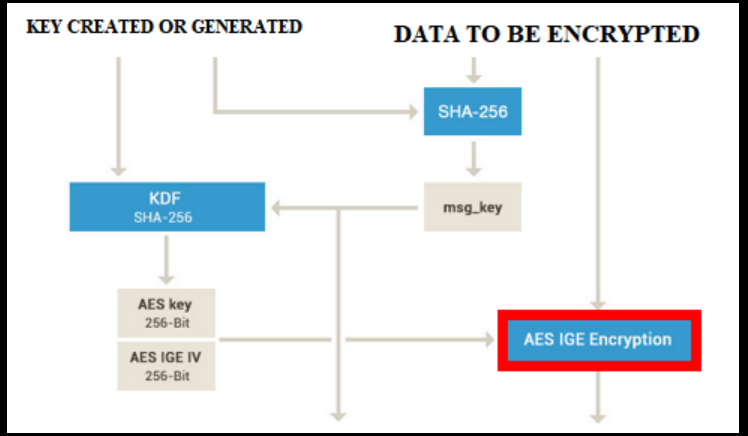
CLOUD CHAT

UAD360

Cifrado de la información (AES+IEG)

Infinite Garble Extension (IGE) block cipher mode





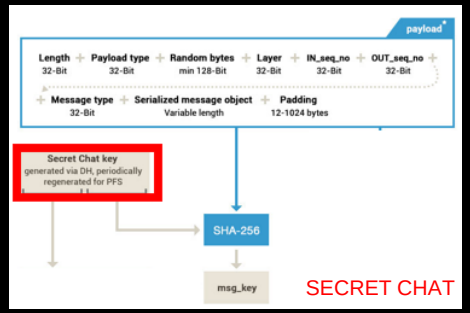
$$y_i = f_K(x_i \oplus y_{i-1}) \oplus x_{i-1}$$

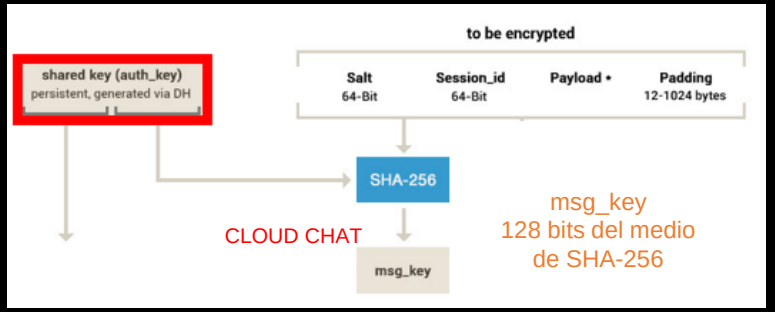
- **Cada fichero** (foto, vídeo, doc, …) son **cifrados CON UNA CLAVE ÚNICA**, “no relacionada” con la clave compartida del chat, y no *conocida por el servidor*.
- **Cifrado y creación de clave: AES+IEG, se crean dos números aleatorios de 256 bits (clave AES y el vector de inicialización).**
- **La clave y el IV es enviada al receptor CIFRADA con LA CLAVE del CHAT.**
- **Los ficheros (en chats secretos) SE ALMACENAN EN EL SERVIDOR** (igual que en cloud chats) generando un *file_ID* que es enviado al receptor. En teoría, pueden ser reenviados a otros secret chats (ahorran espacio en el servidor)

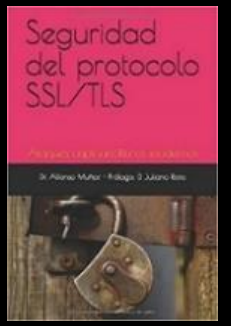
https://core.telegram.org/api/end-to-end#sending-encrypted-files & https://core.telegram.org/api/files

Autenticación de la información

- Computar SHA-256[clave de autenticación + AES_decrypt(…,encrypted_message)] y comparar con el valor de *msg_key* recibido en el mensaje cifrado.





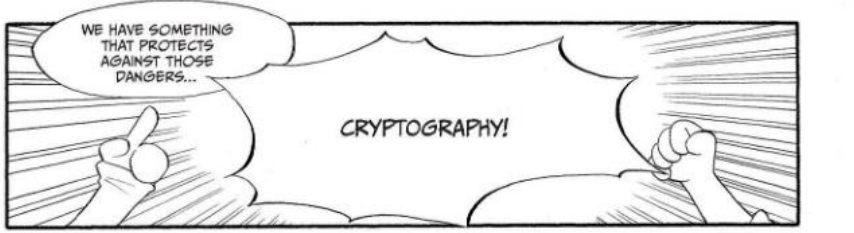


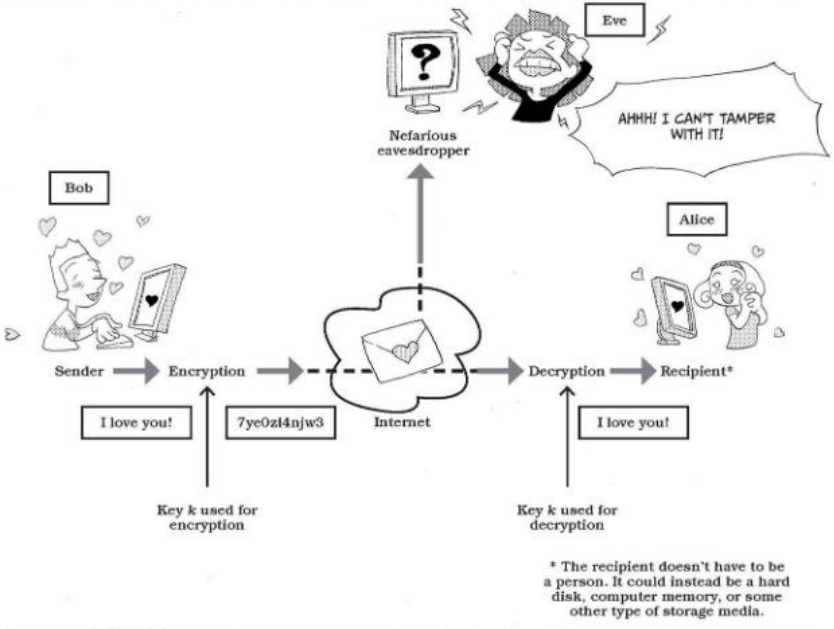
https://github.com/mindcrypt/libros/

Key Identifier (auth_key_id) - The 64 lower-order bits of the SHA1 hash of the authorization key are used to indicate which particular key was used to encrypt a message

Q: Why don't you go for a standard encrypt-then-MAC approach? (to detect unauthorized or modified ciphertexts, thus eliminating the need to decrypt them in case of tampering)

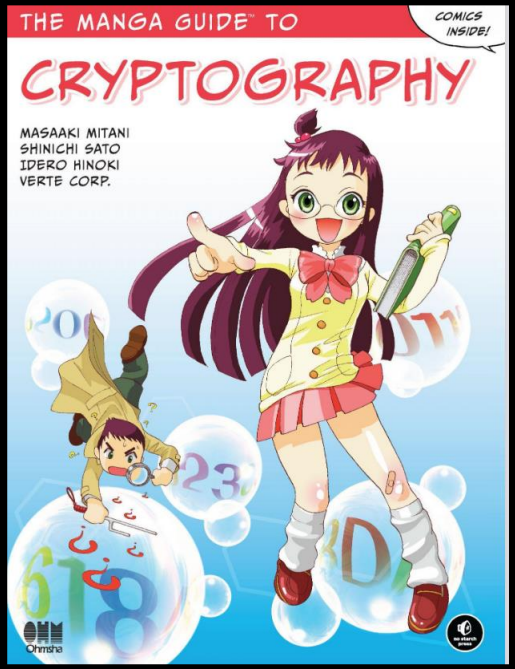
In MTProto, the clients and the server authenticate messages by ensuring that SHA-256(auth_key_fragment + plaintext + padding) = msg_key and that the plaintext always contains message length, server salt, session_id and other data not known to a potential attacker before accepting any message. These security checks performed on the client before any message is accepted ensure that invalid or tampered with messages will always be safely (and silently) discarded. This way we arrive at the same result. The difference is that the security check is performed before decryption in Encrypt-then-MAC and after decryption in MTProto – but in either case before a message is accepted. AES encryption / decryption on devices currently in use is comparable in speed with the additional HMAC computation required for the encrypt-then-MAC approach.


WE HAVE SOMETHING THAT PROTECTS AGAINST THOSE DANGERS...
CRYPTOGRAPHY!


Eve
AHHH! I CAN'T TAMPER WITH IT!
Nefarious eavesdropper
Bob
Alice
Sender
Encryption
Decryption
Recipient*
I love you!
7ye0zl4njw3
Internet
I love you!
Key k used for encryption
Key k used for decryption
* The recipient doesn't have to be a person. It could instead be a hard disk, computer memory, or some other type of storage media.

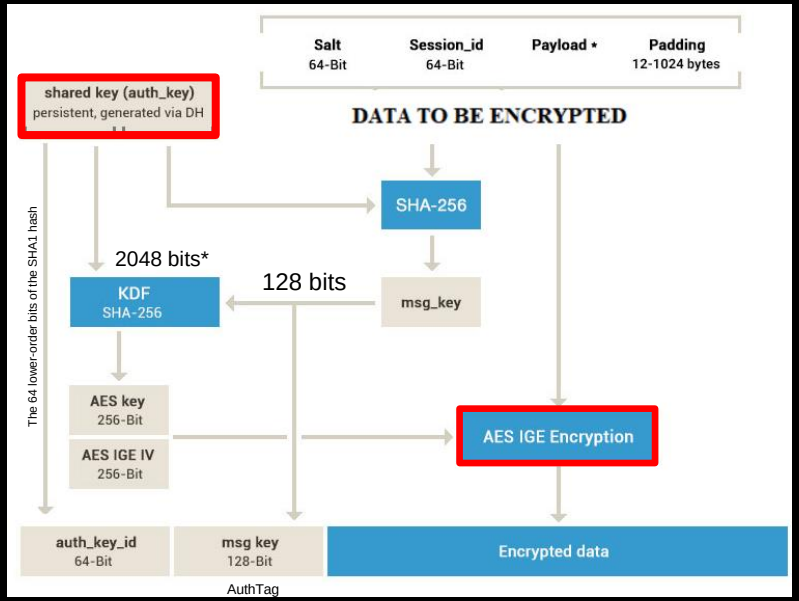

OOOH, SO CRYPTOGRAPHY REALLY IS USEFUL!
SEE? STARTING TO GET INTERESTED?

¿Seguimos…?


THE MANGA GUIDE™ TO
COMICS INSIDE!
CRYPTOGRAPHY
MASAAKI MITANI
SHINICHI SATO
IDERO HINOKI
VERTE CORP.
Ohmsha

3. Generación de claves – Cloud chats (server-client Encryption)

https://core.telegram.org/mtproto



KDF (Key Derivation Function)

x = 0 for messages from client to server and x = 64 for those from server to client.

auth_key (2048 bits)

msg_key_tmp (256 bits)
= SHA256(auth_key[704+x, 960+x] || dataToBeEncryped)
(Usa 256 bits o 32 bytes de auth_key)

msg_key (128 bits) = msg_key_tmp(64,192)

A (256 bits) = SHA256 (msg_key || auth_key[x, x+288])
(Usa 288 bits de auth_key)
B (256 bits) = SHA256 (msg_key || auth_key[320+x, x+608])
(Usa 288 bits de auth_key)

AES_KEY (256 bits) = A[0,64] || B[64,192] || A[192,256]
AES_IV (256 bits) = B[0,64] || A[64,192] || B[192,256]

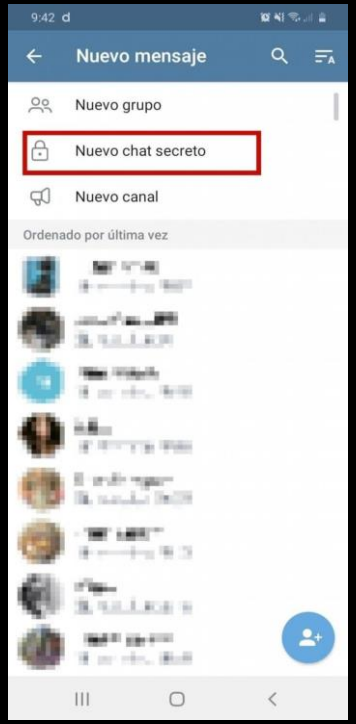
msg_key = 128 bits del medio de SHA-256(fragment of auth_key+data to be encrypted)

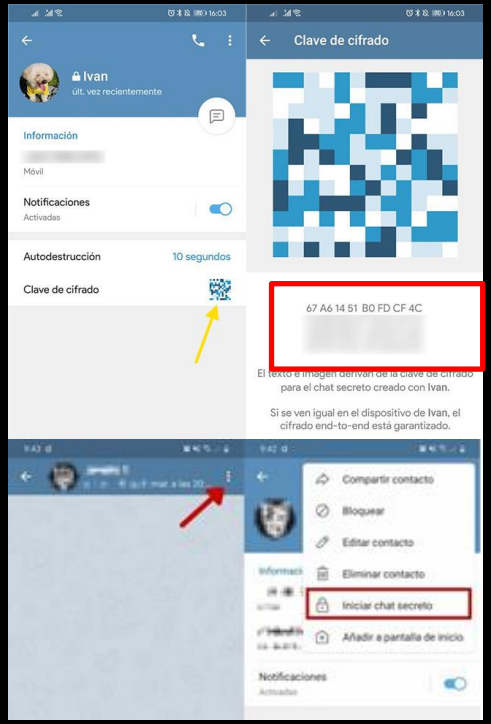
Session = A (random) 64-bit number generated by the client to distinguish between individual sessions
(Server Salt) = A (random) 64-bit number changed every 30 minutes (separately for each session) at the request of the server. All subsequent messages must contain the new salt (although, messages with the old salt are still accepted for a further 1800 seconds).

UAD360

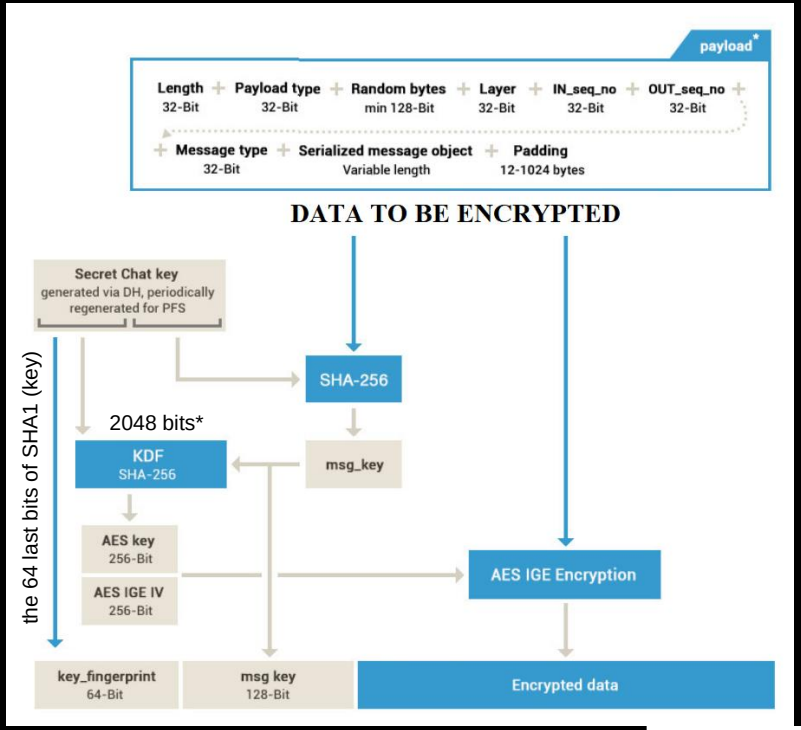
- Generación de claves – Secret chats

- **Móvil => Chat “especial forzado” uno a uno** (“desde móvil, no multidispositivo”) (Unigram, …)
- Verificar “el hash” de la clave de cifrado (muy importante) ⚠️





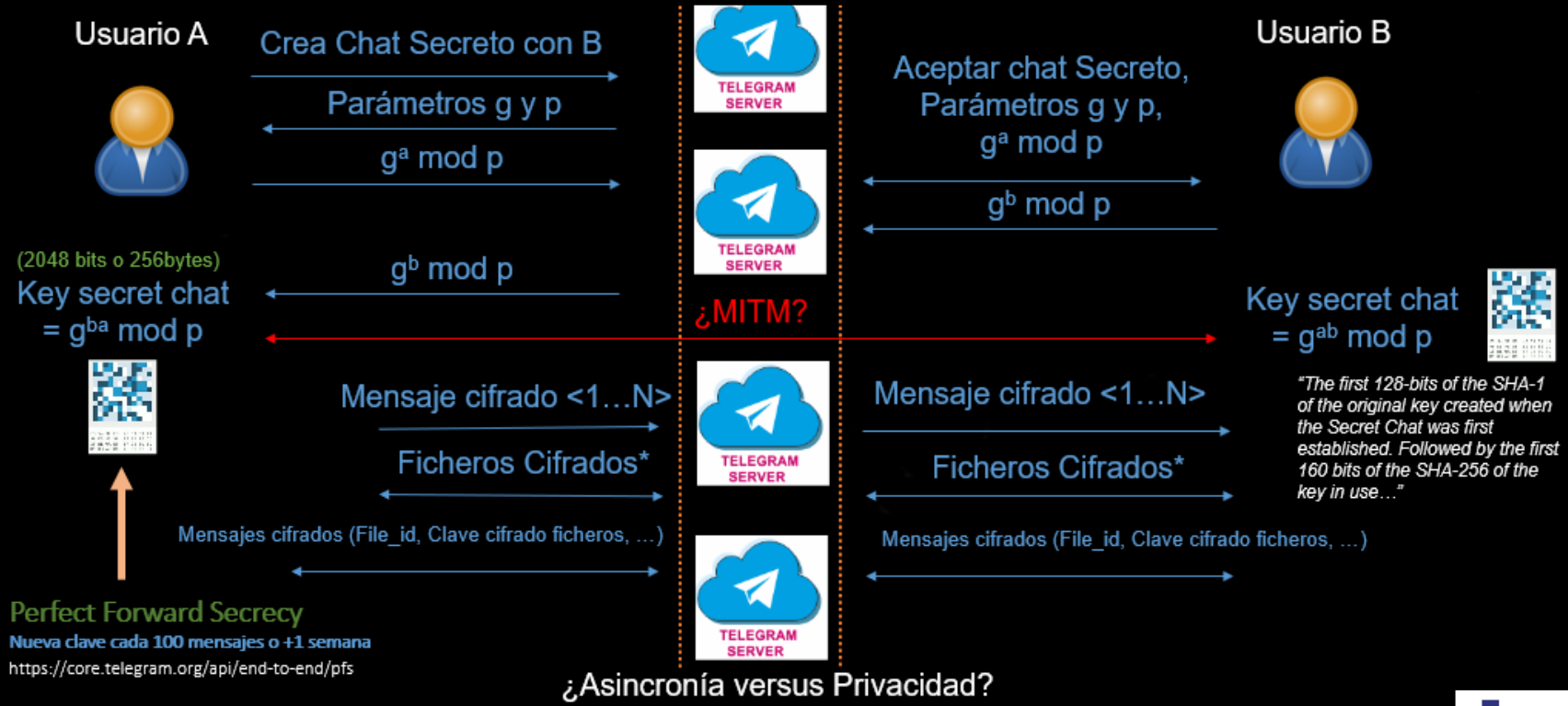
https://acortar.link/0UGUAX



UAD360

- Generación de claves y PFS – Secret chats - Resumen

KDF igual que Cloud chats pero depende de Secret chat key, msg_key
TODO - generación de claves y chat (mensajes, ficheros) - pasa por los SERVIDORES (con quién me conecto y cuando)



UAD360

(*) - Registro del dispositivo/sesión – Clave de autorización

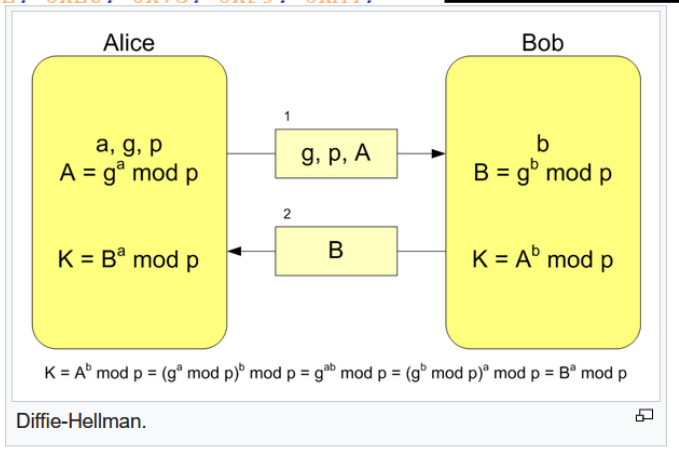
mtproto_dh_utils.cpp (Tdesktop > v.3.4.X) (Utilities.java -> versión movil)

```
bool IsPrimeAndGood(bytes::const_span primeBytes, int g) {
    static constexpr unsigned char GoodPrime[] = {
        0xC7, 0x1C, 0xAE, 0xB9, 0xC6, 0xB1, 0xC9, 0x04, 0x8E, 0x6C, 0x52, 0x2F, 0x70, 0xF1, 0x3F, 0x73,
        0x98, 0x0D, 0x40, 0x23, 0x8E, 0x3E, 0x21, 0xC1, 0x49, 0x34, 0xD0, 0x37, 0x56, 0x3D, 0x93, 0x0F,
        0x48, 0x19, 0x8A, 0x0A, 0xA7, 0xC1, 0x40, 0x58, 0x22, 0x94, 0x93, 0xD2, 0x25, 0x30, 0xF4, 0xDB,
        0xFA, 0x33, 0x6F, 0x6E, 0x0A, 0xC9, 0x25, 0x13, 0x95, 0x43, 0xAE, 0xD4, 0x4C, 0xCE, 0x7C, 0x37,
        0x20, 0xFD, 0x51, 0xF6, 0x94, 0x58, 0x70, 0x5A, 0xC6, 0x8C, 0xD4, 0xFE, 0x6B, 0x6B, 0x13, 0xAB,
        0xDC, 0x97, 0x46, 0x51, 0x29, 0x69, 0x32, 0x84, 0x54, 0xF1, 0x8F, 0xAF, 0x8C, 0x59, 0x5F, 0x64,
        0x24, 0x77, 0xFE, 0x96, 0xBB, 0x2A, 0x94, 0x1D, 0x5B, 0xCD, 0x1D, 0x4A, 0xC8, 0xCC, 0x49, 0x88,
        0x07, 0x08, 0xFA, 0x9B, 0x37, 0x8E, 0x3C, 0x4F, 0x3A, 0x90, 0x60, 0xBE, 0xE6, 0x7C, 0xF9, 0xA4,
        0xA4, 0xA6, 0x95, 0x81, 0x10, 0x51, 0x90, 0x7E, 0x16, 0x27, 0x53, 0x0I
        0x0D, 0xBA, 0x74, 0xD8, 0xA8, 0x4B, 0x2A, 0x14, 0xB3, 0x14, 0x4E, 0x0(
        0xFD, 0x17, 0xED, 0x95, 0x0D, 0x59, 0x65, 0xB4, 0xB9, 0xDD, 0x46, 0x0!
        0x16, 0x9C, 0x6B, 0xC4, 0x65, 0xB0, 0xD6, 0xFF, 0x9C, 0xA3, 0x92, 0x0!
        0xE4, 0x18, 0xFC, 0x15, 0xE8, 0x3E, 0xBE, 0xA0, 0xF8, 0x7F, 0xA9, 0x0I
        0x0D, 0xED, 0x28, 0x49, 0xF4, 0x7B, 0xF9, 0x59, 0xD9, 0x56, 0x85, 0x0(
        0x0D, 0x81, 0x15, 0xF6, 0x35, 0xB1, 0x05, 0xEE, 0x2E, 0x4E, 0x15, 0x0I
        0x6F, 0x4F, 0xAD, 0xF0, 0x34, 0xB1, 0x04, 0x03, 0x11, 0x9C, 0xD8, 0x0I

    if (!bytes::compare(bytes::make_span(GoodPrime), primeBytes)) {
        if (g == 3 || g == 4 || g == 5 || g == 7) {
            return true;
        }
    }

    return IsPrimeAndGoodCheck(openssl::BigNum(primeBytes), g);
}
```

Al menos desde 03 Apr 2017, v 1.0.28!!!! (casi 5 años)



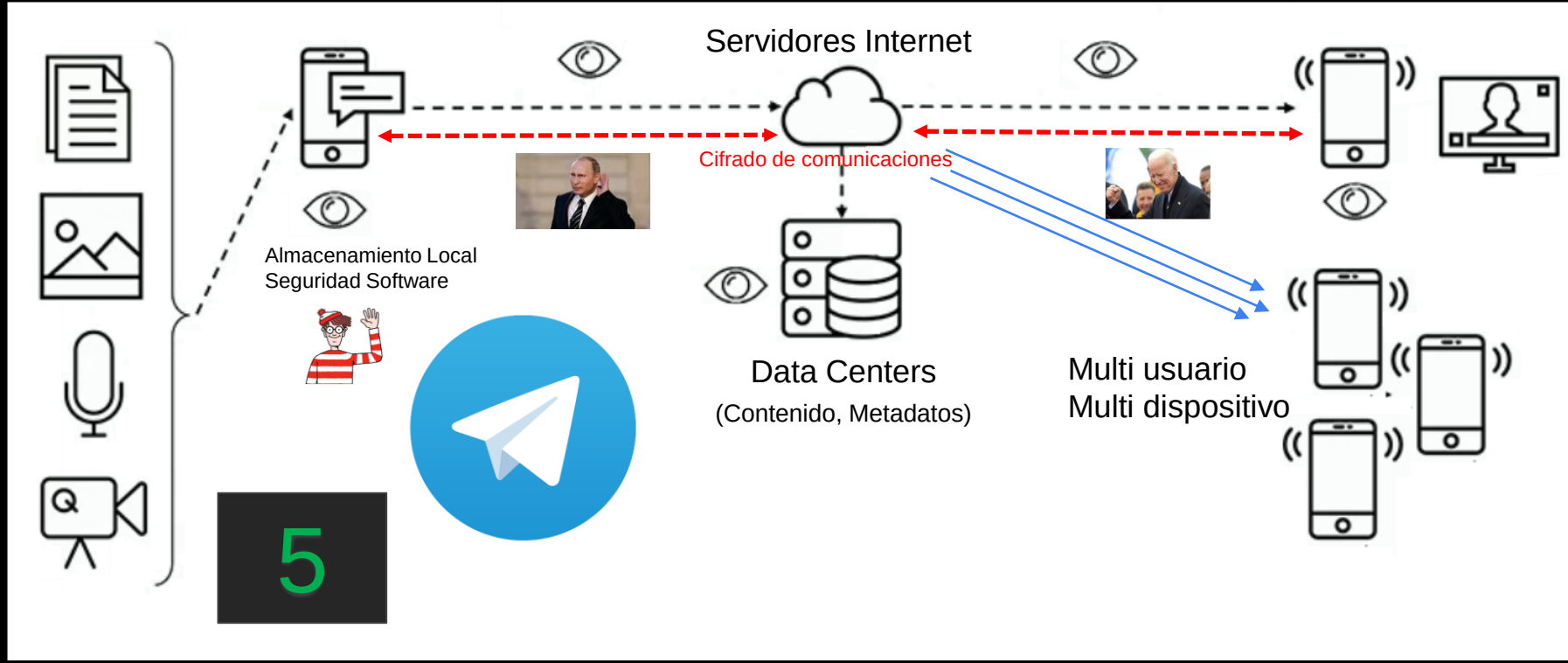
Diffie-Hellman.

Valida número 2048 bits y primo (Miller-Rabin, 30 pasadas) → openssl BN_generate_prime_ex

UAD360

BONUS TRACK - Voice and Video Calls – “Puntos de dolor”

¿Diferentes servicios – Diferentes protocolos de comunicación y protección de mensajes?



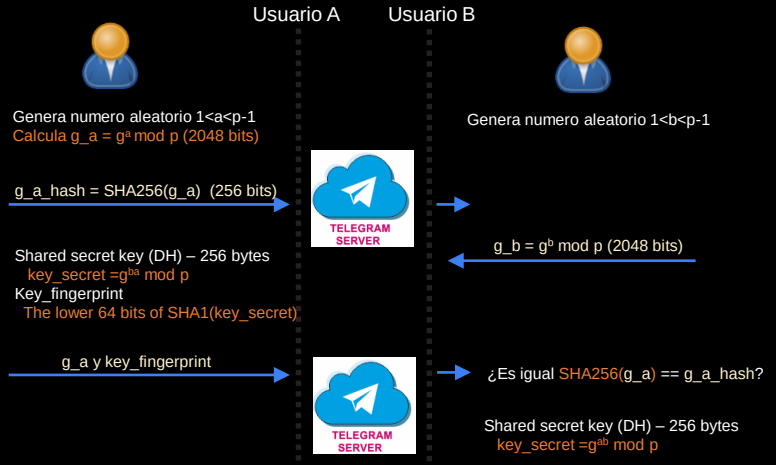
https://core.telegram.org/mtproto | Código fuente clientes + Binarios Ej. Última versión Telegram Desktop (Windows, >3.4.X) y Telegram X (Android, > 8.5.X)

TDLIB (Telegram Database library) + Código fuente | Investigaciones académicas y terceros

E2E encryption Voice and Video Calls – Intercambio de claves

https://core.telegram.org/api/end-to-end/video-calls

- El servidor (Telegram) “PROPORCIONA” la dirección IP de los comunicantes (MitM?) ⚠
- El intercambio de claves pasa por el SERVIDOR ☹ y proporciona p y g para Diffie-Hellman a los interlocutores
- Generación e intercambio de CLAVE CRIPTOGRAFICA UNICA POR LLAMADA/VIDEO (key_secret, 2048 bits) usando una pequeña variación de Diffie-Hellman con “parámetros” estándar (similar a Secret chats y sus validaciones) – Clave compartida de 256 bytes



Users who are on a call can ensure that there is no MitM by comparing key visualizations.

both parties concatenate the *secret key with the value g_a* of the Caller (*A*), compute SHA256 and use it to generate a sequence of emoticons. More precisely, the SHA256 hash is split into four 64-bit integers; each of them is divided by the total number of emoticons used (currently 333), and the remainder is used to select specific emoticons. The specifics of the protocol guarantee that comparing four emoticons out of a set of 333 is sufficient to prevent eavesdropping (MiTM attack on DH) with a probability of **0.9999999999 -**

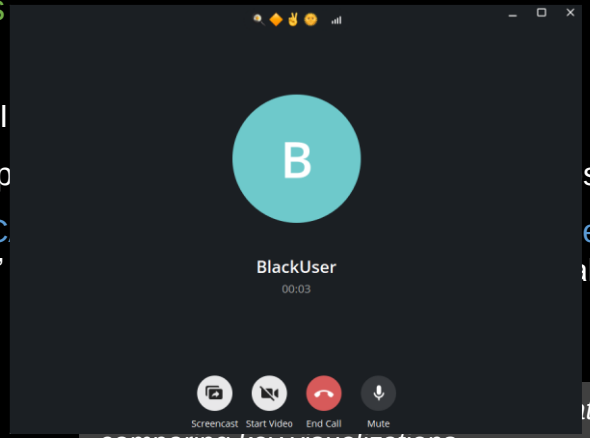
https://core.telegram.org/techfaq#q-how-are-voice-calls-authenticated

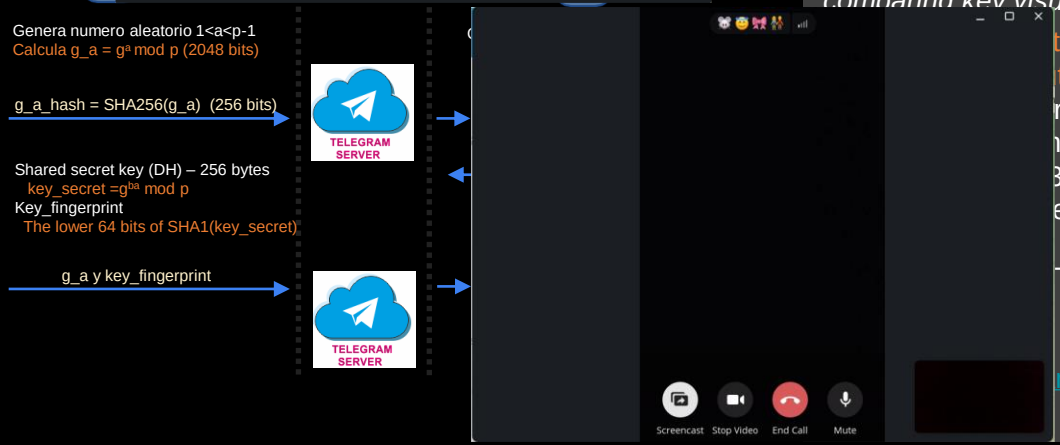
UAD360

E2E encryption Voice and Video Calls – Intercambio de claves

https://core.t…s

- El servidor …
- El intercam… …s interlocutores
- Generació… …ecret, 2048 bits) usando una pequeña va… …alidaciones) – Clave compartida





…t there is no MitM by comparing key visualizations.

…tenate the *secret key with the value g_a* of the …te SHA256 and use it to generate a sequence of …recisely, the SHA256 hash is split into four 64-bit …hem is divided by the total number of emoticons …3), and the remainder is used to select specific …ecifics of the protocol guarantee that comparing … of a set of 333 is sufficient to prevent …TM attack on DH) with a probability of …

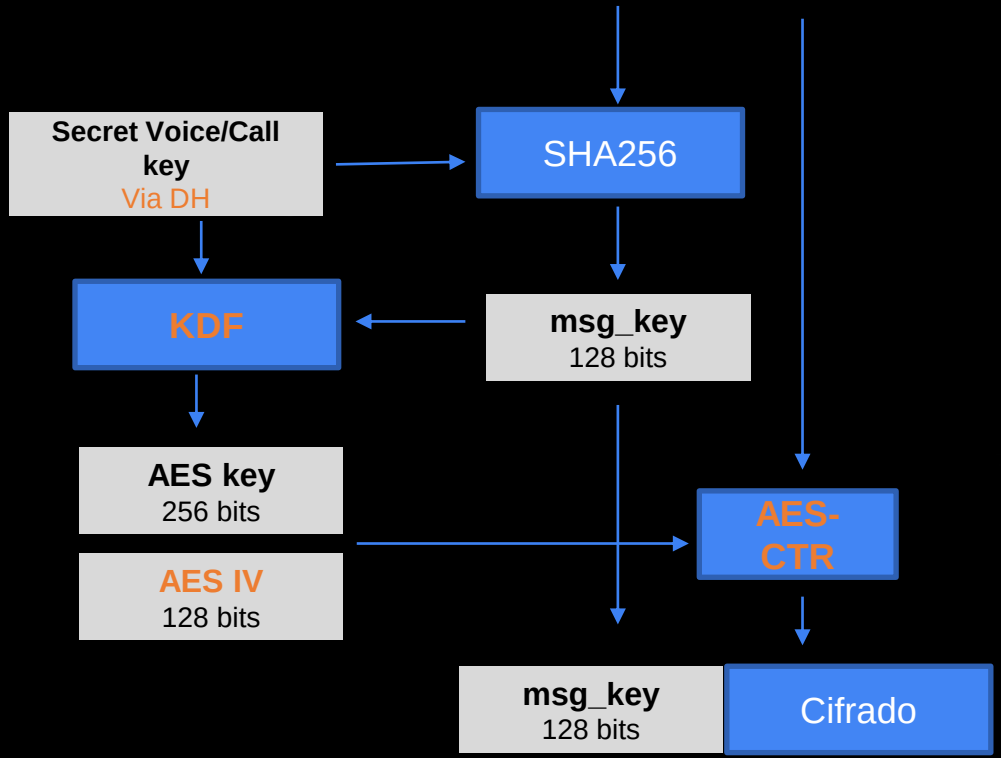
…m.org/techfaq#q-how-are-voice-calls-

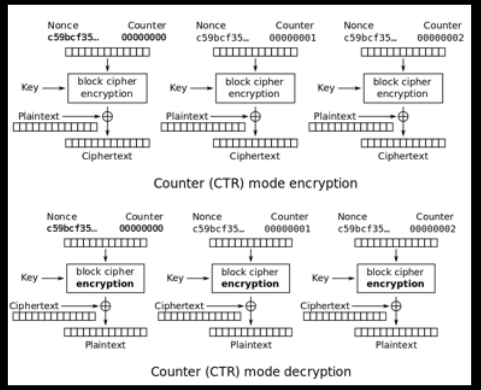
UAD360

E2E encryption Voice and Video Calls - Cifrado

https://core.telegram.org/api/end-to-end/video-calls

decrypted_body = message_seq1 + message_body1 + message_seq2 + message_body2…





Claves para cifrado de los datos (key_secret por llamada, datos)
KDF (Key Derivation Function) “igual” a los otros esquemas

key_secret (2048 bits)

msg_key_tmp (256 bits)
= SHA256(key_secret[704+x, 960+x] || decrypted_body)
msg_key (128 bits) = msg_key_tmp(64,192)
A (256 bits) = SHA256 (msg_key || key_secret[x, x+288])
B (256 bits) = SHA256 (msg_key || key_secret[320+x, x+608])

AES_KEY (256 bits) = A[0,64] || B[64,192] || A[192,256]
AES_IV (128 bits) = B[0,32] || A[64,128] || B[192,224]

x depends on whether the call is **outgoing** or **incoming** and on the connection type:

x = 0 for **outgoing** + **transport**
x = 64 for **incoming** + **transport**
x = 1024 for **outgoing** + **signaling**
x = 1088 for **incoming** + **signaling**

Two data transfer channels: **signaling**, offered by the Telegram API, and **transport** based on WebRTC.

Conclusiones

- Telegram es una herramienta MUY DAÑINA desde el punto de vista de la PRIVACIDAD (metadatos)
- El usuario debe CONFIAR en la BONDAD y SEGURIDAD INTERNA de la infraestructura "CENTRALIZADA" de Telegram
  - Decisiones controvertidas, algunas erróneas, y opacidad desde el punto de vista criptográfico y de seguridad.
  - Auditoria de seguridad complicada. Documentación "oscura", deficientes políticas de gestión de claves, etc.

- "No parece" que la criptografía en tránsito pueda ser anulada por un tercero sin colaboración de Telegram y los parámetros criptográficos "parecen" estar bien calculados y verificados.
  - Una criptografía "imperfecta" no implica "necesariamente" vulnerabilidades prácticas (al menos a corto plazo ☺)
  - Los chat secretos no son end-to-end. Afecta a la PRIVACIDAD (metadatos)
  - Realmente… pocas claves y parámetros criptográficos definen la seguridad de Telegram (RSA y goodPrime)

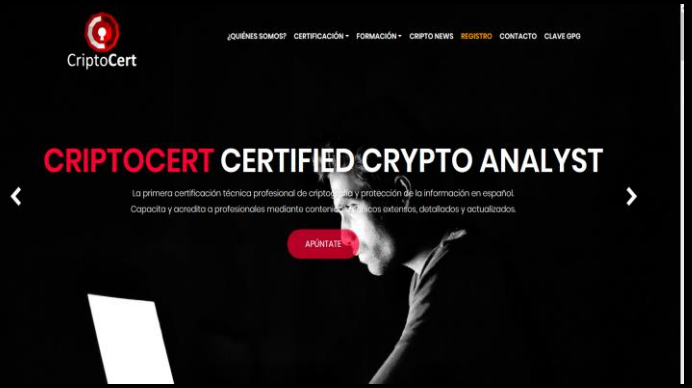
Soluciones

- ¿Qué hago si soy una "empresa"? – Un grupo "controlado" de usuarios
  - Desarrollos propios, ¿soluciones comerciales?... Ej, XMPP+XEPs (extensions)+Signal protocol (Oh, MEMO! Otra Mensajería Encriptada Merece tu Organización – XV Jornadas STIC CCN CERT https://www.youtube.com/watch?v=bFHV4PEsdbk

- ¿Qué hago si soy un individuo? – El problema real es el "efecto red"…
  - REFLEXIONAR: "La seguridad como falta de conectividad es la seguridad mal entendida…"
  - Uso Telegram: SIM particulares para el servicio, configuración de parametros más "privados", recifrado de información (Frida, clientes modificados, …), chat secretos, …
  - Alternativas: ¿Hacen falta más estudios? Session, Threema, Signal, Wire… https://www.securemessagingapps.com/

Lecturas ☺

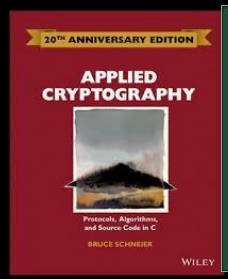
https://bookauthority.org/books/best-cryptography-books

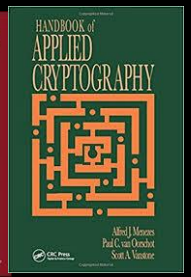


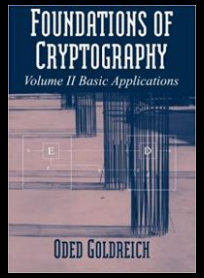
https://www.criptocert.com/CriptoCert_Analyst.html

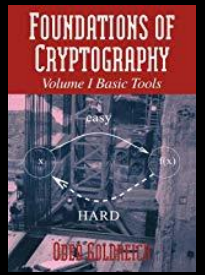
https://github.com/mindcrypt/libros

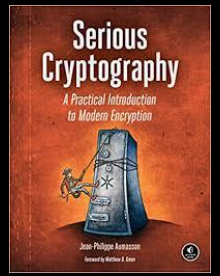
https://www.amazon.com/Criptografía-Ofensiva-Atacando-defendiendo-organizaciones/dp/B08RB6LGRK

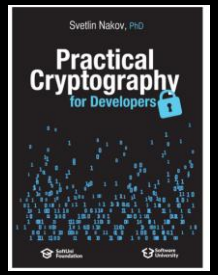


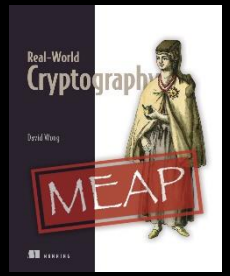












Con faldas y a lo loco - https://www.youtube.com/watch?v=-mHhr-aaLnI

Dr. Alfonso Muñoz

Alfonso@criptored.com
Twitter: @mindcrypt

UAD360

¡Gracias!

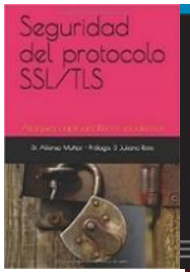
About.me

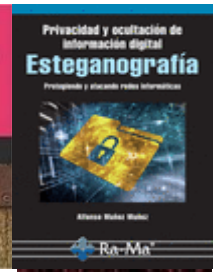
- **Leading Cybersecurity – SandboxAQ (sandbox@alphabet)**
- Doctor Ingeniero Telecomunicación (UPM)
- 18 años de “carretera”…
- Expert security member – Europol (EC3)
- Libros (5), patentes (2), certificaciones de seguridad (+10)…
- ***Investigador y ponente en conferencias de prestigio*** *(RootedCon (12), Ekoparty, Blackhat USA & Europe, 8.8, BSIDES, VirusBulletin, HackInTheBox (3), DeepSec, STIC CCN/CERT (4)…), tools, premios académicos e industriales (3 premios SIC, IDG 2020-Top 50 Blue Team, etc.), artículos científicos en revistas de impacto (+70), docente en másteres universitarios (4)….*
- **Bug hunter** - Security bulletins (Microsoft, Foxit, Google - Hall of fame, etc.).
- *Founder CriptoCert Certified Crypto Analyst & Criptored* https://www.criptocert.com

Perfil:

- Offensive security (sw/hw)
- Cryptography & covert channels/stego
- Cutting-edge research (defensive & offensive)

alfonso@criptored.com
t.me/criptored
http://github.com/mindcrypt
https://es.linkedin.com/in/alfonsomuñoz
@mindcrypt





https://www.amazon.com/Criptografía-Ofensiva-Atacando-defendiendo-organizaciones/dp/B08RB6LGRK

UAD360