Kriptografia: Idazkera Ezkutuaren Artea

Domingo Ramirez-Alzola

Matematika saila
Euskal Herriko Unibertsitatea
644 p. k., 48080 BILBAO
E-mail: mtpraald@lg.ehu.es

Laburpena: Kriptografiaren munduan murgilduko gara. Gainbegirada bat emango diogu bere historiari, Julio Cesarren garaitik gaurko egunera arte erabili diren teknika ezagunenak azalduz. Ez dugu tratamendu oso sakona egingo. Gure helburua ikuspegi orokorra ematea izan da, gaur egun dituen erabilpenak aipatuz.

1. SARRERA

Kriptografia seguraski K. a. 2000. urtearen inguruan hasi zen Egipto aldean; bertan hieroglifoak erabiltzen ziren errege eta jende garrantzitsuen hilobiak apaintzeko. Hieroglifoen bidez erregearen bizitza kontatzen zen eta adierazi erregearen ekintzarik handienak. Idazkera ezkutua nahita erabiltzen zen baina ez testua ezkutatzeko. Seguraski, testuak itxura garrantzitsua izatea zuten helburu. Denbora pasa ahala, idazkera hauek geroz eta korapilatsuagoak ziren eta jendeak utzi egin zion testua deskodetzeari.

Kriptografia modernoa ordenagailuekin batera jaio zen. Bigarren Mundu Gerran, «Bletchley Park» deitutako toki batean, zientzialari talde batek, hauetako bat Alan Turing izanik, *ULTRA* proiektuan lan egiten zuen germaniar armadak bidalitako ezkutuko mezuak deskodetzen. Germaniarrek *ENIGMA* makina eta *Lorenz* zifratua erabiltzen zuten kodetzeko. Zientzialari talde honek asmatu eta erabili zuen historiako lehenengo ordenagailua, *Colossus* deitutakoa, baina informazio hau 70eko hamarkadaren erdialdera arte ezkutuan mantendu zen.

Ordutik hona kriptografiaren teknologia nabarmen hazi da baina, hala ere, aurrerakuntza gehienak ezkutuan mantentzen ziren eta mantentzen dira, batzuek esaten dutenaren arabera. *NSA*-k (AEB-ko Segurtasun Agentzia Nazionala) finantziatuta ikerkuntzaren zatirik handiena sekretu militar

bezala tratatu da. Dena den, azkenengo urteetan unibertsitate askotan egindako ikerketa ganorazkoek kriptografia denon eskura dagoen zerbait izatea lortu dute. Gainera, funtsezko tresna bilakatu da arlo garrantzitsuetan, hala nola *merkatu elektronikoan, sakelako telefonian* edo *multimedia-egitura duten zenbait banaketa-plataformatan*. Bikoiztasun zibil-militar honek Kriptografiaren historia bikoitza sortu du, eta honela algoritmo berdinak lortzen zituzten, urte gutxiren buruan, lehenengo talde militarrek eta ondoren matematikari zibilek.

Jende asko kriptografia publikoa izatearen alde dago. Esperientziak frogatu du algoritmo onak edukitzeko modu bakarra hauek gizartearen esku egotea dela. Kontrako joeraren adibide ugari daude. *GSM* sakelako telefonoen egiaztatze-algoritmoak erabilitako kode ezkutua berrogeita zortzi orduan agerian gelditu zen. Berdin aipa daitezke *DVD*-ak babesteko dauden algoritmoak, ezdeus bihurtu zirenak, edo disko-etxeek pirateria geldiarazteko alferrik egiten dituzten ahaleginak. Segurtasuna ez da lortu behar algoritmoak ezkutatuz. Algoritmo baten indarra frogatzeko modu bakarra mota guztietako erasoen aurrean jartzea da. Historiako kapitulurik garrantzitsuena 1999ko udan gertatutakoa da, izan ere programadore batek *atzeko ate* bat salatu zuen Windows sistema eragileko bertsio guztietan erabilitako kode kriptografikoan. Kode kriptografiko hori ezkutuan mantentzen da eta delitua da horren analisia.

Erabat ezinezkoa da Kriptografia modernoa politika, filosofia eta moraletik at uztea. Gogora dezagun software kriptografikoak AEBn armamentu nuklearrak duen lege berak dituela eta Europan antzeko zerbait egin nahi dela. Ondorioz, esportatzen diren nabigatzailerik garrantzitsuenek (Netscape eta Explorer) segurtasun *ahula* dute eta, honela, oztopatu egiten dute adibidez banku batekin konexio seguruak egitea. Beste ildo batetik, gobernu batzuen nahia da biztanle guztien gako pribatuak (*sinadura digitala* egiteko beharrezkoak) gordetzea eta legez kanpokotzat jotzea erregistratu gabekoak.

Echelon sarea aipatu beharra dugu. 1980. urtean NSA-k sortutako sarea da eta bertan monitorizatu nahi dira planetako komunikazio elektroniko guztiak (telefonoa, e-maila eta faxa) eta automatikoki bilatu zenbait gakohitz. Lortutako informazioa NSA-ra joango da, eta honek beste herrialde batzuei bidaliko die. Aitzakia terrorismoaren aurkako borroka da baina espioitza industrialerako ere erabil liteke. Berez, horixe egin bide du frantziar gobernuak. Etsai politikoak izan daitezkeenak *zaintzapean* izateko modu bat ere bada.

Europar Batasunari dagokionez, badirudi bere sare propioa eraiki duela, *Enfopol* deitutakoa. Sare honek berezitasun harrigarriak omen ditu: besteak beste, europar guztien gako pribatuen informazioa, telefonoena, ahots-buzoiak, faxak, *chatak* eta posta elektronikoa, eta atzeko ateen sorkuntza Interneteko hornitzaileentzat. Bada sare hau gauzatzearen alde egi-

ten duen dokumentu bat, gobernu guztiek sinatua. Hala ere, inork ez du onartzen haren sorrera.

Zalantzarik gabe, informazioa gizateriak ezagutu duen botererik garrantzitsuena da eta kriptografia funtsezko tresna bihurtu da hau guztia bideratzeko.

2. **KRIPTOGRAFIA TEORIKOA**

Kriptografiaren esanahia hiztegian bilatuz gero honako hau aurki daiteke: *gako sekretuan edo modu enigmatiko batean idazteko artea*. Gaur egun kriptografia artea izatetik teknika izatera heldu da. Teknika honen helburua informazioaren babesa da (onartzen ez dituen begiraleen aurkakoa). Kriptografiak hainbat arlo hartzen ditu bere baitan, hala nola Informazio-teoria, Zenbaki-teoria eta algoritmoen zailtasuna.

Gaur egungo kriptografia hainbat lanetan oinarrituta dago. Alde batetik, *Claude Shannonek* idatzitako *A Mathematical Theory of Communication* (1948) eta *Communication Theory of Secret Systems* (1949) artikuluek Informazio-teoriaren eta Kriptografia modernoaren oinarriak finkatu dituzte. Bestetik, Whitfield Diffie eta Martin Hellman-ek 1976an argitaratutako *New directions in Cryptography* artikulua, gako publikoko kriptografiaren definizioa eman eta arlo handi bat zabaldu du.

Nabarmendu nahi genuke kriptografia hitzak kodeen erabilpenei egiten diela erreferentzia eta ez kode hauek apurtzeko erabiltzen diren teknikei. Bigarren zeregin horri *kriptoanalisia* deritzo. Edozein kasutan, bi adar hauek oso loturik daude; informazioa zifratzeko sistema bat disenatzen denean bere kriptoanalisia kontuan hartzekoa da, bestela sorpresa desatseginak edukiko genituzke.

Azkenik, *Kriptologia* hitza, nahiz eta hiztegian ez agertu, kriptografia eta kriptoanalisia zientzia-izen baten barruan elkartzeko erabiltzen da.

2.1. **Kriptosistema**

Kriptosistema (edo kriptografia-sistema) bat (*M*,*C*,*K*,*E*,*D*) boskote bat da:

—*M*: Bidali nahi diren *mezu zifratu gabeen multzoa* (testu argia edo plaintext» deitzen dena).

—*C*: *Mezu zifratuen edo kriptogramen multzoa*.

—*K*: Kriptosisteman erabili ahal diren *gakoen multzoa*.

—*E*: *Kodetzeko transformazioak* edo funtzio-familia. Funtzioa *M* multzoko elementu bakoitzari aplikatzen zaio *C* multzoko elementu bat lortzeko. *k* gako bakoitzarentzat E_k transformazio bat existitzen da.

—*D*: *Deskodetzeko transformazioak*. *E*-ren alderantzizkoa da.

Edozein kriptosistemak hurrengo baldintza bete behar du:

$$D_k(E_k(m)) = m.$$

Hots, *m* mezua *k* gako beraren bidez kodetu eta deskodetzen badugu, hasierako mezua lortuko dugu.

Bi motatako kriptosistemak daude:

—**Kriptosistema simetrikoak edo gako pribatukoak.** Hauetan gako bera erabiltzen da kodetu eta deskodetzeko. Honek arazo bat sortzen du: komunikazioetan erabili ahal izateko, gakoak igorle eta hartzailearen esku egon beharko du. Eta arrisku bat du: modu seguruan bidali beharko zaio gakoa hartzaileari.

—**Kriptosistema asimetrikoak edo gako publikokoak.** Hauek gako bikoitza erabiltzen dute (k_p, k_P). k_p *gako pribatua* deitzen da eta k_P *gako publikoa*. Hauetako bat mezua kodetzeko eta bestea deskodetzeko erabiltzen dira. Kasu askotan, gako hauek elkartrukatu ahal dira, hau da, bat erabiltzen badugu zifratzeko bestea deszifratzeko erabili ahal da. Kriptosistema hauek hurrengo erregela bete behar dute: k_P gako publikoaren bidez ez da posible k_p gako pribatua lortzea. Mota honetako kriptosistemak posibilitate gehiago dituzte kanal ez-seguruetan mezuak modu seguruan bidaltzeko; gako publikoa da kanaletik zehar doan bakarra, eta honek mezua zifratzeko edo egiaztatzeko besterik ez du balio.

Praktikan bi motak nahasian erabiltzen dira, bigarren motakoak konputazionalki garestiagoak baitira. Mundu errealean mezuak (luzeak) algoritmo simetrikoen bidez kodetzen dira, oso eraginkorrak baitira, eta gero kriptografia asimetrikoa erabiltzen da gakoa (laburra) kodetzeko.

2.2. **Esteganografia**

Esteganografia, edo kanal subliminalen erabilpena, informazio baten barruan beste mota bateko informazioa ezkutatzea da. Metodo honen bidez kontrol-sistema batzuk gainditu daitezke. Adibide gisa, demagun disidente politiko batek mezua bidali nahi duela bere herrialdetik kanpo, zentsuraren gainetik pasatuz. Kodetzen badu, agintariek ez dute onartuko mezua bidal-

tzerik, baina mezu hau gabonak zoriontzeko irudi digital baten azpian badoa, seguraski bere helburura iritsiko da.

Aipatzekoa da esteganografia, legeak oztopatzen ez duena, mezuak bidaltzeko metodo bat dela. Mezua kodetu gabe bidaltzen da baina *zabor* askoren artean. Hartzaileak esteganografia-teknikak erabiliko ditu mezua besteetatik banatzeko. Teknika hau *chaffing and winnowing* deitzen da, eta itzulpena *lastoz bete eta garia lastotik banatu* izango litzateke. Ondorioz, mezua kodetu gabe bidaltzeko metodoa izango genuke baina mezu hau hartzaileak bakarrik berreraikiko luke. Sistema hau 1998.eko martxoan sortu zen, Ronald L. Rivestek, RSA sistemaren sortzaileetako batek, proposatuta kriptografiarenganako AEB-ko Gobernuaren politika errepresiboaren aurka protesta gisa.

2.3. **Kriptoanalisia**

Kriptoanalisia kriptosistema baten segurtasuna zalantzan jartzea da. Hau gakoa ezagutu gabe mezu bat deskodetuz egin daiteke, edo kriptograma batetik edo gehiagotik kodetzeko erabiltzen den gakoa lortuz.

Orokorrean, kriptoanalisia gako beraren bidez sortutako (mezuak, kriptogramak) bikote asko aztertu ondoren egiten da. Erabiltzen den metodo motak ez du garrantzirik; izan daiteke komunikazio-kanal batean erantzun bat *harrapatzea* edo sistemari zerbait bidaliz lortzea (*erasoa*). Noski, zenbat eta bikote kopuru handiagoa aztertu, orduan eta kriptoanalisiaren arrakasta handiagoa izango da.

Analisi mota interesgarriena *hautatutako testu argia* da. Honela funtzionatzen du. Demagun testu argi batzuk ezagutzen ditugula eta beraien kriptograma ere. Egoera hau gertatzen da kodetzeko erabiltzen den tresnetara sar gaitezkeenean eta eragiketak egin ahal ditugunean ere; ez digu, ordea, gakoa irakurtzen uzten (horixe gertatzen da GSM *sakelako telefonoen txarteletan*, adibidez). Gakoa lortzeko behar ditugun bikoteen kopurua jaitsi egiten da. Sistema ahula denean mezu gutxi batzuekin lor daiteke nahikoa informazio erabiltzen den gakoa eskuratzeko.

Beste modu bat izan daiteke guk dugun mezu kodetu bati deskodetzeko dauden algoritmo guztiak aplikatzea eta ikusi lortutako guztien artean zeinek duen *testu argiaren itxura*. Metodo hau, eta honek bezala, *K* gakoen espazioa zehatz eta mehatz aztertzen duten metodo guztiei *landu gabeko indarrezko erasoa* deritze eta kasu askotan ez daude kriptoanalisitzat onartuta; izen honek kodetzeko erabiltzen den algoritmoak dituen *ahultasunak* argitara eramaten dituzten teknikei egiten die erreferentzia. Suposatzen da landugabeko indarrezko teknika erabiltzea ezinezko bihurtzeko bezain handia dela gakoen espazioa. Ohartu, hala ere, konputagailuek duten kalkuluahalmena geroz eta handiagoa dela eta horregatik duela zenbait urte oso se-

guruak ziren sistema batzuk gaur egun oso hauskorrak dira, DES sistema bezala. Dena dela, badira luzera nahiko handiko gakoak non era honetako eraso bat ezinezkoa den. Adibidez, diseinatzen badugu 256 bit dituzten konbinazio posible guztiak eraikitzen dituen makina bat, ez litzateke Unibertso osoan nahikoa energia egongo gako guztiak aztertzeko.

Aipatu beharrekoak dira emaitza interesgarriak eskaintzen dituzten bi kriptoanalisi-metodoak: *analisi diferentziala* eta *analisi lineala*. Lehenengoak, patroi komunak lortu nahian, kodetutakoen arteko aldaketak aztertzen ditu, bit batetik beherako desberdintasuna duten (mezuak, kriptograma) bikoteak baditugu. Bigarrenak, XOR eragiketak erabiltzen ditu testu argiko bit batzuen eta kodetutako testuko bit batzuen artean, ondorioz bit bakarra lortzeko. Hau (mezuak, kriptogramak) bikote askorekin egiten badugu p probabilitatea lor genezake bit horretan. p 1/2-ra hurbiltzen ez bada, orduan aukera izango genuke gakoa berreskuratzeko.

Beste analisi mota bat, hau algoritmo asimetrikoetarako, gako pribatua gako publikoarekin lortzea izango litzateke. Analisi-teknika hauek konputazionalki kostu handia duten problemak ebazte aldera garatu dira: faktorizazioa, logaritmo diskretuak, etab. Problema hauek ebazpenik gabe dauden bitartean, algoritmo hauetaz fidatu ahal gara.

Kriptografia informazioa babesteko ez ezik, egiaztapenean ere erabiltzen da, hots, mezua bidaltzen duena identifikatzeko eta beste norbaitek aurrekoaren tokia hartzea oztopatzeko. Kasu hauetan kriptoanalisi-teknikek elementu faltsu bat ontzat ematea dute helburu nagusia. Gerta daiteke mezua ezagutu nahi ez izatea, faltsuena dena egia bezala agertzea soilik.

Ikusten dugun bezala, sistema kriptografikoen ugaritasunak kriptoanalisi-tekniken ugaritasuna dakar, teknika bakoitza sistema bakoitzari lotuta agertzen delarik. Seguruenik, hurrengo urteetan sistema kriptografiko berriak sortzen direnean kriptoanalisi-metodo berriak ere sortuko dira. Gainera, ikerketa-arlo hauetan kriptosistema bezain garrantzitsua da kriptoanalisia. Zergatik ote? Hona erantzuna: posible da kriptosistema baten akatsak agerian jartzea baina ezinezkoa da, ordea, akatsik ez duela frogatzea.

3. GAKO PRIBATUKO KRIPTOGRAFIA

Betidanik, gizakiak sekretu mota asko izan ditu eta hauek begirada indiskretuetatik at mantentzeko mekanismoak lortu izan ditu. Julio Cesarrek algoritmo sinplea erabiltzen zuen bere komunikazio militarrak sekretupean mantentzeko. Leonardo da Vincik bere lanei buruzko oharrak eskuinetik ezkerrera idazten zituen ezkerreko eskua erabiliz. Beste pertsonaia batzuk, Sir Francis Bacon edo Edgar Allan Poe esate baterako, ezagunak ziren kode kriptografikoekiko zaletasunagatik, kasu gehienetan jolas bat baitzen edo/eta erronka.

Hasieran esan dugun bezala, lehendabiziko metodo kriptografikoak Egipto aldean sortu ziren.

Indian, idazkera ezkutua garatuagoa zegoen eta gobernuak ezkutuko kodeak erabiltzen zituen herrialdean zabaldurik zegoen espioi-sareko kideekin komunikatzeko. Lehendabiziko metodoak alfabeto-ordezkapenak baino ez ziren, gehienetan fonetikan oinarrituta. Adibidez, *txerri latinoa*-ren ordez *xerritay atinoalay*; nabaritzen den bezala, lehenengo kontsonantea bukaeran jartzen da eta ”ay” itsasten zaio hitz bakoitzari.

Mesopotamian idazkera kuneiformea erabiltzen zen testuak kodetzeko. Teknika hau Babilonian eta Asirian erabili zen. Biblian, batzuetan, kodetzeko metodo hebrearra erabiltzen zen. Metodo honetan, alfabetoaren azken letraren ordez lehenengoa jartzen zen eta horrela besteak. *Atbash* deitzen zen. Ondorengo taulan dago erregela:

$$A\ B\ C\ D\ E\ F\ G\ H\ \cdots$$
$$Z\ Y\ X\ W\ V\ U\ T\ S\ \cdots$$

Honela ”KAIXO” hitza ”PZRCL” bihurtzen da.

Grezian askotan erabili ziren kodetzeko metodoak; adibidez, «Iliada» liburuan, Bellerophonek taula sekretu bat zuen eskuen artean erregearen aurrera eraman zutenean eta horretan Bellerophon bera hil behar zuela esaten zitzaion erregeari. Polybusek beste metodo bat garatu zuen, egun *Polybius square* izena duena. Alfabetoko letrak bost bider bosteko karratu baten barruan sartzen dira:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y/Z

Honela, $T = 54$, $H = 32$, $I = 42$, $S = 44$.

Julio Cesarrek erabiltzen zuen kriptografia-sistema (*Caesar Cipher*) zen letra bakoitzaren kokapena aurreratzea. Honela, aurrerapena bikoa bada, hauxe dugu:

$$A\ B\ C\ D\ E\ F\ \cdots$$
$$C\ D\ E\ F\ G\ H\ \cdots$$

Letra bakoitzari zenbaki bat egokitzen badiogu eta 26 letrako alfabetoa hartu, orduan transformazio kriptografikoa hurrengoa izango zen:

$$C \equiv (M + 2) \bmod 26 \Leftrightarrow 26 | C - (M + 2).$$

Mezua berreskuratzeko zenbaki bakoitzari bi kendu behar zaio.

Kasu orokorra *ordezkapen monoalfabetikoa* izenekoa izango litzateke. Hau da, letra bakoitzari beste bat egokitzen zaio aplikazio injektibo baten bidez.

1518. urtean kriptografian urrats handia eman zen. Fraide germaniar batek, *Trithemius*-ek, sei liburuko serie bat idatzi zuen, *Polygraphia* izenekoa, eta bosgarren liburuan taula bat jarri zuen; taula horretan alfabetoa errepikatzen da, baina lerro bakoitza aurrekoaren berdina da letra bat aurrera mugituz.

A	*B*	*C*	*D*	*E*	*F*	Testua
F	*G*	*U*	*Q*	*H*	*X*	*T*00
O	*F*	*G*	*U*	*Q*	*H*	*T*01
⋮	⋮	⋮	⋮	⋮	⋮	⋮
G	*U*	*Q*	*H*	*X*	*S*	*T*25

Mezu bat kodetzeko, testuko lehenengo letra zerrendako lehenengo lerroarekin kodetzen da, bigarren letra bigarren lerroarekin, etab. Sistema honetan gakoa 26 letran behin errepikatzen da.

XVI. mendeko kriptograforik garrantzitsuena Blaise de Vigenère (1523-1596) izan zen. 1585. urtean *Tracte des Chiffres* liburua idatzi zuen. Liburu honetan Trithemiusen taula erabili zuen baina gakoa sortzeko sistema aldatuz. Gako hau hain ezaguna den *DES* sistemaren oinarria da. Honela labur daiteke:

Vigenère-ren zifratua

$K = \{k_0,\ldots,k_{d-1}\}$ da gakoen multzoa eta kodetzeko, hurrengo funtzioa erabiltzen du:

$$E_k(m_i) \equiv m_i + k_{(i \bmod d)} (\bmod n),$$

m_i testu argiko i-garren ikurra eta n erabiltzen dugun alfabetoaren kardinala izanik.

Kriptosistema hauek guztiek gaur egun garrantzia galdu dute zeren erraz kriptoanalizatu ahal baitira. Hala ere, esan beharra dago sistema hauek arrakasta handia izan zutela XX. mendera arte.

Orokorrean zifratu simetrikoak bi taldetan sailkatu ahal dira: *n* luzerako hitzak sortzen duten iturburuetatik datozenak eta letrak sortzen dituztenetatik datozenak. Lehenengo kasuan blokekako zifratuei buruz hitz egiten da eta bigarrenean fluxuzko zifratuei buruz.

3.1. **Blokekako zifratuak, DES**

Blokekako zifratuak n luzerako hitzez osatutako testuetan du eragina, honela hitz bakoitza hitz berri bat bihurtzen delarik.

Mota honetako zifraturik ezagunena DES da. Sistema hau transposizio eta ordezkapenen arteko biderkadura da.

40ko hamarkadaren bukaeran, Shannonek ideia berri batzuk plazaratu zituen sistema zifratuei buruz. Berak eragiketa anitzen erabilpena gomendatzen zuen transposizioa eta ordezkapenak nahastuz. Ideia hauek IBM-k erabili zituen 70eko hamarkadan, *LUCIFER* sistema diseinatu zuenean. 1976. urtean, AEB-ko Gobernuak sistema hau estandar gisa hartu zuen eta DES (Data Encryption Standard) deitu zion. Ondorioz, munduko ia herrialde guztiek onartu zuten sistema hau estandar bezala banku eta merkataritza-sareetan.

DES sisteman, *M* hitzari lehenengo transposizio bat ezartzen zaio eta *IP* deitzen den permutazio baten bidez, $T_0 = IP(M)$ lortzen da. T_0-ri funtzio finko bat hamasei aldiz ezarri ondoren *IP*-ren alderantzizkoa aplikatzen zaio.

3.2. **Fluxuzko zifratuak**

1917. urtean J. Mauborgue eta G. Vernamek kriptosistema perfektua (Shannonen irizpidearen arabera) asmatu zuten. Metodo horrek mezuaren luzera berberako ausazko sekuentzia bat erabiltzen zuen, behin bakarrik. Metodo honen arazo nagusia: gakoa mezua bezain luzea dela.

Argi eta garbi, Vernamen sistema ez da eraginkorra baina demagun posible dela sasiausazko sortzaile batekin sekuentzia kritografikoki ausazkoak sortzea, zikloen luzera oso handia izanik. Kasu honetan, sortzailearen hazia gako bezala erabiliz, erabili eta botatzeko diren kateak lortuko genituzke eta mezuak zifratzeko *xor* funtzioa erabiliko genuke sistema perfektua lortuz. Ideia hau erabili zuten germaniarrek Lorenz zifratuan, ENIGMA makinarekin.

4. **GAKO PUBLIKOKO KRIPTOGRAFIA**

Gako publikoko algoritmoek edo algoritmo asimetrikoek komunikazio-sare ez seguruetan (Internet) erabiltzeko gaitasuna frogatu dute. Whitfield Diffiek eta Martin Hellmanek sortuak, abantaila bat dute algoritmo simetrikoe-

kiko: gako bakarra erabili beharrean bikote bat erabiltzen da. Orain arte zenbait algoritmo asimetriko agertu dira baina gehienak ez dira oso seguruak; beste batzuk aldiz ez dira oso erabilgarriak. Beraien oinarria ebatzi gabeko problema matematikoak planteatzea da.

Esan dugun bezala, algoritmo asimetrikoek bi gako dituzte, k_p eta k_P, gako pribatua eta gako publikoa deitzen direnak. Bata kodetzeko erabiltzen da eta bestea deskodetzeko. Funtsezkoa da gako bat ezagututa beste gakoaren kalkulua oso zaila izatea. Diagrama baten bidez argituko dugu kontua.

	A		B
1.	m	$\rightarrow$	k_P, k_p
2.	m, k_p	$\leftarrow$	k_P, k_p
3.	m, k_P	$\rightarrow (E_P(m))\rightarrow$	k_P, k_p

Demagun *A*-k *B*-ri *m* mezua bidali nahi diola. *B*-k bi gako ditu, bat kodetzeko eta bestea deskodetzeko. Bigarren urratsean, *B*-k *A*-ri k_p gakoa bidaltzen dio. Ondoren, *A*-k *m* mezua k_p -ren arabera kodetzen du eta lortutako $E_P(m)$ *B*-ri bidaltzen dio. Orain *B*-k $E_P(m)$ gako pribatuarekin deskodetu eta *m* lortzen du.

Ondoren gako publikoko sistema ezagunen berri emango dugu.

—Zenbakiak faktorizatzeko metodo eraginkorren faltan oinarrituta daudenak: *RSA* eta *Rabinen* sistemak.
—**ElGamal sistema**: logaritmo diskretuaren probleman oinarrituta dago.
—**Merkle-Hellman sistema**: motxilaren probleman oinarrituta dago.
—**McEliece sistema**: kodeketa algebraikoaren teorian oinarrituta dago. Kode lineal baten deskodeketa *NP*-osoa motako arazoan oinarrituta dago.
—**Kurba eliptikoetan oinarritutako sistemak**: logaritmo diskretuen arazoa kurba eliptiko baten gainean.
—**Probabilitate-sistema**: gako publikoetan arazo bat dugu: $C = E_k(M)$ testu zifratuari testuari buruzko informazio apur bat isurtzen zaio beti. Probabilitate-kriptografiaren nahia (Goldwaser eta Micaliren ideia) mezuak zifratzea da eta helburua, oinarrizko testuari buruz informazioa ematen duen inolako kalkulurik ez egotea.

Algoritmo asimetrikoek, simetrikoekin konparatuta, gako handiagoak erabiltzen dituzte. Adibidez, algoritmo simetrikoentzat 126 biteko luzerako gako bat segurutzat jotzen den bitartean, algoritmo asimetrikoetarako

(kurba eliptikoetan oinarritutakoak salbu) 1024 biteko luzerako gakoak erabiltzea gomendatzen da. Gainera, algoritmo hauek duten kalkulu-konplexutasunagatik simetrikoak baino askoz geldoagoak dira. Praktikan, metodo asimetrikoak mezu bakoitzaren *sinadura digitala* kodetzeko baizik ez dira erabiltzen.

4.1. **RSA algoritmoa**

RSA-ren segurtasuna hurrengoan datza: ez dago modu egokirik zenbakiak faktorizatzeko.

1977. urtean plazaratu zen. Bere izena sortzaileengandik dator: Ronald Rivest, Aldi Shamir eta Leonard Adleman, eta 2000. urtera arte murriztuta egon zen. Gaur egun, algoritmo asimetriko seguruenetarikoa dela esaten da.

Ondoren algoritmoaren deskribapena egingo dugu, parentesi artean sistemaren zati sekretuak eta publikoak adierazita.

Testu bat kodetzeko, k luzerako hitzetan banatzen da lehenengo. Ondoren, finkatutako ϕ funtzio injektiboa ezartzen zaio hitz bakoitzari. Demagun hasierako testuan A alfabetoko letrak erabiltzen ditugula; orduan, honelako funtzio injektiboa definituko dugu $\Phi : A \to \mathbf{Z}/n\mathbf{Z}$ ($|A|^k \leq n$ behar da).

RSA algoritmoaren kasuan, hurrengo urratsean berreketa modularra erabiltzen da:

$$\begin{array}{rccc} f: & \mathbf{Z}/n\mathbf{Z} & \longrightarrow & \mathbf{Z}/n\mathbf{Z} \\ & \overline{m} & \to & \overline{m}^e \end{array}$$

e lortzeko ondokoa egiten da.

—Lortu bi zenbaki lehen oso handiak (sekretuak), p,q, eta kalkulatu $n = pq$ (n publikoa).

—Lortu kodetzeko gakoa, e. Gako hau (sekretua) $\varphi(n)$ zenbakiarekiko lehena izan behar da, $\varphi(n)$ Euler-en funtzioa izanik.

—Existitzen da d zenbakia (pribatua) hurrengoa betetzen duena:

$$de \equiv 1 \mod((p-1)(q-1)).$$

Hau da, d e-ren alderantzizkoa da $(p-1)(q-1)$ moduluarekiko. Ohartu alderantzizkoa Euklidesen algoritmoarekin kalkulatu ahal dela baina ezinezkoa izango dela d lortzea p eta q ezagutzen ez badira.

—Kodetzeko gakoa (e,n) publiko egiten da.

f funtzioa erabili ondoren, lortutako emaitza testu bezala idazteko beste aplikazio bat behar dugu $\phi' : \mathbf{Z}/n\mathbf{Z} \rightarrow A^l$, injektiboa hau ere; beraz, $n \leq A^l$ izan behar da.

—Deskodetzeko alderantzizko pausuak ematen ditugu:

$$A^l \xrightarrow{\phi'^{-1}} \mathbf{Z}/n\mathbf{Z} \xrightarrow{f^{-1}} \mathbf{Z}/n\mathbf{Z} \xrightarrow{\phi^{-1}} A^k$$

Ohartu $f^{-1}(\overline{m}) = \overline{m}^d$ aplikazioa dela. Beraz d ezagutu behar da deskodetzeko.

Praktikan, p eta q bit-kopuru handikoak aukeratuko ditugu: 200, adibidez. Norbaitek algoritmoari eraso egin nahi badio, p eta q lortu beharko ditu eta hau konputazionalki ezinezkoa da p eta q oso handiak badira.

4.2. **Kurba eliptikoetan oinarritutako sistemak**

Kurba eliptikoen kriptografia zifratu asimetrikoen artean etorkizun handienetakoa da. Kurba eliptikoak erabiltzearen aldeko lehenengo urratsak N. Koblitzek eta V. Millerek eman zituzten 1985. urtean.

Izan bedi K gorputza. K-ren gaineko kurba eliptikoa 1 generoko kurba leuna da puntu gehigarri batekin $\mathcal{O} \in E(K)$. Edo, modu baliokidean, E kurba leuna eta proiektiboa da eta hurrengo itxura du:

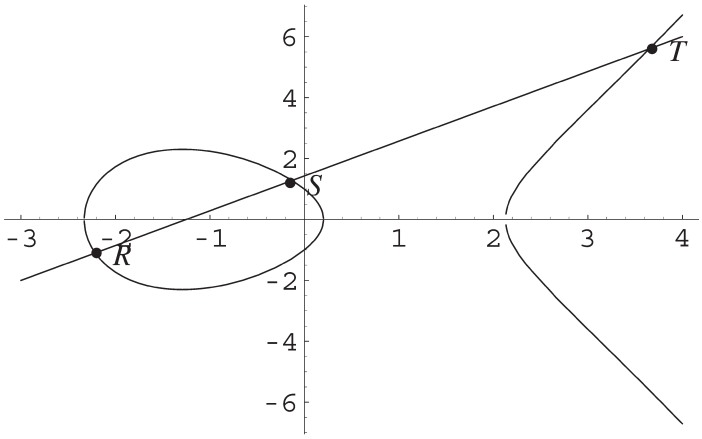
$$Y^2Z + a_1XY\,Z + a_3Y\,Z^2 = X^3 + a_2X^2Z + a_4X\,Z^2 + a_6Z^3.$$

$\mathbf{R}$-ren gaineko kurba eliptiko batek $y^2 = x^3 + ax + b$ ekuazioa betetzen du.

$x^3 + ax + b$ polinomioak erro anizkoitzak ez baditu, hau da, $4a^3 + 27b^2 = 0$, orduan kurba eliptikoaren puntuek eta beste puntu batek, infinituko puntua deitzen denak ($\mathcal{O}$), talde egitura dute.

Izan bitez $R = (r_x, r_y)$, $S = (s_x, s_y) \in E(\mathbf{R})$. Batura honela definitzen da: R eta S puntuetatik pasatzen den zuzena irudikatzen dugu; zuzen horrek gure kurba hirugarren puntu batean ebakiko du; R eta S-ren batura puntu honen aurkakoa izango da.

Metodo kriptografikoak gorputz finituen gainean eraikitzen dira. $\mathbf{R}$ gorputzean batura definitu dugun bezala gorputz finituetan ere definitu ahal da.



1. irudia. $y^2 = x^3 - 5x + 1$.

Izan bedi R kurba eliptikoko puntu bat; R-k sortutako azpitaldea $< R > = \{\mathcal{O}, R, 2R, \ldots\}$ taldea da. Beraz, $S \in < R >$ bada, existitzen da $k \in \mathbf{Z}$ non $S = kR$ den. Logaritmo diskretuen arazoa kurba eliptikoetan da k lortzea S eta R ezagututa. Orain arte ez da lortu k kalkulatzen duen algoritmo eraginkorrik.

ElGamal-en zifratua kurba eliptikoen gainean

Izan bedi R kurba eliptikoaren puntu bat. $< R >$ azpitaldearen kardinalari n deituko diogu. Hautatzen dugu x, 1 eta $n - 1$ bitarteko zenbaki arrunta, eta kalkulatzen dugu $Y = xR$.

(R, Y, n) publiko egiten da eta x pribatua izango da.

Zifratua n zenbakiarekiko lehena den k zenbaki bat hautatuz egingo da. Ondorengo kalkuluak egiten ditugu: $a = kR$ eta $b = m + kY$, m bidali nahi dugun mezua izanik, kurba eliptikoaren gaineko puntutzat hartuta. Kriptograma (a, b) bikotea da. Hau deskodetzeko $m = -(xa) + b$ kalkulatu beharko da.

5. EGIAZTATZE-METODOAK

Egiaztatze-metodoek mezuaren jatorria, osotasuna, identitatea… modu seguruan egiaztatzeko balioko digute. Hiru motako egiaztatze-metodoak aipatuko ditugu.

—**Mezuen egiaztatzea**. Ezagutzen ez dugun mezu baten jatorria jakin nahi dugu, faltsua ez dela egiaztatzeko. Mekanismo hau **sinadura digitala** deitzen da.

—**Erabiltzailearen egiaztatzea pasahitzaren bidez**. Honekin kanal batean legala den erabiltzaile baten presentzia ziurtatzen da. Erabiltzaileak pasahitz sekretu bat izan beharko du.
—**Gailuaren egiaztatzea**. Gailu baliagarri baten presentzia ziurtatu nahi da. Gailu hau bera bakarrik egon daiteke edo *giltza elektroniko* bat izan daiteke erabiltzaileak duen pasahitzaren ordez dagoena.

5.1. **Sinadura digitala. Laburpen-funtzioak**

Mezuen egiaztatzea, laburpen-funtzioen bidez egiten da. Funtzio hauekin sinadura digitala lor dezakegu. Sinadura hau mezua baino laburragoa da eta oso zaila da sinadura bera sortzen duen beste mezu bat lortzea. Demagun *A*-k *B*-tik *m* mezua hartzen duela eta egiaztatu nahi duela benetan *B*-k bidalitakoa dela. Horretarako, *B*-k $r(m)$ laburpen-funtzioa sortzen du eta gako pribatua erabiliz kodetzen du. Deskodetzeko erabiltzen den gakoa publikoa izango da eta *A*-k ezagutuko du. *B*-k $r(m)$-ri dagokion kriptograma bidaltzen du. *A*-k orain bere $r'(m)$ propioa lor dezake eta $r(m)$-rekin alderatu ere. Berdinak badira, mezua benetakoa izango da.

Laburpen-funtzioa segurua izan dadin hurrengo ezaugarriak izan beharko ditu:

—$r(m)$ luzera finkokoa da, *m*-ren luzerarekin zerikusirik ez duena.

—*m* emanik, $r(m)$ kalkulatzea erraza da.

—$r(m)$ emanik, ezinezkoa da *m* berreskuratzea konputazionalki.

—*m* emanik, ezinezkoa da konputazionalki beste mezu bat lortzea, m', $r(m) = r(m')$ betetzen duena.

Laburpen-funtzio hauek, MDC (modification detection codes) izenaz ezagutzen dira eta *sinadura digitalak* lortzeko modua emango digute.

$r(m)$ laburpen-funtzioa kodetuz, $E_{k_p}(r(m))$ lortuko dugu. Informazio gehigarri hau (*m* mezuaren sinadura izenekoa) k_p gako pribatua duenak bakarrik sor dezake. Gako publikoa duen edonork deskodetu ahal du eta sinadura egiaztatu ere. Sinadurak sortzeko algoritmo ezagunenak MD5 eta SHA-1 dira.

Ikusitako MDC-ren aurrean, badira beste mota bateko laburpen-funtzioak, MAC (message authentication codes) izena dutenak. Hauek gako sekretua erabiltzen dute mezuaren osotasuna kalkulatu ahal izateko. Gako hau igorleak eta hartzaileak bakarrik ezagutzen dutenez, jasotzaileak mezua eta nondik datorren jakin dezake.

5.2. **Erabiltzailearen egiaztapena pasahitzaren bidez**

Egiaztatze-sistema hau erabiltzaileak bakarrik ezagutzen duen informazio sekretu batean datza; honek sistemaren aurrean identifikatzeko balio dio. Terminal seguru baten aurrean gaudela suposatuz, bi kasu bereizi ahal dira:

—Sistema erabiltzailearekin komunikatzen da baina erabiltzaileak ez du bertan sartzerik; adibidez, *kutxazain automatikoa*.
—Sistemak erabiltzaileari sartzen uzten dio; adibidez, *UNIX sistema eragilea*.

Lehenengo kasua da ebazteko errazena. Horretarako, sistemak fitxategi baten barruan erabiltzaile eta pasahitzen zerrenda bat gordetzea nahikoa da. Erasoak galarazteko (pasahitzak babesteko) nahikoa izango da saialdi kopurua murriztea eta atzerapenak sartzea pasahitza okerra denean.

Bigarren kasua zailagoa da. Alde batetik, aurreko kasuan hartutako neurriak hartu behar ditugu, eta bestetik, kontuan izan behar dugu edozein erabiltzaile ibili ahal dela fitxategietan. Unix-eko bertsio zaharrenetan posible zen pasahitzen artxiboa edozeinek deskargatzea eta beraz gako-hitzak ezin ziren testu argi bezala idatzi fitxategi hartan. Orduan, gakoen fitxategian pasahitzaren sinadura gordetzea da erabiltzen den prozedura.

5.3. **Gailuaren egiaztapena**

MAC algoritmoak gailuak egiaztatzeko erabili ahal dira. GSM *sakelako telefonoek* erabiltzen duten SIM txartela da mekanismo horren adibide bat. Txartel hauek COMP128 izeneko MAC algoritmo bat daukate: mezu batekin balio bat sortzen du eta k gakoa. Gako hau memoriako toki batean gordeta dago eta ezin da kanpotik irakurri. Txartel bakoitzean gako bakarra gordetzen da, eta kopia bat gordetzen da leku seguru batean. Konpaniak txartel bat identifikatu nahi badu X bit-bloke ausazko bat sortu eta elkartutako $E_k(X)$ laburpen-funtzioa kalkulatuko du. Ondoren X txartelera bidaltzen du kalkulu berdina egin dezan eta lortutako kalkulua itzuli behar du. Biak berdinak badira, txartela benetakotzat jotzen da. Teknika honi *erronka-egiaztatzea* deritzo.

5.4. **Diru elektronikoa**

Egiaztapenaren kontrako hitza faltsifikazioa da. Eta faltsifikazio hitza erabiltzen dugunean berehala etortzen zaigu burura historian gehien faltsifikatu den objektua: dirua.

Diru fisikoa gainean eramateko deserosoa da, higatu egiten da eta posible da faltsifikatzea. Gainera, periodikoki txanponak aldatu behar dira. Ordezkatzeko *kreditu txartelak* eta *txekeak* daude, baina horrela, anonimatua eta pribatutasuna galtzen ditu erabiltzaileak. Gaur egun ez dago herrialde guztiek onartzen duten protokolorik, baina bai proposamen ugari. Ondoren, horrelako protokolo bat nolakoa izan litekeen finkatzen saiatuko gara.

Demagun txeke anonimo bat bidali nahi dugula. Horretarako, diru-kopuru bateko ehun txeke sortzen ditugu, bakoitza kartazal batean sartu eta bankura bidaltzen ditugu. Bankuak hautazko laurogeita hemeretzi irekiko ditu eta egiaztatuko du denak kopuru berekoak direla. Geratzen denari bere zigilua jarriko dio eta itzuliko digu, gure kontutik kantitatea kenduz. Orain bankuak onartutako txeke bat dugu, baina bankuak ez daki ezer hartaz. Txekea entregatzen dugunean, norbaitek kobratu nahi badu, nahikoa izango du bankura eramatea; honek bere zigilua baieztatu eta kopurua ordainduko dio, nondik datorren jakin gabe. Protokolo hau era honetan inplementatu ahal dugu kriptografia asimetrikoaren bidez: ehun ordainketa-agindu anonimo sortu eta bankura bidaltzen dira; bankuak egiaztatu eta batean sinadura digitala jartzen du, gure kontutik diru-kopurua kenduz. Hartzaileak nahi duenean kobratu ahal du.

Proposatutako protokoloak hiru taldetan sailkatu ahal dira:

—Kriptografia simetrikoa erabiltzen dutenak: NetBill eta NetCheque.
—Kriptografia asimetrikoa erabiltzen dutenak: CAFE proiektua, ECash, NetCash, CyberCash, IBM-ren iKP, eta AT & Bell laborategien Anonymous Credit Cards (ACC).
—Kriptografiarik gabekoak: ISN, Compuserve eta FIRST VIRTUAL Holdings Incorporated.

6. ERANSKINA: KRIPTOGRAFIA KUANTIKOA

Fisika Kuantikoak materiak maila oso txikietan (atomo mailan) duen portaera du aztergai. Mundu kuantikoan Mekanika Klasikoaren arauak ez dira betetzen eta gertatzen diren fenomeno harrigarri eta interesgarriak erabilgarriak dira Kriptografian ere.

Gaur egun, badira Mekanina Kuantikoaren aplikazio praktiko batzuk Kriptografian; konputagailu kuantikoetan oinarritutakoak, aldiz, oraindik ez dira abian jarri.

Zuzeneko aplikazio batek hurrengo teorian du jatorria: objektu batek ezin du beste batekin interakzionatu aldaketa bat izan gabe. Honek komunikazio kanalak fabrikatzea ahalbidetu du, hauetan datuak ezaugarri desberdinak dituzten fotoietan bidaiatzen dute. Erasotzaile batek informazio

bat atera nahi balio, sistemak fotoiak aldatuko lituzke eta berehala jabetuko litzateke egoeraz.

Hori dela eta, egindako hainbat saiotan lortu da informazioa behar bezainbesteko abiaduraz eta distantziara bidaltzea. Kanal mota hauek kanal elektrikoak edo optikoak bezain azkarrak ez diren arren, egokiak izango dira hurrengo urteetan informazioa bidaltzeko.

7. **BITXIKERIA KRIPTOGRAFIKOAK**

Kriptografiaren historian bitxikeria eta pertsonaia berezi asko daude. David Kahn-ek «The Codebreakers» (MacMillan 1967) izeneko liburuan Thomas Jefferson Beale-rena kontatzen du, beste istorio batzuekin batera. Pertsonaia horrek 1821. urtean bidaia arriskutsu bat hasi zuen. Irten aurretik, bere apopilo Robert Morris-i bi dokumentu zifratu utzi zizkion, baldintza bakarrarekin: bera desagertzen bazen irekitzea. Morrisek 20 urte pasa ondoren ireki zituen. Lagun batzuekin batera, bigarren testua deskodetu zuen: 1 eta 1322 bitarteko zenbakien sekuentzia bat zen eta Independentzia Adierazpenari zegokion. Zenbaki bakoitzaren lekuan Adierazpenaren hitzen hasierako letra jarriz, altxor baten deskribapena zegoen: tona bat eta erdi urre, bi eta erdi zilar eta bitxi asko. Altxorra zegoen tokia lehenengo testuan zegoen markartuta. Lehenengo testu hau 520 zenbakiz osatuta dago, 1 eta 2906 bitartekoak, baina inork ez du aurkitu zein dokumentutan dagoen oinarrituta, mezua deskodetzeko. Mende bat eta erdiz saiatu dira Estatu Batuetako Konstituzioarekin eta Bibliarekin erlazionatzen, beste testuen artean, eta ordenagailu bidezko analisi garestiak egin dira inolako emaitzarik gabe.

Agian txantxa bat besterik ez da, baina badaezpada, hemen daude 520 zenbakiok.

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975, 14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 458, 604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 4866, 225 401, 370, 11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500, 538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283, 118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21, 24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131, 160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62, 116, 97, 10, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568, 614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4, 30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461, 44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38,

416, 89, 71, 216, 728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5, 81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86, 36, 219, 320, 829, 840, 68, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985, 233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62, 194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895, 10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62, 31, 501, 823, 216, 280, 34, 24, 250, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31, 86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216, 548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56, 216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617, 84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 36, 261, 543, 897, 624, 18, 212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88, 612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132, 40, 102, 34, 858, 975, 1101, 84, 16, 97, 23, 16, 81, 122, 324, 403, 912, 814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84, 221, 736, 820, 214, 11, 60, 760.

BIBLIOGRAFIA

[1] CABALLERO GIL, P., *Introducción a la Criptografí a*, RA-MA, 1996.
[2] MENEZES, A., VAN OORSCHOT, P. eta VANSTONE, S., *Handbook of Applied Cryptography*, CRC Press, 1996.
[3] MUNUERA, C. eta Tena, J., *Codificación de la Información*, Universidad de Valladolid, 1987.
[4] http://www.kriptopolis.com web orria.