Criptarea - nu știi ce mult ți-a folosit până n-o pierzi

3 august 2023 /
online

Alex Ștefănescu
alex.stefanescu@protonmail.com

pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentr

Cine suntem și ce facem

- **Advocacy**
- **Educație**
- **Conștientizare**

Susține și promovează o lume digitală liberă și deschisă, prin respectarea drepturilor fundamentale ale omului.

ApTI pentru libertatea Internetului

ApTI pentru dreptul la viață privată

ApTI pentru cultură liberă

Istoric

ApTI

- Societatea civilă
- Obține personalitate juridică în 2004
- Website-ul ApTI
- Canalul de Telegram
- ~~Twitter~~, pardon! X
- Mastodon
- Facebook
- LinkedIn

ApTI

Spionaj și monitorizare

- Laura Kovesi a fost monitorizată de Black Cube pe vremea când ocupa șefia DNA, în 2016.
- Cel puțin 180 de jurnaliști au fost monitorizați folosind spyware-ul Pegasus din 2016 până în prezent (2 din Ungaria).

Confiscarea dispozitivelor

- DIICOT a confiscat dispozitivele jurnalistului Alin Cristea (debraila.ro) de la domiciliul acestuia, al părinților și al redacției. Ulterior, Tribunalul Brăila a decis că jurnalistul și publicația nu s-au făcut vinovate de comiterea infracțiunii de distribuire sau deținere de materiale de pornografie infantilă (cum susținea DIICOT).

ApTI

Protecția sursei

- Sursele și avertizorii de integritate se vulnerabilizează atunci când vorbesc cu presa.
- Ce îi protejează?
  - Legea (deși cea mai recentă formă le diminuează impactul și siguranța)
  - **Comunicarea sigură cu jurnaliștii**

ApTI

Organizare

- Unor activiști de mediu le-a fost refuzată intrarea la o dezbatere cu primarul Londrei.
  Forțele de ordine de la intrare au identificat activiștii după nume și le-au refuzat intrare în baza unor “informații” despre intenția activiștilor de a lua cuvântul. (2022)

ApTI

Comunicarea de toate zilele

- WeChat, cea mai folosită aplicație de chat din China, monitorizează toate mesajele și fișierele trimise. Orice mesaj care conține cuvinte / fraze interzise este cenzurat.
- Toate mesajele utilizatorilor rețelei Parler au fost descărcate în format lizibil. Acestea expun detaliile organizării atacului asupra Capitolului SUA din 2021.

ApTI

Ce este criptarea?

Criptarea este procesul de codificare a informației astfel încât ea să fie înțeleasă doar de persoane autorizate. (dexonline - defininiția nu e parte din DEX)

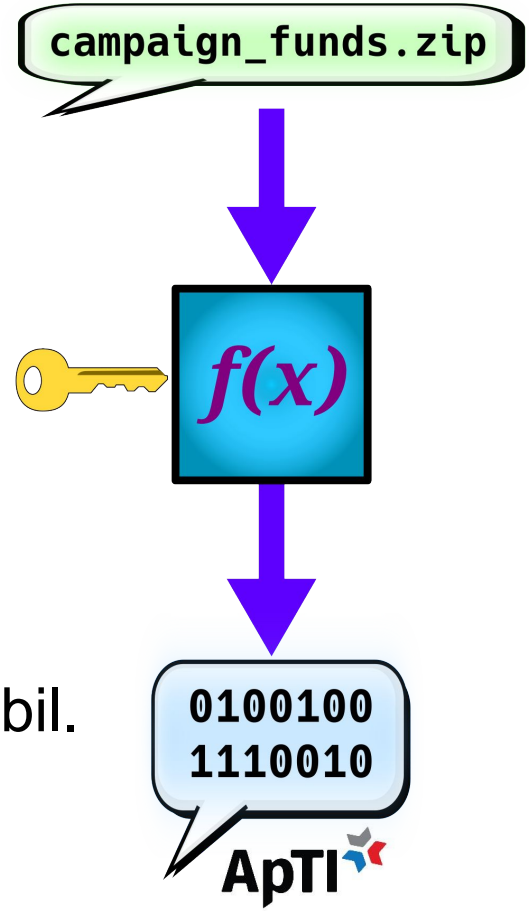
Criptarea este **reversibilă** (în sensul că mesajul poate fi decriptat) doar atunci când avem la dispoziție **cheia de criptare**.


115,792,089,237,316,195,42
,570,985,008,687,907,853,
69,984,665,640,564,039,4
57,584,007,913,129,639,935
POSSIBLE KEYS
Encryption
KSMG RPCHE PS UPG EHIMXLW
Khan Academy


E2EE
<end-to-end
encryption>

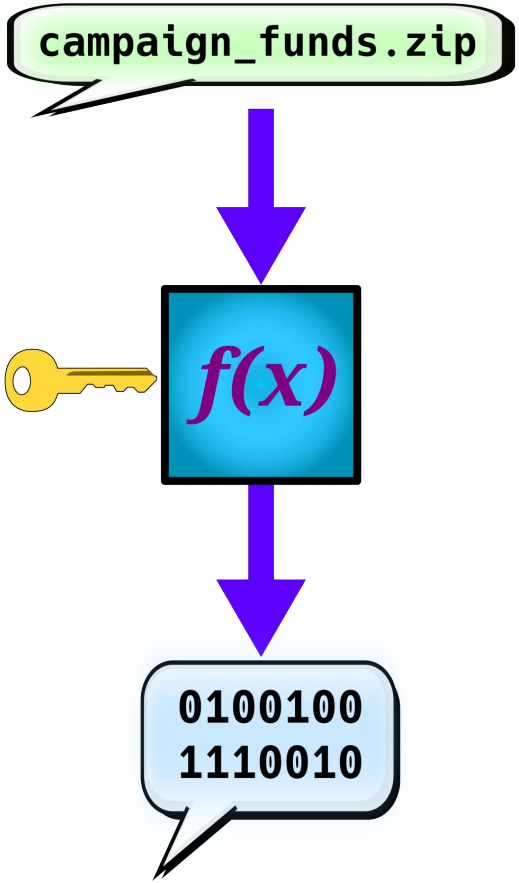
Componentele criptării

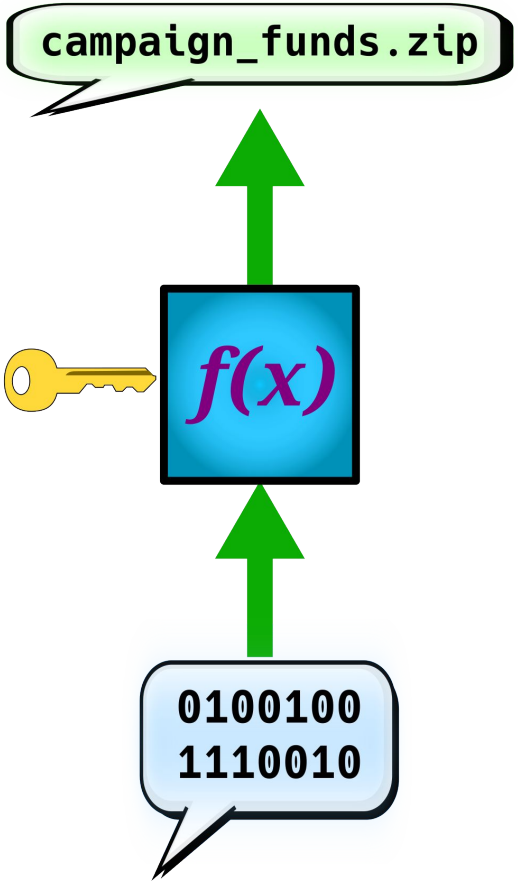
- **Mesajul** - lizibil oamenilor
- **Cheia** de criptare
- **Funcția** de criptare
- **Textul criptat** - ilizibil



- O dată criptat, un mesaj nu mai e inteligibil.
- **Dacă cheia de criptare e pierdută, mesajul nu mai poate fi recuperat.**

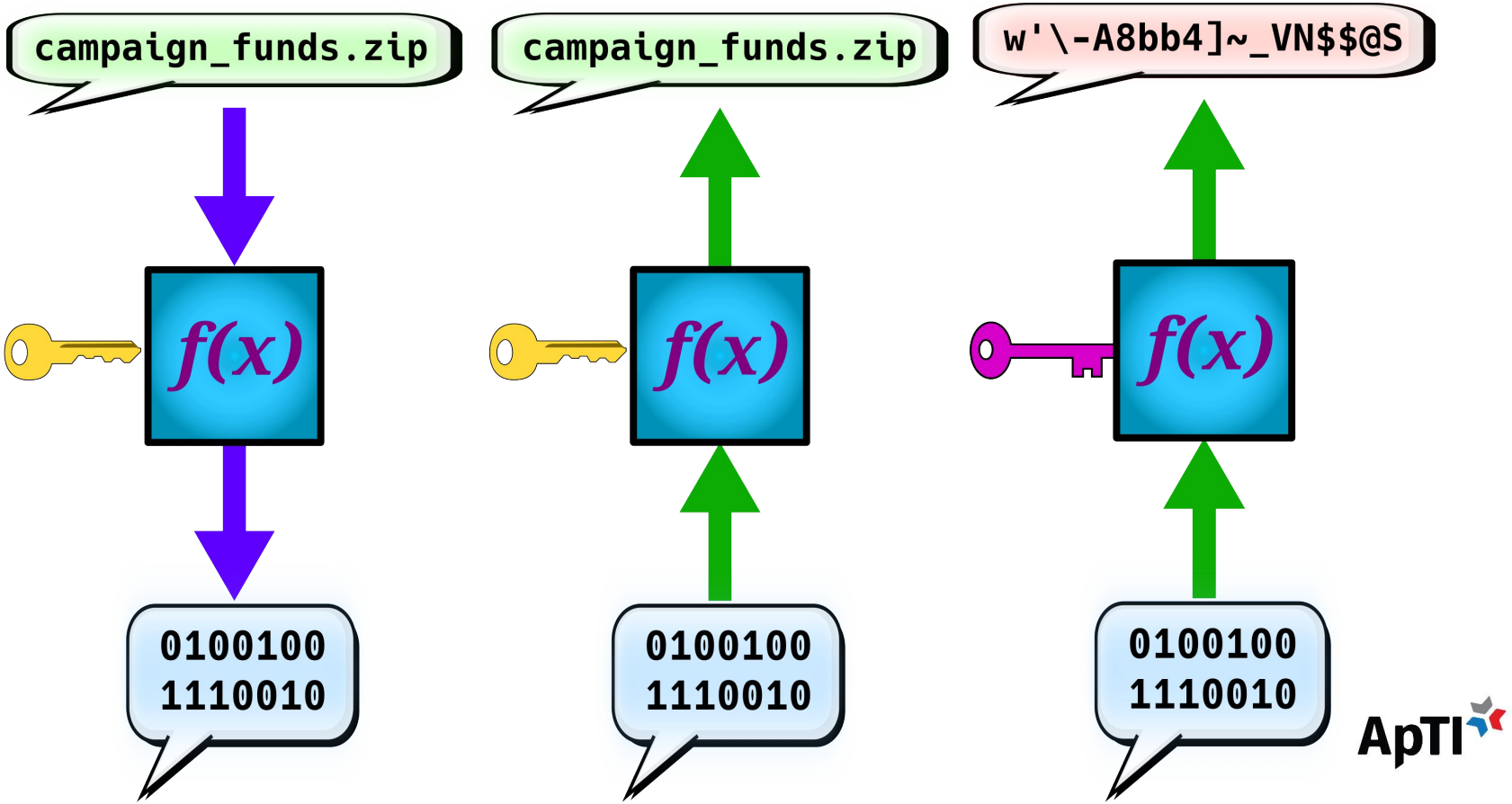
Criptarea - o introducere domoală





ApTI

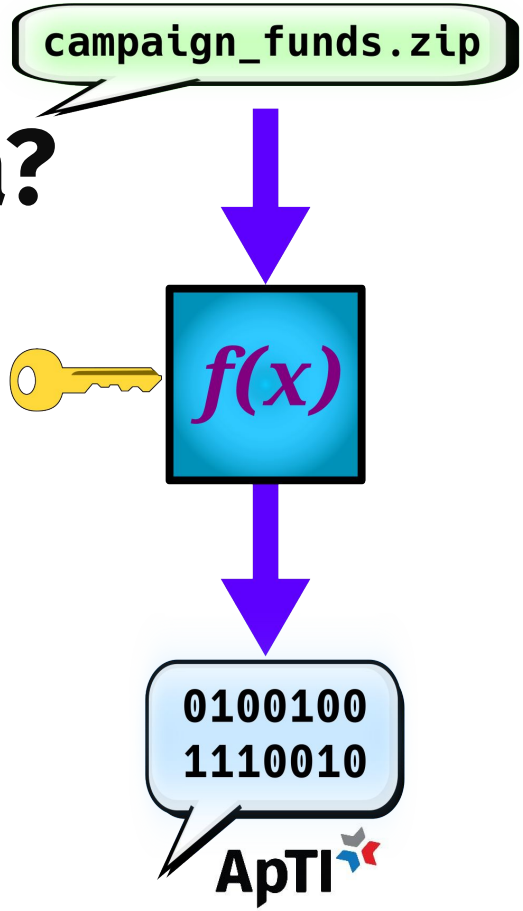
Criptarea - o introducere domoală



Criptarea poate fi spartă?

Pe scurt:

- 😱 **Da!**
- 😓 Dar durează atât de mult timp
- 😤 Încât nu e fezabil să încercăm
- 😵 Nici măcar pentru un singur mesaj.



Cum arată criptarea în practică?

Criptare simetrică

- Expeditorul și destinatarul folosesc aceeași cheie
- AES cu cheie de 128 sau 256 biți
- Nu a fost spart

Ar dura cam de 156 de ori mai mult decât vârsta universului nostru să ghicim o singură cheie.

ApTI

Cum arată criptarea în practică?

Criptare asimetrică (criptare cu cheie publică)

- Expeditorul și destinatarul folosesc **o cheie publică** pentru criptare și **o cheie privată** pentru decriptare
- RSA inițial, acum ECC (elliptic curve)

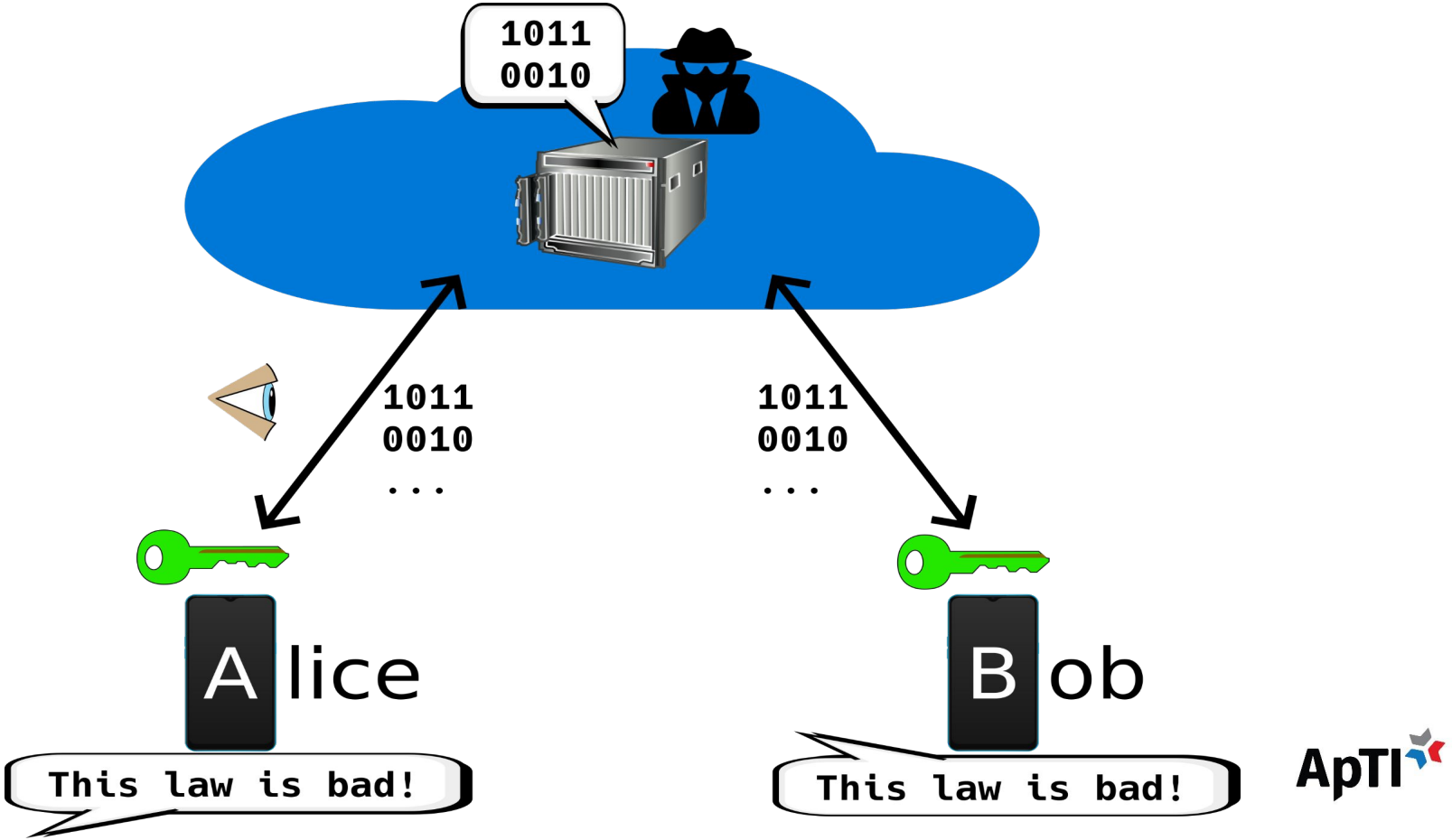
Și RSA și ECC sunt folosite pentru HTTPS.

Care e cea mai șmecheră criptare?

 **end-to-end encryption** 

ApTI

End-to-end encryption



Care sunt avantajele?

- **Doar participanții la o conversație pot citi mesajele**
- Dacă serverele aplicației sunt sparte, comunicațiile rămân ilizibile și confidențiale
- Conținutul mesajelor nu poate fi alterat

Ce aplicații folosesc E2EE?

- **Signal!**🥰💙
- WhatsApp
- Telegram (dacă creăm private chats)
- Facebook Messenger (dacă creăm private chats)
- Threema
- Wire

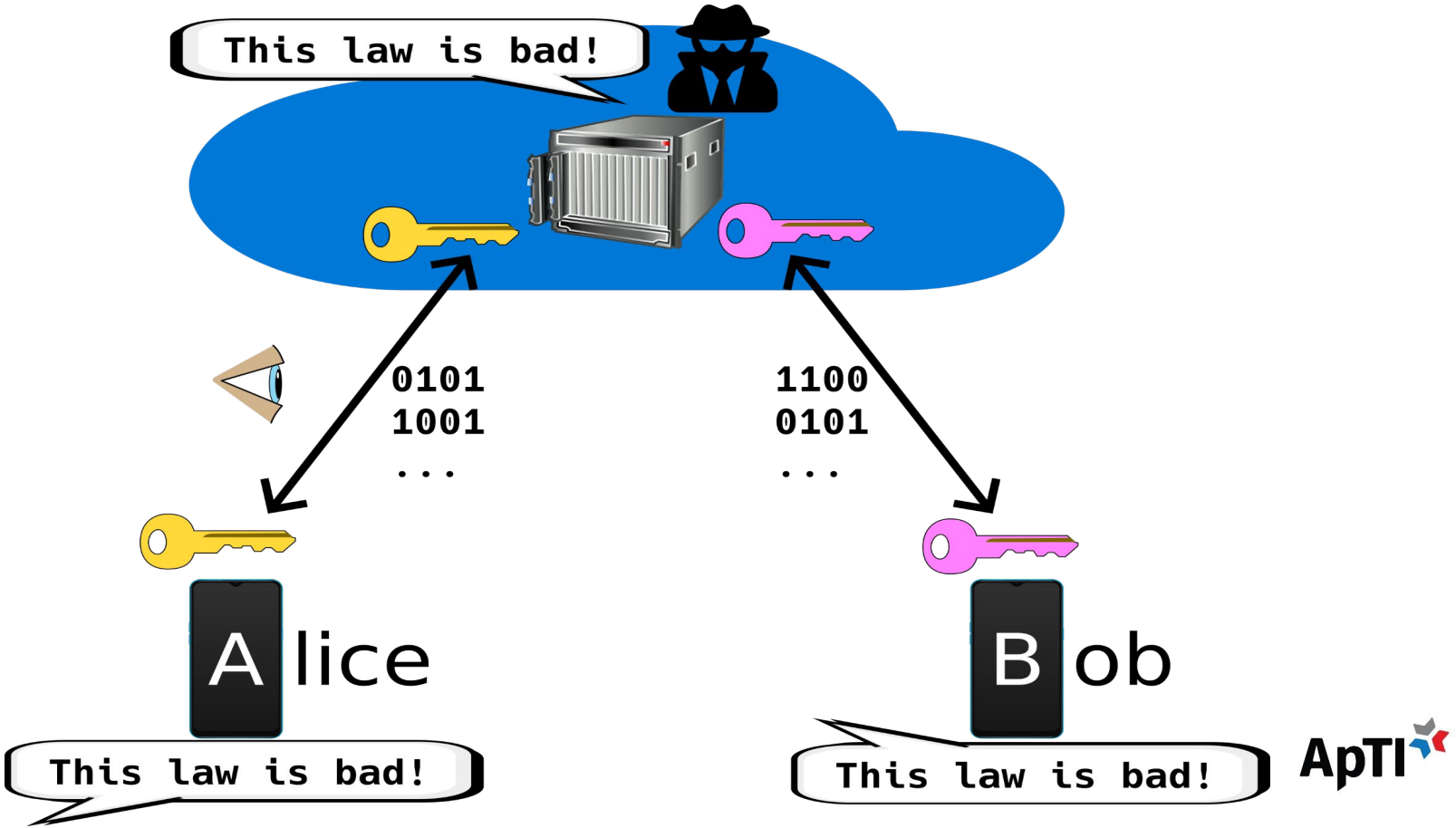
ApTI

Însă majoritatea aplicațiilor implementează...

 client-to-server encryption 

ApTI

Client-to-server encryption



De ce nu e la fel de șmecher?

- **Conținutul tuturor mesajelor e stocat, lizibil, pe server.**
- Cine deține (sau sparge😱) serverul are acces la conținutul mesajelor.
- Cine poate obține un mandat de copiere a serverului poate citi mesajele.

Ce aplicații folosesc C2SE?

- Telegram
- Facebook Messenger
- TikTok
- Instagram (în unele țări oferă E2EE, dar nu în România)
- ~~Twitter~~ X

ApTI

Intră în scenă: CSAR

Child Sexual Abuse Regulation

- O propunere de Regulament a Comisiei Europene din **2022**
- Denumit și **#ChatControl**

Intră în scenă: CSAR

Child Sexual Abuse Regulation
(textul integral: RO, HU, EN)

- **Scopul**: să protejeze copiii
- **Metoda**: să “scaneze cu Inteligență Artificială” toate mesajele trimise pe chat și conținutul stocat pe platforme pentru a găsi material conținând abuzuri împotriva minorilor.

ApTI

CSAR

În slide-urile următoare vom folosi acronimul **CSAM** (child sexual abuse material) pentru a ne referi la **material conținând abuzuri împotriva minorilor**.

Practic, ne referim nu doar la pornografie infantilă, ci la orice material care înfățișează sau simulează un minor care întreprinde activități sexuale.

CSAR: mecanisme

Entitățile vizate de CSAR trebuie să:

- **Raporteze** riscul stocării / diseminării de CSAR pe propriile platforme, plus strategiile de mitigare implementate
- Se supună unor **ordine de detectare**, emise de autoritățile coordonatoare.

Ordin de detectare?

Autoritatea coordonatoare dintr-un stat membru UE poate trimite un ordin de detectare către o platformă online dacă există riscul ca această să stocheze sau disemineze CSAM.

Ordinul e valabil până la 2 ani și **obligă compania să monitorizeze tot conținutul încărcat și creat de utilizatori.**

ApTI

Cine e vizat de CSAR?

Lista e lungă.

Servicii cu chat:

- Facebook Messenger, WhatsApp, Signal etc.
- Servicii de e-mail
- Aplicații de dating (Tinder, Grindr etc.)
- Jocuri online cu chat integrat

Cine e vizat de CSAR?

Lista continuă.

- Toate apelurile telefonice
- Toate SMS-urile și MMS-urile

App Store-urile (Google Play Store, Apple App Store).
Repository-uri de cod (GitHub).

ApTI

Cine e vizat de CSAR?

N-am terminat.

Platforme de găzduire de conținut

- iCloud, Google Cloud, Microsoft Azure etc.
- Dropbox, WeTransfer etc.
- Wordpress, Medium, Substack etc.
- Facebook, Reddit, YouTube, ~~Twitter~~ X, TikTok etc.

ApTI

Cine e vizat de CSAR?

Ultimul slide din listă, promit.

Orice platformă care permite găzduirea de conținut **chiar și pentru consum privat** trebuie să implementeze mecanisme de detecție a CSAM și de diminuare a riscului.

ApTI

Deci, cu un ordin de detectare, e scanat, practic, totul? 😱

Cam da.

- Tot ce **trimitem** prin aplicații de chat
- Orice **încărcăm** pe un website care găzduiește conținut


#StopScanningMe
EUROPEAN COMMISSION
SCANNING PRIVATE MESSAGES AND CONTROLLING HOW CITIZENS USE THE INTERNET
FUNDAMENTAL RIGHTS

Cum e scanat conținutul?

Folosind algoritmi de Inteligență Artificială care pot detecta:

- fișiere **deja-cunoscute** care conțin CSAM
- fișiere **noi** care conțin CSAM
- text care conține **grooming** [1]

[1] **Grooming** - activități care au scopul de a câștiga încrederea unei persoane minore cu scopul de a obține favoruri sexuale.

Nu știm cât de bună e detecția

Comisia Europene citează, în analiza de impact, statistici de detecție **raportate de firmele care fac software-ul**.

O cerere FOIA[1] trimisă către CE confirmă că nu există o verificare independentă a algoritmilor de detecție.

[1] **FOIA** - Freedom of Information Act. În România, **legea 544/2001.**

Studiu de caz: Thorn

Thorn raportează că algoritmii săi detectează CSAM cu precizie de 99.9%.

Nu știm însă nici câte materiale care nu sunt CSAM sunt detectate greșit (**fals-pozitiv**), nici cât de des Thorn eșuează în a detecta CSAM (**fals-negativ**).

Tot conținutul? Nu-i cam mult?

Ba da!

Legislația UE privind drepturile fundamentale spune că supravegherea sau interceptarea comunicațiilor unor persoane trebuie să se limiteze la persoane împotriva cărora există **suspiciuni rezonabile**.

Ușa din spate a chat-urilor

Companiile care oferă servicii de chat ar putea opta pentru **client-side scanning**.
Fiecare dispozitiv ar verifica **local** mesajele înainte de a le trimite.

Comunitatea de securitate repetă de ani întregi: **nu există o "ușă din spate" pe care o poate folosi doar poliția**.

ApTI

Bugs In Our Pockets

“CSS by its nature creates **serious security and privacy risks for all society** while the assistance it can provide for law enforcement is at best problematic. **There are multiple ways in which client-side scanning can fail, can be evaded, and can be abused.**”

CSAR invalidează E2EE?

Da.

Platformele care oferă E2EE sunt privite ca având un risc foarte mare de diseminare / stocare de CSAM.

Vor fi forțate, prin ordine de detecție, să monitorizeze conținutul. **Deci, adio E2EE!**

ApTI

CSAR invalidează E2EE? (Da)

În privința chat-urilor, implementarea client-side scanning nu împiedică E2EE, teoretic.

Dar, **pe dispozitiv**, conținutul este **scanat**, deci **accesat**. Dacă un dispozitiv e infectat, atacatorul ar putea acea același acces facil la toate mesajele pe care îl au algoritmii de client-side scanning.

ApTI

Grooming

Detecția s-ar baza pe **analizarea limbajului natural** (NLP - natural language processing).

Chiar și algoritmii cei mai performanți de inteligență artificială nu sunt suficient de precișI în orice limbă folosită în UE pentru a fi folosiți pe scară largă. **Și asta înainte să ne gândim câte nuanțe diferite există în limbajul nostru…**

ApTI

Cum decidem cine este un minor?

😢În momentul de față, **nu putem**.
😁Ceea ce e bine - **dreptul de a folosi Internetul sub anonimat.**

Ar trebui să ne identificăm pe Internet 🤯

Doar UE e alergică la cripatre?

Nu! UK a propus Online Safety Bill.

Aceeași strategie:

- e de dragul copiilor!
- vor să scaneze mesajele private direct pe dispozitiv (client-side scanning)
- vor să știe cine-i minor pe Internet
- ne-am pronunțat și împotriva ăsteia

ApTI

Care e poziția ApTI?

ApTI a semnat o scrisoare deschisă alături de 124 de organizații din societatea civilă din UE care cere **retragerea CSAR**.

ApTI este partener al coaliției Stop Scanning Me!

În curând, vom lansa o platformă de campanie similară, în limba română.

ApTI

Care e poziția companiilor?

ProtonMail și MullvadVPN se opun categoric.

Apple își va retrage serviciile iMessage și FaceTime dacă legea similară cu #ChatControl, din UK, trece.

Signal și WhatsApp refuză să compromită securitatea chat-urilor.

ApTI

ONG-urile care apără copii ce zic?

Experți în domeniul protecției copilului spun că #ChatControl face ca exprimarea explorării sexuale între persoane tinere să fie faptă penală.

ONG-uri din Germania și Portugalia spun că #ChatControl expune persoanele tinere la riscuri de șantaj și fraudă. **Nu există dovezi că abordarea #ChatControl este eficientă.**

ApTI

Care-s alternativele?

1. Educație, sensibilizare și resurse dedicate supraviețuitorilor abuzurilor. Prevenție!
2. Schimbare socială și structurală (mai multe fonduri pentru servicii sociale și de susținere a supraviețuitorilor)
3. Reformarea poliției și a sistemului juridic
4. Punerea în aplicare a normelor existente (Directiva Child Sexual Abuse din 2011)

Resurse

- ApTI despre Chat Control
- Ce trebuie să știe europarlamentarii noștri
- Studiu de caz: scanarea comunicațiilor private în Irlanda.
- Analiza CSAR făcută de European Digital Rights (EDRi):
  - Sumar
  - Analiza completă

ApTI

Resurse

- Sondaj: **80%** dintre tinerii cu vârste cuprinse între 13 și 17 ani din 13 state membre ale UE **nu s-ar simți confortabil să fie activi din punct de vedere politic sau să își exploreze sexualitatea** dacă autoritățile ar putea să le monitorizeze comunicațiile digitale, pentru a căuta abuzuri sexuale asupra copiilor.

Mulțumim!

alex.stefanescu@protonmail.com
https://chaos.social/@catileptic

pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentru cultură liberă pentru libertatea Internetului pentru dreptul la viață privată pentr