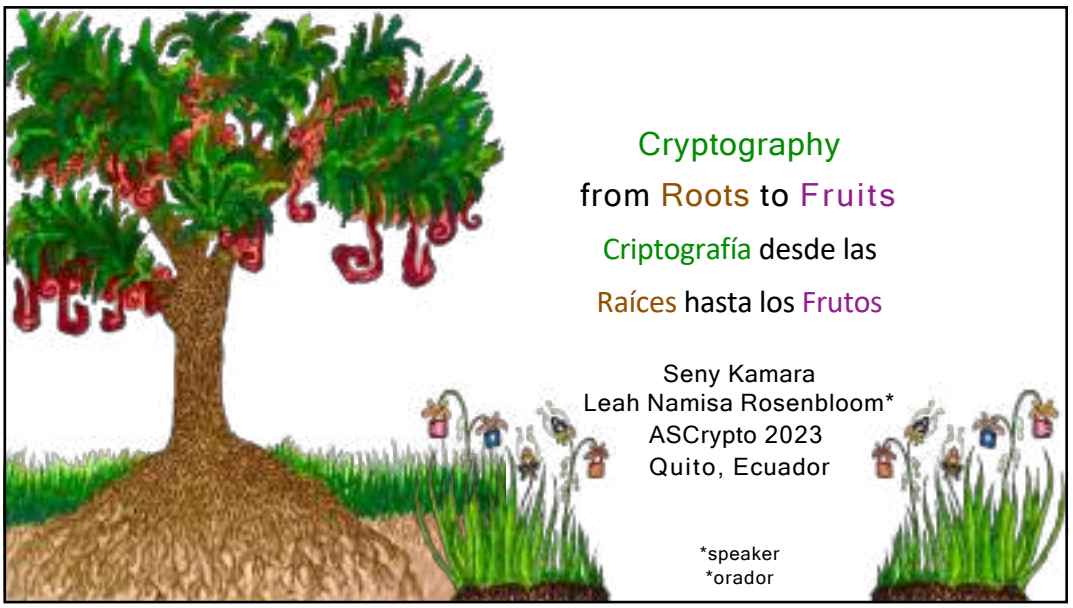


Cryptography
from Roots to Fruits
Criptografía desde las
Raíces hasta los Frutos

Seny Kamara
Leah Namisa Rosenbloom*
ASCrypto 2023
Quito, Ecuador

*speaker
*orador

1

Grounding Questions — Preguntas Fundamentales

What is the "root" of cryptography? Where does it come from?

¿Cuál es la "raíz" de la criptografía? ¿De dónde viene?

2

Grounding Questions — Preguntas Fundamentales

What is the "root" of cryptography? Where does it come from?

¿Cuál es la "raíz" de la criptografía? ¿De dónde viene?

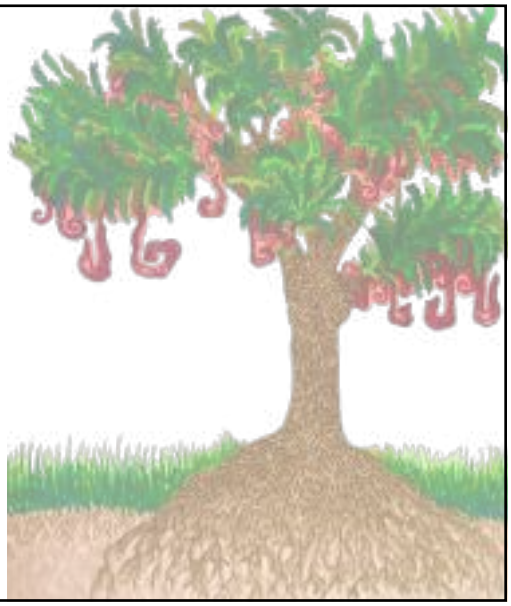
Why do we care? What "fruit" are we trying to produce?

¿Por qué nos importa? ¿Qué "fruto" estamos tratando de producir?

3

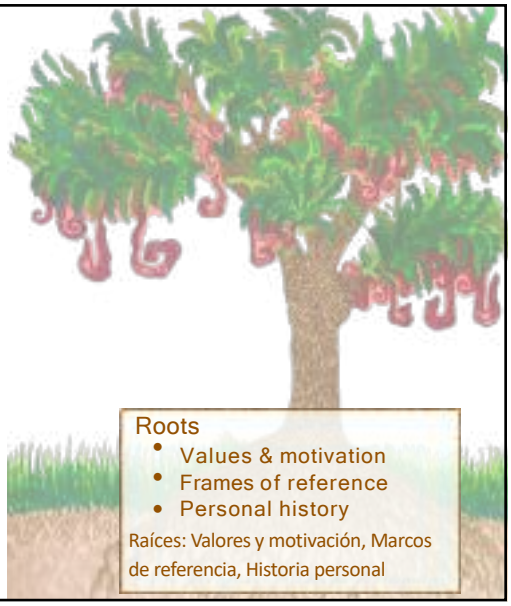
The Many-Tree Metaphor

La metáfora de los muchos árboles



4

The Many-Tree Metaphor
La metáfora de los muchos árboles



5

The Many-Tree Metaphor
La metáfora de los muchos árboles

6

The Many-Tree Metaphor
La metáfora de los muchos árboles

7

The Many-Tree Metaphor
La metáfora de los muchos árboles

"Cryptographers are not a monolith" means...

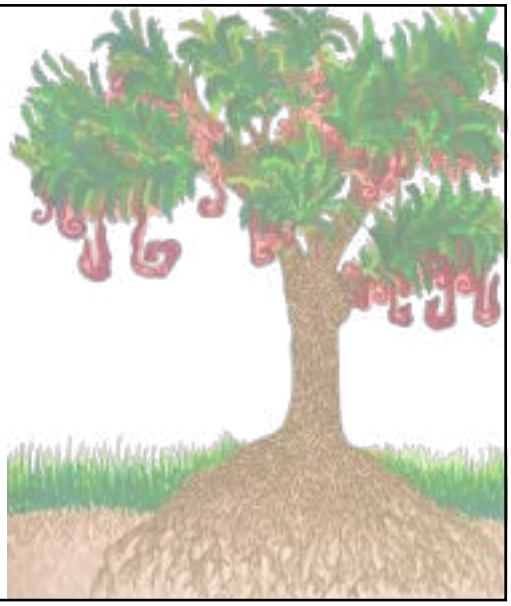
- We all have different roots
- Our identities are multiple and complex
- The following trees are meant to capture aspects of cryptographers, not stereotype individuals

"Criptógrafes no son un monolito" significa...

- Todos tenemos raíces diferentes
- Nuestras identidades son múltiples y complejas.
- Los siguientes árboles están destinados a capturar aspectos de los criptógrafos, no a estereotipar a individuos

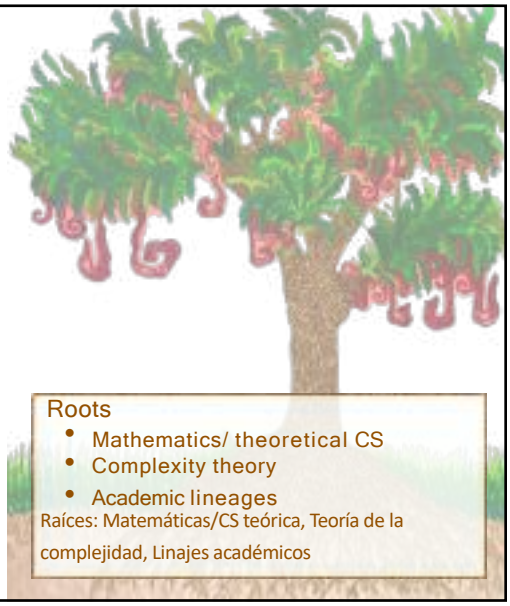
8

Theoretical Cryptographer
Criptógrafe Teórico



9

Theoretical Cryptographer
Criptógrafe Teórico



10

Theoretical Cryptographer
Criptógrafe Teórico

Trunk
- Foundational open problems
- Objective: primitives from minimal assumptions and computation/ communication complexity

Tronco: Problemas abiertos fundamentales; Objetivo: primitivos a partir de suposiciones mínimas y complejidad de computación/comunicación

Roots
- Mathematics/ theoretical CS
- Complexity theory
- Academic lineages

Raíces: Matemáticas/CS teórica, Teoría de la complejidad, Linajes académicos

11

Theoretical Cryptographer
Criptógrafe Teórico

Fruit
- Publications
- Conference talks
- Intellectual property
- Continued lineage

Fruta: Publicaciones, Conferencias, Propiedad intelectual, Linaje continuo

Trunk
- Foundational open problems
- Objective: primitives from minimal assumptions and computation/ communication complexity

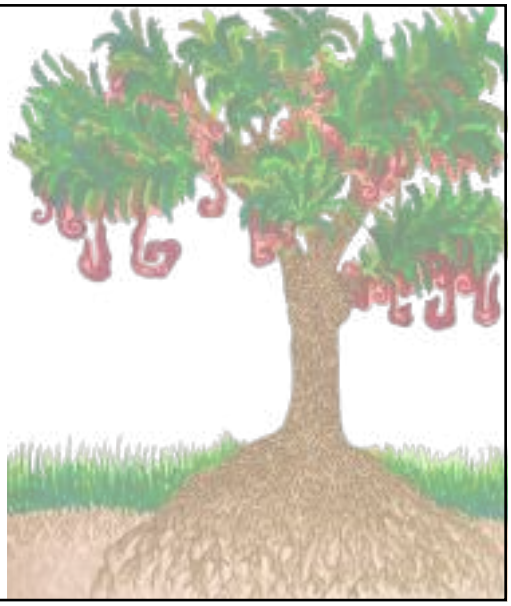
Tronco: Problemas abiertos fundamentales; Objetivo: primitivos a partir de suposiciones mínimas y complejidad de computación/comunicación

Roots
- Mathematics/ theoretical CS
- Complexity theory
- Academic lineages

Raíces: Matemáticas/CS teórica, Teoría de la complejidad, Linajes académicos

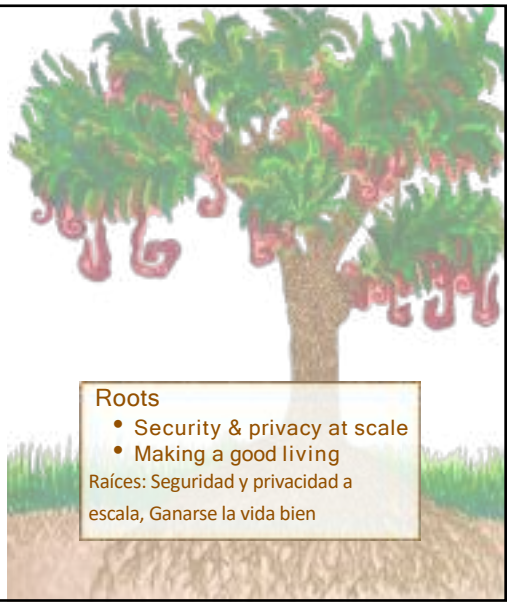
12

Industry Cryptographer
Criptógrafe de la Industria



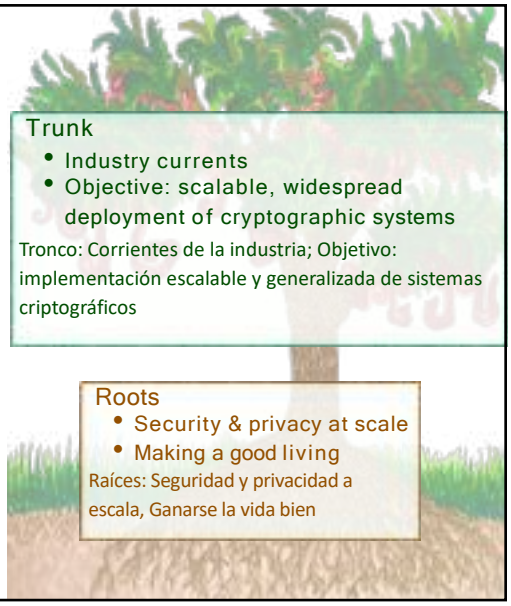
13

Industry Cryptographer
Criptógrafe de la Industria



14

Industry Cryptographer
Criptógrafe de la Industria

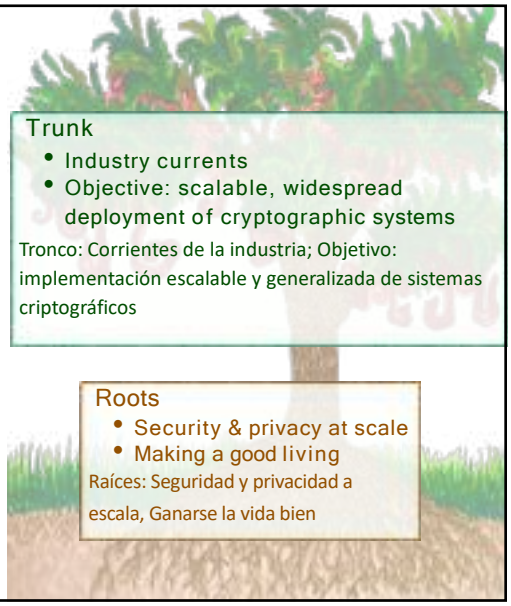


15

Industry Cryptographer
Criptógrafe de la Industria

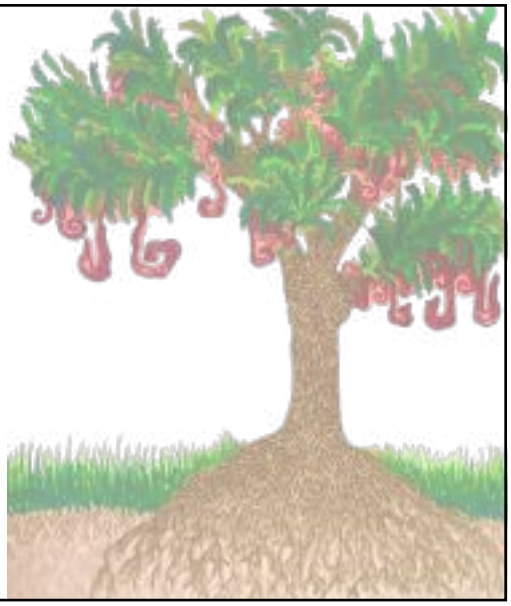
Fruit
- Implementations
- Widespread deployment
- Making, protecting property (capital, IP)

Fruta: Implementaciones, despliegue generalizada y creación, protección de la propiedad (capital, propiedad intelectual)



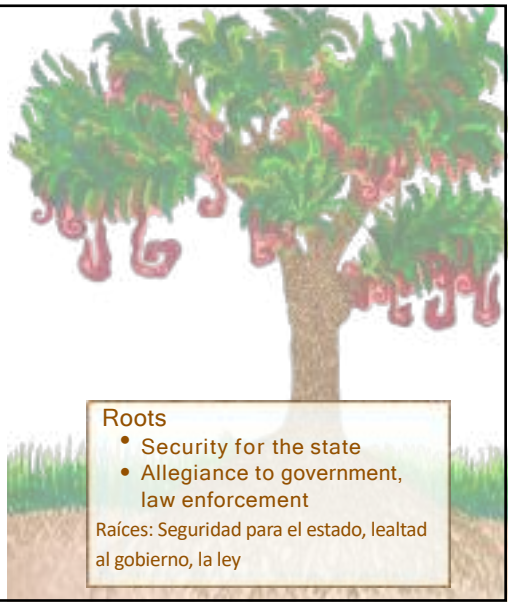
16

State Cryptographer
Criptógrafe Estatal



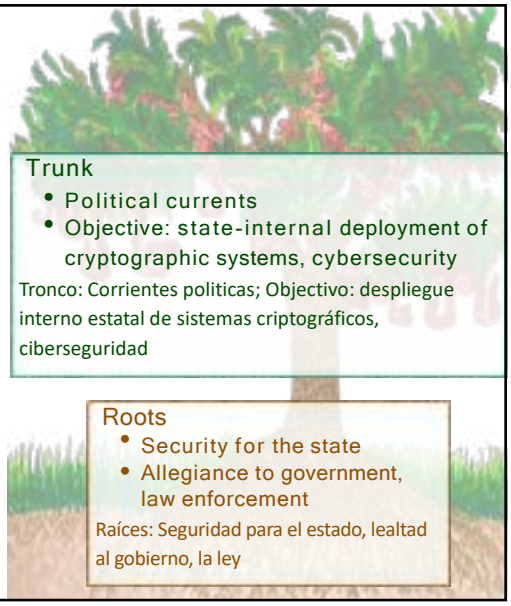
17

State Cryptographer
Criptógrafe Estatal



18

State Cryptographer
Criptógrafe Estatal

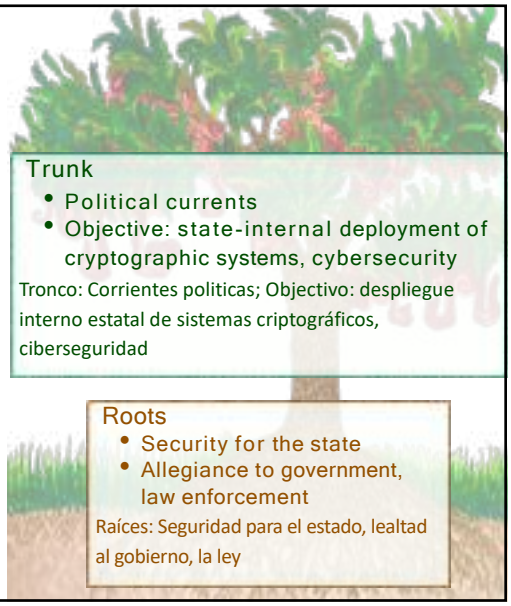


19

State Cryptographer
Criptógrafe Estatal

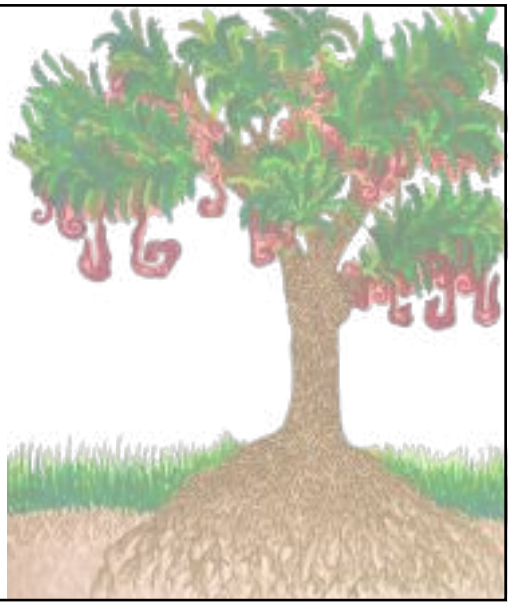
Fruit
- Implementations
- State-internal deployment
- Making, protecting state-owned property and power

Fruta: Implementaciones, Despliegue interno del Estado, Fabricación y protección de la propiedad y el poder del Estado



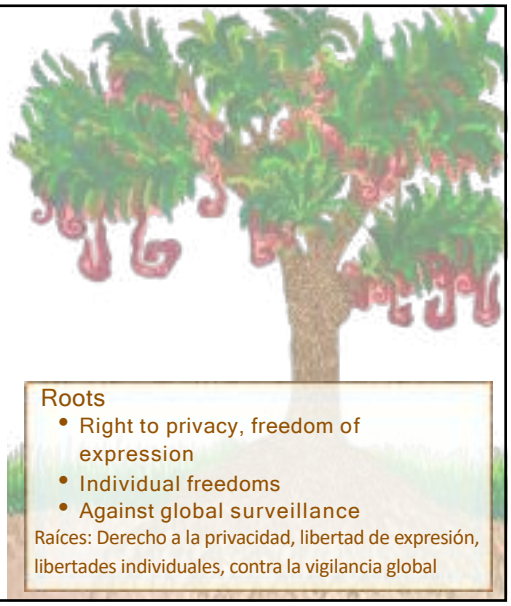
20

Cypherpunk Cryptographer
Criptógrafe Cypherpunk



21

Cypherpunk Cryptographer
Criptógrafe Cypherpunk



22

Cypherpunk Cryptographer
Criptógrafe Cypherpunk

Trunk
- Privacy in practice: E2EE, anonymity, unlinkability
- Objective: minimize state and corporate surveillance of individuals

Tronco: Privacidad en la práctica—E2EE, anonimato, desvinculación; Objetivo: minimizar la vigilancia estatal y corporativa de las personas

Roots
- Right to privacy, freedom of expression
- Individual freedoms
- Against global surveillance

Raíces: Derecho a la privacidad, libertad de expresión, libertades individuales, contra la vigilancia global

23

Cypherpunk Cryptographer
Criptógrafe Cypherpunk

Fruit
- Implementations
- Widespread, open source deployment
- Media coverage

Fruta: Implementaciones, Implementación generalizada de código abierto, Cobertura mediática

Trunk
- Privacy in practice: E2EE, anonymity, unlinkability
- Objective: minimize state and corporate surveillance of individuals

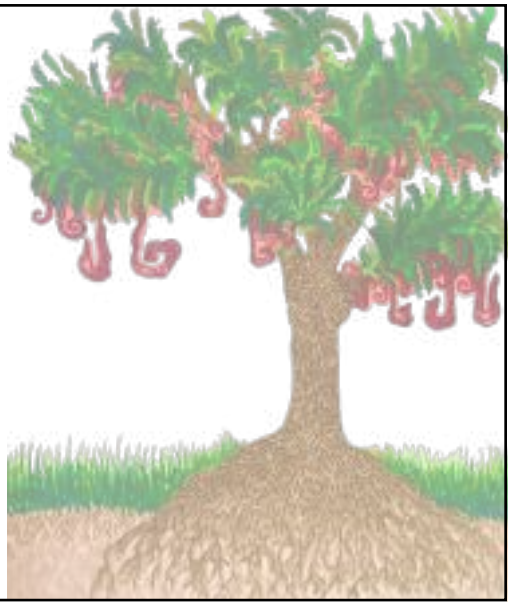
Tronco: Privacidad en la práctica—E2EE, anonimato, desvinculación; Objetivo: minimizar la vigilancia estatal y corporativa de las personas

Roots
- Right to privacy, freedom of expression
- Individual freedoms
- Against global surveillance

Raíces: Derecho a la privacidad, libertad de expresión, libertades individuales, contra la vigilancia global

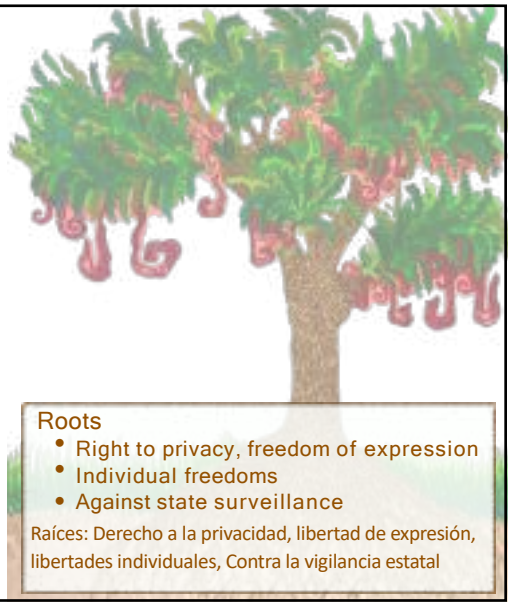
24

Policy Cryptographer
Criptógrafe de Políticas



25

Policy Cryptographer
Criptógrafe de Políticas



26

Policy Cryptographer
Criptógrafe de Políticas

Trunk
- Political currents
- Objective: create government policies that protect right to privacy, free expression

Tronco: Corrientes politicas; Objetivo: crear políticas gubernamentales que protejan el derecho a la privacidad y la libertad de expresión.

Roots
- Right to privacy, freedom of expression
- Individual freedoms
- Against state surveillance

Raíces: Derecho a la privacidad, libertad de expresión, libertades individuales, Contra la vigilancia estatal

27

Policy Cryptographer
Criptógrafe de Políticas

Fruit
- Legal policy, precedent
- Implementation
- Government

Fruta: Política jurídica, precedente, implementación, gobierno

Trunk
- Political currents
- Objective: create government policies that protect right to privacy, free expression

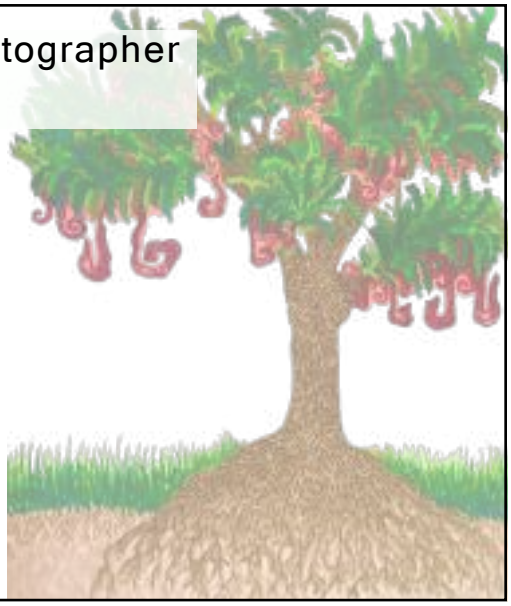
Tronco: Corrientes politicas; Objetivo: crear políticas gubernamentales que protejan el derecho a la privacidad y la libertad de expresión.

Roots
- Right to privacy, freedom of expression
- Individual freedoms
- Against state surveillance

Raíces: Derecho a la privacidad, libertad de expresión, libertades individuales, Contra la vigilancia estatal

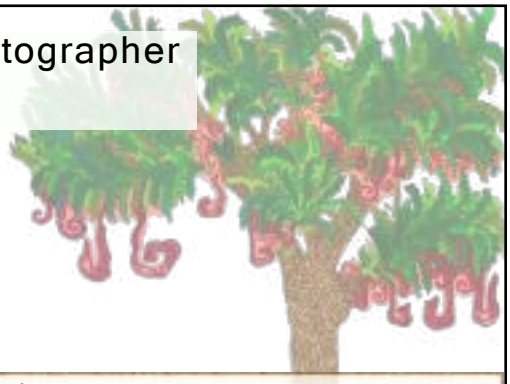
28

“Crypto for the People” Cryptographer
“Criptó para la Gente” Criptógrafe



29

“Crypto for the People” Cryptographer
“Criptó para la Gente” Criptógrafe



Roots
- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- “Cryptography rearranges power”

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, “La criptografía reordena el poder”

30

"Crypto for the People" Cryptographer

"Criptó para la Gente" Criptógrafe

Trunk

- Systemic, tech-facilitated privacy and security problems of marginalized people
- Objective: work with marginalized people to understand, solve problems

Tronco: Problemas sistémicos de privacidad y seguridad de las personas marginadas facilitados por la tecnología; Objetivo: trabajar con personas marginadas para comprender y resolver problemas.

Roots

- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- "Cryptography rearranges power"

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, "La criptografía reordena el poder"

31

"Crypto for the People" Cryptographer

"Criptó para la Gente" Criptógrafe

Fruit

- New reference frame
- Implementations
- Local deployment
- New lineages

Fruta: Nuevo marco de referencia, implementaciones, espliegue local, nuevos linajes

Trunk

- Systemic, tech-facilitated privacy and security problems of marginalized people
- Objective: work with marginalized people to understand, solve problems

Tronco: Problemas sistémicos de privacidad y seguridad de las personas marginadas facilitados por la tecnología; Objetivo: trabajar con personas marginadas para comprender y resolver problemas.

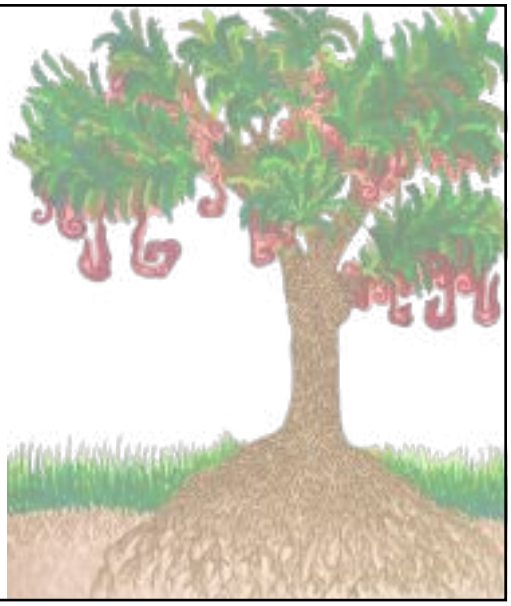
Roots

- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- "Cryptography rearranges power"

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, "La criptografía reordena el poder"

32

Organizing Cryptographer
Criptógrafe Organizador



33

Organizing Cryptographer
Criptógrafe Organizador

Roots
- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- "Cryptography rearranges power"
- Cryptography should rearrange power

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, "La criptografía reordena el poder,"
La criptografía debería reorganizar el poder

34

Organizing Cryptographer
Criptógrafe Organizador

Trunk
- Systemic, tech-facilitated privacy and security problems of marginalized people
- Objective: work with marginalized people to understand, solve problems
- Leverage cryptography to facilitate organizing against all systems of oppression

Tronco: Problemas sistémicos de privacidad y seguridad de las personas marginadas facilitados por la tecnología; Objetivo: trabajar con personas marginadas para comprender y resolver problemas, Aprovechar la criptografía para facilitar la organización contra todos los sistemas de opresión

Roots
- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- "Cryptography rearranges power"
- Cryptography should rearrange power

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, "La criptografía reordena el poder," La criptografía debería reorganizar el poder

35

Organizing Cryptographer
Criptógrafe Organizador

Fruit
- New reference frame
- Implementations
- Local deployment
- New lineages
- (Hopefully) Dismantling systems of oppression, replacing them with systems of our collective imagination

Fruta: Nuevo marco de referencia, implementaciones, despliegue local, nuevos linajes, (con suerte) desmantelar los sistemas de opresión, reemplazándolos con sistemas de nuestra imaginación colectiva

Trunk
- Systemic, tech-facilitated privacy and security problems of marginalized people
- Objective: work with marginalized people to understand, solve problems
- Leverage cryptography to facilitate organizing against all systems of oppression

Tronco: Problemas sistémicos de privacidad y seguridad de las personas marginadas facilitados por la tecnología; Objetivo: trabajar con personas marginadas para comprender y resolver problemas, Aprovechar la criptografía para facilitar la organización contra todos los sistemas de opresión

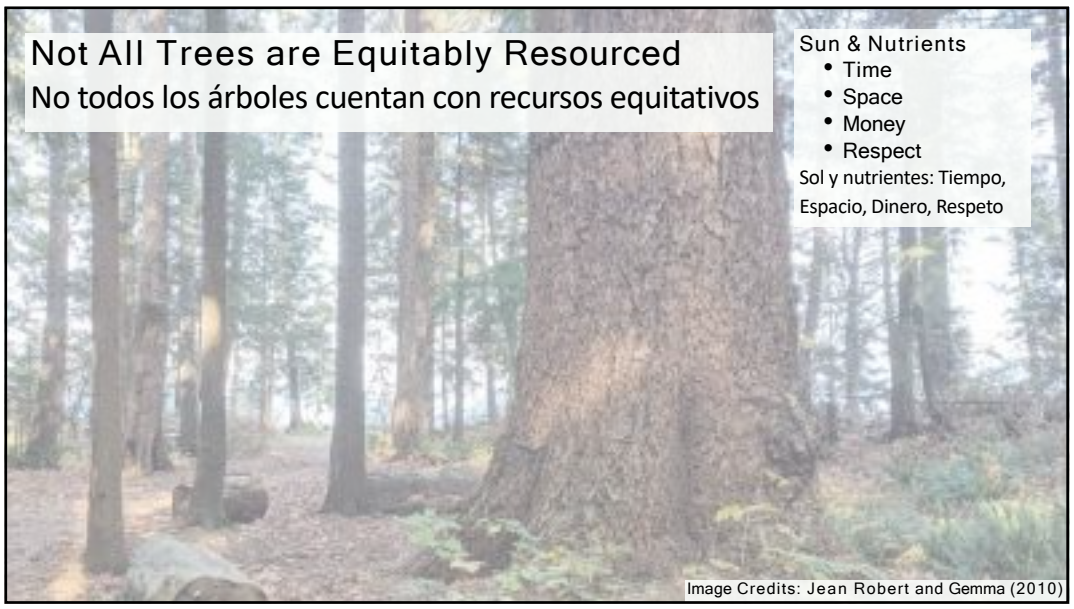
Roots
- Right to privacy, free expression for people and communities who are marginalized and oppressed by longevic, instutionalized systems
- "Cryptography rearranges power"
- Cryptography should rearrange power

Raíces: Derecho a la privacidad y libre expresión para las personas y comunidades marginadas y oprimidas por sistemas institucionalizados longevos, "La criptografía reordena el poder," La criptografía debería reorganizar el poder

36


Not All Trees are Equitably Resourced
No todos los árboles cuentan con recursos equitativos
Image Credits: Jean Robert and Gemma (2010)

37


Not All Trees are Equitably Resourced
No todos los árboles cuentan con recursos equitativos
Sun & Nutrients
• Time
• Space
• Money
• Respect
Sol y nutrientes: Tiempo, Espacio, Dinero, Respeto
Image Credits: Jean Robert and Gemma (2010)

38

Not All Trees are Equitably Resourced
No todos los árboles cuentan con recursos equitativos

Sun & Nutrients
- Time
- Space
- Money
- Respect

Sol y nutrientes: Tiempo, Espacio, Dinero, Respeto

Existing Paradigms
- Theoretical v. Applied
- Crypto-for-Security v. Crypto-for-Privacy (Narayanan 2013)
- Crypto-for-Crypto v. Crypto-for-Privacy (Rogaway 2015)
- Crypto for the People (Kamara 2020)

Paradigmas existentes: Teórico versus Aplicado, Cripto-para-seguridad contra Cripto-para-privacidad (Narayanan 2013), Cripto-para-Cripto contra Cripto-para-Privacidad (Rogaway 2015), Cripto para la gente (Kamara 2020)

Image Credits: Jean Robert and Gemma (2010)

39

Not All Trees are Equitably Resourced
No todos los árboles cuentan con recursos equitativos

Sun & Nutrients
- Time
- Space
- Money
- Respect

Sol y nutrientes: Tiempo, Espacio, Dinero, Respeto

Existing Paradigms
- Theoretical v. Applied
- Crypto-for-Security v. Crypto-for-Privacy (Narayanan 2013)
- Crypto-for-Crypto v. Crypto-for-Privacy (Rogaway 2015)
- Crypto for the People (Kamara 2020)

Paradigmas existentes: Teórico versus Aplicado, Cripto-para-seguridad contra Cripto-para-privacidad (Narayanan 2013), Cripto-para-Cripto contra Cripto-para-Privacidad (Rogaway 2015), Cripto para la gente (Kamara 2020)

The Many-Tree Metaphor
- Honoring diverse roots, paradigms
- Let's refocus our time, space, money, and respect to center those who are (and have been) marginalized

La metáfora de los muchos árboles: Honrando diversas raíces y paradigmas, Reorientemos nuestro tiempo, espacio, dinero y respeto para centrarnos en aquellos que están (y han estado) marginados

Image Credits: Jean Robert and Gemma (2010)

40

Grounding Questions — Preguntas Fundamentales

What is the "root" of cryptography? Where does it come from?

¿Cuál es la "raíz" de la criptografía? ¿De dónde viene?

Which roots and histories will we nourish moving forward?

¿Qué raíces e historias alimentaremos en el futuro?

41

Grounding Questions — Preguntas Fundamentales

What is the "root" of cryptography? Where does it come from?

¿Cuál es la "raíz" de la criptografía? ¿De dónde viene?

Which roots and histories will we nourish moving forward?

¿Qué raíces e historias alimentaremos en el futuro?

Why do we care? What "fruit" are we trying to produce?

¿Por qué nos importa? ¿Qué "fruto" estamos tratando de producir?

How does our work reflect our histories, values, and motivations?

¿Cómo refleja nuestro trabajo nuestras historias, valores y motivaciones?

42

Cryptography from Roots to Fruits — Criptografía desde las Raíces hasta los Frutos

- Grounding Questions — Preguntas Fundamentales ✓
- The Many-Tree Metaphor — La metáfora de los muchos árboles ✓
- Threat Modeling Paradigm Shift — Cambio de paradigma en el modelado de amenazas ←
- Cryptography & Technology for Grassroots Organizing — Criptografía y tecnología para la organización de base
- Trust Infrastructure for Grassroots Organizing — Infraestructura de confianza para la organización de base
- Activity: What is Your Tree? — Actividad: ¿Cuál es tu árbol?
- From Roots to Fruits, Revisited — De las raíces a los frutos, revisados

43

Threat Modeling Paradigm Shift

Cambio de paradigma en el modelado de amenazas

44

Threat Modeling Paradigm Shift

Cambio de paradigma en el modelado de amenazas

One Size Fits One: Protocol design begins with the unique needs of the population the protocol is meant to serve — Talla única para una: El diseño del protocolo comienza con las necesidades únicas de la población a la que está destinado el protocolo

45

Threat Modeling Paradigm Shift

Cambio de paradigma en el modelado de amenazas

One Size Fits One: Protocol design begins with the unique needs of the population the protocol is meant to serve — Talla única para una: El diseño del protocolo comienza con las necesidades únicas de la población a la que está destinado el protocolo

Trust Is Human: Digital trust is recognized as an extension of highly complex human trust relationships — La confianza es humana: la confianza digital se reconoce como una extensión de relaciones de confianza humana altamente complejas

46

Threat Modeling Paradigm Shift

Cambio de paradigma en el modelado de amenazas

One Size Fits One: Protocol design begins with the unique needs of the population the protocol is meant to serve — Talla única para una: El diseño del protocolo comienza con las necesidades únicas de la población a la que está destinado el protocolo

Trust Is Human: Digital trust is recognized as an extension of highly complex human trust relationships — La confianza es humana: la confianza digital se reconoce como una extensión de relaciones de confianza humana altamente complejas

Full Compromise Security: Threat modeling is redesigned to center people's actual needs and lived experiences — Seguridad de compromiso total: el modelado de amenazas se rediseñó para centrar las necesidades reales y las experiencias vividas de las personas.

47

Threat Modeling Paradigm Shift

Cambio de paradigma en el modelado de amenazas

One Size Fits One: Protocol design begins with the unique needs of the population the protocol is meant to serve — Talla única para una: El diseño del protocolo comienza con las necesidades únicas de la población a la que está destinado el protocolo

Trust Is Human: Digital trust is recognized as an extension of highly complex human trust relationships — La confianza es humana: la confianza digital se reconoce como una extensión de relaciones de confianza humana altamente complejas

Full Compromise Security: Threat modeling is redesigned to center people's actual needs and lived experiences — Seguridad de compromiso total: el modelado de amenazas se rediseñó para centrar las necesidades reales y las experiencias vividas de las personas.

Grassroots Optimization: Scale, efficiency, and accessibility are optimized for communities (not coroporations and governments) — Optimización de base: la escala, la eficiencia y la accesibilidad están optimizadas para las comunidades (no para las corporaciones ni los gobiernos).

48

Cryptography from Roots to Fruits — Criptografía desde las Raíces hasta los Frutos

- Grounding Questions — Preguntas Fundamentales ✓
- The Many-Tree Metaphor — La metáfora de los muchos árboles ✓
- Threat Modeling Paradigm Shift — Cambio de paradigma en el modelado de amenazas ✓
- Cryptography & Technology for Grassroots Organizing — Criptografía y tecnología para la organización de base ←
- Trust Infrastructure for Grassroots Organizing — Infraestructura de confianza para la organización de base
- Activity: What is Your Tree? — Actividad: ¿Cuál es tu árbol?
- From Roots to Fruits, Revisited — De las raíces a los frutos, revisados

49

Definition of Grassroots Organizing

Definición de organización de base

Grassroots organizing is a process by which people work from within marginalized communities to effect social, political, economic, and environmental change.

La organización de base es un proceso mediante el cual las personas trabajan desde dentro de comunidades marginadas para lograr cambios sociales, políticos, económicos y ambientales.

50

Takeaways from History

Conclusiones de la Historia

51

Project Cybersyn — Proyecto Synco

Chile (1971-1973): Popular Unity governemnt envisions distributed decision-making platform

Chile (1971-1973): El gobierno de la Unidad Popular imagina una plataforma distribuida para la toma de decisiones

Image Credits: Rama, Jamie (2010)

52

Project Cybersyn — Proyecto Synco

Chile (1971-1973): Popular Unity governemnt envisions distributed decision-making platform

Chile (1971-1973): El gobierno de la Unidad Popular imagina una plataforma distribuida para la toma de decisiones

Grassroots Economy: Workers speak straight to the government — Economía de base: los trabajadores hablan directamente con el gobierno

Image Credits: Rama, Jamie (2010)

53

Project Cybersyn — Proyecto Synco

Chile (1971-1973): Popular Unity governemnt envisions distributed decision-making platform

Chile (1971-1973): El gobierno de la Unidad Popular imagina una plataforma distribuida para la toma de decisiones

Grassroots Economy: Workers speak straight to the government — Economía de base: los trabajadores hablan directamente con el gobierno

An Alternate Vision of the Internet

- Decentralized, worker-owned
- Secondary plan for households
- Destroyed in military coup (1973)

Una visión alternativa de Internet: Descentralizado, propiedad de los trabajadores; Plan secundario para hogares; Destruido en golpe militar (1973)

Image Credits: Rama, Jamie (2010)

54

Operation Vula — Operación Vula

South Africa (1986-1990): African National Congress (ANC) creates cryptography for grassroots organizing

Sudáfrica (1986-1990): El Congreso Nacional Africano (ANC) crea criptografía para la organización de base

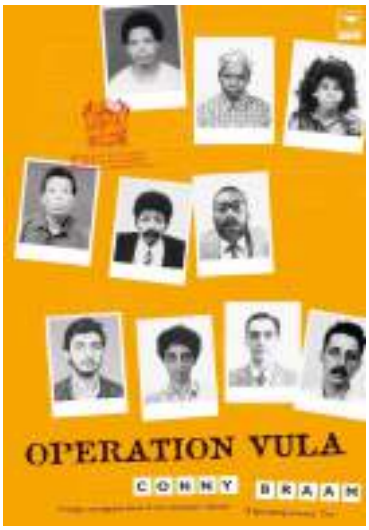


Image Credits: Jacana Media (2004), AP Photo/Udo Weitz, File (1990) via The Washington Post (2019)

55

Operation Vula — Operación Vula

South Africa (1986-1990): African National Congress (ANC) creates cryptography for grassroots organizing

Sudáfrica (1986-1990): El Congreso Nacional Africano (ANC) crea criptografía para la organización de base

Requirements: Asysnchronous, Covert, Long Distance, Public

Requisitos: asíncrono, secreto, larga distancia, público

Image Credits: Kamara, CRYPTO (2020)

56

Operation Vula — Operación Vula

ANC Activist Tim Jenkin (1995): "I went to find out about secure encryption algorithms…All I discovered was that cryptology was an arcane science for bored mathematicians, not for underground activists. However I learned a few tricks and used these to develop a system to meet our security needs."

Tim Jenkin, activista del ANC (1995): "Fui a investigar sobre algoritmos de cifrado seguros… Todo lo que descubrí fue que la criptología era una ciencia arcana para matemáticos aburridos, no para activistas clandestinos. Sin embargo, aprendí algunos trucos y los usé para desarrollar un sistema que satisfaga nuestras necesidades de seguridad".

57

COINTELPRO

United States (1956–1971): Federal Bureau of Investigation (FBI) illegally & extensively surveils activists

Estados Unidos (1956-1971): El Buró Federal de Investigaciones (FBI) monitorea de forma extensiva e ilegal a activistas

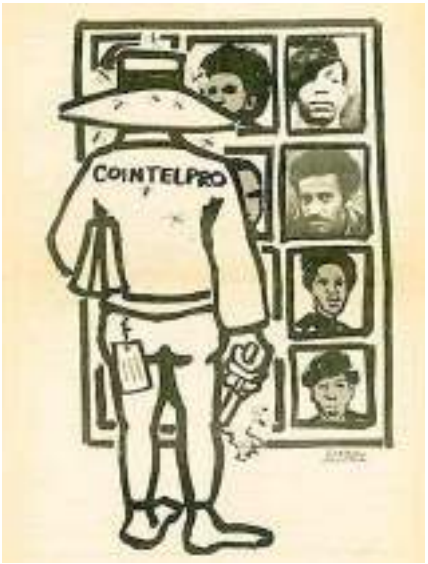


Image Credits: The Melanated Press (2014), Emory Douglas (1976)

58

COINTELPRO

United States (1956–1971): Federal Bureau of Investigation (FBI) illegally & extensively surveils activists

Estados Unidos (1956-1971): El Buró Federal de Investigaciones (FBI) monitorea de forma extensiva e ilegal a activistas

Blurred Boundaries: Surveillance leads to assassination, incarceration

Líneas Borrosas: el monitoreo lleva a asesinatos, encarcelamiento

Fred Hampton (1948-1969)

Angela Davis

Mae Mallory

Ericka Huggins

Image Credits: Atlanta Black Star (2015), Madison365 (2019), What'sHerName Podcast (2018), Ericka Huggins Official Website (2016)

59

COINTELPRO

United States (1956–1971): Federal Bureau of Investigation (FBI) illegally & extensively surveils activists

Estados Unidos (1956-1971): El Buró Federal de Investigaciones (FBI) monitorea de forma extensiva e ilegal a activistas

Blurred Boundaries: Surveillance leads to assassination, incarceration

Líneas Borrosas: el monitoreo lleva a asesinatos, encarcelamiento

The Church Committee Report (1975):

- Intimidation, manipulation, dragnet tactics
- No meaningful oversight & accountability
- Digital equivalents (Snowden 2013)

Informe del Comité de Church (1975): Intimidación, manipulación, tácticas de redada; No hay supervisión ni rendición de cuentas significativas; Equivalentes digitales (Snowden 2013)

Image Credit: U.S. Senate Select Committee on Intelligence (1975)

60

The Arab Spring — La Primavera Árabe

Many Countries (2010-2012): Tunisia, Libya, Egypt, Yemen, Syria, Bahrain, Morocco, Iraq, Algeria, Lebanon, Jordan, Kuwait, and many more with minor protests

Muchos países (2010-2012): Túnez, Libia, Egipto, Yemen, Siria, Bahrein, Marruecos, Irak, Argelia, Líbano, Jordania, Kuwait y muchos más con protestas menores

Image Credits: CBS News (2012), Reuters (2012)

61

The Arab Spring — La Primavera Árabe

Many Countries (2010-2012): Tunisia, Libya, Egypt, Yemen, Syria, Bahrain, Morocco, Iraq, Algeria, Lebanon, Jordan, Kuwait, and many more with minor protests

Muchos países (2010-2012): Túnez, Libia, Egipto, Yemen, Siria, Bahrein, Marruecos, Irak, Argelia, Líbano, Jordania, Kuwait y muchos más con protestas menores.

The Role of Social Media

- Speed, Scope, and Scale
- Facilitator rather than direct or independent cause of chage

El papel de las redes sociales: Velocidad, alcance y escala; Facilitador en lugar de causa directa o independiente del cambio.

Image Credits: Amin Ansari (2012), Anna Lena Schiller (2012), Wikimedia Commons (2011)

62

The Arab Spring — La Primavera Árabe

Many Countries (2010-2012): Tunisia, Libya, Egypt, Yemen, Syria, Bahrain, Morocco, Iraq, Algeria, Lebanon, Jordan, Kuwait, and many more with minor protests

Muchos países (2010-2012): Túnez, Libia, Egipto, Yemen, Siria, Bahrein, Marruecos, Irak, Argelia, Líbano, Jordania, Kuwait y muchos más con protestas menores.

The Role of Social Media

- Speed, Scope, and Scale
- Facilitator rather than direct or independent cause of chage

El papel de las redes sociales: Velocidad, alcance y escala; Facilitador en lugar de causa directa o independiente del cambio.

Inspired Countless Movements — Innumerables movimientos inspirados

63

Takeaways from Studies of Contemporary Movements

Conclusiones de los estudios de los movimientos contemporáneos

64

Be Safe or Be Seen? (Lokot 2018) — ¿Estar seguro o ser visto?

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)

Observación etnográfica de activistas de la Fundación Anticorrupción (Rusia)

Image Credit: Evgeny Feldman/AP (2018)

65

Be Safe or Be Seen? (Lokot 2018) — ¿Estar seguro o ser visto?

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)

Observación etnográfica de activistas de la Fundación Anticorrupción (Rusia)

Conspicuous Security:

Tools and Education

Seguridad visible: Herramientas y educación

Figure 2. Screen grab from YouTube talk show "The Cloud," hosted by Leonid Volkov, explaining the basics of the Tor network. Episode 002 was devoted to online anonymity and circumventing website blocks.

Image Credit: Lokot (2018)

66

Be Safe or Be Seen? (Lokot 2018) — ¿Estar seguro o ser visto?

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)
Observación etnográfica de activistas de la Fundación Anticorrupción (Rusia)

Conspicuous Security:

Tools and Education

Seguridad visible: Herramientas y educación

Strategic Visibility:

Transparency and Community

Visibilidad estratégica: transparencia y comunidad

Image Credit: Lokot (2018)

67

Be Safe or Be Seen? (Lokot 2018) — ¿Estar seguro o ser visto?

Ethnographic Observation of Anti-Corruption Foundation Activists (Russia)
Observación etnográfica de activistas de la Fundación Anticorrupción (Rusia)

Conspicuous Security:

Tools and Education

Seguridad visible: Herramientas y educación

Strategic Visibility:

Transparency and Community

Visibilidad estratégica: transparencia y comunidad

Hong Kong (Albrecht, Blasco, Jensen, & Marekova 2021): Bigger public groups, smaller encrypted groups with rigorous onboarding process —

Grupos públicos más grandes, grupos cifrados más pequeños con un riguroso proceso de incorporación

Image Credit: Reclaim The Net (2019)

68

Digital Trust is Physical Trust (Rosenbloom 2020) — La confianza digital es confianza física

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Entrevistas semiestructuradas con 50 activistas de Black Lives Matter (EE. UU.)

Image Credit: Tyger Williams/AP (2020)

69

Digital Trust is Physical Trust (Rosenbloom 2020) — La confianza digital es confianza física

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Entrevistas semiestructuradas con 50 activistas de Black Lives Matter (EE. UU.)

Dangers of Immediacy, Anonymity:
Lack of information integrity online
Peligros de la inmediatez y el anonimato:
Falta de integridad de la información en línea.

Image Credit: Jason Peters (2020)

70

Digital Trust is Physical Trust (Rosenbloom 2020) — La confianza digital es confianza física

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Entrevistas semiestructuradas con 50 activistas de Black Lives Matter (EE. UU.)

Dangers of Immediacy, Anonymity:
Lack of information integrity online
Peligros de la inmediatez y el anonimato:
Falta de integridad de la información en línea.

Direct Action Decision-Making: Word of mouth, community evaluation
Toma de decisiones de acción directa: Boca a boca, evaluación comunitaria

Image Credits: Jason Peters (2020), Matt Rourke/AP (2020)

71

Digital Trust is Physical Trust (Rosenbloom 2020) — La confianza digital es confianza física

Semi-Structured Interviews with 50 Black Lives Matter Activists (U.S.)

Entrevistas semiestructuradas con 50 activistas de Black Lives Matter (EE. UU.)

Dangers of Immediacy, Anonymity:
Lack of information integrity online
Peligros de la inmediatez y el anonimato:
Falta de integridad de la información en línea.

Direct Action Decision-Making: Word of mouth, community evaluation
Toma de decisiones de acción directa: Boca a boca, evaluación comunitaria

Hong Kong (ABJM 2021): face-to-face preceds phone-to-phone because "'standing on the front line together is very important for trust' (P10)" — el cara a cara precede al teléfono a teléfono porque "'estar juntos en primera línea es muy importante para la confianza' (P10)"

Image Credits: Justin Chin/Bloomberg/Getty (2020)

72

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

La accesibilidad digital es accesibilidad física

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Estudio del papel de las redes sociales y las TIC en el levantamiento de Euromaidan (Ucrania)

Image Credit: Kostyantyn Chernichkin (2014)

73

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

La accesibilidad digital es accesibilidad física

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Estudio del papel de las redes sociales y las TIC en el levantamiento de Euromaidan (Ucrania)

Physical IT Tents: Internet access, equipment

Tiendas de TI físicas: acceso a internet, equipo

Image Credit: Rosipro (2014), NBC News (2013)

74

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

La accesibilidad digital es accesibilidad física

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Estudio del papel de las redes sociales y las TIC en el levantamiento de Euromaidan (Ucrania)

Physical IT Tents: Internet access, equipment

Tiendas de TI físicas: acceso a internet, equipo

Crowdsourcing: Ad-hoc groups of people with resources

Colaboración colectiva: Grupos ad-hoc de personas con recursos

Image Credit: Rosipro (2014), NBC News (2013)

75

Digital Accessibility is Physical Accessibility (Bohdanova 2014)

La accesibilidad digital es accesibilidad física

Study of the role of social media and ICTs in the Euromaidan uprising (Ukraine)

Estudio del papel de las redes sociales y las TIC en el levantamiento de Euromaidan (Ucrania)

Physical IT Tents: Internet access, equipment

Tiendas de TI físicas: acceso a internet, equipo

Crowdsourcing: Ad-hoc groups of people with resources

Colaboración colectiva: Grupos ad-hoc de personas con recursos

Led to Technologist-Activist Collaboration: IT tents evolved into idea-generating spaces, development of new, needed tech — Conducido a la colaboración tecnólogo-activista: las tiendas de TI evolucionaron hasta convertirse en espacios de generación de ideas y desarrollo de tecnología nueva y necesaria.

Image Credit: Rosipro (2014), NBC News (2013)

76

Circumventing Censorship and Accessibility Issues

Eludir la censura y los problemas de accesibilidad

Lower-Tech Fallbacks: Audio transmission (Operation Vula), Satellite phones + dialup (Arab Spring), Word of Mouth (Black Lives Matter)

Refugios de baja tecnología: Transmisión de audio (Operación Vula), Teléfonos satelitales + acceso telefónico (Primavera Árabe), Boca a boca (Black Lives Matter)

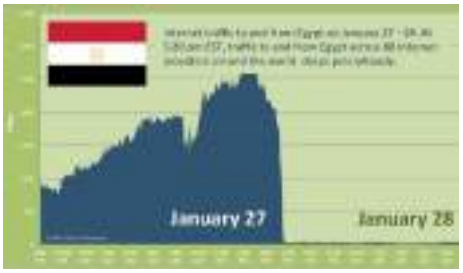


Image Credits: Labovitz/Arbor Networks (2011), Rob Wilson/Facebook (2016)

77

Circumventing Censorship and Accessibility Issues

Eludir la censura y los problemas de accesibilidad

Lower-Tech Fallbacks: Audio transmission (Operation Vula), Satellite phones + dialup (Arab Spring), Word of Mouth (Black Lives Matter)

Refugios de baja tecnología: Transmisión de audio (Operación Vula), Teléfonos satelitales + acceso telefónico (Primavera Árabe), Boca a boca (Black Lives Matter)

Physical Pre-Planning: IT tents (Euromaidan Uprising), "Facebook Hill" (Standing Rock)

Planificación previa física: Tiendas de campaña de TI (Levantamiento de Euromaidán), "Colina de Facebook" (Standing Rock)

Image Credits: Labovitz/Arbor Networks (2011), Rob Wilson/Facebook (2016)

78

Circumventing Censorship and Accessibility Issues

Eludir la censura y los problemas de accesibilidad

Lower-Tech Fallbacks: Audio transmission (Operation Vula), Satellite phones + dialup (Arab Spring), Word of Mouth (Black Lives Matter)

Refugios de baja tecnología: Transmisión de audio (Operación Vula), Teléfonos satelitales + acceso telefónico (Primavera Árabe), Boca a boca (Black Lives Matter)

Physical Pre-Planning: IT tents (Euromaidan Uprising), "Facebook Hill" (Standing Rock)

Planificación previa física: Tiendas de campaña de TI (Levantamiento de Euromaidán), "Colina de Facebook" (Standing Rock)

Toward Community-Based Networks: Local accessibility, physical ownership, increases effort required to obtain data — Hacia redes comunitarias: accesibilidad local, propiedad física, aumenta el esfuerzo requerido para obtener datos

Image Credits: Labovitz/Arbor Networks (2011), Rob Wilson/Facebook (2016)

79

Device Compromise and Deletion (ABJM 2021) — Compromiso y eliminación del dispositivo

Semi-Structured Interviews with 11 Anti-ELAB Protesters (Hong Kong)

Entrevistas semiestructuradas con 11 manifestantes anti-ELAB (Hong Kong)

Full Compromise Security:

Detection and mitigation

Seguridad de compromiso total:

Detección y mitigación

Image Credit: AFP/Getty (2019)

80

Device Compromise and Deletion (ABJM 2021) — Compromiso y eliminación del dispositivo

Semi-Structured Interviews with 11 Anti-ELAB Protesters (Hong Kong)
Entrevistas semiestructuradas con 11 manifestantes anti-ELAB (Hong Kong)

Full Compromise Security:
Detection and mitigation
Seguridad de compromiso total:
Detección y mitigación

Scheduled v. Remote Deletion:
Arrest compromises contacts, logs
Eliminación programada versus remota:
El arresto compromete contactos y registros

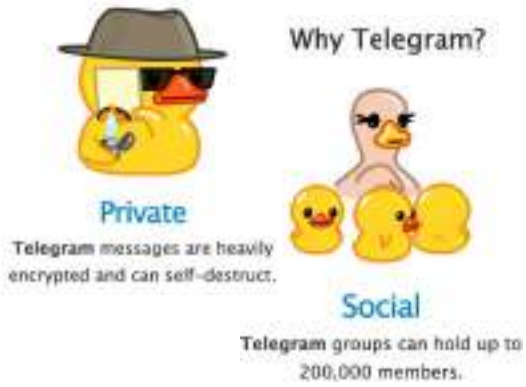


Image Credit: Telegram

81

Device Compromise and Deletion (ABJM 2021) — Compromiso y eliminación del dispositivo

Semi-Structured Interviews with 11 Anti-ELAB Protesters (Hong Kong)
Entrevistas semiestructuradas con 11 manifestantes anti-ELAB (Hong Kong)

Full Compromise Security:
Detection and mitigation
Seguridad de compromiso total:
Detección y mitigación

Scheduled v. Remote Deletion:
Arrest compromises contacts, logs
Eliminación programada versus remota:
El arresto compromete contactos y registros

Collective Security Culture (Borradaile 2021): Group reflex to minimize information sharing, digitizing, and retaining — Cultura de seguridad colectiva: reflejo grupal para minimizar el intercambio, la digitalización y la retención de información

Image Credit: Alamy Live News (2019)

82

Cryptography from Roots to Fruits — Criptografía desde las Raíces hasta los Frutos

- Grounding Questions — Preguntas Fundamentales ✓
- The Many-Tree Metaphor — La metáfora de los muchos árboles ✓
- Threat Modeling Paradigm Shift — Cambio de paradigma en el modelado de amenazas ✓
- Cryptography & Technology for Grassroots Organizing — Criptografía y tecnología para la organización de base ✓
- Trust Infrastructure for Grassroots Organizing — Infraestructura de confianza para la organización de base ←
- Activity: What is Your Tree? — Actividad: ¿Cuál es tu árbol?
- From Roots to Fruits, Revisited — De las raíces a los frutos, revisados

83

tigro: Trust Infrastructure for Grassroots Organizing

tigro: Infraestructura de confianza para la organización de base

84

tigro: Trust Infrastructure for Grassroots Organizing

tigro: Infraestructura de confianza para la organización de base

One Size Fits One: Flexible library of primitives; applies (private) trust network information to any digital setting — Talla única: biblioteca flexible de primitivas; aplica información de la red de confianza (privada) a cualquier entorno digital

85

tigro: Trust Infrastructure for Grassroots Organizing

tigro: Infraestructura de confianza para la organización de base

One Size Fits One: Flexible library of primitives; applies (private) trust network information to any digital setting — Talla única: biblioteca flexible de primitivas; aplica información de la red de confianza (privada) a cualquier entorno digital

Trust is Human: “On-the-ground” key agreement using Bluetooth; roots digital trust in interpersonal interaction — La confianza es humana: acuerdo clave “sobre el terreno” mediante Bluetooth; Arraiga la confianza digital en la interacción interpersonal.

86

tigro: Trust Infrastructure for Grassroots Organizing

tigro: Infraestructura de confianza para la organización de base

One Size Fits One: Flexible library of primitives; applies (private) trust network information to any digital setting — Talla única: biblioteca flexible de primitivas; aplica información de la red de confianza (privada) a cualquier entorno digital

Trust is Human: "On-the-ground" key agreement using Bluetooth; roots digital trust in interpersonal interaction — La confianza es humana: acuerdo clave "sobre el terreno" mediante Bluetooth; Arraiga la confianza digital en la interacción interpersonal.

Toward Full Compromise Security: Contacts hold minimal information; anyone with shared key can delete — Hacia un compromiso total de seguridad: los contactos contienen información mínima; cualquiera con clave compartida puede eliminar

87

tigro: Trust Infrastructure for Grassroots Organizing

tigro: Infraestructura de confianza para la organización de base

One Size Fits One: Flexible library of primitives; applies (private) trust network information to any digital setting — Talla única: biblioteca flexible de primitivas; aplica información de la red de confianza (privada) a cualquier entorno digital

Trust is Human: "On-the-ground" key agreement using Bluetooth; roots digital trust in interpersonal interaction — La confianza es humana: acuerdo clave "sobre el terreno" mediante Bluetooth; Arraiga la confianza digital en la interacción interpersonal.

Toward Full Compromise Security: Contacts hold minimal information; anyone with shared key can delete — Hacia un compromiso total de seguridad: los contactos contienen información mínima; cualquiera con clave compartida puede eliminar

Grassroots Optimization: Local, co-located computation v. server computation over relatively small data sets — Optimización de base: cálculo local ubicado en el mismo lugar versus cálculo del servidor sobre conjuntos de datos relativamente pequeños

88

tigro Adversarial Model — Modelo adversario

How might we model existing threats and mitigation strategies in digital space?

¿Cómo podríamos modelar las amenazas existentes y las estrategias de mitigación en el espacio digital?

89

tigro Adversarial Model — Modelo adversario

How might we model existing threats and mitigation strategies in digital space?

¿Cómo podríamos modelar las amenazas existentes y las estrategias de mitigación en el espacio digital?

Digital Infiltration Adversary

- collects and aggregates as much information as possible
- corrupts (subpoenas) the server, corrupts (seizes) devices
- poses as a group member, spreads false information, entraps

Adversario de la infiltración digital: recopila y agrega tanta información como sea posible, corrompe (citaciones) el servidor, corrompe (incauta) dispositivos, se hace pasar por miembro de un grupo, difunde información falsa, tiende trampas

90

tigro Adversarial Model — Modelo adversario

How might we model existing threats and mitigation strategies in digital space?

¿Cómo podríamos modelar las amenazas existentes y las estrategias de mitigación en el espacio digital?

Digital Infiltration Adversary

- collects and aggregates as much information as possible
- corrupts (subpoenas) the server, corrupts (seizes) devices
- poses as a group member, spreads false information, entraps

Adversario de la infiltración digital: recopila y agrega tanta información como sea posible, corrompe (citaciones) el servidor, corrompe (incauta) dispositivos, se hace pasar por miembro de un grupo, difunde información falsa, tiende trampas

Semi-Honest Server: Privacy and Correctness

Malicious Server: Privacy but Not Correctness, Deletion

Servidor semihonesto: privacidad y corrección; Servidor malicioso: privacidad pero no corrección, eliminación

91

tigro Adversarial Model — Modelo adversario

How might we model existing threats and mitigation strategies in digital space?

¿Cómo podríamos modelar las amenazas existentes y las estrategias de mitigación en el espacio digital?

Digital Infiltration Adversary

- collects and aggregates as much information as possible
- corrupts (subpoenas) the server, corrupts (seizes) devices
- poses as a group member, spreads false information, entraps

Adversario de la infiltración digital: recopila y agrega tanta información como sea posible, corrompe (citaciones) el servidor, corrompe (incauta) dispositivos, se hace pasar por miembro de un grupo, difunde información falsa, tiende trampas

Semi-Honest Server: Privacy and Correctness

Malicious Server: Privacy but Not Correctness, Deletion

Servidor semihonesto: privacidad y corrección; Servidor malicioso: privacidad pero no corrección, eliminación

Security Strategy

Establish digital equivalents of existing security practices

Estrategia de seguridad: Establecer equivalentes digitales de las prácticas de seguridad existentes.

92

Establishing Security = Trust — Establecer Seguridad = Confianza

Human trust as a core digital security concept
La confianza humana como concepto central de seguridad digital

93

Establishing Security = Trust — Establecer Seguridad = Confianza

Human trust as a core digital security concept
La confianza humana como concepto central de seguridad digital

One Size Fits One

How organizers build and assess trust depends on:

- the person, place, or thing to be trusted (profiles, events, posts)
- the risk level associated with trust
- personal experience, collective security culture, etc.

talla única para una: La forma en que los organizadores generan y evalúan la confianza depende de la persona, lugar o cosa en la que se puede confiar (perfiles, eventos, publicaciones), el nivel de riesgo asociado con la confianza, experiencia personal, cultura de seguridad colectiva, etc.

94

Establishing Security = Trust — Establecer Seguridad = Confianza

Human trust as a core digital security concept
La confianza humana como concepto central de seguridad digital

One Size Fits One

How organizers build and assess trust depends on:

- the person, place, or thing to be trusted (profiles, events, posts)
- the risk level associated with trust
- personal experience, collective security culture, etc.

talla única para una: La forma en que los organizadores generan y evalúan la confianza depende de la persona, lugar o cosa en la que se puede confiar (perfiles, eventos, publicaciones), el nivel de riesgo asociado con la confianza, experiencia personal, cultura de seguridad colectiva, etc.

"Grounded" Cryptographic Protocols

Digital trust reduces to:

- physical interactions that establish "grounded pairs"
- qualitative trust measurements between grounded pairs

Protocolos criptográficos "conectado a tierra": La confianza digital se reduce a interacciones físicas que establecen "pares conectados a tierra," mediciones de confianza cualitativas entre pares conectados a tierra

95

tigro Core Protocols — Protocolos Principales de tigro

96

tigro Core Protocols — Protocolos Principales de tigro

Ground Trust Ceremony

Like a key signing ceremony in spirit, but:

- Establishes a symmetric key linked to a physical meeting
- No PKI: digital activity is not linkable to a persistent identifier

Ceremonia de confianza en el terreno: En espíritu parece una ceremonia de firma de llaves, pero establece una llave simétrica vinculada a una reunión física; Sin PKI: no se puede vincular la actividad digital a un identificador persistente

97

tigro Core Protocols — Protocolos Principales de tigro

Ground Trust Ceremony

Like a key signing ceremony in spirit, but:

- Establishes a symmetric key linked to a physical meeting
- No PKI: digital activity is not linkable to a persistent identifier

Ceremonia de confianza en el terreno: En espíritu parece una ceremonia de firma de llaves, pero establece una llave simétrica vinculada a una reunión física; Sin PKI: no se puede vincular la actividad digital a un identificador persistente

Grounded Annotation System

Allows grounded pairs to share digital annotations of arbitrary people, places, and things

Sistema de anotación conectado a tierra: Permite que pares conectados a tierra compartan anotaciones digitales de personas, lugares y cosas arbitrarias.

98

Ground Trust Ceremony — Ceremonia de confianza en el terreno

Alice
Alicia

Bob
Roberto

99

Ground Trust Ceremony — Ceremonia de confianza en el terreno

Alice
Alicia

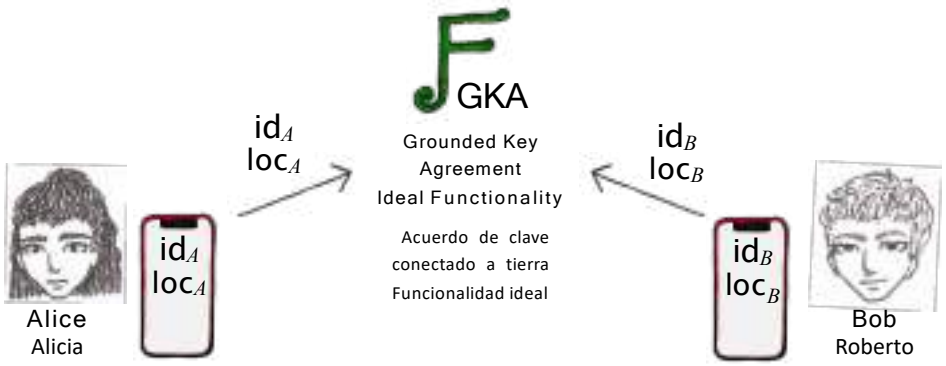
Grounded Key
Agreement
Ideal Functionality

Acuerdo de clave
conectado a tierra
Funcionalidad ideal

Bob
Roberto

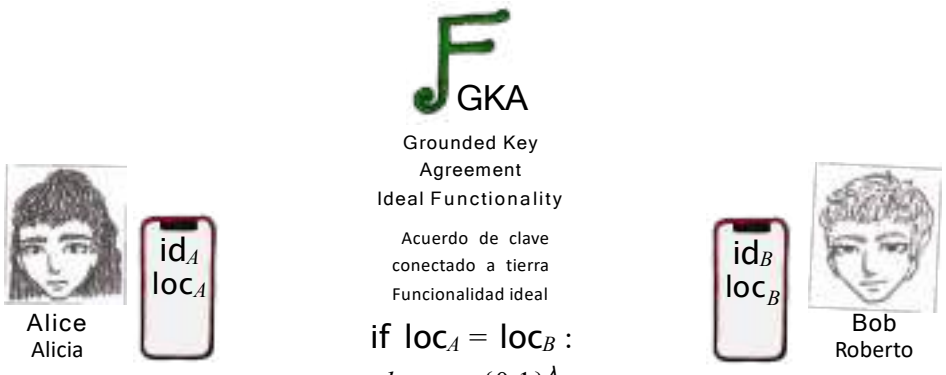
100

Ground Trust Ceremony — Ceremonia de confianza en el terreno



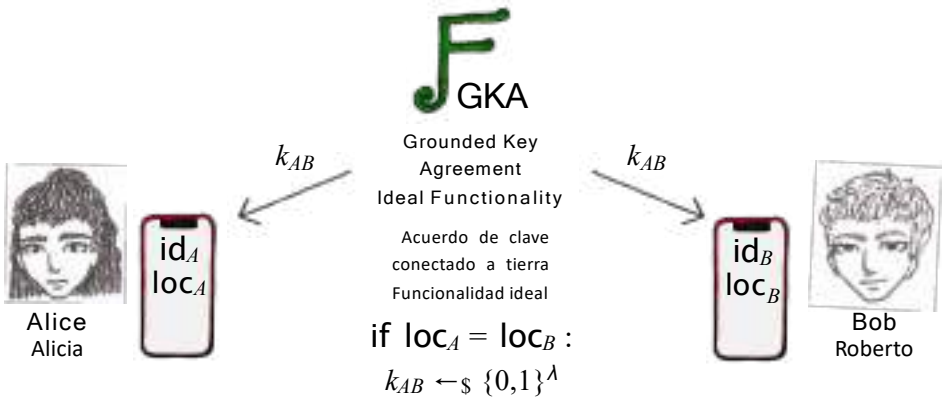
101

Ground Trust Ceremony — Ceremonia de confianza en el terreno



102

Ground Trust Ceremony — Ceremonia de confianza en el terreno



103

Ground Trust Ceremony — Ceremonia de confianza en el terreno

104

Ground Trust Ceremony — Ceremonia de confianza en el terreno

In practice, we can replace the key agreement ideal functionality with Diffie-Hellman over QR code exchange.

En la práctica, podemos reemplazar la funcionalidad ideal del acuerdo clave con Diffie-Hellman a través del intercambio de códigos QR.

Alice
Alicia

Bob
Roberto

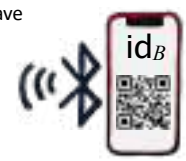
105

Ground Trust Ceremony — Ceremonia de confianza en el terreno

In practice, we can replace the key agreement ideal functionality with Diffie-Hellman over QR code exchange.

En la práctica, podemos reemplazar la funcionalidad ideal del acuerdo clave con Diffie-Hellman a través del intercambio de códigos QR.

Alice
Alicia



Bob
Roberto

Alice & Bob can run more computations over an authenticated Bluetooth channel.
Alicia y Roberto pueden ejecutar más cálculos a través de un canal Bluetooth autenticado.

106

Ground Trust Ceremony — Ceremonia de confianza en el terreno

Alice and Bob now share a key that is rooted in their physical interaction.

Alice y Bob ahora comparten una clave que tiene sus raíces en su interacción física.

Alice
Alicia

Bob
Roberto

107

Annotation System — Sistema de anotación

Alice
Alicia

Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

108

Annotation System — Sistema de anotación

Alice
Alicia

Charlie

Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

109

Annotation System — Sistema de anotación

Alice
Alicia

Annotate id_C :
I met them at a mutual aid event. They seem trustworthy.

Anotar id_C :
Los conocí en un evento de ayuda mutua. Parecen dignos de confianza.

Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

110

Annotation System — Sistema de anotación

Alice
Alicia

Annotate id_C : This person was agitating at a sit-in. Vibes were off.

Anotar id_C : Esta persona estaba haciendo agitación en una sentada. Las vibraciones estaban apagadas.

Bob
Roberto

tigro Server
Servidor tigro

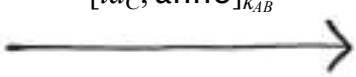
Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

111

Annotation System — Sistema de anotación

Alice
Alicia

SendMail
EnviarCorreo
$[id_C, \text{anno}]_{k_{AB}}$



Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

112

Annotation System — Sistema de anotación

Alice
Alicia

Bob
Roberto

tigro Server
Servidor tigro

$[id_C, \text{anno}]_{k_{AB}}$

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

113

Annotation System — Sistema de anotación

Alice
Alicia

Bob
Roberto

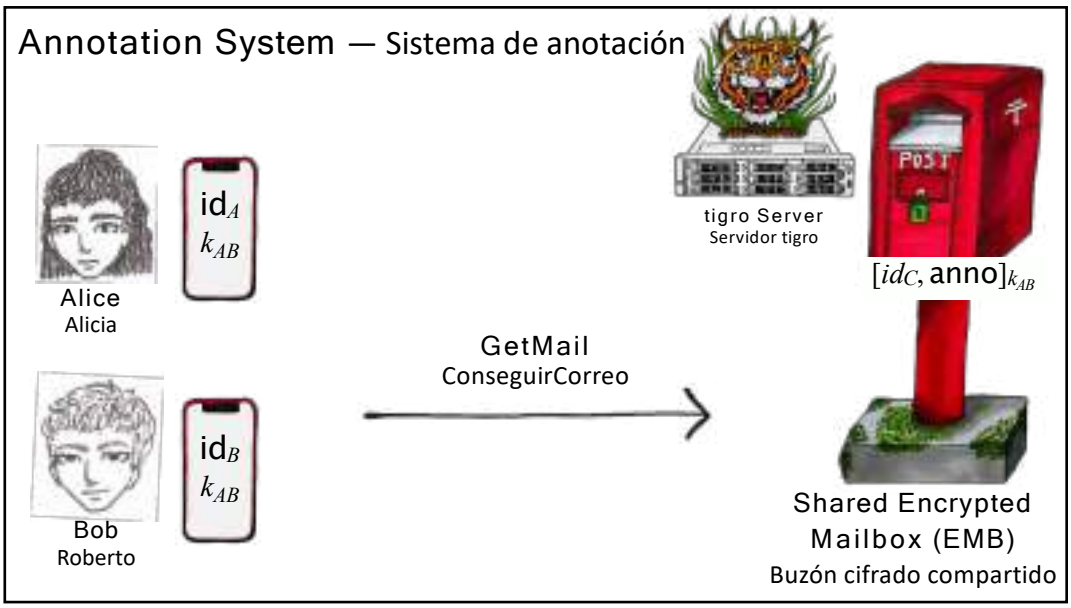
Charlie

tigro Server
Servidor tigro

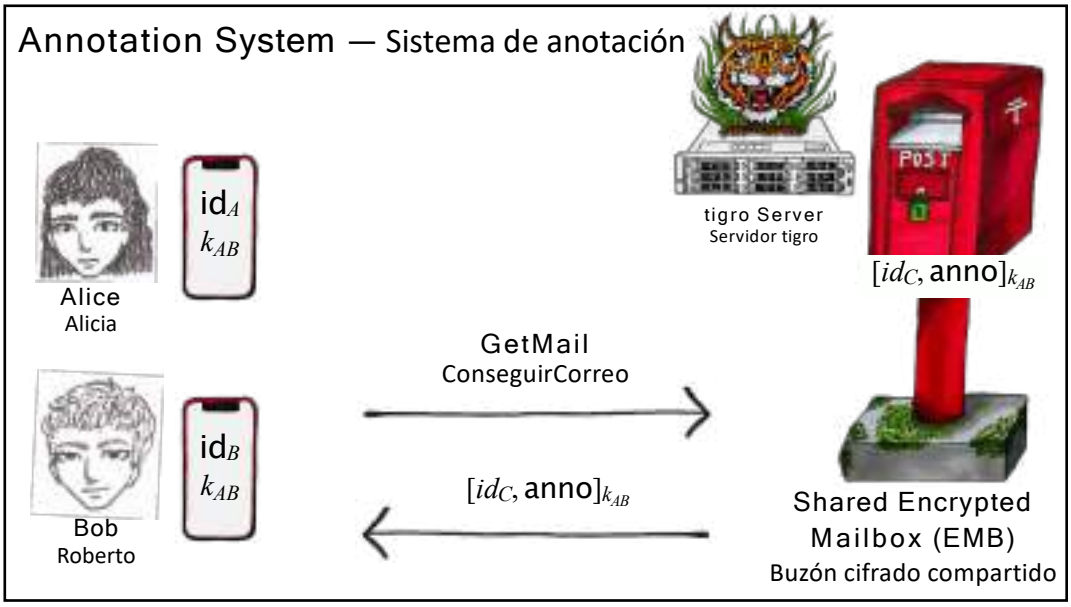
$[id_C, \text{anno}]_{k_{AB}}$

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

114


Annotation System — Sistema de anotación
Alice
Alicia
id_A
k_{AB}
Bob
Roberto
id_B
k_{AB}
tigro Server
Servidor tigro
$[id_C, \text{anno}]_{k_{AB}}$
GetMail
ConseguirCorreo
Shared Encrypted
Mailbox (EMB)
Buzón cifrado compartido

115


Annotation System — Sistema de anotación
Alice
Alicia
id_A
k_{AB}
Bob
Roberto
id_B
k_{AB}
tigro Server
Servidor tigro
$[id_C, \text{anno}]_{k_{AB}}$
GetMail
ConseguirCorreo
$[id_C, \text{anno}]_{k_{AB}}$
Shared Encrypted
Mailbox (EMB)
Buzón cifrado compartido

116

Annotation System — Sistema de anotación

Alice
Alicia

Event: Protest
Organizer: Eve
Evento: Protesta
Organizador: Eve

Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

117

Annotation System — Sistema de anotación

Alice
Alicia

Event: Protest
Organizer: Eve
Evento: Protesta
Organizador: Eve
oid_E

Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

118

Annotation System — Sistema de anotación

Alice
Alicia

Annotate oid_E: This event is being organized by friends. Hope to see you there.

Anotar oid_E: Este evento está siendo organizado por amigos. Espero verte allí.

Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

119

Annotation System — Sistema de anotación

Alice
Alicia

Annotate oid_E: No one I know can confirm the identity of Eve. Proceed with caution.

Anotar oid_E: Nadie que yo conozca puede confirmar la identidad de Eve. Proceda con precaución.

Bob
Roberto

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

120

Annotation System — Sistema de anotación

Alice
Alicia

SendMail
EnviarCorreo
$[oid_E, anno]_{k_{AB}}$

tigro Server
Servidor tigro

Bob
Roberto

Shared Encrypted
Mailbox (EMB)
Buzón cifrado compartido

121

Annotation System — Sistema de anotación

Alice
Alicia

tigro Server
Servidor tigro

$[oid_E, anno]_{k_{AB}}$

Bob
Roberto

Shared Encrypted
Mailbox (EMB)
Buzón cifrado compartido

122

Annotation System — Sistema de anotación

Alice
Alicia

Bob
Roberto

Event: Protest
Organizer: Eve
Evento: Protesta
Organizador: Eve
oid_E

tigro Server
Servidor tigro

$[oid_E, anno]_{k_{AB}}$

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

123

Annotation System — Sistema de anotación

Alice
Alicia

Bob
Roberto

Event: Protest
Organizer: Eve
Evento: Protesta
Organizador: Eve
oid_E

GetMail
ConseguirCorreo

tigro Server
Servidor tigro

$[oid_E, anno]_{k_{AB}}$

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

124

Annotation System — Sistema de anotación

Alice
Alicia

Bob
Roberto

Event: Protest
Organizer: Eve
Evento: Protesta
Organizador: Eve
oid_E

GetMail
ConseguirCorreo

$[oid_E, anno]_{k_{AB}}$

tigro Server
Servidor tigro

$[oid_E, anno]_{k_{AB}}$

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

125

Annotation System — Sistema de anotación

Alice
Alicia

Bob
Roberto

Alice and Bob can digitally & confidentially share trust assessments of any person, place, or thing.

Alicia y Roberto pueden compartir de forma digital y confidencial evaluaciones de confianza de cualquier persona, lugar o cosa.

tigro Server
Servidor tigro

Shared Encrypted Mailbox (EMB)
Buzón cifrado compartido

126

Cryptography from Roots to Fruits — Criptografía desde las Raíces hasta los Frutos

- Grounding Questions — Preguntas Fundamentales ✓
- The Many-Tree Metaphor — La metáfora de los muchos árboles ✓
- Threat Modeling Paradigm Shift — Cambio de paradigma en el modelado de amenazas ✓
- Cryptography & Technology for Grassroots Organizing — Criptografía y tecnología para la organización de base ✓
- Trust Infrastructure for Grassroots Organizing — Infraestructura de confianza para la organización de base ✓
- Activity: What is Your Tree? — Actividad: ¿Cuál es tu árbol? ←
- From Roots to Fruits, Revisited — De las raíces a los frutos, revisados

127

Think-Pair-Discuss Activity
Actividad: Pensar, Emparejar, Discutir

1. Think, Write, Draw (5 min)
   a. What does your tree look like?

Piensa, escribe, dibuja: ¿Cómo es tu árbol?

Roots: values & motivation, frames of reference, personal history
Trunk: problems of interest, solution toolbox, work environment
Fruit: (re)produced work, environment, values & motivation

Raíces: valores y motivación, marcos de referencia, historia personal
Tronco: problemas de interés, caja de herramientas de solución, ambiente de trabajo
Fruta: trabajo (re)producido, entorno, valores y motivación.

128

Think-Pair-Discuss Activity
Actividad: Pensar, Emparejar, Discutir

1. Think, Write, Draw (5 min)
   a. What does your tree look like?

   Piensa, escribe, dibuja: ¿Cómo es tu árbol?

Roots: values & motivation, frames of reference, personal history
Trunk: problems of interest, solution toolbox, work environment
Fruit: (re)produced work, environment, values & motivation

Raíces: valores y motivación, marcos de referencia, historia personal
Tronco: problemas de interés, caja de herramientas de solución, ambiente de trabajo
Fruta: trabajo (re)producido, entorno, valores y motivación.

2. Pair (10 min)
   a. Find a partner and introduce yourself.
   b. Share 1-2 aspects of your tree that you are the most excited about.
   c. Discuss: How are various parts of your tree represented in the wider cryptography community? Which aspects (if any) would you like to see take up more or less space?

   Emparejar: Encuentra un compañero y preséntate. Comparte 1 o 2 aspectos de tu árbol que más te entusiasmen. Discutir: ¿Cómo se representan las distintas partes de su árbol en la comunidad criptográfica más amplia? ¿Qué aspectos (si los hay) le gustaría que ocuparan más o menos espacio?

3. Group Discussion (10 min) — Discusión de grupo

129

Cryptography from Roots to Fruits — Criptografía desde las Raíces hasta los Frutos

- Grounding Questions — Preguntas Fundamentales ✓
- The Many-Tree Metaphor — La metáfora de los muchos árboles ✓
- Threat Modeling Paradigm Shift — Cambio de paradigma en el modelado de amenazas ✓
- Cryptography & Technology for Grassroots Organizing — Criptografía y tecnología para la organización de base ✓
- Trust Infrastructure for Grassroots Organizing — Infraestructura de confianza para la organización de base ✓
- Activity: What is Your Tree? — Actividad: ¿Cuál es tu árbol? ✓
- From Roots to Fruits, Revisited — De las raíces a los frutos, revisados ←

130

Grounding Questions — Preguntas Fundamentales

What is the "root" of cryptography? Where does it come from?

¿Cuál es la "raíz" de la criptografía? ¿De dónde viene?

Which roots and histories will we nourish moving forward?

¿Qué raíces e historias alimentaremos en el futuro?

Why do we care? What "fruit" are we trying to produce?

¿Por qué nos importa? ¿Qué "fruto" estamos tratando de producir?

How does our work reflect our histories, values, and motivations?

¿Cómo refleja nuestro trabajo nuestras historias, valores y motivaciones?

131

Community-Driven Cryptography Project

Proyecto de criptografía impulsado por la comunidad

132

Community-Driven Cryptography Project

Proyecto de criptografía impulsado por la comunidad

"We shared our work, provided feedback and support to each other, and most importantly, built a network and a community where we felt safe to rebel."

"Compartimos nuestro trabajo, nos brindamos retroalimentación y apoyo mutuo y, lo más importante, construimos una red y una comunidad donde nos sentimos seguros para rebelarnos."

- Lorgia García Peña, Community as Rebellion — La Comunidad como Rebelión

133

Community-Driven Cryptography Project

Proyecto de criptografía impulsado por la comunidad

"We shared our work, provided feedback and support to each other, and most importantly, built a network and a community where we felt safe to rebel."

"Compartimos nuestro trabajo, nos brindamos retroalimentación y apoyo mutuo y, lo más importante, construimos una red y una comunidad donde nos sentimos seguros para rebelarnos."

- Lorgia García Peña, Community as Rebellion — La Comunidad como Rebelión

- Building community is a step toward resistance, systemic change

Construir comunidad es un paso hacia la resistencia y el cambio sistémico

- "Community-Driven" in opposition to Corporate-Driven

"Impulsado por la comunidad" en oposición a impulsado por las empresas

- "Community-Driven" as making sunny spaces for trees in the margins

"Impulsado por la comunidad" como creación de espacios soleados para los árboles en los márgenes

134

Community-Driven Cryptography Project
Proyecto de criptografía impulsado por la comunidad

communitydrivencrypto.github.io
En Solidaridad: criptolatino.org

"We shared our work, provided feedback and support to each other, and most importantly, built a network and a community where we felt safe to rebel."

"Compartimos nuestro trabajo, nos brindamos retroalimentación y apoyo mutuo y, lo más importante, construimos una red y una comunidad donde nos sentimos seguros para rebelarnos."

- Lorgia García Peña, Community as Rebellion — La Comunidad como Rebelión

- Building community is a step toward resistance, systemic change

Construir comunidad es un paso hacia la resistencia y el cambio sistémico

- "Community-Driven" in opposition to Corporate-Driven

"Impulsado por la comunidad" en oposición a impulsado por las empresas

- "Community-Driven" as making sunny spaces for trees in the margins

"Impulsado por la comunidad" como creación de espacios soleados para los árboles en los márgenes

135

Thank you for listening!

¡Gracias por escuchar!

Interested in getting involved in the tigro or Community-Driven Cryptography projects? Please Email: leah_rosenbloom@brown.edu

¿Está interesado en participar en los proyectos tigro o de criptografía impulsada por la comunidad? Por favor envíe un correo electrónico: leah_rosenbloom@brown.edu

136

References — Referencias

1. Martin R Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková. Collective information security in large-scale urban protests: the case of hong kong. *arXiv preprint arXiv:2105.14869*, 2021.
2. Tetyana Bohdanova. Unexpected revolution: the role of social media in ukraine's euromaidan uprising. *European View*, 13(1):133–142, 2014.
3. Glencora Borradaile. *Defend Dissent*. Oregon State University Corvallis, 2021.
4. J.L. Hall, M.D. Aaron, A. Andersdotter, B. Jones, Feamster N., and Knodel M. *A Survey of Worldwide Censorship Techniques*. The Internet Engineering Task Force peang Workgroup draft-irtf-pearg-censorship-09, 2023.
5. Philip N Howard, Aiden Duffy, Deen Freelon, Muzammil M Hussain, Will Mari, and Marwa Maziad. Opening closed regimes: what was the role of social media during the arab spring? *Available at SSRN 2595096*, 2011.
6. Seny Kamara. *COINTELPRO*. Algorithms for the People, 2020.
7. Seny Kamara. *Crypto for the People Invited Talk*. The International Association for Cryptologic Research, 2020.
8. Tetyana Lokot. Be safe or be seen? how russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society*, 16(3):332–346, 2018.
9. N. ten Oever, S. Couture, and Knodel M. *Internet Protocols and the Human Rights to Freedom of Association and Assembly*. The Internet Engineering Task Force Human Rights Protocols Considerations Research Group draft-irtf-hrpc-association-12, 2022.
10. Lorgia García Peña. *Community as rebellion: A syllabus for surviving academia as a woman of color*. Haymarket Books, 2022.
11. Phillip Rogaway. The moral character of cryptographic work. *Cryptology ePrint Archive*, 2015.
12. Leah Namisa Rosenbloom. Toward secure social networks for activists. In *Moving technology ethics at the forefront of society, organisations and governments*, pages 491–502. ETHICOMP, 2021.
13. Leah Namisa Rosenbloom. Activists want better, safer technology. *arXiv preprint arXiv:2209.01273*, 2022.