Olga Oleinik

Oleinik va obtenir resultats fonamentals i extremadament originals en aquest camp, escrivint fins a 350 articles i 8 llibres, a més de supervisar 50 tesis doctorals en la seva especialitat: les equacions amb derivades parcials. Quan va morir el seu mentor, va prendre el relleu i va ser assignada com a directora del Departament d'Equacions Diferencials de la Universitat Estatal de Moscou. Malgrat les dificultats i restriccions imposades per la Guerra Freda durant els anys 70 i 80, Oleinik va impulsar la cooperació científica entre Orient i Occident, que va tenir com a resultat la Teoria de l'Homogeneïtzació, la qual estudia com resoldre problemes en què apareixen, simultàniament, diverses escales de mida. Durant tota la seva carrera, Oleinik va organitzar una xarxa d'investigadors matemàtics per tot el món, i va protagonitzar molts intercanvis entre la Unió Soviètica i Occident, desafiant les convencions de l'època i dedicant gran part de la seva vida a promoure la pau.

Aquestes són algunes de les trajectòries que el programa *Musimáticas* ha donat a conèixer, demostrant que, malgrat les dificultats, tenim molts models científics femenins que s'han de continuar potenciant. Esperem que, ben aviat, totes elles siguin vox populi. Però, fins a que no arribi aquest dia, queda molta feina a fer.

Referències

[1] Bolívar, J. (2018) Científicas. Córdoba: Guadalmazán.

[2] Dodig-Crnkovic, G. (2001) History of Computer Science. Västerås: Mälardalen University.

[3] Muñoz Páez, A. (2017) Sabias: La cara oculta de la ciencia. Barcelona: Penguin Random House.

[4] Péter, R. ([1943] 2010) Playing with Infinity: Mathematical Explorations and Excursions. New York: Dover.

[5] Rhodes, R. (2011) Hedy's Folly: The Life and Breakthrough Inventions of Hedy Lamarr. New York: Vintage.

[6] Turing, A. M. (1950) Computing Machinery and Intelligence. Mind, 49, pp. 433-460.

Parlem de llibres

La criptografia que et cal saber, de Cristina Pérez i Jordi Herrera

Redacció de la SCM/Notícies

Us presentem un llibre publicat per Sant Jordi 2023, que els autors van publicar en obert al web `https://criptografia.cat/`.

En parlem amb els autors, professors a la UAB. Ambdós treballen en temes de criptografia i seguretat, que tenen una forta base matemàtica.

Cristina Pérez és enginyera Informàtica de formació i actualment professora agregada al Departament d'Enginyeria de la Informació i les Comunicacions de la UAB, on du a terme tant recerca com docència en l'àmbit de la privadesa i la seguretat de les dades.

Jordi Herrera també és professor agregat al mateix departament i, és llicenciat en matemàtiques, tot i que la seva trajectòria tant docent com de recerca sempre ha transitat pels camins de la informàtica i la telemàtica, concretament en temes relacionats amb la criptografia i la seguretat de la informació.

Títol: *La criptografia que et cal saber*

Autors: Cristina Pérez Solà, Jordi Herrera Joancomartí

Com sorgeix la idea d'escriure el llibre?

Jordi: La idea d'escriure un llibre de criptografia en català ja feia molt temps que ens rondava pel cap. Al llarg dels anys havíem escrit els materials de l'assignatura de Criptografia de la UOC i també materials d'altres assignatures on la criptografia hi era present. Volíem compilar tots aquests continguts, i alguns de nous, en un sol llibre.

Què hi trobarem al llibre?

Cristina: El llibre té com a objectiu ser un manual de referència de criptografia en català i per això s'hi presenten un gran ventall de temàtiques relacionades amb la criptografia, que van des de definicions molt simples i efemèrides històriques fins a conceptes força complexos que inclouen protocols i eines criptogràfiques d'última generació.

En els primers capítols s'hi presenta un breu repàs històric de la criptografia així com algunes definicions molt bàsiques tant de conceptes criptogràfics com de matemàtics.

Posteriorment, es passen a descriure els criptosistemes de clau simètrica, explicant les dues grans famílies: les xifres de flux i les xifres de bloc, per acabar parlant d'una eina criptogràfica àmpliament utilitzada actualment en múltiples aplicacions: les funcions hash.

La següent part del llibre està dedicada a la criptografia de clau pública, i en aquest apartat s'expliquen algunes de les xifres més utilitzades així com els esquemes de signatura digital i les seves propietats. També, en aquesta part, expliquem les infraestructures de clau pública, que inclouen totes les tècniques necessàries perquè la criptografia de clau pública es pugui utilitzar a la pràctica.

Després d'aquesta part, el llibre presenta dos capítols d'una complexitat més elevada, que introdueixen les corbes el·líptiques i els pairings, tot explicant com aquestes eines matemàtiques s'utilitzen per obtenir sistemes criptogràfics més eficients.

Finalment, l'últim capítol del llibre està dedicat als protocols criptogràfics i s'hi inclouen un conjunt de protocols que permeten copsar la varietat d'aplicacions en què es pot utilitzar la criptografia, més enllà de les dues més conegudes, el xifrat i la signatura de missatges.

A quin públic va dirigit?

Cristina: El llibre va dirigit a un públic força ampli, tot i que per a entendre alguns dels conceptes que s'hi presenten es pressuposa que el lector té una bona base tècnica i, per tant, és titulat en algun grau en informàtica, telecomunicacions, física o matemàtiques.

Jordi: D'altra banda, el títol del llibre també vol ser provocador. Amb aquest títol, intentem interpel·lar el possible lector de la necessitat de conèixer i entendre els diferents conceptes criptogràfics que s'hi presenten. En una societat cada vegada més digitalitzada i alhora més intervencionista per part dels estats i les grans corporacions, la criptografia pot ser l'última eina de protecció de l'individu.

Hi trobarem molta matemàtica?

Jordi: Efectivament, tractant-se d'un llibre de criptografia, al llarg dels seus capítols es van tocant diferents conceptes matemàtics. No obstant això, no és un llibre pensat únicament per a matemàtics i, per tant, hem fugit una mica dels formalismes i les demostracions que podrien distreure els lectors amb menys bagatge en aquest camp. Per exemple, el matemàtic que

faci una ullada al segon capítol de "Fonaments matemàtics" potser el trobarà massa superficial i poc rigorós, però la idea darrere de la presentació dels continguts en aquest format és que sigui accessible a un públic el més ampli possible i que, aquesta base matemàtica de la criptografia no desmotivi, sinó que engresqui a continuar-ne aprenent. De fet, creiem que aquest capítol de fonaments matemàtics és del tot assequible fins i tot per a estudiants de batxillerat. Val a dir, però, que a mesura que van avançant els capítols, els conceptes es van complicant i els continguts presentats en els capítols de "Corbes el·líptiques" i el de "Criptografia basada en pairings" presenten una complexitat notable. Volem remarcar, també, que l'enfocament que fem d'aquests temes en aquests capítols és més d'enginyeria que matemàtic, perquè és el gruix del que creiem que seran els nostres potencials lectors. De tota manera, tots els capítols del llibre incorporen una secció de bibliografia on, aquí sí, hem intentat incloure textos amb diferents enfocaments, des dels més aplicats fins als més formals.

Per què l'heu publicat en obert?

Cristina: Com a professors universitaris, part de la nostra tasca és ajudar a la difusió del coneixement a la societat i, avui dia, creiem que la manera més efectiva de fer-ho és penjant de forma lliure els continguts a través d'internet per tal que tothom qui vulgui pugui accedir-hi lliurement. A més, el fet de publicar el llibre directament nosaltres sense cap intermediari ni procés editorial ens permet una flexibilitat molt gran a l'hora d'actualitzar i afegir continguts. Aquest punt ens semblava de gran importància, ja que en aquest àmbit en concret apareixen constantment nous protocols i noves tècniques de protecció de la informació que és interessant poder incloure en el llibre.

Per tant, en veurem més edicions?

Jordi: Aquesta és la intenció! Ja tenim un llistat d'alguns dels temes que ens agradaria afegir. Ara "només" ens falta temps per fer-ho. De fet, hem tingut cura en etiquetar bé el contingut d'aquesta edició i cada pàgina del pdf té el codi que n'identifica la versió. A més, a l'inici del llibre hi ha una pàgina amb una taula amb l'històric de versions i els canvis que s'hi han anat introduint, de manera que el lector pugui identificar sempre quina versió del llibre està consultant i mirar a la web si aquesta és l'última disponible.

Gràcies per la vostra col·laboració!

Noves col·laboracions

Invitació

Us agrada escriure? Us agrada llegir? Sou dels que descobriu matemàtiques a tot arreu?

Animeu-vos a compartir amb els socis de la SCM i la comunitat matemàtica els vostres escrits. Ens podeu fer arribar ressenyes de llibres, obres de teatre o pel·lícules en relació a les matemàtiques.

En aquesta part, es publiquen aportacions que mostrin les matemàtiques arreu, que relacionin les matemàtiques amb l'art, el món de l'empresa o la indústria, o fins i tot la llengua. També en relació amb aquests temes s'hi publiquen, a mena de píndoles, recursos de Geogebra i de programari divers.

Esperem les vostres col·laboracions. Correu de contacte: scm.noticies@correu.iec.cat.