Iniciació a la Criptografia

Artur Travesa

(versió 2024-07)

Introducció

El conjunt d'aquestes notes només s'hauria d'interpretar com un "Curs elemental d'*iniciació* a la Criptografia", i remarco els dos sintagmes *elemental* i *d'iniciació*. Està pensat per a estudiants de nivell d'un primer curs universitari.

Efectivament, un "Curs de Criptografia", fins i tot un "Curs elemental de Criptografia", s'hauria d'encabir en espais més amplis de coneixements que haurien d'incloure, probablement, parts de teoria de la comunicació, de complexitat algorítmica o computacional, d'aprenentatge automàtic, o d'estudi de teories de compartició de secrets, entre d'altres.

L'origen de les notes es remunta a diferents cursos d'Aritmètica o de (iniciació a la) Criptografia que he desenvolupat per a estudiants de Matemàtiques o d'Informàtica a la Universitat de Barcelona. El resultat és conseqüència d'una reflexió sobre com fer accessibles uns continguts bàsics que, d'una banda, es puguin presentar acompanyats d'exemples no trivials, i, alhora, puguin ser útils com a inici per a un estudi més profund de Criptografia o, també, endinsar-se en la comprensió d'altres criptosistemes pràctics d'ús habitual.

El format que he triat per a la presentació d'aquestes notes és "una llibreta de *SageMath* per a cada capítol". N'esmentaré dues raons.

Primerament, aquest programari permet desenvolupar càlculs no trivials de manera prou senzilla i entenedora i, a més a més, és d'accés lliure per a tothom interessat i funciona en plataformes també d'accés lliure.

I en segon lloc, permet fer una presentació prou agradable del material escrit; en particular, la possibilitat d'intercalar els càlculs dins del text de manera natural en fan una bona eina comunicativa i, alhora, facilita molt el càlcul d'exemples no trivials.

A fi de veure tot el contingut de cada llibreta, convé executar-la. Això es pot fer de cop o bé, i així és més recomanable, cel·la a cel·la a mesura que s'avança en la lectura i la comprensió dels diferents continguts. I a fi de facilitar la seva lectura i, més important, el seu ús, a l'inici de cada capítol s'incorporen les funcions necessàries de capítols anteriors. Això fa innecessari tornar a programar-les cada vegada que es necessiten.

Convencions

Utilitzarem la convenció, habitual en Matemàtiques tot i que no és l'única que es fa servir, que el primer nombre natural és el zero, 0, el segon, l'u, 1, etcètera. En particular, això es reflecteix en el fet que el primer capítol és el capítol 0 i, anàlogament, la primera secció del capítol 0 és la secció 0.0; i el primer apèndix és l'apèndix 0.

Aquesta també és la convenció habitual de *SageMath* que, per exemple, numera els elements d'una llista, o els components d'un vector, o els caràcters d'una tira, a partir del 0-èsim. Caldrà tenir-ho present a l'hora de programar els diferents exemples.

En particular, usualment considerarem els intervals d'extrems a i b con els intervals tancats en a i oberts en b; és a dir, per a nombres a i b, $a < b$, l'interval d'extrems a i b contindrà els nombres x tals que $a \leq x < b$ (i, iusualment, només els nombres enters d'aquest interval). Per exemple, l'interval unitat, d'extrems 0 i 1, conté 0 però no conté 1.

Què entendrem per Criptografia?

És habitual entendre per Criptografia la disciplina que estudia l'intercanvi d'informació de manera que només l'entitat emissora i la destinatària (que no cal confondre amb la receptora) puguin conèixer aquesta informació. Probablement, aquest estudi hauria de ser anomenat *Criptologia* i hauríem de reservar l'expressió *Criptografia* per a la transmissió de missatges xifrats; és a dir, per a l'escriptura, l'enviament, la recepció i la lectura de missatges xifrats, més que no pas per a la disciplina que ho estudia. Però com que *Criptologia* encara no apareix al diccionari de l'Institut d'Estudis Catalans, utilitzarem el mot habitual, *Criptografia*, també per a referir-nos a la ciència.

Així, doncs, en aquest estudi caldrà tenir en compte alguns actors importants. D'una banda, l'emissor del missatge; d'altra banda, el destinatari del missatge; i en tercer lloc, i molt important, els possibles receptors o interceptors del missatge. I encara cal tenir en compte altres possibles actors, sovint atacants actius, que intentin fer-se passar per l'emissor o pel destinatari del missatge a fi d'obtenir la informació confidencial.

Difícilment es podria estudiar criptografia científicament si no poguéssim manipular els missatges d'una manera coherent, mesurar el grau de dificultat dels processos de xifratge i de desxifratge dels missatges, o disposar d'eines per a construir (o destruir) criptosistemes cada cop més robustos. A fi de mostrar la potència de les matemàtiques i, en particular, de l'Aritmètica, en aquestes qüestions, començarem amb un estudi elemental dels criptosistemes clàssics, i veurem que podem permetre'ns assegurar que la majoria d'aquests criptosistemes clàssics són molt febles. De fet, això fa que cap d'ells no sigui emprat en l'actualitat sense una modificació profunda. Més endavant veurem altres criptosistemes que encara es fan servir de manera habitual en el moment d'escriure aquestes notes, però que segurament deixaran de ser-ho en un futur més o menys proper, probablement substituïts per criptosistemes quàntics. Però no ens avancem en el temps, ni en aconteixements (futurs?).

Contingut

Fi de la introducció