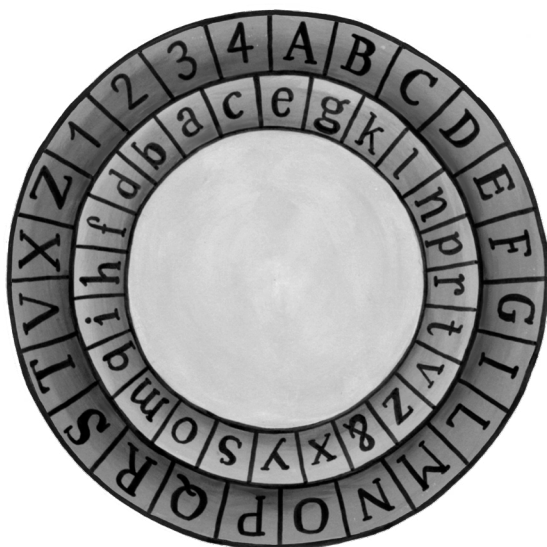


CRIPTORIA

de Turing a Nakamoto



ALFRE MANCERA

PROMETEA

CRIPTORIA: de Turing a Nakamoto

© Alfre Mancera, 2024

ISBN tapa dura: 978-9916-4-2571-8

ISBN tapa blanda: 978-9916-4-2572-5

Portada: © Cytherpunknow / cytherpunknow.com / info@cytherpunknow.com

Ilustraciones: Bianca Rizzalli / @biancabtcart

Corrección: Mercedes Leaden / mleaden@gmail.com

Colaboradores: DrJonesKlaus, Ieray, Cruda

Editado por PROMETEA / prometeabtc.com

Criptoria: de Turing a Nakamoto, por Alfre Mancera está licenciado bajo CC BY-NC-ND 4.0. Para ver una copia de esta licencia, visite: <https://creativecommons.org/licenses/by-nc-nd/4.0/>

*A mi abuela Mami,
con quien tanto quería.*

ÍNDICE

Prefacio	13
ALIZE.....	19
1. EL PRINCIPIO DEL FIN.....	23
Los niños que amaban los puzles.....	23
Alan Turing.....	23
Irving John Good	24
Los hombres que amaban sus genes.....	26
La quimera de Galton	26
Mutación de la eugenesia	32
El poder de la ciencia ficción.....	34
Hugo Gernsback.....	35
Amazing Stories	35
El descenso de Saint Jude.....	37
Elige tu propia aventura.....	39
2. EN BUSCA DE LA VERDAD	41
Cómo conocemos	42
Organon	46
Efecto mosaico de la ciencia.....	47
3. LOS NÚMEROS OS HARÁN LIBRES.....	49
Matemática soberana	51
El lenguaje formal	53
Teoría de conjuntos.....	54
Aritmética modular	56
Congruencia	58

Gauss.....	59
Gauss, Fermat y Euler.....	60
Álgebra de Boole	62
Tablas de verdad	64
Axiomatizar o morir	65
Problemas sin resolver	67
Principia Mathematica	69
Bolonia 1928.....	71
La revelación de Gödel.....	73
La máquina de Turing.....	75
Números computables.....	77
Máquina de computación	78
Conclusiones 1936.....	80
4. LA MATEMÁTICA DEL SECRETO.....	85
Breve historia de las cifras	86
Herramienta de guerra.....	92
Unidos por las señales.....	93
La fábrica de persuasión	94
Bletchley Park.....	98
Ratio Club.....	102
Inteligencias metálicas	104
Eterno Alan.....	106
5. LA INFORMÁTICA MODERNA.....	113
Bell Labs.....	114
Claude Shannon.....	115
Qué bueno que viniste.....	117
Teoría de la información	118
La época UNIX	122
Nuevos lenguajes.....	122
Nuevo reloj.....	124
El primer microprocesador	124

Horst Feistel.....	126
Lucifer.....	127
DES.....	128
ARPANET.....	130
Primeras compañías.....	132
Complejidad computacional.....	134
6. EL AMANECER DE LA CRIPTOGRAFÍA FUERTE.....	137
Criptografía prohibida.....	137
Una ley para prohibirlos a todos.....	138
Criptografía de clave pública.....	139
Diffie-Hellman-Merkle.....	142
Martin Hellman.....	142
Whitfield Diffie.....	146
Whit conoce a Martin.....	150
Diffie investiga con Hellman.....	151
Técnicas criptográficas multiusuario.....	153
Ralph Merkle.....	156
Merkle 1974.....	156
Puzles de Merkle.....	158
Ralph conoce a Whit y Martin.....	159
Nuevas direcciones en criptografía.....	160
El equipo RSA.....	162
Ron, Adi y Len.....	163
El sistema RSA.....	165
Centros de distribución de claves (KDC).....	167
Redes distribuidas.....	168
Árbol de Merkle.....	169
7. HACIENDO LEGIÓN.....	173
Universo Internet.....	173
USENET.....	175
CPSR.....	178

David Chaum	179
Crypto Conferences	182
CRYPTO '82	183
Prueba de conocimiento cero	183
Software libre	186
GNU Project	186
Free Software Foundation	187
8. CAMINO A LIBERTARIA	189
Firmas digitales	189
Taher Elgamal	190
Claus Schnorr	192
Curvas elípticas	193
David contra Gran Hermano	195
Criptoanarquía	196
Extropianos	198
9. SOLDADOS DE LA PRIVACIDAD	203
EFF	203
John Perry Barlow	204
John Gilmore	206
Mitch Kapor	207
Frontera electrónica	209
Independencia del ciberespacio	211
EPIC	212
PGP	213
Phil Zimmermann	213
Hal Finney	215
Bailando con lobos	216
OpenPGP	217
Cypherpunks	218
Cyphernomicon	220
Manifiesto Cypherpunk	221
Clipper Chip	222

10. DINERO DIGITAL	225
Tatsuaki Okamoto.....	226
Proof of Dwork	227
Digicash.....	230
Hal 1993	233
Magic Money Digicash	235
Smart contracts	236
La ceca de palacio	238
Hashcash	238
B-money.....	239
Bit gold	240
RPOW	241
11. LA ERA SATOSHI.....	243
Satoshi Nakamoto	244
Whitepaper	244
Binarios	246
Primera TX.....	247
Bitcoin	247
Referencias	251
Mecenazgo.....	265