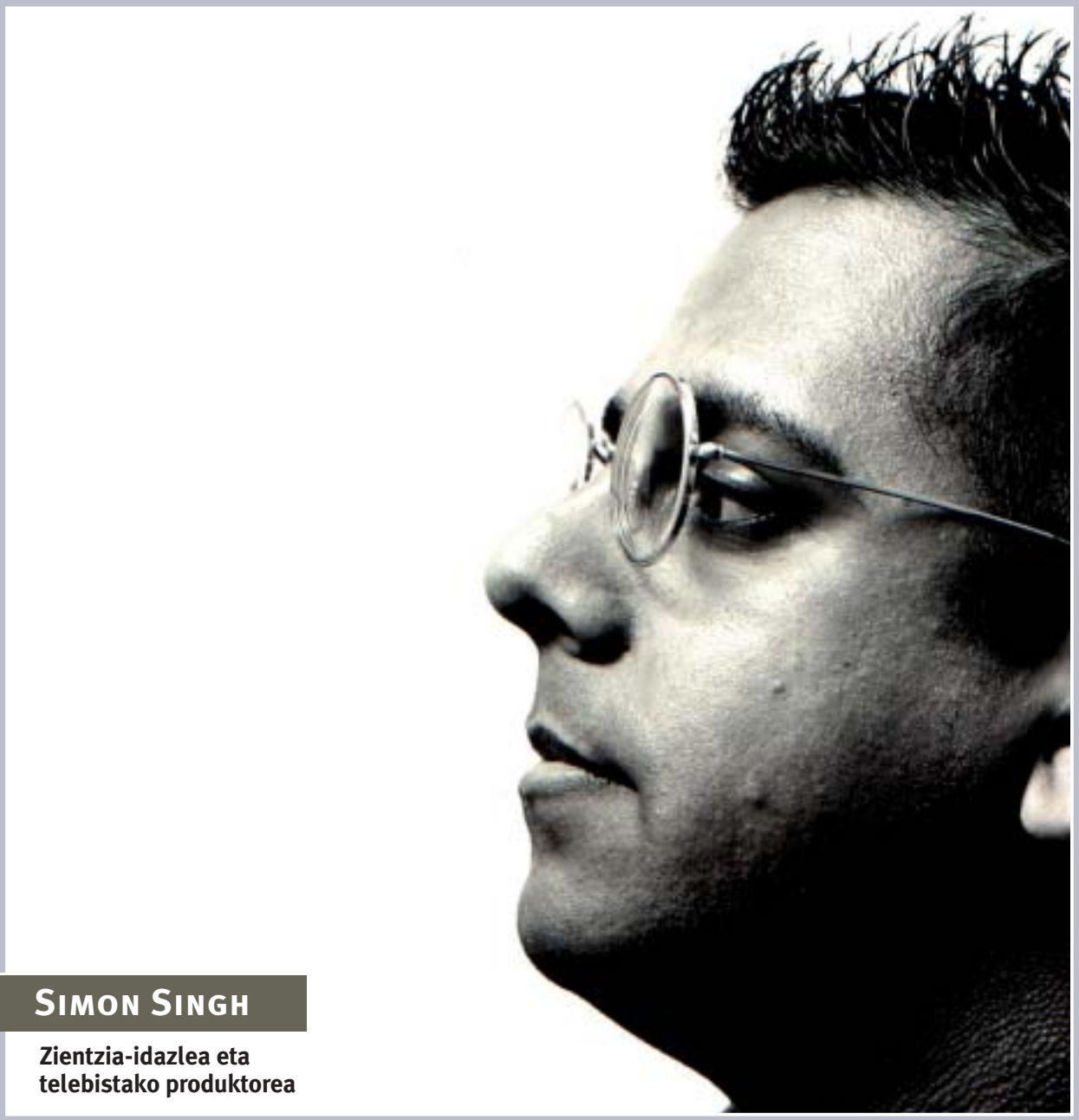


Simon Singh

Zientzia-idazlea eta telebistako produktorea

ARG.: NIGEL SPALDING ©

“Enkriptazioa gure inguruko gauza guztietan dago”

Guillermo Roa Zubia
Elhuyar Zientziaren Komunikazioa

Eskoziako Maria I.aren exekuziotik enkriptatze kuantikorainoko bidea egiten du Simon Singhek *Kodeen liburua* liburuan: Bigarren Mundu Gerrako mezu alemaniarrak nola deskodetu zituzten ingelesek, zer hizkuntza galdu "deskodetu" ahal izan diren edo nola tematu ziren Diffie eta Hellman Interneteko mezu zibilak ezkutatzeko kode bat sortzen. *Kodeen liburua*k mota guztietako kontakizunak ditu. Orain, euskarazko bertsioa argitaratu du Elhuyar Fundazioak.

Simon Singh idazleak —kultura zientifikoaren aldeko borrokaren ikono bat— liburua aurkeztu zuen *Norteko Ferrokarrilla* irratsaioan, eta *Sendabide ala iruzurbide* liburuarengatik izan dituen arazoez ere hitz egin zuen.

Kodeen liburua
Simon Singh
Elhuyar Fundazioa
225 x 132 mm
ISBN: 978-84-92457-78-6
Jatorrizko izenburua:
The Code Book

Zer aurkituko du irakurleak *Kodeen liburua*n?
Uste dut hauxe dela ideia nagusia: elkarrekin komunikatzen hasi ginenetik, bai idatziz, edo telegrafoaren bidez, edo agian eskutitzak bidalita, informazio garrantzitsua bidali edo agirietan gorde nahi izan dugu. Informazio sentikorra izan daiteke, erromantikoa izan daiteke, osasunarekin zerikusia izan dezake, asmakuntza berri batekin zerikusia izan dezake, plan militar bat izan daiteke... Informazio sekretua dugunean, hura babesteko modua informazioa kodetzea da. Duela urte asko hasi zen kontu hau. Liburuaren gaia kode ezberdinen asmakuntza da: jendea kode horiek hausten saiatu zen; orduan, kode hobeak asmatzen saiatu ziren; gero, kode horiek ere hautsi zituzten eta abar. Gaur egun arte. Eta gaur egun gai horrek inoiz baino garrantzi handiagoa du.

Ez dakit jendea jabetuta dagoen mezu elektroniko bat bidaltze hutsak kodetze-prozesu bat eskatzen duela.
Mezu elektroniko bat bidaltzen dugunean, bi gauza daude. Alde batetik, mezua itzuli egiten da kode bitar batera edo ordenagailuaren lengoaia batera, ordenagailua bera gai izan dadin mezua maneiatzeko. Kodetzemodu horrek erraztu egiten dio komunikazioa teknologiarentzat. Beste alde batetik, gehien interesatzen zaidan kodifikazioa da jendeari mezua irakurtzea zailtzen diona. Adibidez, elkarri mezuak bidaltzen dizkiogu, eta ez dugu ezer ezkutatu nahi, eta ez dugu sekreturik. Baina nire kreditu-txartelaren informazioa bidaltzen badiot Interneteko liburu-denda bati, nik nahi dut kreditu-txartelaren xehetasunak sekretupean gordetzea. Ez dut nahi inork datuak lapurtzea. Beraz,

Simon Singh

Somerset konderrian jaio zen, Ingalaterran, 1964an. Zientzia-dibulgazioa idazteaz gain, telebistako produktorea da BBCn. Haren liburuek ospe handia hartu dute, eta hizkuntza askotara itzuli dituzte. Azken urteetan, ospe handia izan du BCA Britainia Handiko kiropraktikoen elkarteak salatu egin zuelako. Singhek irabazi zuen auzia.

enkriptatu egin behar dira kreditu-txartelaren xehetasunak, nire banku-kontua babesteko. Esan nahi dut enkriptazioa gure inguruko gauza guztietan dagoela: finantza-transakzioetan, Interneten, salerosketa elektronikoetan; ikusten ditugun telebista-programak, batzuetan, sateliteek enkriptatzen dituzte, eta deskodetu behar izaten ditugu; gure osasunaren analisien datuak enkriptatzen dituzte pribatutasuna babesteko.

Denbora da *Kodeen liburua* Ingalaterran argitaratu zenuenetik. Ez dakit jarraitu dituzun enkriptatzearen zientziaren albisteak. Ez da oso azkar aldatzen den zientziaren adar bat.
Nire ustez, seguru asko oso azkar ari da aldatzen, oso teknologikoa delako, eta teknologia oso azkar ari da aldatzen. Internet hasi zenean, gehienbat mezuak, dokumentuak eta horrelakoak bidaltzen genituen, eta horiek nahiko erraz kodetzen dira. Baina orain bideoak bidaltzen ditugu eta bideoek askoz datu gehiago dute, enkriptatze azkarragoa behar dute, kopuru handiagoetan, eta beraz erronka berriak sortzen dira. Liburua 1999an argitaratu zen, eta geroztik, irailaren 11koa gertatu da, eta terrorismoaren beldurra zabaldu da. Gaur egungo kodeak inoiz baino ahaltsuagoak dira, eta, beraz, nola hautsiko dituzte segurtasun-zerbitzuek haien kodeak? Nola lortuko dute gizartea ahuldu nahi duten pertsonei buruzko informazioa? Neurri batean kontu teknologikoa da, neurri batean kontu matematikoa, baina bada baita neurri batean kontu politiko bat ere. Estatu Batuetan urtetan izan dute enkriptazioa arautu behar ote den eztabaida. Praktikan ideia horrek ez du funtzionatzen, enkriptatzea denontzat dagoelako eskuragarri.

Deigarria da zure webgunean propio eskatzen duzula ez bidaltzeko zuri mezu kodetuak, zu ez zarela deskodetzaile bat. Askotan bidaltzen dizkizute?
Zientzia-idazle bat naiz, zientzia-kazetari bat naiz, eta gai askori buruz idazten dut. Matematikari buruz idatzi dut, kosmologiari buruz, osasunari buruz, eta kriptografiari buruz ere idatzi dut. Askotan jendeak uste du gai bati buruz idazten dudanez, gai horretako aditu bat naizela. Gustuko dudan gauza bati buruz idazten dudanean, noski, badakit zerbait gaiari buruz, baina nire jakinduria adituekin egindako solasaldietatik dator. Asko ikasten dut haiengandik, baina ez nuke hartuko neure burua kriptografiako aditutzat. Ez nioke aholkurik emango inori bere informazioa seguru gordetzeko moduari buruz. Baina bai, hori da norbaitek erraz egin dezakeen akats bat.

> *"Gai bati buruz idazten dudanez, gai horretako aditu bat naizela uste du askotan jendeak"*

Elhuyar Fundazioak zure beste liburu baten euskarazko bertsioa argitaratu zuen: *Sendabide ala iruzurbide*. Ezard Ernst medikuarekin batera idatzi zenuen. Liburu horretan, medikuntza alternatiboaren hainbat terapia aztertu eta puntu batzuetan kritikatzen zenuten. Eta liburu horrekin zerikusia duen zutabe batengatik salatu zintuen BCA Ingalaterrako Kiropraktikaren Erakundeak difamazioagatik. Auzi hura irabazi zenuen, baina arrakasta auziarena baino zerbait zabalagoa izan zen.
Bai. Liburua medikuntza alternatiboari buruzkoa da. Eta jende askok uste du gu medikuntza alternatiboaren kontra gaudela, oso kritikoak garelako. Baina ez dut uste medikuntza alternatiboaren kontrakoak garenik. Aldiz, ebidentziaren aldekoak gara. Beraz, argi dagoenean zer-

Lau liburu, lau gai handi

Singhek garrantzi handiko gaiak aukeratu ditu liburuak idazteko. Lehendabizikoa, 1997an argitaratua, Fermaten azken teoremaren frogari buruzkoa da: *Fermat's Last Theorem*, matematika modernoan oihartzun handiena izan duena lana. Bigarrena *Kodeen liburua* da (*The Code Book*, 1999), Elhuyar Fundazioak argitaratu berri duena. 2005 urtean argitaratu zuen hirugarrena: *Big Bang*, kosmologiaren teoria handienari buruzkoa. Eta, 2008an, *Trick or Treatment* argitaratu zuen Ezard Ernst medikuarekin batera, medikuntza alternatiboen azterketa bat zientziaren ikuspuntutik. Azken hori ere Elhuyar Fundazioak argitaratu du euskaraz: *Sendabide ala iruzurbide*.

baitek funtzionatzen duela, guk esaten dugu: “Hau ondo dago”. Ebidentzia hori ez dagoenean, guk esaten dugu “kontuz ibili”. Medikuntza alternatiboek duten arazoa da gehienetan ez dutela aldeko ebidentziarik. Izan ere, gainera, kasu batzuetan arriskutsuak dira.

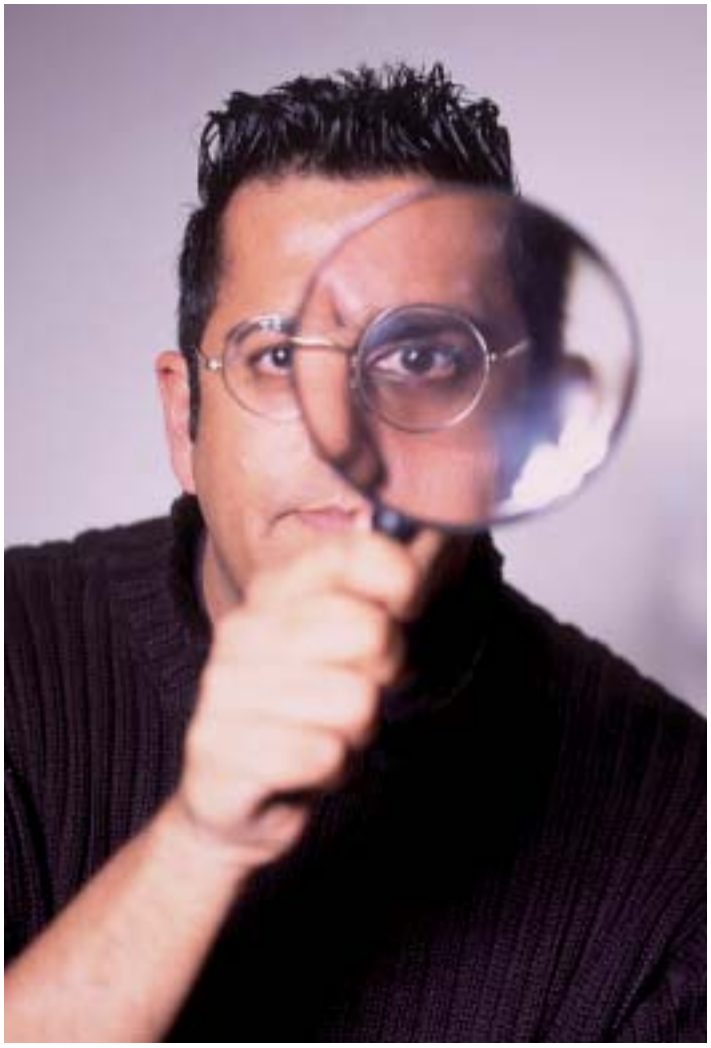
Bestalde, esan duzun bezala, liburua argitaratu ondoren difamazioagatik salatu ninduten; kiropratikoei buruz idatzi nuen artikulu batengatik izan zen. Kasuak bi urte iraun zuen. Oso zaila izan zen, baina azkenean irabazi egin nuen. Nire artikulua defendatu nuen. Kiropraktikari egiten nion kritika defendatu nuen. Eta hori garrantzitsua da, zientziak aurrera egiteko modua kritikatzea delako. Norbaitek ideia bat plazaratzen du; ez banago ados, kontrako ebidentzia baldin badut edo beste ikuspuntu bat baldin badut, aukera izan behar dut hori argudiatzeko. Bestela, zientziak, medikuntzak eta teknologiak ezin dute aurrera egin. Eta zoritxarrez Ingalaterran difamazioaren kontrako lege oso zorrotzak ditugu.

> *“Norbaitek ideia bat plazaratzen du; kontrako ebidentzia baldin badut, aukera izan behar dut hori argudiatzeko”*

Kritikatzen duen pertsonaren oso kontrako legeak dira, eta oso aldeko jarrera izaten dute defendatzen denarekin. Nik zorte handia izan nuen. Erraz gal nezakeen auzia, difamazio legeak ez baitira oso bidezkoak. Baina albiste oso ona da orain badagoela difamazioaren legeak aldatzearen aldeko kanpaina bat. Badugu lege-proiektu bat Parlamentuan. Hilabete honetan iritsi da Lorden Ganberaren bitartez. Eta horregatik espero dugu laster, urte honen bukaera baino lehen akaso, difamazioaren lege berria izatea; jendearen kritika onartzen duen lege bat, bidegabeko kritika bat izan gabe, zentzuzkoa izanda, baina aukera ematen duena kritikatzeko eztabaidek aurrera egin dezaten. Izan ere, lege-proiektuak bereziki zaintzen ditu argitalpen akademikoak. Aldizkari akademiko batean —*journal* batean— argitaratzen baduzu, babes berezi bat izango duzu. Babes gehigarria. Hori da nahi dugulako legeak onartzea eztabaida akademikoa oso gauza preziatua dela.

Ez al duzu uste liburuak arrakasta duela jadanik konbentzituta dagoen jendearen artean?

Nire ustez, hiru pertsona-mota daude. Badira inoiz konbentzituko ez ditugunak; adibidez, terapiak aplikatzen dituztenak. Ez ditugu konbentzituko haien bizitza osoa, haien karrerak eta haien sinesmenak sartuta daudelako terapia alternatiboen munduan. Bestalde, badago askoz ere ikuspuntu zientifikoagoa duen jendea, adibidez ni, adibidez mediku profesionalak.



ARG.: SIMONSINGH.NET

Baina bi talde horien artean, bada erantzunak besterik bilatzen ez duen pertsona-talde bat. Ez zaie inporta erantzuna alternatiboa edo konbentzionala den: erantzunak bilatzen dituzte, besterik ez. Eta nire ustez, liburua pertsona horiei zuzenduta dago. Alegia, zuzenduta dago ikuspegi ideologikoa ez dutenei. Haien osasunerako eta senideen osasunerako onena nahi dute. Nire ustez, gure liburua erdian dagoen pertsona-talde horri zuzenduta dago. Gutako inork ez ditu erantzun guztiak. Baina jendeak informazioa nahi du, eta espero dut gure liburuak eskuratuko diola jendeari informazio hori. ●