Zenbakien deskonposaketa, zenbait koderen aurkako gakoa

Elisabete Alberdi Celaya
Matematikaria
Lea Artibai Ikastetxea

Erakunde batek RSA sistema erabiltzen duenean mezuak kodifikatzeko, zenbaki arrunt bat erabiltzen du oinarrian, bi zenbaki lehenen biderkadura dena. Zenbaki hori publikoa izaten da, baina hain da zenbaki handia, non ia ezinezkoa baita hura deskonposatzea. Zenbaki horren deskonposaketak erakunde horretara iristen diren mezu kodetu guztiak deszifratzen lagunduko liguke. Zenbakiak deskonposatzeko algoritmo eraginkor bat asmatzeak hankaz gora jarriko luke zifratzeko eta deszifratzeko teknika hori, RSA delakoa. Hau da, gure datuak ingurune seguruetan jarri ahal izateko, beste tresna bat bilatu beharko genuke.

Inoiz web-orrialde "seguru" batean sartu bazara —hegazkin-bidaia bat Internet bidez erosi duzulako, kontu korronteko azken eragiketak ikustera sartu zarelako eta abar—, komunikazioa plataforma seguru baten bidez egin da, SSL deitzen dena eta https (secure) protokolo baten barnean dagoena. Horrelakoetan ohartuko zinen nabigatzaileko ataza-barran giltzarrapo bat agertzen dela. Orri horretara sartzeko klabea edo gakoa behar dela adierazten du, gakoa ez duen inor ezin dela sartu. Hau da, mezua deskodetuko duen bakarra jasotzailea den neurrian da segurua komunikazioa. Hortaz, Iberian bidaia-txartel bat erostean, Iberiak zure VISA-zenbakia zifratzen edo kodetzen du. Mezu zifratuak sarean zehar bidaiatzen du, eta, Iberiara iristean, mezu zifratua deszifratzen edo deskodetzen dute. Komunikazioa segurua da, mezua deszifratzen dakien bakarra jasotzailea den neurrian.

ARG.: FOTOLIA ©

Kriptografia deritzo mezu bat babesteko zenbait metodo erabiltzen dituen teknikari. Hasiera batean matematikaren alorrean kokatzen bazen ere, gaur egun informatika eta telematikara ere zabalduta dago. Kriptografia-tekniken erabilera aspalditik dator, ordea. Lehenengo zibilizazioetakoek kanpaina militarretan mezuak bidaltzeko teknikak garatu zituzten. Mezularia etsaiaren eskuetan jausi arren, etsaia mezuaren jabe ez egitea lortzen zuten, mezua kriptografia-teknikak erabiliz zifratua bidaltzen baitzuten. Mezua jaso behar zuenak hura jasotzean, alderantzizko eragiketa eginez mezu kodetua deszifratzen zuen. Kristo aurreko V. mendean, eszital izeneko tresna erabiltzen zen mezuak zifratzeko. Makila batean larruzko xingola bat kiribildu, eta bertan mezua idazten zen. Xingola makilatik kendutakoan, mezuko hizkiak nahasirik agertzen ziren, eta eszitalaren diametro bereko makila zuenak baino ezin zuen mezua deszifratu. Garai haietan, makila horiek ziren herrien indarra, eta ordutik dator gaur egun herrietako alkateei ematen zaien makila.

ZIFRATZEKO METODO KLASIKOAK

Mezuak zifratzeko metodoak bi multzo handitan banatzen dira: klasikoak eta modernoak. Metodo klasikoetako batzuk ordezkapenean oinarritzen dira. Metodo horiek mezuko hizki bakoitza beste hizki edo zenbaki batez ordezten dute. Horrelako metodoen adibide bat K.a. I. mendean Julio Zesarrek erabiltzen zuen zifratzailea da, zeinetan hizki bakoitza alfabetoan bera baino hiru espazio eskuinerago dagoen hizkiaz ordezten baitzen. Hala, A hizkia D-z ordezten zen, B hizkia E-z, eta abar. Zesarren teknika erabiliz kodetutako mezu bat jasotzen zuenak, hizki bakoitza alfabetoan 3 espazio ezkerrerago zegoenaz ordeztuz, hasierako mezua lortzen zuen. Metodo hori ez zen batere segurua.

Zesarren zifratzailea hizki bakoitza hura baino b espazio eskuinerago dagoen hizkiaz ordeztuta orokortu daiteke. Hogeita zazpi hizkiko alfabeto batean, hizki bat beste batez ordezteko 26 era daude. Hogeita sei erak probatuz gero, mezua lortzen da. Beraz, metodo orokortu hori ere oso ahula da. Gainera, metodo hori erabiltzen denean hizki bat ordezteko dauden era guztiekin proba egitea ez da mezu kodetua argitzeko dagoen era bakarra. Mezua idatzita dagoen hizkuntza eta hizkuntza horretan hizkiek duten maiztasuna ezagututa ere argitu daiteke mezu kodetua. Horretarako, aski da mezu kodetuan gehien agertzen den hizkia hizkuntza horretan maiztasun handiena duen hizkiaz ordeztea; bestetik, bi hizki horien arteko distantzia da metodoko b aldagaia, hau da, hizki bakoitza zenbat posizio mugitu behar dugun esango diguna. Behin b-ren balioa ezagutuz gero, mezu zifratuko hizki bakoitza b espazio ezkerrera mugituz, mezu osoa lortuko dugu. Bistan da metodo hori ez dela segurua.

Zifratu sofistikatuago bat zifratu afina da; $K_i = a \cdot M_i + b$ (mod27) eragiketa eginda, mezuko M_i hizki bakoitza kodetzea lortzen da. Emaitza hori lortzeko, hizki bakoitzari zenbaki bat egokitzen zaio, eta hizkiari dagokion zenbakia formula horren bidez ordezten da. Ondoren, $a \cdot M_i + b$ balioa 27 zenbakiaz zatitzen da, eta lortzen den hondarra da K_i-ren balioa. Bukatzeko, zenbaki horri dagokion hizkia jartzen da. Adibidez, H hizkiari 7 zenbakia dagokio, eta $a = 5$, $b = 7$ diren kasuan, $K_i = 5 \cdot 7 + 7 = 42 = 15$ (mod27) ematen du. 15 zenbakiari O hizkia dagokio. Horrek esan nahi du ezen, zifratu hori erabiliz, H hizkia O bihurtzen dela. Nahiz eta metodo horrek aurrekoak baino konplexuagoa dirudien, mezu kodetua luzea denean, hizkuntza bateko hizkien maiztasunak erabilita, erraz hautematen da mezua zein den.

ZIFRATZEKO METODO MODERNOAK

Zifratzeko metodo modernoek klabe pribatua edo klabe publikoa erabil dezakete. Klabe pribatua darabiltenak blokekoak edo fluxuzkoak izan daitezke. Blokeko zifratzaileek algoritmoa behin baino gehiagotan aplikatzen dute informazioaren karaktere-multzo batean, klabe bera erabiliz. Blokeko zifratzaileen adibide dira, DES (Data Encryption Standard) eta AES (Advanced Encryption Standard). Bi metodo horietan, algoritmoa ezaguna da, eta klabea, ezezaguna (pribatua). Fluxuzkoetan, karaktere bakoitza ausazko klabe luze bat erabiliz zifratzen da, eta horietan ere klabea da ezezaguna.

Baina modernotasunak ere ez ditu libratu metodo horiek segurtasun ezaren hatzaparretatik. DES zifratzailearen desabantaila nagusia klabearen neurri txikia da (56 bitekoa). Horrek esan nahi du $2^{56} = 72.057.594.037.927.936$ aukera daudela klabea aukeratzeko, eta ordenagailuen munduan zenbaki hori txiki geratzen da. Horren adibide da 1998ko urtarrilean antolatu zen DES *challenge* batean 56 ordutan klabea apurtzea lortu izana, segundoko 90.000 klabe ebaluatzen zituzten ordenagailuak erabili baitziren. Klabe luzeagoa duelako, 112 bit-ekoa, gaur egun gehiago erabiltzen da DES hirukoitza, 2^{112} aukera eskaintzen baititu klabearentzat. AES metodoaren klabea ere luzeagoa da: 128, 129 eta 256 bit-ekoa. Fluxuzkoen desabantaila, berriz, beste era batekoa da: karaktereak banaka zifratzearen ondorioz, mezu kodetuko karaktereen arteko lotura ahula izaten da.

Klabe publikoa erabiltzen duten metodoen artean ezaguna da RSA izenekoa (Rivest, Shamir, Adleman). Orain arte segurua den metodoa da, baina nola lor liteke ziurtasuna guztiontzat ezaguna den klabe bat erabiliz? Deszifratzeko eragiketa zaila izatean dago gakoa.

Eszital baten irudia.
ITURRIA: HTTP://ES.WIKIPEDIA.ORG/WIKI

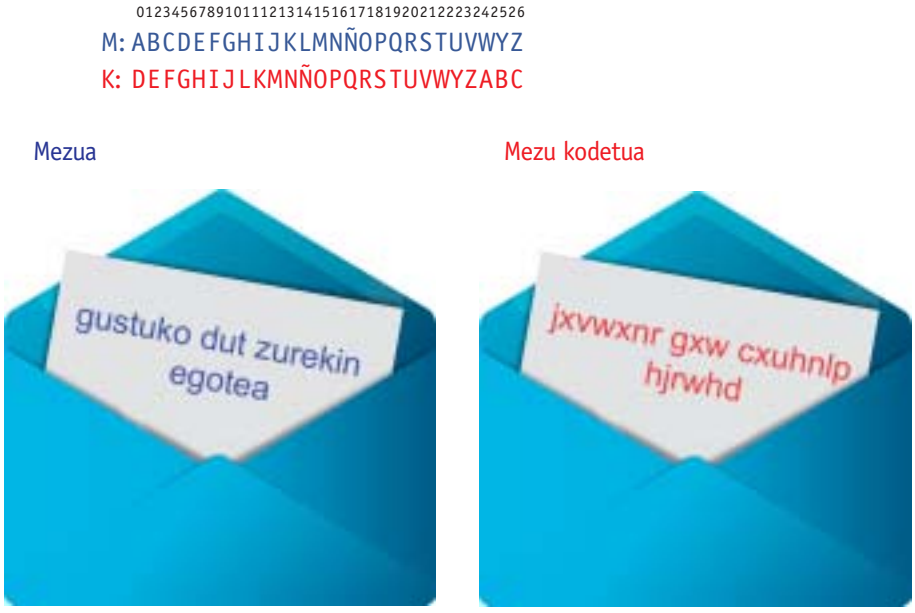
ZENBAKIEN DESKONPOSAKETA

Gizakiok oso umetatik hasten gara zenbakiak deskonposatzen. Lehenengo ikasten dugun kontzeptuetako bat da zenbaki lehenarena: a zenbakia lehena da, baldin eta bakarrik $\pm a$ eta ± 1 zenbakiez zatitu badaiteke. Hortaz, 2, 3, 5, 7… zenbakiak lehenak dira. Zenbaki bat deskonposatu nahi dugunean, hura baino txikiagoak diren zenbaki lehenez zatitzen hasten gara. Adibidez, 15 zenbakia, 3 eta 5 zenbaki lehenen biderkadura moduan deskonposatzen da. Zenbaki bat hura baino txikiagoak diren zenbaki lehenek zatitzen ez dutenean, lehena dela esaten da. Horrenbestez, aurretik eman dugun zenbaki lehenen zerrendari beste zenbaki lehen hauen zerrenda erantsiz goaz: 11, 13, 17, 19, 23,…,131, 137,… Edota aurreko guztiak baino askoz handiagoak diren beste hauek: $2^{44497}-1$, $2^{13466917}-1$,... Bai, ez dago ho-

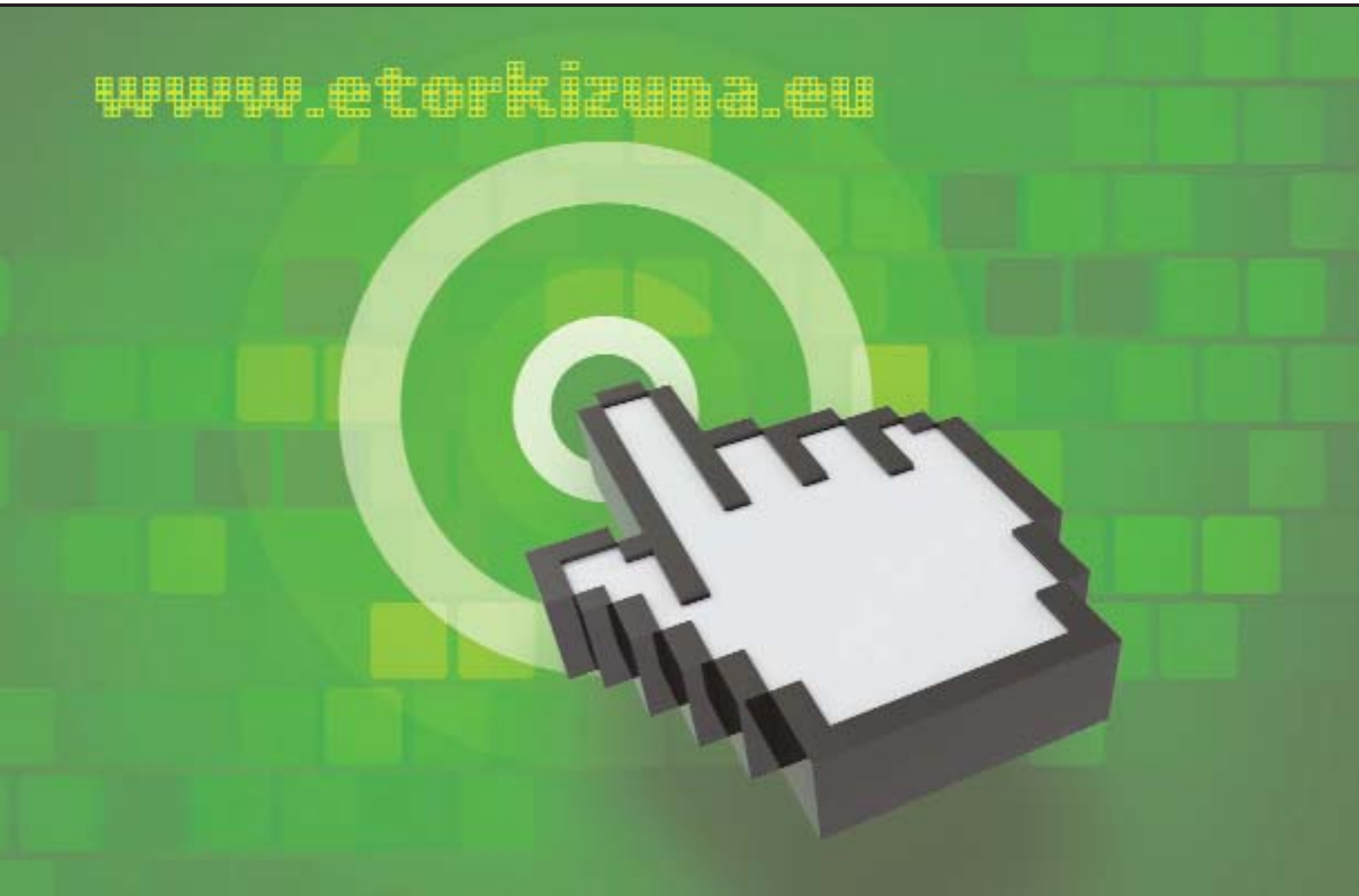
riek baino zenbaki lehen txikiagorik horiek zati ditzakeenik.

Zenbaki txikiek lana ematen badute ere, nahiko erraz esan dezakegu lehenak diren ala ez. Baina zer esan dezakegu 94550!-1 zenbakiari buruz? Lehena da? Matematikan badaude zenbaki bat lehena den edo ez esateko zenbait tresna. Eta zenbaki bat lehena ez bada, zelan deskonposatzen da?

Zenbait zenbaki deskonposatzeko algoritmo eraginkorrak badauden arren, edozein zenbakiren deskonposaketa oraindik misterio bat da matematikan, eta RSA sistema misterio horretaz baliatzen da bere kodifikazioa eraikitzeko. RSA erabiliz, mezua jasoko duenak publiko egiten ditu bi zenbaki: e eta n. Lehenengo zenbakia, e, bidaltzaileak mezua kodifikatzeko erabiliko duena da. Hau da, $\bar{x}$ mezua bada, eragiketa hau egingo du bidaltzaileak: $\bar{x}^e$; eta horixe izango da sarean barna joango den mezu kodetua. Jasotzailea, jaso duen mezu kodetua deszifratzeko, e' zenbakiaz baliatuko da, n zenbakia



Zesarren zifratzailea, non M mezua eta K mezu kodetua baitira. ARG.: ELISABETE ALBERDI.



Hizki bakoitzaren
maiztasuna mezu kodetuan:
F: 9; J: 8;
W,Z: 4; X,O,E,Y: 3;
I,Ñ,P,N,R: 3;
L,M,G,U: 1

Ordezkapenezko metodo bat erabiliz zifratutako euskaraz idatzitako mezu baten adibidea. Euskaraz maiztasunik handieneko hizkiak A eta E dira. ARG.: ELISABETE ALBERDI.

ARG.: ELISABETE ALBERDI

ezagutuz kalkulatuko duena eta $(\tilde{x}^{e})^{e'} = \tilde{x}$ betetzen duena. Hala, jasotzaileak hasierako mezua berreskuratuko du. RSA sisteman, *n* zenbakia bi zenbaki lehenen biderkadura moduan aukeratzen da, eta zenbakien deskonposaketaren inguruan dagoen misterioak *n* zenbaki hori ia deskonposaezin bihurtzen du. Ondorioz, mezua argitzeko egin beharreko eragiketarako behar den *e'* zenbakia, ia bakarrik *n*-ren deskonposaketa dakienak lor dezake, hau da, zenbakia sortu duenak.

ONDORIOAK

Bere garaian, ordezkapen-metodoak atzera geratu ziren bezalaxe, ordenagailuen abiadurak handitu ahala, klabe laburrak darabiltzaten kriptografia-teknikak atzean geratuz joan dira eta joango dira, gaur egungo klabe luzea bihar laburra izan baitaiteke. RSA sistemak horrelako desabantailarik ez badu ere, zenbakien deskonposaketaren mende dago; zenbakiak deskonposatzeko algoritmo eraginkor bat aurkituko balitz, orain arte segurutzat izan dugun RSA sistemaren amaiera izango litzateke. Horrelakorik gertatuz gero, kodifikazio-sistema berri bat beharko genuke. Nork emango du zenbakien deskonposaketarako algoritmo eraginkorra? Eta nork sortuko du ordenagailuen abiadurak mendera ezin dezakeen zifratzeko sistema segurua? ●

BIBLIOGRAFIA

Menezes, Alfred J.; Van Oorschot, Paul C.; Vanstone, Scott A.: *Handbook of applied cryptography.* CRC Press LLC, 1997.

Vera López, Antonio; Vera López, Francisco: *Aljebrarako sarrera.* Editorial Ellacuría, 1991.

Vera López, Antonio: *Introducción al álgebra.* Tomo II. Editorial Ellacuría, 1986.

Stinson, Douglas R.: *Crytography. Theory and practice.* CRC Press, 1995.

Jorge Ramió Aguirrek idatzitako liburu elektronikoa: http://www.criptored.upm.es/guiateoria/gt_mo01a.htm

http://en.wikipedia.org/wiki/Letter_frequency

http://primes.utm.edu/largest.html.