

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.