

Chi ha paura della crittografia ?

De Componendis Cifris - 25 gennaio 2022
Antonino Alì

«Extant et ad Ciceronem, item ad familiares, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum, id est D pro A et perinde reliquas commutet».

Vite dei Cesari (56, I), Svetonio

La domanda è pleonastica.

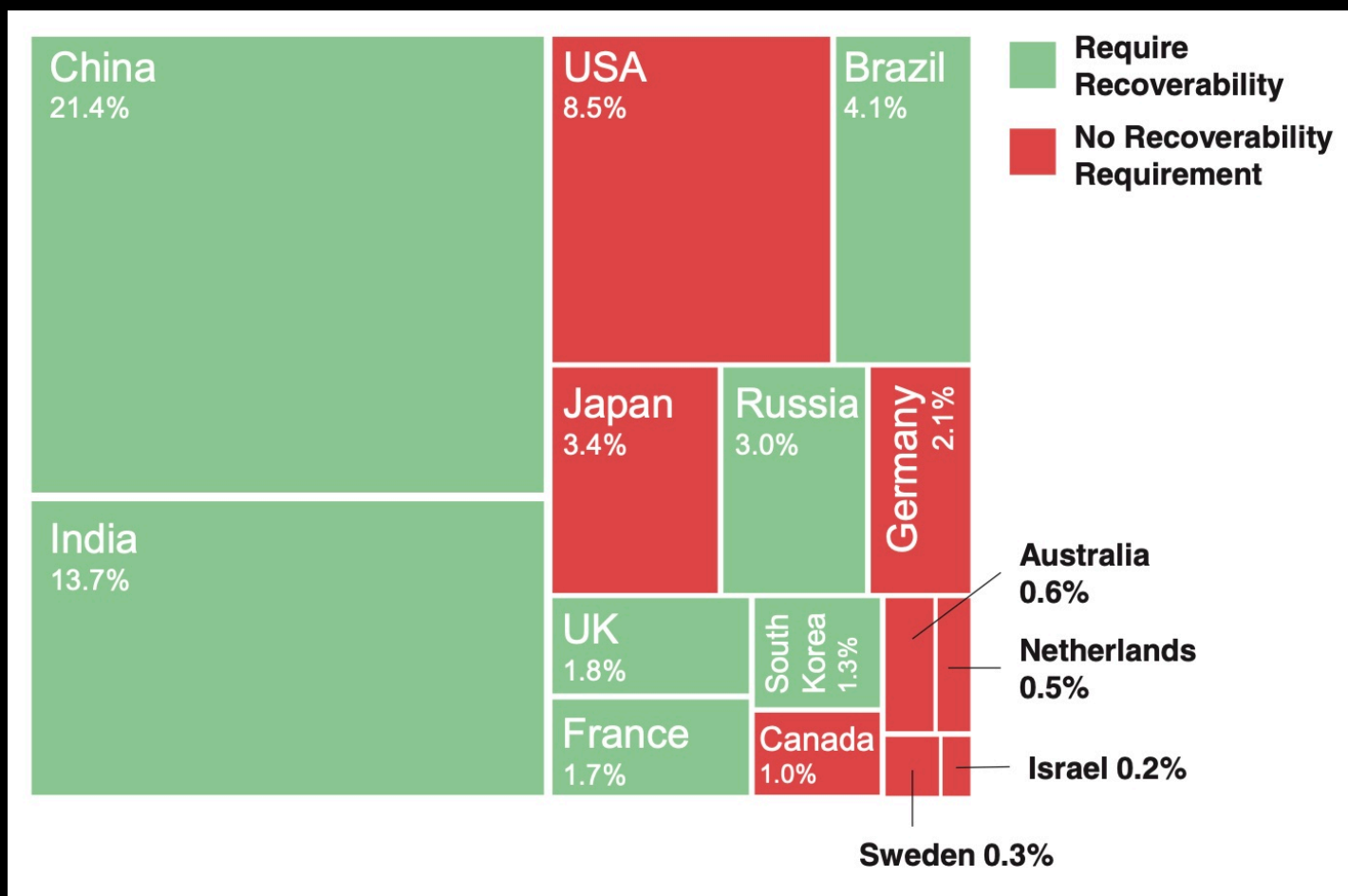
- Inizialmente, gli sforzi dei governi si sono concentrati sulla violazione della crittografia utilizzata da altri governi.
- La crittografia sofisticata era al di là delle capacità della maggior parte del pubblico.
- Oggi, invece, tecniche crittografiche di livello elevato sono disponibili per il grande pubblico.
- E-commerce: l'ampia disponibilità di crittografia avanzata è stata un vantaggio per i consumatori, i cui dati digitali godono oggi di una maggiore protezione.
- La crittografia crea problemi non indifferenti per le forze dell'ordine, la magistratura e l'intelligence degli Stati.
- Anche in presenza dell'autorizzazione all'accesso dei dati (attraverso un mandato della magistratura). L'accesso a informazioni su *devices* che possono contenere prove essenziali per le loro indagini sul comportamento criminale.

- I governi, per conto sia delle forze dell'ordine che degli enti di sicurezza nazionale, hanno chiesto alle aziende di creare "backdoor" negli algoritmi di crittografia per consentire al governo l'accesso alle informazioni protette nel momento del bisogno.
- Resistenza delle società private alle richieste di backdoors governative ?
- Clipper
- Crypto AG
- Implementare un algoritmo che consenta una backdoor affidabile e sicura è difficile (*difetti sfruttabili - sistema intrinsecamente insicuro*). Il caso delle backdoors poi diventate la base di sistemi utilizzati dalla criminalità. Vault 7
- Una backdoor creata per le autorità statali è un obiettivo per terzi che intendono accedere ai dati. (Caso Grecia)
- Governi autoritari > richiesta di backdoors

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (David Kaye)

- Rapporto presentato ai sensi della risoluzione 25/2 del Consiglio per i diritti umani
- Il Relatore speciale affronta l'uso della crittografia e dell'anonimato nelle comunicazioni digitali.
- Attingendo dalla ricerca sulle norme e sulla giurisprudenza internazionali e nazionali e dal contributo degli Stati e della società civile, il rapporto conclude che la crittografia e l'anonimato consentono alle persone di esercitare i propri diritti alla libertà di opinione e di espressione nell'era digitale e, in quanto tali, meritano un forte protezione.
- Divieti di crittografia per uso individuale (ad es. restrizioni all'uso di strumenti di codifica per proteggere l'anonimato)
- Indebolimento intenzionale della crittografia
- Deposito delle chiavi (e obblighi di localizzazione dati)
- Divulgazione della chiave obbligatoria con ordini di decrittazione mirati
- Presunzioni legali

Stati con legislazioni che richiedono la “recuperabilità” dei dati



CSIS 2017


Methods of obtaining digital data for intelligence purposes

David Oman - Mark Phythian, Principled Spying, Oxford, 2018

- **Intercepting data about an individual's communications that is carried in the "header" of each data packet.** Essentially this data is the "who is calling whom, where, when, how, and for how long" of the communication and is analogous to the information in an old-fashioned itemized telephone bill.
- **Intercepting the actual content of a communication.**
- **Hacking into a suspect's computer or mobile device or a target network by equipment interference to access the data directly or to facilitate access.** This hacking may be accomplished by physical interference (e.g., covertly down-loading data from a device to which physical access has been gained), remote interference (e.g., installing a piece of software on a device over a wired or wireless network to remotely extract information from the device), or equipment interfering (e.g., planting malware on the relevant communications system to enable access).
- **Applying advanced data-mining techniques to databases.** This effort targets databases containing personal information relating to numerous individuals that comes from either government sources (passport records, vehicle licenses, etc.) or the private sector (e.g., airline passenger information) to derive information about a suspect. Because these datasets are very large, they cannot be processed manually.

Un attacco alla crittografia ?

La Risoluzione del Consiglio dell'Unione Europea sulla crittografia del 24 novembre 2020

 Consiglio dell'Unione europea

Bruxelles, 24 novembre 2020
(OR. en)

ALLEGATO

Risoluzione del Consiglio sulla crittografia
La sicurezza attraverso la crittografia e nonostante la crittografia

NOTA

Origine:	Presider
Destinatario:	Delegaz
n. doc. prec.:	12863/2
Oggetto:	Risoluzi - La sicu

1. Preambolo: la sicurezza attraverso la crittografia e nonostante la crittografia

L'Unione europea sostiene pienamente lo sviluppo, l'attuazione e l'utilizzo di una crittografia forte.

L'Unione europea sottolinea la necessità di garantire il pieno rispetto dei diritti fondamentali, dei diritti umani e dello Stato di diritto in tutte le azioni connesse alla presente risoluzione, sia online che offline. La crittografia è uno strumento necessario per tutelare i diritti fondamentali e la sicurezza digitale dei governi, dell'industria e della società. Nel contempo, l'Unione europea deve garantire che le autorità competenti nel settore della sicurezza e della giustizia penale, quali le autorità di contrasto e giudiziarie, siano in grado di esercitare i loro legittimi poteri, sia online che offline, proteggendo le nostre società e i nostri cittadini.

Si allega per le delegazioni la

Secondo le conclusioni del Consiglio europeo del 1° e 2 ottobre 2020 (EUCO 13/20), l'UE farà leva sui suoi strumenti e i suoi poteri normativi per contribuire a definire norme e regole globali. È stato convenuto che i fondi a titolo del dispositivo per la ripresa e la resilienza sarebbero stati utilizzati per perseguire, tra gli altri, gli obiettivi di potenziare la capacità dell'UE di proteggersi dalle minacce informatiche, provvedere a un ambiente di comunicazione sicuro, soprattutto attraverso la crittografia quantistica e garantire l'accesso ai dati a fini giudiziari e di contrasto.

- “La sicurezza attraverso la crittografia e nonostante la crittografia”
- Secondo le conclusioni del Consiglio europeo del 1° e 2 ottobre 2020, l'UE farà leva **sui suoi strumenti e i suoi poteri normativi** per contribuire a definire norme e regole globali. È stato convenuto che i fondi a titolo del dispositivo per la ripresa e la resilienza sarebbero stati utilizzati per perseguire, tra gli altri, gli obiettivi di potenziare la capacità dell'UE di proteggersi dalle minacce informatiche, provvedere a un ambiente di comunicazione sicuro, soprattutto attraverso la crittografia quantistica **e garantire l'accesso ai dati a fini giudiziari e di contrasto.**

I generatori pseudocasuali *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG)

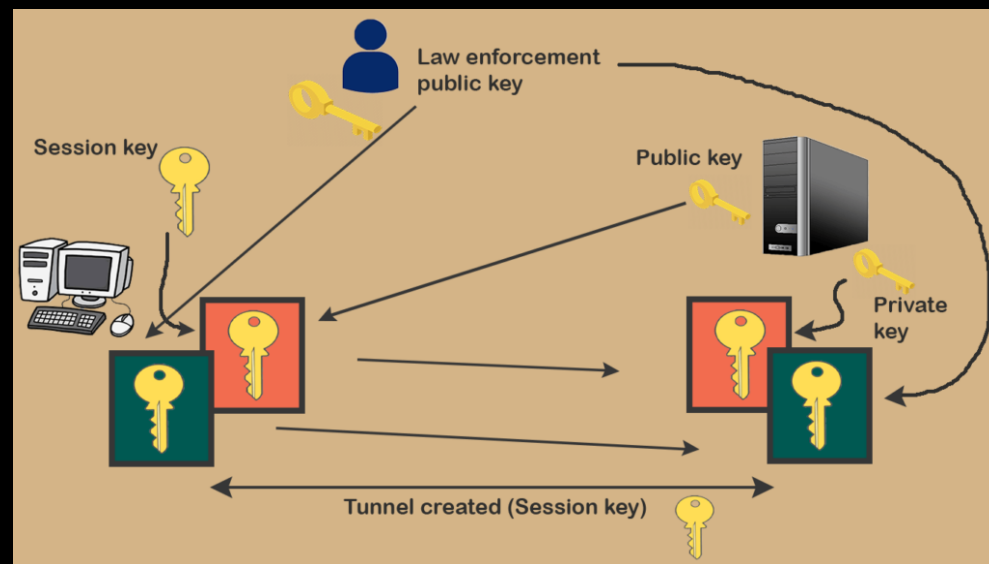
- La generazione di numeri pseudo-casuali e sequenze random per creare coppie di chiavi robuste in sistemi a chiave pubblica. Se le sequenze hanno una bassa qualità gli algoritmi di cifratura sono indeboliti.
- I generatori pseudocasuali *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG)
- Un esempio è il **Dual_EC_DRBG** (Dual Elliptic Curve Deterministic Random Bit Generator) basato sull'Elliptic Curve Cryptography e la sua "standardizzazione" da parte del National Institute of Standards and Technology (NIST).
- Critiche: predire le sequenze random con limitati sforzi.

Datagate:

- NSA finanzia la società RSA. NSA spinge affinché l'algoritmo fosse incluso in diversi standards e viene favorita l'ampia diffusione e accettazione nell'industria informatica e negli utilizzatori.
- La formulazione adottata da NIST.
- Gli implementatori invogliati ad adottare l'algoritmo Dual_EC_DRBG affinché i loro prodotti potessero conseguire la certificazione richiesta dalle amministrazioni USA.
- Anche tra gli sviluppatori del software open source OpenSSL (incluso nei sistemi operativi Linux e Unix).
- V. Comella 2016

Key Escrow

- Tecnica mediante la quale la chiave necessaria a decriptare dei dati criptati è conservata con un acconto di garanzia da terze parti in modo che, in particolari situazioni, possa essere recuperata per avere accesso a quei dati anche se coloro che hanno cifrato i dati non vogliono renderla disponibile.
- Le terze parti interessate alla conservazione delle chiavi possono essere sia enti privati che governativi e le eventualità in cui la chiave può essere recuperata sono generalmente esplicitate in appositi contratti privati o leggi.
- v. Clipper chip - hardware



Cryptography's role in securing the information society

- Nel novembre 1992 il Congresso USA costituisce una commissione ad hoc il National Research Council (NRC).
- La politica nazionale riguardo alla crittografia

CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY

Kenneth W. Dam and Herbert S. Lin, *Editors*

Committee to Study National Cryptography Policy
Computer Science and Telecommunications Board
Commission on Physical Sciences, Mathematics, and Applications

National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. 1996

Committee to Study National Cryptography Policy

- Il comitato ritiene che le sue raccomandazioni porteranno a una maggiore riservatezza e protezione delle informazioni per individui e aziende, riducendo così i crimini economici e finanziari e lo spionaggio economico da fonti sia nazionali che estere. Inoltre, si tradurranno in una maggiore sicurezza e garanzia per i sistemi informativi e le reti utilizzati dalla nazione, un'infrastruttura informatica nazionale più sicura. **Sebbene le raccomandazioni contribuiranno in questo modo alla prevenzione della criminalità e al miglioramento della sicurezza nazionale, il comitato riconosce che la diffusione della crittografia aumenterà l'onere di coloro che al governo sono incaricati di svolgere determinate attività specifiche di applicazione della legge e di intelligence.** **Ritiene che l'uso diffuso commerciale e privato della crittografia negli Stati Uniti e all'estero sia inevitabile a lungo termine e che i suoi vantaggi, nel complesso, superino i suoi svantaggi.** Pertanto, il comitato ha concluso che gli interessi generali del governo e della nazione sarebbero meglio serviti da una politica che promuova una transizione giudiziosa verso un ampio uso della crittografia.



Communicated on 29 October 2020

Published on 16 November 2020

THIRD SECTION

Application no. 13232/18
TELEGRAM MESSENGER LLP and TELEGRAM MESSENGER INC.
against Russia
lodged on 14 March 2018 and 23 April 2019

STATEMENT OF FACTS

1. The applicant, Telegram Messenger Limited Liability Partnership (hereinafter, “Telegram Messenger LLP”), until 2 April 2019, was a company incorporated in the United Kingdom and having its registered address in London. On 2 April 2019 it was struck off the Companies House Register on the application of its members – Telegram Messenger Inc. and Telegraph Inc.

2. On 23 April 2019 Telegram Messenger Inc., a company incorporated on the British Virgin Islands and having its registered address there, notified the Court of its wish to pursue the proceedings before the Court in Telegram Messenger LLP’s stead, and in its own name.

3. Both companies were/are represented before the Court by Mr D. Gaynutdinov, a lawyer authorised to practice in Russia.

A. The circumstances of the case

4. The facts of the case, as submitted by the applicants, may be summarised as follows.

1. Background information

5. Until May or June 2018 Telegram Messenger LLP owned and operated Telegram, a messaging application, which can be used free of charge on various devices such as mobile telephones, tablets or computers.



1. Internet communications organisers and their statutory obligations

33. Section 10.1 of the Information Technologies Act (Federal Law No. 149-FZ of 27 July 2006) was introduced into the Act in 2014. It defines an “Internet communications organiser” (ICO) and lists its statutory obligations.

An ICO is a person or an entity that ensures the functioning of information systems and (or) programmes for electronic devices, with the aim of receiving, transmitting, delivering and (or) processing electronic communications on the Internet. An ICO must notify the competent federal authority about its activity.

In July 2016 sub-section 4.1 was added and read as follows:

“4.1. Where additional coding is used in relation to receiving, transmitting, delivering and (or) processing of electronic communications of Internet users, an Internet communications organiser must submit, to the federal authority on information security, the information which is necessary for decoding ...”

34. The FSB Act (Federal Law No. 40-FZ of 3 April 1995) appoints the FSB as the federal authority in charge of the security and gives it a statutory competence to enact legal acts of general application in the areas of its competence.

the Code of Civil Procedure (CCP).

26. Having heard the representatives of Roskomnadzor and the FSB, by a judgment of 13 April 2018 the District Court ordered the blocking of the Telegram application in Russia. The court held as follows:

(a) Telegram Messenger LLP had been listed as an Internet communications organiser (ICO). It had then failed in its statutory obligation to comply with the disclosure order and had been fined. It had subsequently refused to provide the necessary data again.

(b) The argument about the impossibility to submit the decoding data was rejected because an ICO providing a possibility of coded communications was bound to comply with its statutory obligation to submit decoding data. In any event, the argument was not substantiated.

(c) The judgment was to be enforced immediately because its prolonged non-enforcement could result in “substantial violations of the constitutional rights relating to one’s personal data and cause important damage to public and private interests”.

27. On 18 April 2018 Telegram Messenger LLP lodged an ancillary


Telegram Messenger contro Russia

- 18 giugno 2020 - REUTERS
- La Russia revoca il divieto all'app di messaggistica di Telegram dopo aver fallito nel bloccarla
- MOSCA (Reuters) - La Russia ha revocato giovedì il divieto all'app di messaggistica Telegram di cui non era riuscita a fermare il funzionamento e nonostante il blocco dell'app fosse in vigore da più di due anni.
- Roskomnadzor ha affermato di aver agito perché il fondatore russo dell'app, Pavel Durov, era pronto a cooperare nella lotta al terrorismo e all'estremismo sulla piattaforma. "Roskomnadzor sta ritirando le sue richieste di limitare l'accesso a Telegram Messenger in accordo con l'ufficio del procuratore generale russo", si legge in una nota.
- Roskomnadzor ha deciso di vietare l'app nell'aprile 2018, ma nonostante il blocco degli indirizzi IP, non è stato in grado di portare a termine la sua minaccia, con Telegram che ha continuato a prosperare in Russia, dove è un servizio leader per i canali di notizie.
- Nonostante il divieto di utilizzare l'app, i dipartimenti governativi come il ministero degli Esteri russo e la task force nazionale per il coronavirus hanno canali ufficiali su Telegram.

Signal (Open whisper systems OWS)

- Nella "prima metà del 2016" Signal riceve una citazione dal distretto orientale della Virginia.
- La citazione ci richiedeva di fornire informazioni su due utenti di Signal per un'indagine del gran giurì federale.
- La risposta di Signal: *abbiamo progettato il servizio Signal per ridurre al minimo i dati che conserviamo sugli utenti di Signal, quindi le uniche informazioni che possiamo produrre in risposta a una richiesta come questa sono la data e l'ora in cui un utente si è registrato con Signal e l'ultima data della connettività di un utente al servizio.*
- In particolare, non abbiamo memorizzato includono nulla sui contatti di un utente (come i contatti stessi, un hash dei contatti, qualsiasi altra informazione di contatto derivata), qualsiasi cosa sui gruppi di un utente (come il numero di gruppi in cui si trova un utente, in quali gruppi si trova un utente, gli elenchi di appartenenza dei gruppi di un utente) o qualsiasi record di chi ha comunicato un utente.
- Tutti i contenuti dei messaggi sono crittografati end-to-end, quindi non abbiamo nemmeno queste informazioni.

LEGAL DEPARTMENT

 **ACLU**
AMERICAN CIVIL LIBERTIES UNION FOUNDATION

July 14, 2016

BY EMAIL

Special Agent Tracy J. Minnich
Federal Bureau of Investigation,
Northern Virginia Region
9325 Discovery Blvd.
Manassas, Virginia 20109
Tracy.Minnich@ic.fbi.gov

Re: Response to Grand-Jury Subpoena Directed at Open Whisper Systems (16-3 / A01-246 / 476 / 16-1090)

Dear Special Agent Minnich,

This letter responds to the June 30, 2016 grand-jury subpoena directed at Open Whisper Systems ("OWS") that seeks "subscriber account information" for two phone numbers. The American Civil Liberties Union represents OWS for purposes of responding to the subpoena. Please direct future correspondence about this matter to undersigned counsel.

Only one of the two listed phone numbers is associated with a Signal account: "+[REDACTED]". Open Whisper Systems has no record of an account associated with the second listed phone number, "+[REDACTED]", and therefore has no records to provide as to that number.

The only information responsive to the subpoena held by OWS is the time of account creation and the date of the last connection to Signal servers for account "+[REDACTED]". Consistent with the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703(c)(2), OWS is providing this information in response to the subpoena. See Attachment A.

Although OWS does not have, and therefore cannot produce, other categories of information listed in the subpoena, OWS notes that not all of those types of information can be appropriately requested with a subpoena. Under ECPA, the government can use a subpoena to compel disclosure of information from an electronic communications service provider only if that information falls within the categories listed at 18 U.S.C. § 2703(c)(2). For other types of information, the government must obtain a court order or search warrant. OWS objects to use of the grand-jury subpoena to request information beyond what is authorized in Section 2703(c)(2).

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 15TH FL.
NEW YORK, NY 10004-2400
T:212.549.2100
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
KUSAN S. HERNAN
PRESIDENT
ANTHONY D. ROMERO
EXECUTIVE DIRECTOR
ROBERT B. DEMAR
TREASURER

Attachment A

<u>Account</u>	<u>Information</u>
+ [REDACTED]	N/A
+ [REDACTED]	Last connection date: 1454198400000 Unix millis Account created: 1453475222063 Unix millis