LA VANGUARDIA
TARRAGONA

EDITA: La Vanguardia Ediciones, SL.
Redacció: Diagonal, 477, 7è (08036) Barcelona
Tel.: 93 481 22 00

REDACCIÓ TARRAGONA: Sara Sans. Tel.: 977 25 54 00

ANUNCIS: Publipress Media, SLU.
C/ Méndez Núñez, 2, 1r 1a (43004) Tarragona
Tel.: 977 240 136 / 977 243 570. Fax: 977 213 237

Nascut a Sabadell l'any 1965, sóc veí de Vilanova i la Geltrú i catedràtic de Ciència de la Computació a la Universitat Rovira i Virgili a Tarragona. Recentment he pronunciat una conferència al CaixaFòrum de Tarragona sobre l'origen històric i les utiltats actuals de la criptografia o escriptura xifrada

"Tenir un virus a l'ordinador és com tenir la casa plena de micròfons"

VICENÇ LLURBA

Josep Domingo, *catedràtic de Ciència de la Computació*

A nem a pams: què és la criptografia?
La criptografia, històricament, ha estat l'art de l'escriptura xifrada, d'ocultar els missatges. Un seguit de tècniques que, al llarg dels segles, molt sovint s'han fet servir militarment.

Des de quan?
Se sap que els espartans, cinc segles abans de Crist, ja en feien anar. I també sabem que Juli Cèsar utilitzava criptografia.

I com funcionava?
Per exemple, utilitzaven la substitució de lletres, atorgant-los un altre valor d'acord amb una lògica preestablerta. Així, suposem que a una lletra qualsevol li dónes el valor de dos lletres més a la dreta a l'abecedari... Segons això, la lletra a passa a ser la c i així successivament.

Vol dir que la a es llegeix com a c, la b com a d, la c com a e, la d com a f...
Exactament. Si no coneixes aquesta regla, per simple que sembli, tu no pots desxifrar el missatge.

Avui dia, però, la criptografia no és tan sols això.
No. Avui dia la criptografia, a banda de fer confidencial les informacions que siguin, el que busca és garantir la seva seguretat i la seva autenticitat. És a dir, la criptografia també permet garantir que una informació o un document no han estat ni retallats ni modificats ni alterats.

I com es fa, això?
En bona mesura, avui dia és possible gràcies a la signatura digital, que va aparéixer ara fa uns 34 anys.

34 anys!!
Sí, és tan vella com la Constitució espanyola... La idea va sorgir el 1976 i la seva primera aplicació pràctica és del 1978.

I ja es feia servir, als setanta, la signatura digital?
Molt poc, tan sols en alguns cercles diplomàtics i militars. La signatura digital, com és lògic, no es generalitza fins que no es popularitza internet.

La signatura digital és la part més visible de la criptografia digital?
Potser sí, però tan sols perquè la gent no és conscient de com funcionen alguns aparells que fa anar quotidianament.

Com ara?
El telèfon mòbil, per exemple. Qualsevol aparell de telefonia mòbil xifra les veus per transmetre-les amb seguretat.

Com ho diu, això?
Que el seu mòbil transforma la seva veu en una tira de zeros i uns que, abans de ser enviats a la central telefònica més propera, són xifrats en sumar-los-hi aleatoriament altres zeros i uns.

Un mòbil codifica binàriament la meva veu?
Sí... I en arribar a la central, la tira de zeros i uns que ha estat enviada xifradament és desxifrada i torna a reaparèixer la veu de la trucada.

I per què ho fan, això?
Perquè si no es codifiquessin el missatges, qualsevol persona que interceptés la freqüència del seu telèfon, podria interceptar les converses.

M'està dient que s'usa encriptació en cada trucada de telefonia mòbil?
Sí. Els únics mòbils que no encriptaven les converses eren els de primera generació. ¿Recorda que als anys vuitanta es van interceptar converses telefòniques del socialista Txiki Benegas en què parlava de Felipe González com a *Dios*?

I tant! Va ser un escàndol polític.
Allò li va passar a Txiki Benegas perquè els mòbils analògics d'aquella època no encriptaven els missatges. Eren molt fàcils d'interceptar, cosa que era un xollo pels espies i els periodistes.

Més exemples
N'hi ha molts. Cada cop que introduïm una contrassenya o el número de la nostra targeta de crèdit en una operació bancària o en una compra per internet, també hi ha encriptació.

Sempre?
Sempre que sigui un lloc segur, cosa que es pot saber fixant-se en el navegador: si dalt de tot hi apareix https en comptes de http, això vol dir que tots els missatges s'encripten per tal que només l'entitat bancària, per exemple, pugui desxifrar-los.

Què passa quan jo entro una contrasenya?
Que automàticament es codifica i que, en cas de ser interceptada, no pot ser desxifrada. Si no es fes això, la seva contrasenya viatjaria per la xarxa i podria ser interceptada per qualsevol.

I això és tan segur?
Sí, sempre que es donin dos requisits. El primer, que la pàgina sigui https. I el segon, que no tinguis cap virus a l'ordinador.

Què tenen a veure els virus amb això?
Tenir un virus a l'ordinador és com tenir la casa plena de micròfons. Si tens virus, no pots saber quin ús pot estar fent algú de la teva informació.

TONI ORENSANZ