Els salvadors d'Europa

Extreta de teringa.net

Corria l'any 1943, plena II Guerra Mundial. El capità Dean Watson estava atemorit. La invasió nazi era immediata. Corria el rumor que la Wehrmacht preparava un atac aeri per debilitar la Gran Bretanya. El capità coneixia l'enemic. Els alemanys disposaven de les noves Junker Ju, avionetes molt ràpides, àgils i potents, en res comparables amb les avionetes antigues que els britànics tenien a l'abast. La RAF (Real Aereal Force) no s'havia modernitzat. La Gran Bretanya no s'havia recuperat encara del crac del 29 i tenia la mateixa tecnologia aèria que feia 15 anys. El capità estava en aquells moments preparant la defensa a Bletchley Park, una ciutat estratègica. Es donava per suposat que els nazis intentarien bombardejar el cor de la Gran Bretanya, Londres. Aquesta era la seva ciutat natal, el lloc on vivien gran part dels seus familiars i on normalment treballava, així que havia de fer el possible per protegir-la.

Des de la mansió de Bletchley Park es planejava la defensa. L'estratègia encara no estava ben definida. La flota aèria nazi era 3 cops superior a la britànica en nombre i, infinitament superior en armament. En menys d'un mes la RAF hauria quedat destrossada i no hi hauria res que impedís que Londres fos bombardejada fins convertir-se en cendres.

D'altra banda, existia la rendició. El capità n'era partidari. Amb 60 anys i una gran família amb molt jovent, preferia viure sense certs privilegis que no pas més morts de les que ja havia vist. En els seus anys com a tinent havia servit l'exèrcit a Uganda, lloc on havia presenciat vertaderes massacres que encara li treien el son algunes nits d'estiu. El problema era que el President, Winston Churchill, acabava d'anunciar una resistència a ultrança. Si el Regne Unit acabava caient, la venjança per part dels alemanys seria molt cruel. Calia doncs, guanyar la batalla.

El capità sabia que la RAF només aguantaria l'ofensiva nazi com a molt un mes i se sospitava que l'atac es produiria en menys de dues setmanes. Calia doncs, pensar en una alternativa.

S'havia passat tota la tarda a la butaca del menjador, fumant uns puros cubans que guardava per comptades ocasions, amb la mirada perduda entre el fum. La tarda havia portat en si una allau d' idees. Havia pensat en realitzar un contraatac. Vendre la seguretat de Londres per atacar per sorpresa l'enemic, però, era ja massa tard per això. Havia pensat en una rendició pactada, però sabia que el President no l'acceptaria. En un moment de lucidesa va pensar d'infiltrar-se en els serveis de comunicació nazis. No de la manera habitual, a través d'espies, sinó intentant captar i interpretar les ones de ràdio per les quals es comunicaven les ordres del Reich a la Wehrmacht.

Captar les ones era quelcom realment senzill, fins i tot per l'abatuda Anglaterra. Només calia una parabòlica suficientment gran per captar els senyals de ràdio que provenien d'Alemanya. El problema venia després. Tot missatge que s'enviava i es rebia anava encriptat i era completament necessari conèixer el patró d'encriptació per entendre'l.

D'aquesta manera el capità es disposà a entregar noves ordres als serveis secrets britànics. Aquests però, que dominen més el tema que en Dean, li dirien que qualsevol intent d'accedir a aquests missatges era en va. Així que, el capità, com a últim recurs, optaria per anar a la Univeristat de Cambridge, dotada de gran reconeixement acadèmic, per a lliurar els codis als membres de la universitat, no fos dit que ell no hi va posar de la seva part.

Quan el capità entra a la classe, ningú s'immuta. Tots observen atents el professor. Aquest gaudeix d'un gran respecte per part dels alumnes. És d'aquelles persones a qui admirar. Busca la mirada innocent dels joves amb intensitat, mentre descriu un somriure gairebé inapreciable. Es mou lentament per la classe, combinant mirades als alumnes i mirades perdudes a un semihoritzó cercant el toc de magnificència que pretén transmetre. Parla un llenguatge fluid i alhora extremadament tècnic. No alça la veu, no li és necessari. Mostra una profunda passió pel que ensenya i, per la manera com s'explica, denota un coneixement absolut de la matèria. Domina en tot moment la classe i els seus alumnes. Passa ara a escriure una sèrie de números a la pissarra:

1 / 5 / 19 / 49 / 101 / 181

Els demana que en trobin el patró. Passen menys de dos minuts quan un jove enuncia la següent conjectura: La diferència de la diferència de la diferència entre dos nombres consecutius és 6. Això és particularment diferent a una progressió aritmètica, i els explica l'anomenat mètode de diferències, per la qual, si una de les diferències esdevé constant, significa que la sèrie té forma general caracteritzable amb un polinomi. Acaba la classe i el professor dóna un parell més de successions als seus alumnes. Tots comencen a comentar entre ells quina és la solució. S'aprecien les ganes d'aprendre, la competitivitat que mantenen, tots volen ser el primer a trobar-ne la solució.

El capità s'acosta i es presenta cordialment al professor. Aquest es fa anomenar Alan Turing. Ronda pel Regne Unit que un tal Turing està revolucionant el naixent món de la informàtica a través de tècniques com la criptoanàlisi i, donat el que acaba de veure, està més que segur que és ell. El capità li explica el seu problema i aquest no tan sols accepta ajudar-lo, sinó que s'hi posa a treballar de forma

immediata, com si fos quelcom que estigués esperant. Sembla un nen al qui li acaben de regalar la joguina que porta temps demanant. Escriu les seqüències de codi a la pissarra de la paret que sense exagerar mesura més de 10 metres de llargada per 3 d'alçada. El guix flueix entre seus dits. Escriu els números amb el cor. El fet de deixar escrita l'essència del nombre no és un simple fet. És en certa manera, l'alliberament de la seva ànima, que ansia poder expressar allò que per ell ho és tot, el què tot ho representa, el que tot ho abarca. Els números són els seus amics i els tracta amb suma cautela. Els moviments són ràpids, forts i consistents, assaborint la naturalesa del poder que li és concedit en poder entendre la natura a través dels nombres. Al cap de 10 minuts ha escrit tota la seqüència de nombres del primer paràgraf. Té una escriptura corbada i molt marcada, com si escrivís en un pergamí. Tot és tosc, els números es mesclen entre si degut a les fortes corbes a les que són sotmesos. Allà on hi veig el caos ell hi veu la veritat.

(Dins de la ment de l'Alan Turing)

Col·loco tots els números com si entressin en un eix de coordenades. Deu números i els següents salten a la fila de dalt. És el més probable, tenint en compte que segurament estan xifrats en sistema decimal o binari, i veient que hi ha altres números més grans que dos; és el més probable. Aviam, algún patró, repeticions, irregularitats...
Miro els primers nombres. Algun que es repeteixi més, seqüències estranyes, números especials, notació matemàtico/informàtica particular, seqüències diferents... Espera! Seqüències diferents! Com puc ser tant ingenu per pensar que tots els números seguiran el mateix patró? Segur que hi ha diferents pautes entre aquests. Potser les seqüències venen en funció de si el número és parell o no, de si aquest és primer o no, poden venir en funció de moltíssimes coses. No les puc provar totes. Si fos el cap d'informàtica dels serveis secrets alemanys què faria...? El temps d'encriptació necessari repercuteix directament en el temps de desencriptació. Això significa que si volgués encriptar un missatge amb un patró complicadíssim, el temps per traduir aquest missatge a llenguatge estàndard seria més lent, cosa que dificulta la comunicació a temps real. Això descarta directament que la seqüència vingui donada en funció de si el nombre és primer o no, ja que l'algorisme per factoritzar un número en els seus factors primers és extremadament lent i ineficaç a temps real. Tenint en compte el temps d'execució, separar

seqüències en funció de si el nombre és parell o no, és extremadament ràpid. Com que per algun lloc he de començar, separo els números del codi en funció del lloc que ocupen, parells cap a un lloc i imparells cap a l'altre. D'aquesta manera la seqüència original queda dividida en dues subseqüències. Aquestes dues segurament estaran relacionades entre si, fent d'aquesta manera més difícil la desencriptació del missatge original.

Fins aquí ha arribat la meva aportació. Ara hauria de començar a realitzar milers de comprovacions i els humans som extremadament ineficaços realitzant aquestes operacions. Per això es va crear la màquina "Typex". Aquesta és l'equivalent a la més coneguda "Enigma" alemanya. Són màquines capaces de realitzar milers de comprovacions de caire matemàtic a velocitats infinitament superiors a la dels humans. Engego la màquina, passo les dues seqüències de codi i deixo que aquesta es posi a treballar. Mentrestant segueixo buscant. Busco ara, la forma que té la seqüència. Té pinta més aviat a recurrència. El codi no sembla ser del tot aleatori. Si el patró pel qual s'ha encriptat el missatge seguís una fórmula explícita, s'hauríen assegurat que aquesta tingués la pinta més aleatòria possible. Per exemple, la fórmula que vaig inventar per generar nombres aleatoris és:

$x_n = \frac{3{x_n}^2+7x_n}{x_n^2+3} \pmod{100}$

Aquesta fórmula dóna números pseudoaleatoris ja que, encara que la distribuició de x_n sembli aleàtoria veiem que segueix una fórmula tancada. El codi aquest, però, no acabava de tenir una forma explícitament aleatòria. Ni de bon tros sé quin patró existeix, però la experiència em diu que alguna cosa està lligada aquí. Passen dues hores quan la màquina treu quelcom. Aquesta afirma que: $x_{n+1} = \frac{x_n+y_n}{2}$ i que

$$2^n\sqrt{y_n^2-x_n^2} = \sqrt{y_0^2-x_0^2} \Rightarrow 2\sqrt{y_{n+1}^2-x_{n+1}^2} = \sqrt{y_n^2-x_n^2} \Rightarrow y_{n+1}^2-x_{n+1}^2 = \frac{y_n^2-x_n^2}{4}.$$

Bingo! Sabem que existeix una relació entre les dues subseqüències, però a partir de la informació que hem deduït és encara impossible establir una fórmula, ja sigui explícita o recurrent. Eps, espera... La màquina ha trobat una altra relació. Ens diu que:

$2^n \arccos\frac{x_n}{y_n} = \arccos\frac{x_0}{y_0}$. Què?! Això sí que no m'ho esperava. Trobar un invariant amb un cosinus pel mig. El primer cop que ho veig en tota la meva carrera. Això implica en si que aquesta seqüència pot tenir un marcat caràcter geomètric. Potser distribuint bé les seqüències al pla cartesià veuria que tots els números compleixen una relació, o potser no. Potser és fruit de l'atzar, vés a saber. Seguiré treballant, tinc un punt de suport. Faré un canvi de variable $\frac{x_n}{y_n} = \cos\alpha_n$. Aquest és possible ja que empíricament constata que els y_n són sempre més grans que els respectius x_n, donant així sempre uns

quocients entre el 0 i l'1. Així queda que:

$$2^n \arccos \frac{x_n}{y_n} = \arccos \frac{x_0}{y_0}$$

$$2^n \arccos\cos \alpha_n = \arccos\cos \alpha_0.$$

$$2^n \alpha_n = \alpha_0 \Rightarrow \alpha_n = \frac{\alpha_0}{2^n} \Rightarrow \alpha_{n+1} = \frac{\alpha_n}{2} \Rightarrow \cos \alpha_{n+1} = \cos \frac{\alpha_n}{2}.$$

Recorda però la identitat de $\cos\frac{\alpha}{2}$ per la qual $\cos\frac{\alpha}{2} = \pm\sqrt{\frac{1+\cos\alpha}{2}}$. Agafem la positiva ja que empíricament la màquina ha verificat que tant x_n com y_n són positius, cosa que significa que les seves raons trigonomètriques es troben al primer quadrant i són positives. Així doncs tenim, $\cos\alpha_{n+1} = \cos\frac{a_n}{2} = \sqrt{\frac{1+\cos\alpha_n}{2}}$ Desfent el canvi de variable d'abans, on $\frac{x_{n+1}}{y_{n+1}} = \cos\alpha_{n+1}$, arribem que, $\frac{x_{n+1}}{y_{n+1}} = \sqrt{\frac{1+\frac{x_n}{y_n}}{2}}$

Tenint en compte que $x_{n+1} = \frac{x_n+y_n}{2}$, simplificant l'experssió arriba a que:

$$\frac{x_{n+1}}{y_{n+1}} = \sqrt{\frac{1+\frac{x_n}{y_n}}{2}} = \sqrt{\frac{x_n+y_n}{2y_n}} = \sqrt{\frac{2x_{n+1}}{2y_n}} = \sqrt{\frac{x_{n+1}}{y_n}}.$$

$$\frac{x_{n+1}}{y_{n+1}} = \sqrt{\frac{x_{n+1}}{y_n}} \Rightarrow y_{n+1} = \sqrt{x_{n+1}y_n}.$$

D'aquesta manera he trobat dues fórmules recursives que ens donen quin serà cada terme $n+1$ en funció de l'anterior.

$x_{n+1} = \frac{x_n+y_n}{2}$ i $y_{n+1} = \sqrt{y_n x_{n+1}}$. Ara a partir d'aquestes fòrmules i sabent x_1 i y_1, puc executar en una computadora tots els valors que aquesta prendrà. És a dir, sóc capaç de transcriure els missatges. Ara la questió és desxifrar la bijecció entre els números i les lletres, per la qual a cada valor numèric li correspon una lletra.

Una de les claus a l'hora de buscar aquesta bijecció, és buscar els números que es repeteixen més, ja que probablement aquests es referiran a les vocals "a" i "e". Primer de tot m'adono que els números són bastant més grans que el nombre de lletres de l'abecedari, cosa que em porta a preguntar-me a quins vocables es refereixen aquests nombres. Passo una bona estona observant números quan m'adono que hi ha un conjunt que es repeteix més que els altres. Aquests són l'1 el 28, 55, 82, etc...és a dir, la progressió aritmètica de primer terme 1 i diferència 27 i, els números 5, 32, 59, 86, progressió airtmètica de primer terme 5 i raó 27. A la primera successió, cada terme ve donat per la fórmula tancada $1 + 27(n-1)$ i la segona $5 + 27(n-1)$; si em fixo en els residus que aquests deixen dividits

per 27, número de lletres de l'alfabet, aquests són 1 i 5, que corresponen, per posició, als vocables "a" i "e". Això em permet conjecturar que la successió $x_n \pmod{27}$, és a dir la seqüència formada en agafar el residu de cada terme quan x_n és divitdit per 27, estableix la bijecció directa entre números i lletres, on cada número representa el lloc de la lletra dins l'alfabet. Això implicaria que la successió y_n és una seqüència auxiliar. La seva raó de ser és permetre que x_n prengui els valors desitjats. El fet que qualsevol misstage pot ser traduit utilitzant el patró establert és extremadament tècnic tenint en compte el nostre nivell, però cert. Tradueixo les primeres línies de codi, tot té sentit. Els números passen a cobrar significat verbal. Acabo de desxifrar els codis nazis, cosa que implica en si, que segurament he salvat Anglaterra d'una de les pitjors massacres. Ara només queda programar una màquina perquè desxifri el senyals que envia el Reich a temps real. D'aquesta manera podrem interpretar totes les ordres, instructions i senyals instantàniament, avançant-nos als passos de l'enemic.

(Sortim de la ment de l'Alan)

El capità està mig adormit. Porta 8 hores veient com un home comprova sense parar seqüències de codi, sense aparent moviment, sense menjar, ni sense anar al lavabo. Sent en part una profunda admiració per aquest noi. S'ha de tenir valor per enfrontar-te tu sol al que probablement uns serveis secrets han planejat durant mesos. El capità es pren ja el tercer café de la tarda. De sobte, l'Alan baixa els braços, agafa aire i deixa anar unes paraules com aquell qui no vol. "Ho tinc", diu. El capità el mira amb una mescla d' il·lusió i desconfiança. L'Alan passa 30 minuts explicant-li tot el procés. El capità es perd a les primeres de canvi, però segueix escoltant tota l'estona; la il·lusió pesa més que la ignorància. Quan acaba l'explicació, torna a casa. Un lleuger somriure i una profunda admiració per aquell jove l'acompanyen. Acaben de salvar Anglaterra.

Anys més tard, l'Alan seria perseguit per l'exèrcit per una suposada homosexualitat. L'home que va salvar Anglaterra era més tard jutjat per la mateixa, fins arribar al punt del suïcidi l'any 1954 (41 anys). A títol individual queden les reflexions davant els principis ètics que governen la societat.