EllagoEdiciones

Descodificando el universo

Charles Seife

Traducción de Rosa Agost Canós

EllagoEdiciones · Colección ***Las Islas***

Edición a cargo de Francisco Villegas Belmonte

Colección ***Las Islas***

Título original: Decoding the universe

Primera edición, septiembre 2009

Maquetación: Ramón Pais Martínez

Ellago Ediciones, S. L.
ellagoediciones@ellagoediciones.com / www.ellagoediciones.com
(Edicións do Cumio, S. A.)
A Ramalleira, 5 - 36140 Vilaboa (Pontevedra)
Tel. 986 679 035
cumio@cumio.com / www.cumio.com

ISBN: 978-84-96720-81-7
Impresión: Gráficas Lasa, S. L.
Depósito legal: C 2684 - 2009
Impreso en España

Índice general

Descodificando el universo
Cómo la nueva Ciencia de la Información nos explica todo el cosmos, desde nuestro cerebro hasta los agujeros negros

Charles Seife, autor de *Cero*

Introducción

Todo está hecho de una materia oculta.

–Ralph Waldo Emerson

La civilización está condenada.

Probablemente, esto no es lo que uno quiere leer cuando coge un libro, pero es la verdad. La humanidad –y toda la vida del universo–, se extinguirá. No importa lo avanzada que esté nuestra civilización, no importa si alcanzamos la tecnología suficiente para ir de estrella en estrella o para vivir seiscientos años; tan solo es un tiempo finito antes de que la última criatura viva del universo visible desaparezca. Las leyes de la información han decidido nuestro destino y han hecho lo propio con el destino del universo.

La palabra *información* conjura visiones de ordenadores, discos duros y superautopistas de Internet; al fin y al cabo, la introducción y

popularización de los ordenadores es conocida como la revolución de la información. Sin embargo, la ciencia computacional es solo un aspecto mínimo del macroconcepto conocido como teoría de la información. Aunque esta teoría describe, de hecho, cómo funcionan los ordenadores, es mucho, mucho más que eso. Rige el comportamiento de objetos de niveles muy distintos; nos dice como interactúan los átomos y cómo los agujeros negros se engullen a las estrellas; sus reglas explican cómo morirá el universo e iluminan la estructura de todo el cosmos. Incluso aunque no existieran los ordenadores, la teoría de la información continuaría siendo la tercera revolución del siglo XX de la física.

Las leyes de la termodinámica –las reglas que controlan el movimiento de los átomos de un pedazo de materia– son, a la postre, leyes sobre información. La teoría de la relatividad, que describe cómo se comportan los objetos a velocidades extremas y bajo la enorme influencia de la gravedad, también forma parte, en realidad, de la teoría de la información. Y lo mismo ocurre con la teoría cuántica, que gobierna el reino de las cosas diminutas. El concepto de información va mucho más allá del simple contenido de un disco duro ya que aúna todas estas teorías en una idea extraordinariamente potente.

La teoría de la información resulta tan poderosa porque la información es física. No se trata exclusivamente de un concepto abstracto, ni tampoco únicamente de hechos, representaciones, fechas o nombres. Se trata de una propiedad concreta de la materia y de la energía que es cuantificable y mensurable. Cada bit es tan real como el peso de un trozo de plomo o la energía almacenada en una cabeza nuclear; y al igual que ocurre con la masa y la energía, la información está sujeta a un conjunto de leyes físicas que dictaminan su comportamiento –cómo se manipula, transfiere, duplica, se borra o se elimina la información. Y todo en el universo obedece a las leyes de la información porque todo en el universo está determinado por la información que contiene.

La idea de la información surge en el antiguo arte de la criptografía y el criptoanálisis. Las cifras que escondían secretos de estado fueron,

de hecho, métodos para encubrir la información y transportarla de un lugar a otro. Cuando el arte del criptoanálisis se combinó con la ciencia de la termodinámica –la rama de la física que describe el funcionamiento de las máquinas, el transvase del calor y la producción del trabajo–, surgió la teoría de la información. Esta nueva teoría fue una idea tan revolucionaria como la teoría cuántica y la de la relatividad; al instante, transformó el campo de las comunicaciones y facilitó el camino a la era de la informática, pero eso solo fue el principio. En una década, físicos y biólogos comenzaron a darse cuenta de que los principios de la teoría de la información regulaban mucho más que los bits y los bytes de los ordenadores y de los códigos de comunicación: describían el comportamiento del mundo subatómico, toda la vida terrestre e incluso el universo en su totalidad.

Cada criatura de la Tierra es una criatura de información: la información está presente en cada una de nuestras células y se agita en nuestros cerebros. Sin embargo, no solo los seres vivos son capaces de manipular y procesar información. Cada partícula del universo, cada electrón, cada átomo, cada partícula aún por descubrir, contiene información –que, a menudo, nos resulta inaccesible pero que es información al fin y al cabo, y como tal puede transferirse, procesarse o desvanecerse. Cada estrella del universo, cada una de las innumerables galaxias de los cielos, está llena de información que puede escapar y viajar. Esta información fluye constantemente, se mueve de un lugar a otro y se propaga por el cosmos.

El cometido de la información es moldear el universo. El movimiento de la información puede determinar la estructura física del cosmos. La información parece estar también en el centro de las paradojas científicas más complejas, como los misterios de la relatividad y la mecánica cuántica, el origen y el destino de la vida en el universo, la naturaleza del poder destructivo más extremo de los agujeros negros y el orden oculto de un cosmos aparentemente aleatorio.

Las leyes de la información comienzan a ofrecer respuestas a algunas de las cuestiones más controvertidas de la ciencia; pero estas respuestas son, en ocasiones, más perturbadoras y extrañas que las paradojas que

resuelven. La información nos lleva a una imagen del universo que corre hacia su propio fin, el de los seres vivos como esclavos dentro de él y el de un cosmos increíblemente bizantino hecho de una gran colección de universos paralelos.

Las leyes de la información proporcionan a los físicos una vía para entender los misterios más oscuros sobre los que la humanidad haya reflexionado jamás. Ahora, estas leyes nos muestran una imagen que es tan inexorable como surrealista.

Capítulo 1
Redundancia

¡Un caballero no lee el correo de otro caballero!

–Henry L. Stimson

«AF no tiene suficiente agua». Estas cinco palabras hundieron la flota japonesa.

En la primavera de 1942, las tropas estadounidenses intentaban rehacerse de toda una serie de derrotas. La armada naval japonesa había sido superior en el Pacífico y amenazaba con acercarse cada vez más a territorio americano. Aunque la situación era calamitosa, la guerra no estaba perdida. Los criptoanalistas estadounidenses estaban a punto de utilizar un arma más poderosa que las bombas y las pistolas: la información.

Los criptoanalistas habían descifrado el JN-25, un código usado por la armada japonesa. A pesar de que se trataba de un código

extremadamente complejo, hacia el mes de mayo los criptoanalistas lograron descifrar por completo el valor matemático del código y revelaron la información que contenía.

Según los mensajes interceptados y descodificados, una base americana, con el código AF, iba a convertirse en breve en el objeto del mayor ataque naval hasta el momento. Los analistas estadounidenses se dieron cuenta de que *AF* era una isla del Pacífico (probablemente, la isla Midway), pero no tenían una certeza absoluta de que así fuera. Si los analistas se equivocaban, la armada defendería una isla incorrecta y el enemigo estaría en disposición de atacar el verdadero objetivo indefenso. Pero si eran capaces de concretar qué isla era AF y anticiparse así a la llegada de los japoneses, los norteamericanos podrían concentrar toda su flota y destruir a la fuerza invasora. Todo –la guerra del Pacífico–, dependía de una pieza de información perdida: ¿dónde estaba AF?

El comandante Joseph Rochefort, jefe del centro de criptografía naval de Pearl Harbor, ideó un plan para conseguir la pieza de información que faltaba. Ordenó a la base de Midway que transmitiera un mensaje de petición de socorro falsa. La transmisión decía que la planta de agua de Midway había sufrido desperfectos y que la base estaba a punto de quedarse sin agua potable. Los japoneses, que tenían intervenidas las transmisiones norteamericanas, también escucharon el mensaje. Eso era precisamente lo que Rochefort esperaba que hicieran. Al poco de enviar el mensaje, el Servicio de Inteligencia Naval captó unas señales apenas perceptibles de una transmisión japonesa en las ondas: «AF no tiene suficiente agua». Rochefort había conseguido la última pieza de información: AF era Midway.

La flota naval de los Estados Unidos se reunió para defender la isla. El 4 de junio de 1942, la fuerza invasora del almirante Isoroku Yamamoto se dirigió exactamente hacia donde aguardaba la flota del almirante Chester Nimitz. Durante la batalla, cuatro portaaviones –*Hiryu*, *Soryu*, *Akagi* y *Kaga*– vieron su fin; sin embargo, los Estados Unidos solo perdieron uno. A Japón regresó una flota muy diezmada. Habían perdido la batalla y también la guerra en el Pacífico. La flota japonesa nunca más

amenazó seriamente el territorio americano y los EE.UU. iniciaron el largo y difícil viaje hacia tierras japonesas. Una pieza de información de incalculable valor, el objetivo de la invasión de Yamamoto, se había filtrado a través del sistema de protección de códigos y cifras y había dado una victoria decisiva a los Estados Unidos de América.[1]

La II Guerra Mundial fue la primera guerra de información. Los criptógrafos estadounidenses extrajeron información del JN-25 y de los códigos Púrpura, un cuerpo de elite de criptoanalistas británicos y polacos desentrañaron el (supuestamente) indescifrable código alemán Enigma. Y también fue la información la que permitió a los Estados Unidos vencer al Japón ya que la información de Enigma proporcionó a los aliados el camino para derrotar a los submarinos nazis, que estaban torpedeando a la Gran Bretaña.

Tan pronto como la batalla por la información dejó su huella en la guerra, la guerra dejó la suya en la información. Durante la II Guerra Mundial, la criptografía dejó de ser un arte para convertirse en una ciencia. Los criptoanalistas de aquellas húmedas salas de códigos de Hawai y aquella singular finca de Inglaterra, se convertirían en los heraldos de una revolución bautizada como la teoría de la información.

La criptografía y el criptoanálisis siempre estuvieron relacionados con lo que después se convertiría en la teoría de la información. Sin embargo, durante milenios, criptógrafos y criptoanalistas no tuvieron conciencia de que estaban haciendo incursiones en una nueva disciplina científica. Al fin y al cabo, la encriptación es más antigua que la ciencia. Una y otra vez, desde la antigüedad, los reyes y generales han confiado en la información escondida bajo la frágil seguridad de una cifra o de un mensaje encubierto, torpes intentos para burlar los peligros de la transferencia de información.

1 Irónicamente, Yamamoto moriría tiempo después a causa de una información interceptada por los aliados. En abril de 1943, un grupo de espionaje de transmisiones descubrió en Australia que Yamamoto se dirigía a Nueva Guinea en avión para visitar a las tropas destinadas allí. Un escuadrón de cazas P-38 lo estaba esperando y abatió el avión del almirante cuando sobrevolaba Bougainville, en el Pacífico Sur.

La criptografía nos retrotrae a los albores de la civilización occidental. En el 480 a. C., la Grecia Antigua estaba a punto de ser conquistada por el mucho más poderoso Imperio persa; pero un mensaje secreto, oculto bajo la cera de una tablilla de escritura, le advirtió de la inminente invasión. Alarmados por el mensaje, los griegos se apresturaron a prepararse para la guerra. Los griegos, precavidos, derrotaron clamorosamente a los persas en la batalla de Salamina, acabaron con la amenaza persa y dieron paso a la edad de oro de Grecia. De no haber sido por aquel mensaje oculto, la frágil unión de ciudades-estado griegas no hubieran podido resistir la superioridad de la armada persa; Grecia se hubiera convertido en territorio persa y la civilización occidental hubiera sido muy distinta de la actual.

En ocasiones, un intento fallido en la transmisión de la información también consigue cambiar la historia. Son muchas las cabezas que han literalmente rodado a causa del descubrimiento de algún mensaje secreto o la desencriptación de un código. En 1587, María, la reina de Escocia, acabó ajusticiada por un código falso. María, confinada en la cárcel, estaba preparando una conspiración para asesinar a la reina Isabel y apoderarse del trono de Inglaterra. Como todos los objetos que entraban y salían de la prisión eran objeto de inspección, María recurrió a la criptografía para estar en contacto con sus colaboradores. Ella y el resto de conspiradores idearon un código e intercambiaban pequeños mensajes cifrados en las tapas de los barriles de cerveza. Desgraciadamente para María, Sir Francis Walsingham, un espía inglés, descubrió los mensajes y consiguió descifrarlos llegando incluso a introducir un mensaje falso de María a los conspiradores en el que inducía a los traidores a revelar los nombres de todos los implicados en la intriga. Cuando María fue llevada a juicio por traición, los mensajes constituyeron la primera prueba. Un código descifrado –y dos hachazos– acabaron con su destino.

Los códigos y las cifras presentan numerosas y variadas formas, pero todas persiguen el mismo fin: transportar información de una persona a otra. Pero, al mismo tiempo, tienen que ofrecer seguridad y la capacidad de prevenir que un «escuchador» obtenga la información en caso de que el mensaje sea interceptado.

Durante muchos siglos, los códigos no fueron especialmente seguros. Un criptoanalista inteligente podía desentrañar hasta el código más sofisticado con un poco de concentración; y sin embargo, los monarcas y generales se veían abocados a utilizar estos códigos poco fiables. A menudo, la interceptación o la desencriptación de los mensajes significaba la muerte o la derrota. Enviar mensajes delicados fue siempre peligroso pero un riesgo necesario y una parte importante en los asuntos diplomáticos y bélicos.

No importa cómo engañen los criptógrafos, ya sea con palabras, símbolos, números o códigos; no importa cómo escondan de forma inteligente los mensajes, ya sea en las bocas de los barriles, dentro de calabazas o entre versos: inevitablemente, siempre que la información crucial va de un sitio a otro hay un riesgo de que sea descubierta. Cuando los generales trasladan las tropas, armas y provisiones desde casa al frente hasta que regresan, no cesan de enviar información. Así, la información es cada pedazo tan palpable como el peso de una bala, cada pedazo tan tangible como el alcance de un obús y cada pedazo tan vulnerable como un buque lleno de munición.

Esta propiedad fundamental es lo más difícil de entender acerca de la información: la información es tan real y concreta como la masa, la energía o la temperatura. No podemos ver ninguna de estas propiedades directamente, pero aceptamos su existencia. La información es igual de real. Puede medirse y manipularse de igual forma que el peso de una manzana puede calibrarse con una balanza o redistribuirse con un cuchillo. Esta es la razón por la cual líderes, generales y diplomáticos continúan arriesgándose con cifras poco fiables. La información tiene que pasar del emisor al destinatario como un pedazo de un lingote de oro tiene que viajar desde el Fuerte Knox hasta la Casa de la Moneda. No existe una fórmula mágica para trasmitir la información de manera instantánea, de igual modo que tampoco se puede teletransportar el oro directamente de una cámara acorazada a otra. Incluso el ordenador más potente tiene que encontrar una forma para transferir la información de un lugar a otro –sea a través de una línea telefónica, un cable coaxial o incluso a través del aire en el caso de una conexión inalámbrica–; pero

si queremos enviar información de un ordenador a otro, esta tiene que viajar físicamente entre ambos.

El hecho de que la información de un objeto sea una propiedad concreta y medible como la masa significa que la información puede cambiarse de lugar o robarse al igual que puede ocurrir con la masa. Del mismo modo que si alguien quisiera trasladar el oro de un lugar a otro debería correr el riesgo de topar con salteadores de caminos o ladrones, así un líder que quiera intercambiar información debe correr el riesgo de que esta sea interceptada y descodificada. La información, como el oro, debe trasladarse de modo que no tenga valor para los humanos.

Bajo esta imagen de agentes secretos y espías, los buenos criptógrafos y criptoanalistas son expertos en manipular información. Cuando un criptógrafo diseña un código está intentando asegurarse de que la información pasa del emisor al destinatario sin que nadie más tenga acceso a ella. La información no debe «rezumar» fuera del mensaje encriptado. Y al contrario, un criptoanalista que intercepta un mensaje enemigo está intentando extraer información a partir de una amalgama de letras y símbolos aparentemente sin sentido. Esto solo se consigue cuando el código es imperfecto –si la información «rezuma» a pesar de los esfuerzos del criptógrafo. Pero ni siquiera el mejor de los criptógrafos puede hacer aparecer milagrosamente un mensaje allá donde se requiere; este necesita ser transportado. Y aquí es donde hay más riesgo de que sea descubierto.

Esta idea de que algo tan aparentemente abstracto como la información es, de hecho, mensurable y tangible, es uno de los principios básicos de la teoría de la información. Dicha teoría surgió en los años inmediatos a la Segunda Guerra Mundial, cuando los matemáticos enunciaron una serie de reglas mediante las que definían la información y describían su comportamiento. Esta teoría está revestida de una certeza matemática inusual en el poco sistemático y experimental mundo de la ciencia; sus principios son tan inviolables como las leyes de la termodinámica que pusieron en guardia a los inventores cuando pretendían construir una máquina de movimiento perpetuo. A pesar de que la información ha existido desde hace siglos, no fue hasta la Segunda Guerra Mundial que

los criptógrafos empezaron a ser conscientes de que estaban entrando en los dominios de la teoría de la información.

La ciencia de la criptografía contiene una de las primeras claves sobre la naturaleza de la información. No les contaré ahora la historia completa, pero sí les avanzaré alguna idea de cómo la información es real y mensurable y tiene necesariamente que ser llevada de un lugar a otro como si de un lingote de oro se tratara. Uno de los enemigos de la criptografía –la redundancia–, está íntimamente relacionado con el concepto de información; la comprensión de la redundancia puede ayudarnos a explicar por qué la información puede ser tan perceptible como el átomo de un fragmento de materia.

Cada vez que recibimos un mensaje, incluso uno tan sencillo como «el cielo es azul», tenemos en cuenta las series de palabras y las procesamos para entender el significado del mensaje. Recibimos una serie de marcas en un papel (o de sonidos en el aire) y extraemos el significado codificado en esas marcas. Nuestros cerebros toman ese conjunto básico de líneas y curvas con las que deletreamos «el cielo es azul» y manipulan dichos símbolos hasta comprender que el mensaje es una afirmación sobre el color de la bóveda celeste que vemos. Este proceso, esta extracción de significado de un conjunto de símbolos, es del todo inconsciente. Se trata tan solo de algo para lo que el cerebro humano se ha ido entrenando desde el mismo momento en el que los padres hacen sonidos guturales a los recién nacidos en la cuna. El proceso de tener fluidez en un idioma, en cierto sentido, consiste únicamente en aprender cómo obtener el sentido de los símbolos. Sin embargo, este proceso inconsciente –coger una multitud de símbolos y extraer de ellos un significado– resulta crucial para nuestra habilidad en el uso del lenguaje. Esta es la esencia del concepto de redundancia ya que mediante ella los mensajes se tornan más comprensibles.

La redundancia es una pista adicional existente en una frase o mensaje que permite que su significado sea accesible aunque la forma sea un tanto confusa. Al fin y al cabo, todas y cada una de las frases de una lengua son redundantes. Una frase del inglés –o de cualquier otro idioma–, siempre ofrece más información de la que necesitamos para

descifrarla. Se trata de una redundancia fácil de observar. J-st tr- t- r--d th-s s-nt-nc-. La frase anterior puede resultar confusa al haber eliminado todas las vocales.[2] Sin embargo, es fácil descifrarla y extraer su significado. De hecho, este permanece inalterado aunque se elimine parte del mensaje; esta es la esencia de la redundancia.

Para los humanos, la redundancia es algo positivo porque facilita la comprensión de los mensajes aunque el entorno nos los hagan llegar poco inteligibles. Podemos entender a un amigo que nos habla en un restaurante repleto de gente o por el móvil con interferencias gracias a la redundancia. Esta se convierte en un mecanismo de seguridad al permitir que el mensaje llegue aunque sufra algún daño por ínfimo que sea durante el trayecto. Todas las lenguas tienen incorporadas estas redes de seguridad formadas por modelos y estructuras y conjuntos de normas que las hacen redundantes. Generalmente, no somos conscientes de su existencia, pero nuestro cerebro las usa de forma intuitiva mientras leemos, hablamos, escuchamos y escribimos –cada vez que recibimos un mensaje de alguien en un lenguaje natural. Incluso aunque estas normas no sean obvias, están allí, y podemos sentir su influencia si jugamos un poco con el lenguaje.

Tomemos, por ejemplo, la palabra inventada *fingry*. *Fingry* podría pasar perfectamente por una palabra inglesa. Es más, diríamos que es un adjetivo. («Gee, Bob, your boss looks like he's mighty *fingry* today»). Pero, ¿y si me invento otra palabra como *trzeci?* A diferencia de lo que ocurría con *fingry*, *trzeci* no parece una palabra inglesa en absoluto.[3] El motivo son estas reglas implícitas de las que hablábamos; en este caso, las reglas específicas de la lengua inglesa. La letra *z* se utiliza más bien poco en inglés y nunca sigue a las letras *tr*. Además, es casi imposible que una palabra acabe en *i*, así que *trzeci* no se percibe como una palabra inglesa ya que contraviene las reglas implícitas acerca de las características de los vocablos anglófonos.

2 Por este motivo, algunos centros de formación de taquigrafía publicitan sus cursos con signos que rezan así: «If u cn rd th ad u cn gt btr jb & mo pa.» Nota de la T.: «If you can read this advertisement you can get a better job and be more paid» (Si usted puede leer este anuncio es capaz de tener un buen trabajo y mejor salario).

3 Sin embargo, sería perfectamente válida bajo las normas del polaco. Significa «tercero».

Por otra parte, *fingry*, sigue la estructura correcta de letras y sonidos que le otorgan entidad como expresión auténticamente inglesa y la terminación *–gry* nos recuerda que dicha voz es un adjetivo.

El cerebro humano aprende de forma automática estas reglas y las utiliza para validar los mensajes que recibe. Así es como distinguimos un mensaje con sentido de una retahíla de símbolos o sílabas ininteligibles.

Todos las lenguas tienen reglas que rigen otras reglas que rigen otras reglas. Las reglas de formación de *trzeci* frente a *fingry* operan en el nivel de las letras y los sonidos y determinan cuál es su orden natural. Pero hay cientos de reglas que operan en otros niveles y aunque todas funcionan de manera inconsciente, podemos vislumbrarlas cuando hay algo que no funciona correctamente en un mensaje ya que, de forma automática, encienden la alarma. Por ejemplo, hay reglas que determinan qué palabras deben seguir a otras palabras u oraciones; nuestro cerebro, que monitoriza continuamente las reglas del lenguaje, nos hace saber si el orden de las palabras es el correcto o no. También existen reglas que comprueban el significado de un mensaje mientras lo procesamos. Incluso una frase perfectamente válida puede sonar extraña si no responde a las expectativas de nuestro cerebro. Cuando ocurre esto, una palabra incorrecta destaca como una mosca en la leche.[4]

Estas reglas están por doquier. Nos muestran la diferencia entre un gruñido incomprensible y una consonante con significado, entre una palabra incoherente y una con sentido pleno, o entre una frase estúpida y otra con información relevante. Algunas reglas son válidas para más de una lengua; de hecho, solo hay unos cuantos sonidos que contengan significado en el lenguaje humano. Otras son exclusivas de determinados idiomas: las palabras polacas tienen una apariencia y una fonética muy distinta a las inglesas porque las reglas de las «palabras válidas» son muy distintas. Sin embargo, todas las lenguas disponen de un vasto conjunto de dichas normas y esto es lo que les confiere su estructura y, por ende, su redundancia.

4 Un cliché no es más que una expresión muy manida y, a menudo, altamente redundante. En el momento en que volvemos a colocar las vocales en la frase de la que las habíamos quitado, podemos a menudo insertar la palabra desaparecida si es lo que el doctor...

Cuando en nuestro cerebro se enciende una alarma sobre una regla mal usada, ya sea una palabra que no suena natural en nuestra lengua o una frase en la que hay una palabra incorrecta, nos está diciendo que aquel torrente de letras o sonidos que nos llegan no responde a nuestras expectativas de mensaje aceptable. Hay algo fuera de lugar; algo está desordenado. Si usamos estas reglas y regresamos al principio, nuestro cerebro puede detectar el origen del problema, como por ejemplo, que la palabra esté mal escrita. Sin pérdida de tiempo, nuestro cerebro aplica la regla ortográfica correcta y corrige aquel amasijo incoherente de símbolos. Y nosotros podemos extraer el significado de la frase a pesar del error. Esto no es ni más ni menos que la redundancia en acción.

Asimismo, las reglas nos permiten leer frases sin vocales. Las reglas implícitas de la lengua inglesa nos dicen al instante que «th-s» es, preferentemente *this*, y no *thms* o incluso *thes*. Gracias a ellas, podemos acceder al significado de una frase incluso si la vamos reduciendo... hasta un límite en que no se hayan eliminado demasiados elementos. Porque hay un punto en el que una frase ya no puede ser forzada más allá sin que deje de ser comprensible. Eliminemos más letras de lo debido y nuestra frase dejará de tener significado. Cuando nos desembarazamos de toda la redundancia existente en un grupo de letras, lo que se pierde es el núcleo concreto, tangible, que no se puede comprimir más. En esto consiste la información: es lo central, lo irreducible, lo que subyace en el corazón de cada frase.

Tal vez sea una definición poco elaborada e incompleta pero es exacta. La información y la redundancia son complementarias. Cuando eliminamos la redundancia de una sarta de letras o símbolos, lo que queda es información. Los especialistas en computación son muy conscientes de la existencia de este núcleo irreducible. Ellos mantienen que, cuando escribimos, es importante usar un programa para comprimir los archivos. Estos programas reducen los archivos –como los que contienen el texto de este libro– de forma que ocupan menos espacio en el disco duro o en otros sistemas de almacenamiento similares. Se trata de programas excepcionales pero que no encierran ningún misterio sobre su funcionamiento: trabajan eliminando (casi siempre) toda

la redundancia de un archivo y dejando tan solo lo indispensable. Un programa comercializado de compresión puede coger un archivo de texto y comprimirlo en más de un 60 por ciento. Pero lo que queda es ya irreducible. Si intentamos ejecutar de nuevo el programa no conseguiremos reducir más el archivo. (¡Inténtelo usted mismo!) No podemos minimizarlo más sin perder parte del sentido del mensaje, parte del contenido del archivo de texto. Si alguien intenta vendernos un programa que pueda reducir estos núcleos aún más, tendremos que informar a la policía de un caso de fraude.

Los especialistas en computación no son los únicos que se preocupan por la redundancia. El gran reto de la criptografía es eliminar o enmascarar la redundancia de un mensaje manteniendo la información central. No importa cómo los criptoanalistas o los expertos en computación consigan enmascarar o reducir un mensaje; siempre habrá algo que tenga que viajar desde el emisor al destinatario, ya se transmita por radio, en tablillas de cera o mediante luces en el campanario de la Old North Church. Esta constatación revolucionó el campo de la física. Pero antes, la información y la redundancia ya habían revolucionado el campo de la criptografía y cambiado el curso de la historia del mundo.

Los modernos criptógrafos hablan de su disciplina en términos de información y redundancia. Al fin y al cabo, el objetivo de un criptógrafo consiste en generar un conjunto de símbolos que tenga un significado para el destinatario final. En cierto sentido, el criptógrafo crea un lenguaje artificial. A diferencia de los lenguajes naturales humanos, que están hechos para compartir información de forma libre, los códigos del criptógrafo deben su existencia a la idea de permanecer ocultos a un posible espía. La información del mensaje original permanece en la versión encriptada y, sin embargo, no resulta obvia a quien no sabe cómo descifrarlo. Un buen código protege la información de aquellos que no están autorizados a recibirla. Un mal código deja «rezumar» la información. A menudo, cuando falla un código se debe a una tosca redundancia.

De hecho, si somos aficionados a los códigos ya sabemos todo esto. En las páginas de entretenimiento de algunos periódicos podemos encontrar una especie de puzzles conocidos como criptogramas. A menudo se trata de citas famosas encriptadas de un modo un tanto sencillo: cada letra se ha sustituido por otra letra del alfabeto de tal manera que conforman un amasijo de letras sin sentido. Por ejemplo, podemos ver algo como FUDK DK V NTPVFDOTPM KDIAPT GSHDJX KGUTIT. DF KUSYPH JSF FVWT IYGU FDIT FS ZNTVW DF. Con un poco de práctica, rápidamente podemos descifrar esta especie de puzzle y extraer la información que contiene.

Existen varios procedimientos para descodificar un criptograma y todos ellos explotan las reglas explícitas del inglés. Aunque la información sea confusa, dichas reglas nos permiten imaginar qué dice el mensaje. Una de las reglas dice que si tenemos una letra aislada, seguramente se tratará de una *A* o de una *I*; ninguna letra sola, aparte de estas, constituye per se una palabra correcta. Por tanto, en el criptograma anterior, el símbolo V puede representar cualquiera de estas dos letras. Otra regla afirma que la letra *E* es una de las más habituales en inglés, por lo cual en la frase previamente escrita, el símbolo más frecuente –la T–, probablemente representará la letra *E*. Otras letras, como la *S*, y combinaciones de otras letras, como la *TH*, se usan muy a menudo y suelen aparecer en cualquier frase, mientras que algunas como la *X* o la *KL* son extrañas y pueden no aparecer en un criptograma sencillo. Fijémonos en el criptograma e intentemos trabajar en él un momento y veremos cómo somos capaces de descifrarlo en poco tiempo. Las reglas del inglés nos permiten extraer la información de un mensaje aunque esté oculto. En otras palabras, dichas reglas otorgan redundancia al mensaje y nos facilitan descodificar (romper) el código.[5]

La redundancia, la suma de estos modelos y reglas, es el enemigo de un código seguro; ayuda a que la información se escape y los criptógrafos tienen que llevar a cabo un gran esfuerzo para intentar esconder la redundancia de un mensaje. Es la única forma de que un

5 El criptograma anterior se traduce como: «This is a relatively simple coding scheme. It should not take much time to break it.» Nota de la T.: la frase en inglés se traduce como «Este es un código relativamente sencillo; descifrarlo, no debería llevarle mucho tiempo.»

criptógrafo pueda tener la esperanza de que el nuevo código *pueda* ser seguro. Conocer la relación existente entre la redundancia, la información y la seguridad constituye la piedra angular de la criptografía, pero antes del nacimiento de la teoría de la información nadie poseía un conocimiento exhaustivo de lo que existía en las entrañas de esa relación. Nadie comprendía la naturaleza misma de la información o de la redundancia. Nadie disponía de un método formal para definirlas, medirlas o manipularlas. Como resultado de todo ello, incluso el más sofisticado de los esquemas de codificación de principios del siglo XX resultaba poco seguro. Incluso aquellos que fueron considerados indescifrables.

En febrero de 1918, el inventor alemán Arthur Scherbius registró la patente de una máquina de códigos «indescifrable» que pronto maldeciría todo el mundo: Enigma.

Enigma fue una forma ingeniosa de encriptar un mensaje. Era tan compleja que la mayoría de los criptógrafos y matemáticos contemporáneos pensaron que era casi imposible poder descifrar sus códigos (véase Figura 1).

Máquina de cifrado Enigma
(Figura 1)

La máquina de Scherbius era como una máquina de escribir alucinante. Sin embargo, las teclas no dejaban marcas en el papel sino que, cuando se ponía en marcha aparecían unas luces. Así, si se apretaba la tecla de la letra «A», por ejemplo, se iluminaba la letra de la letra «F»: la letra *A* se codificaba como *F*. Pero si volvíamos a apretar la «A» de nuevo, podía reaparecer como una «S», una «O» o una «P». Cada vez que se pulsaba la letra «A», podía aparecer codificada de formas distintas. El motivo era que el interior de la máquina de Scherbius estaba formado por una serie de rotores. Cada vez que se pulsaba una tecla los rotores giraban, avanzando una posición. Cuando los rotores cambiaban de posición, también lo hacía la encriptación. Cada vez que se pulsaba una tecla aparecía codificada de una forma distinta. Era como si la máquina de cifrado Enigma cambiara los códigos en cada pulsación.

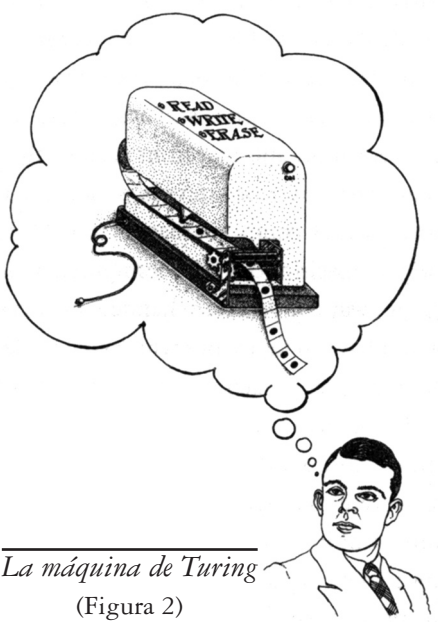
La mayoría de los modelos de Enigma usaban tres rotores, aunque algunos disponían de cuatro; cada uno de los rotores avanza veintiséis posiciones antes de volver a su posición anterior. Podían adoptar innumerables posiciones y también situarse en las ranuras de cualquiera de los tres (o cuatro) rotores. Los cables y clavijas podían intercambiarse al igual que otras piezas. Dicho lo cual, podemos afirmar que una máquina de cifrado Enigma estándar podía configurarse de más de 300 millones de billones de gógoles. Para descifrar un mensaje cifrado con Enigma, uno tiene que haber llegado a la configuración exacta entre las 3 por 10^{114} posibles en las que se encontraba la máquina cuando se empezó a teclear el mensaje.

El esfuerzo es inimaginable; no hay forma de probar a mano todas y cada una de las 3 por 10^{114} configuraciones. Si cada átomo del universo fuera una máquina Enigma y cada uno intentara un millón de billón de combinaciones por segundo desde los inicios del universo hasta la actualidad, solo habrían conseguido probar el 1 por ciento de todas las posibles combinaciones. Era lógico que Enigma tuviera una reputación de indestructible. Por fortuna para la civilización occidental, no lo fue.

Uno de los secretos mejor guardados durante la guerra fue un pequeño cuadro de criptoanalistas en una hacienda victoriana: Bletchley Park en Buckinghamshire, Inglaterra. Winston Churchill llamaría más tarde

a aquel grupo «las gallinas que ponían huevos de oro pero nunca cacareaban». Y Alan Turing fue la más famosa de aquellas gallinas.

Turing nació en Londres en 1912 y se convirtió en uno de los fundadores de la disciplina de la ciencia computacional, un campo que trabaja, dicho sea de forma abstracta, con objetos que manipulan información. Para los matemáticos y los científicos computacionales, una de las contribuciones más valiosas de Turing tiene que ver con una computadora idealizada conocida en la actualidad como máquina de Turing (véase Figura 2), un autómata estúpido que lee sus instrucciones desde una cinta. Esta cinta está dividida en cuadrados que pueden ser blancos o tener una marca escrita. La máquina de Turing es extremadamente sencilla y puede realizar únicamente unas cuantas funciones básicas: leer lo que está en la cinta en una posición determinada, hacer avanzar o retroceder la cinta y escribir o borrar una marca de la cinta. Hacia 1930, Turing y un colega suyo de la Universidad de Princeton, Alonzo Church, demostraron que este robot tan simple era una *computadora universal*: podía llevar a cabo cualquier computación que pueda ser concebida por una computadora, incluso las más modernas supercomputadoras. Esto quiere decir que, en teoría, podemos calcular los algoritmos más complejos, las tareas de computación más enrevesadas, siempre y cuando seamos capaces de leer, escribir o borrar una marca en una cinta y cambiar de lugar la cinta. La idea de una computadora universal sería crucial para el desarrollo de la informática y la teoría de la información, pero no es este el motivo de que Turing sea tan conocido.



La máquina de Turing
(Figura 2)

Turing se hizo famoso por descifrar el código Enigma. Basándose en el trabajo de matemáticos polacos, Turing y sus colegas de Bletchley Park explotaron la redundancia de los mensajes cifrados por Enigma para extraer la información que contenían dichos mensajes. Ciertas imperfecciones del código Enigma habían otorgado redundancia al mensaje cifrado y ayudaron a romper el código. Algunos de estos defectos se debieron a su diseño. Por ejemplo: la máquina de cifrado Enigma nunca dejaba una letra sin mover de modo que una *E* encriptada podía ser cualquier letra *excepto* una *E*, y esto ofrecía una información mínima sobre el mensaje. Otros defectos se debieron al sistema de comunicación de los alemanes. Los criptoanalistas de Bletchley Park fueron capaces de explotar la predictibilidad de los partes meteorológicos cifrados para desvelar el código que escondían. Y, de la misma forma que la predictibilidad del lenguaje, esto constituía una clase de redundancia. Todo ello permitió a Turing y a sus colegas descifrar los mensajes codificados por Enigma con una serie de computadoras muy sencillas, fabricadas expresamente, conocidas como «bombas»[6]. Finalmente, Turing y sus compañeros de Bletchley Park pudieron romper un mensaje de Enigma en cuestión de horas –algo muy lejano de los billones y billones de años que hubiera imaginado un ingenuo análisis de la seguridad del código Enigma. La información se filtraba por el código y los criptoanalistas de Bletchley Park fueron capaces de leerla a pesar de que estaba protegida por Enigma.

Así como la desencriptación de JN-25 cambió el curso de la guerra del Pacífico, la de Enigma cambio la situación de la guerra del Atlántico. En los inicios de la Segunda Guerra Mundial, la flota de submarinos nazis estaba a punto de aniquilar la isla fortaleza, la Gran Bretaña. Años más tarde, el Primer Ministro Winston Churchill escribiría que «lo único que consiguió aterrarme durante toda la guerra fue el peligro de los submarinos nazis». A partir de junio de 1940, durante los llamados «tiempos felices» de la marina

6 Este nombre se debe al espantoso ruido que hacían cuando funcionaban.

nazi, sus submarinos consiguieron enviar al fondo del Atlántico más de medio millón de toneladas de barcos al mes, y casi llegaron a poner a Gran Bretaña de rodillas. Los descrifradores de Enigma invirtieron esta tendencia. En cuanto las comunicaciones de los submarinos nazis comenzaron a encriptar sus comunicaciones con la versión naval de Enigma, los criptoanalistas de Bletchley Park ayudaron a las fuerzas antisubmarinas británicas a perseguir a aquellos submarinos que tanto dolor habían infligido a su nación y ayudaron a ganar la guerra.[7]

La revelación de Enigma fue el último gran esfuerzo de los criptoanalistas antes de que los científicos aprendieran a definir la información, a manipularla y a analizarla. Los criptoanalistas de Bletchley Park, sin ni siquiera tener conciencia de ello, habían estado explotando la irreducible y tangible naturaleza de la información. Habían estado utilizando las redundancias, los algoritmos computacionales y las combinaciones matemáticas para poder llegar al código y extraer la información que había en su interior. En cierto modo, la revelación de Enigma fue la estrella brillante que anunció el nacimiento de la ciencia de la computación y la teoría de la información; y las ideas de Turing ocuparon un lugar importante en ambas.

Desgraciadamente, Turing no tendría un lugar propio en la recién creada Teoría de la ciencia de la información. En 1952, Turing, homosexual, fue condenado culpable de los cargos de «indecencia grave y perversión sexual» por haber mantenido relaciones sexuales con un joven de 19 años. Para evitar la prisión consintió en someterse a un tratamiento con inyecciones de hormonas que, supuestamente, tenían que reducirle la libido. No fue así, y su «inmoralidad manifiesta» fue una mancha que nunca logró borrar. Dos años más tarde, un torturado Turing apareció aparentemente suicidado por ingestión de cianuro.

7 Resulta muy irónico el hecho de que la desencriptación hubiera ayudado a los submarinos nazis tanto como los había perjudicado. Los criptoanalistas alemanes habían roto el código del convoy de los Aliados, lo cual había provocado que la flota nazi enviara toda una manada de lobos de submarinos para interceptarlos.

La tragedia de Turing tuvo lugar en el preciso instante en que los físicos y expertos en computación estaban dispuestos a enfrentarse a la entidad de la información, en el preciso momento en que los científicos veían que este indefinible concepto de la información era capaz de ofrecer la llave para comprender la naturaleza del mundo físico. No fue este el único suicidio que proyectó su sombra sobre la ciencia de la información. De hecho, la tragedia permanecería ligada a las raíces de la teoría de la información, en torno a las primeras investigaciones que sentaron la base de la revolución que estaba a punto de llegar.