Los seres humanos siempre han querido proteger de miradas ajenas el contenido de algunos de los mensajes que se transmiten entre sí. Pero muy pronto resultó evidente el peligro y la insuficiencia que representaba dejar la responsabilidad de mantener tal secreto en manos del mensajero, por fiable que éste pudiera parecer o resultar. El secreto de los mensajes debía residir en el mensaje mismo, y de ahí los diversos sistemas decifrado que, a lo largo de los siglos, han intentado lograr que el contenido real del mensaje transmitido sólo fuera conocido por su verdadero destinatario.

Famoso es el elemental sistema de cifrado que utilizara Julio César hace ya más de 2000 años en algunas de sus comunicaciones a Cicerón y a determinados cónsules. El sistema consistía, simplemente, en substituir cada letra por la tercera que le sigue (de forma cíclica) en el alfabeto. Así JUEZ se cifraría hoy como MXHC. Se trata de un sistema sencillo y claramente vulnerable que, desgraciadamente, hace sumamente fácil la labor del descifrado. Sobre todo hoy, cuando ya tenemos mucha más experiencia en el tema. Es de imaginar que a Julio César pudo servirle...

Fueron precisamente las dos guerras mundiales del siglo XX las que proporcionaron un impulso decisivo a la criptografía y, en especial, a las técnicas criptoanalíticas de descifrado de mensajes. En 1919, el mecánico berlinés Arthur Scherbius construyó la primera versión de ENIGMA, una máquina para crear mensajes encriptados que acabó siendo usada por la marina alemana durante la Segunda Guerra Mundial para, por ejemplo, dar órdenes a los submarinos del Atlántico respecto de los convoyes a atacar. Posiblemente el primer gran reto al que se enfrentó la criptografía moderna.

El ENIGMA parecía una máquina de escribir convencional, pero un conjunto interno de rotores convertía la letra tecleada en la que le correspondía según una determinada codificación. El receptor del mensaje cifrado, si disponía de la misma clave (relacionada con la disposición inicial de esos rotores), obtenía el texto original con su propio ejemplar de la máquina ENIGMA convenientemente configurada.

El matemático británico Alan Mathison Turing fue uno de los primeros grandes especialistas en las labores de descifrado para las cuales, desde 1939, se creó en Bletchley Park un centro específico que llegó a ocupar a casi 6000 personas en el duro trabajo de descifrar los radiogramas alemanes cifrados con el ENIGMA.

Pero ése es sólo el inicio de la criptografía moderna y su compleja base matemática, un saber hoy del todo imprescindible para la seguridad de la nueva sociedad de la información y el uso fiable de la red Internet.

Junto a los problemas básicos de las técnicas criptográficas, hay que considerar también la curiosa mentalidad de quienes atienden con dedicación casi monomaníaca al reto de crear nuevasclaves o de descifrar mensajes creados precisamente para no ser descifrados. Una personalidad sorprendente y un intrincado sistema de motivaciones psicológicas parecen concurrir en quienes se dedican a esa compleja y difícil labor.

Llevar todo ese mundo de matemática, lógica y desafío intelectual al ámbito narrativo es también un descomunal reto que parece haber afrontado con éxito el estadounidense Neal Stephenson con su Criptonomicón (1999), la novela seleccionada como la mejor del año 2000 por los lectores de la influyente revista especializada LOCUS. Se trata de una novela sin igual, que ya ha visto la luz en castellano y que hoy disponemos incluso en edición de bolsillo. Ha sido considerada algo así como el nuevo libro de culto de los hackers, y su autor ha llegado a ser etiquetado como "*el Hemingway de los hackers*" o, mucho más agresivamente y con mayor peso mediático, como el "
Quentin Tarantino de la ciencia-ficción post-ciberpunk
".

Stephenson, conocedor como pocos del mundillo de los hackers y de las complejidades de una futura sociedad informatizada, recurre a una amena prosa cargada del humor más irónico, para ofrecernos al mismo tiempo una divulgación criptográfica brillante y, también, el difícil y ajustado retrato de la mentalidad y las preocupaciones de matemáticos, informáticos, militares y empresarios de alta tecnología involucrados en los sistemas criptográficos. Tal como se ha dicho en Internet, Stephenson convierte la ética hacker en una novela épica a la que ya se han buscado incluso semejanzas estructurales y de personajes con la hoy cinematográfica "*El señor de los Anillos*
" de Tolkien.

En Criptonomicón, Stephenson imagina que, en 1942, Lawrence Pritchard Waterhouse, un genio matemático y capitán de la Marina estadounidense, colabora con Alan Mathison Turing y los especialistas británicos de Betchely Park en el trabajo de descifrar los códigos secretos de las potencias del eje. Paralelamente, aunque sesenta años más tarde, la empresa de su nieto y también brillante cripto-hacker, Randy Waterhouse, proyecta crear, en una isla del sudeste asiático, algo sumamente novedoso llamado "la Cripta", un nuevo paraíso de datos y el mayor exponente de la libertad informática del futuro.

Criptonomicón se traslada también al complejo escenario de la guerra del Pacífico con las aventuras del marine Bobby Shaftoe y su búsqueda de MacArthur. Pero, pensando en los matemáticos, imagino que lo más destacable pueda ser cómo un personaje como Lawrence Waterhouse descubrirá el amor (de una forma, puedo jurarlo, que es sólo caricaturesca y no debe ser vista como la manera cómo todos los matemáticos se enfrentan al fenómeno amoroso...). Sus reflexiones incluyen un imaginativo y sorprendente tratamiento matemático de la cualidad y efectos de las eyaculaciones, lo que resulta ser uno de los puntos más hilarantes y divertidos en el seno de esta compleja y sin par novela.

Si la criptografía puede ser de interés para muchos, lo cierto es que Stephenson la divulga brillantemente al tiempo que disecciona con suma habilidad la mentalidad de algunos personajes tocados por la gracia de la matemática y de la habilidad criptográfica.

Hay en Criptonomicón un tono que exige la atención del lector inteligente (y no me refiero a la presencia esporádica de algunas fórmulas matemáticas que, según se dice, habrían molestado, y mucho, al editor de Stephen Hawking). Se trata de unamuy especial complicidad a la que se presta el personal estilo narrativo de Stephenson, autor dotado de un cuidadoso respeto a la capacidad e inteligencia del lector.

El libro incluye además, como apéndice al final de la novela, un curioso algoritmo de cifrado con un mazo de cartas: el "*Solitario*" creado por Bruce Schneier. Se trata de un algoritmo que, con el nombre de "Pontifex", usa en la novela uno de los personajes emblemáticos de la misma, el misterioso Enoch Root.

El original estadounidense se publicó en 1999 en un sólo volumen, algo que parece que en Europa no resulta conveniente cuando se obtienen, tras la traducción, libros de bastante más de mil páginas. El editor francés, por ejemplo, decidió cortar el libro en tres partes (precisamente, casi a golpes de hacha..., en las páginas 320 y 620 del original) e inventar títulos parciales: "*El código Enigma*", "*La red Kinakuta*" y "*Gólgota* ". En España se usó el mismo "corte" pero se ha optado por otros subtítulos que, a mi entender, reflejan mucho más claramente el tema criptográfico que anuncia el mismo original Criptonomicón (
vid infra
).

¿Y la "alquimia" del título? se preguntarán ustedes. ¿Qué tienen que ver la criptografía, el Criptonomicón y la alquimia?

La respuesta la ha dado el mismo Stephenson escribiendo en la trilogía El ciclo barroco, una curiosa continuación de Criptonomicón que transcurre nada menos que tres siglos antes, en la segunda mitad del siglo XVII, cuando la filosofía natural empezaba a substituir a la alquimia y cuando vivió John Wilkins autor precisamente de un tratado llamado "Criptonomicón". El enlace argumental es la peripecia vital de los antepasados de los protagonistas de Criptonomicón y, sobre todo, el papel que juega el misterioso Enoch Root, un personaje que, como el Gandalf de "*El señor de los Anillos*", parece también resucitar a media novela, al menos en Criptonomicón.

¿Cómo? ¿Porqué? De eso, evidentemente, tendremos que hablar el próximo mes.

Para leer:

Ensayo

- Applied Cryptography*. Bruce Schneier. New York. John Wiley & Sons. 1996.*
- The Codebreakers*. David Kahn. Scribner. 1996.*

Ficción

- *CRIPTONOMICÓN I*: El código Enigma*. Neal Stephenson. Barcelona. Ediciones B. NOVA (núm 148). 2002.*
- *CRIPTONOMICÓN II: El código Pontifex. Neal Stephenson. Barcelona. Ediciones B. NOVA (núm 151). 2002.*
- *CRIPTONOMICÓN II: El código Aretusa. Neal Stephenson. Barcelona. Ediciones B. NOVA (núm 154). 2002.*