LEONARD ADLEMAN, DE LA MATEMÁTICA Y DE LA COMPUTACIÓN

Es uno de los autores del famoso código RSA. Su vida, sin embargo ha sido una búsqueda de la matemática en todos los avatares de la ciencia moderna. Encontró la matemática en la computación y también en problemas actuales de la inmunología y de la genética.

EL INICIO:

El padre de Leonard Adleman era un vendedor, y su madre cajera de un banco. Como cualquier muchacho de San Francisco , tenia poca ambición y era (ver artículo de referencia [1]) "increíblemente ingenuo e inmaduro". Sin embargo, ya en la escuela secundaria, su profesor de inglés le hizo comprender la belleza de las ideas a través de la lectura de Hamlet. Con la impresión de que su maestro le había abierto los ojos "al hecho de que se pueden ver las cosas más profundamente que los aspectos superficiales", se inscribió en la Universidad californiana de Berkeley. Vacilante e indeciso, quiso primero ser químico, antes de volcarse de lleno en la matemática.

Ya había pasado por diferentes expectativas sin estabilizarse en ninguna tarea concreta. Finalmente, después de probar otras opciones, lo único que le quedaría donde podría conseguir algún éxito en un tiempo razonable era la matemática.

Cinco años después se graduó, en 1968, entrando a trabajar como programador de computadores en el Banco de América. Solicitó entrar en la escuela de Medicina, en donde fue aceptado, pero cambió de parecer y nunca se inscribió. En cambio, decidió estudiar ciencias físicas y comenzó a asistir a las clases en la Universidad del Estado de San Francisco, mientras seguía trabajando en el banco. Pero una vez más perdió el interés.

No me gustaba hacer experimentos, solo me gustaba pensar en las cosas.

Adleman volvió nuevamente a Berkeley para hacer un doctorado en informática. Tenía dos motivos, el primero era práctico: "*Pensé que consiguiendo el doctorado potenciaría mucho más mi carrer"..*

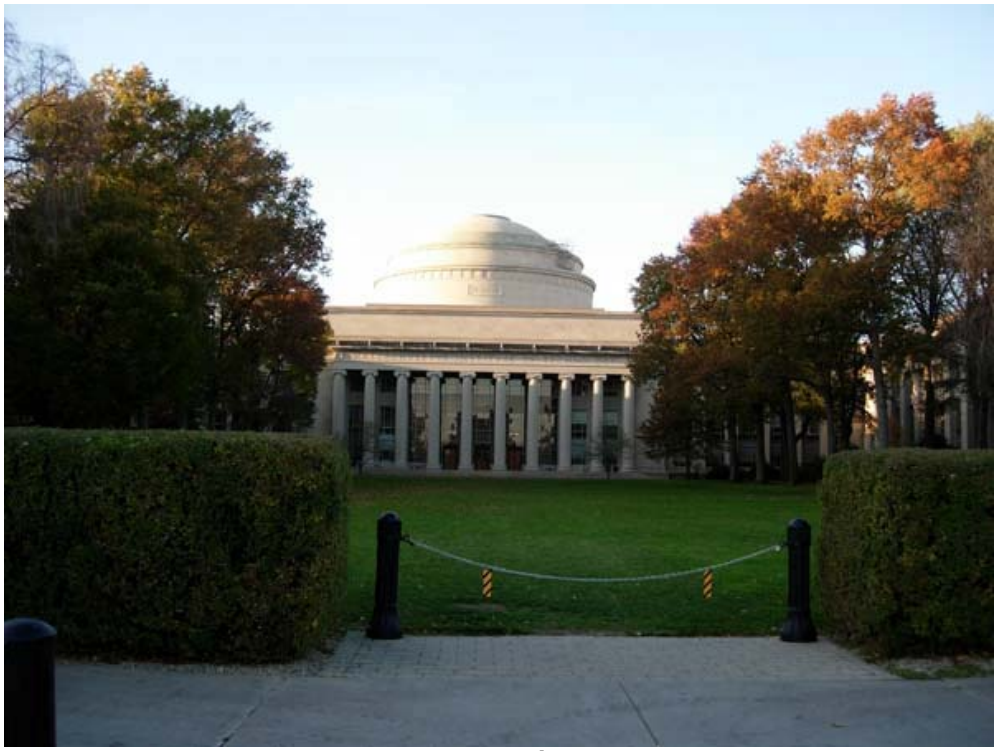
El segundo motivo era más romántico. Martín Gardner había escrito un artículo sobre el Teorema de Gödel en Scientific American que hizo agobiarse a Adleman con sus implicaciones filosóficas profundas. *Pensé: "esto es tan claro", había muchas cosas que yo no encontraba claras, como los agujeros negros, la relatividad general. Pensé que por una vez en mi vida quería entender realmente esos profundos resultados.*

Adleman decide ahora entrar en la escuela de grado en busca de una comprensión del Teorema de Gödel a un nivel más alto que el superficial. Sin embargo, mientras estuvo en la escuela de grado algo importante le influyó –entendió la verdadera naturaleza y la belleza que contenía finalmente la matemática- descubriendo, en particular, que la matemática se relacionaba menos con la contabilidad que con la filosofía. "*La gente piensa en la matemática como algún tipo de arte práctico. Es cuando uno se convierte en matemático cuando de verdad se observa la belleza y el poder de esta disciplina"*.

Completó Adleman su tesis en el año 1976 "Number Theoretic Aspects of Computational Complexities", con lo que recibió el grado de doctor y con ello un puesto asegurado de profesor auxiliar de matemática en el MIT (su padre, sin embargo, le aconsejó que permaneciera en el Banco de América, donde existía un buen plan de jubilaciones).

EL CODIGO RSA:

Uno de los colegas de Adleman en el MIT era Ronald Rivest, que tenía su oficina justo al lado de su despacho. Rivest se sentía muy interesado por un artículo titulado Las transacciones de IEEE en la Teoría de la Información, que habia sido escrito por Martín Hellman, profesor de Informática en Stanford, y su estudiante Whitfield Diffie (ver el artículo de referencia [2]). En dicho artículo habían desarrollado una idea revolucionaria para un nuevo tipo de sistema de encriptación. Estaba basado en presentar distintas "claves" para desencriptar un código determinado, mediante formulas matemáticas descifradoras de mensajes. Hasta entonces, cualquiera que poseyera una clave de encriptación del código también podría desencriptarlo invirtiendo simplemente las instrucciones de encriptación. Lo que Hellman y Diffie propusieron era distinto y novedoso, funcionando la encriptación mediante fórmulas matemáticas fáciles de computar en una dirección, pero imposible de computarlas hacia atrás, salvo que se conozcan los pasos hechos en la encriptación original. La clave de encriptación podría hacerse pública para que cualquiera pudiera enviar un mensaje codificado, pero solo alguien que tuviera conocimiento del proceso de construcción real de la clave podría desencriptar el código y, por tanto, descifrarlo.

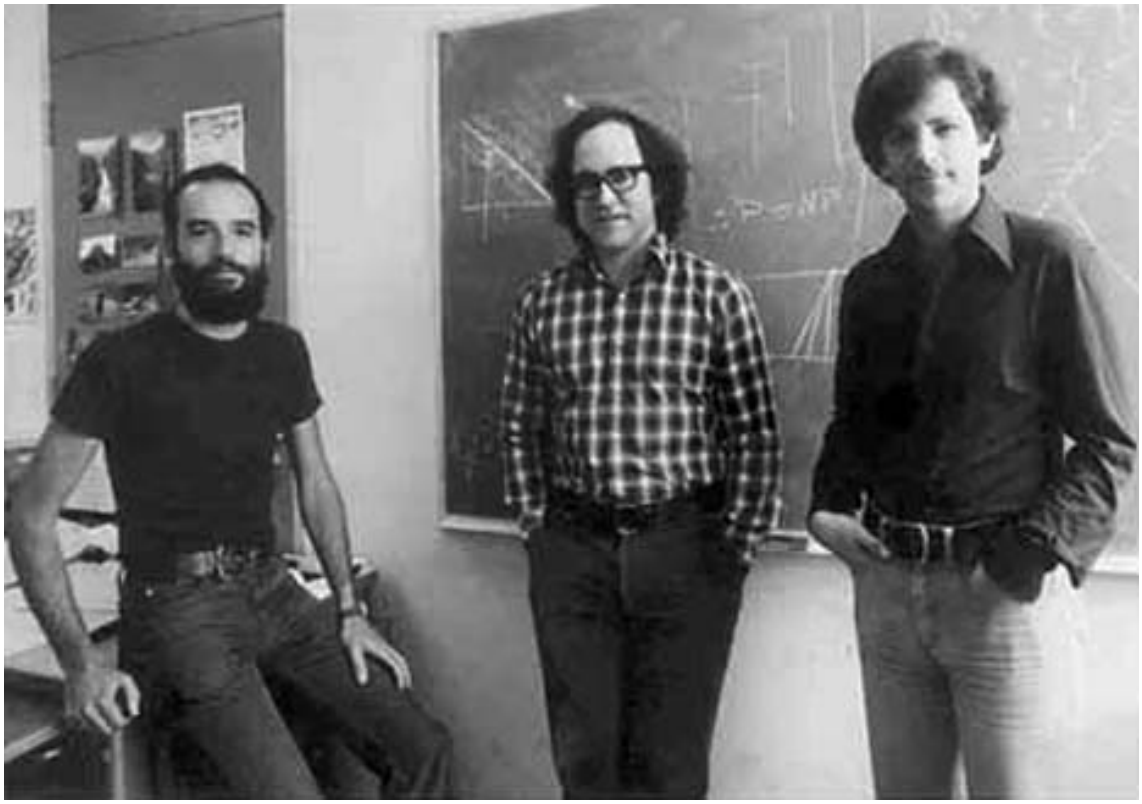


MIT. Instituto de Tecnología de Matshachusets

Rivest anunció que semejante función unidireccional nos llevaría a la creación de un gran sistema de encriptación de clave pública. La propia idea era manifiestamente mejorable, pero encontrar una función solo unidireccional parecía una tarea de una envergadura formidable. Rivest tenía en este asunto un partidario

igualmente entusiasta en uno de sus propios colegas, Adi Shamir. En cambio Adleman parecía bastante menos entusiasmado con el tema, pues la idea le pareció en principio muy poco práctica y consideraba que no valía la pena seguir con ella. Sin embargo, el dúo formado por Rivest y Shamir estaban intentando arduamente inventar alguna codificación de sistema que no se pudiera decodificar, romper.

Convencieron a Adleman para que intentara romper los sistemas de codificación que diseñaban y así comenzaron un trabajo que se mostraría en el futuro de gran importancia. Rivest y Shamir propusieron hasta 42 sistemas de encriptación, que Adleman logró desmontar uno tras otro, hasta que en el número 43, basado en un problema de complicada factorización, Leonard Adleman hubo de confesar que el código era en principio invulnerable debido a la matemática involucrada en su desarrollo, y que podría probablemente tardar siglos de computación en desmontarlo. Una vez conocido esto, Rivest permaneció durante toda una noche escribiendo el manuscrito con el código, antes de mostrarle el desarrollo final a Adleman. Al mencionar los autores del trabajo escribió, por orden alfabético: *Adleman, Rivest, Shamir*. Adleman entonces objetó: *"Deja mi nombre fuera de esto. Es vuestro trabajo, no el mío".* Sin embargo, la opinión de Rivest fue la que prevaleció en el futuro.



Shamir, Rivest y Adleman

Martín Gardner escribió en su columna varios artículos sobre este código, llamado desde entonces *Código RSA*, por los nombres de los autores (ver el artículo de referencia [3]), y con mucho asombro por parte de Adleman, tanto su fama como la del código se extendió con rapidez. Se enviaron numerosas cartas a la Agencia de Seguridad Nacional (National Security Agency (NSA)), la única institución donde el código fue detalladamente analizado, expresándose finalmente el temor de que la publicación de códigos aparentemente irrompibles, como el RSA, pudiera ser un riesgo potencial para la seguridad nacional.

Rivest, Shamir y Adleman obtuvieron la patente para su código en el MIT y en 1983 formaron una compañía, la *RSA Data Security Inc.,* en Redwood, California, construyendo chips de computadoras. Adleman fue el presidente, Rivest presidente ejecutivo y Shamir tesorero. En 1996 vendieron la compañía por 200 millones de dólares.

VUELTA A CALIFORNIA:

El MIT proporcionó a Adleman una estimulante atmósfera intelectual, pero él anhelaba sobre todo California, donde deseaba instalarse y formar una familia. En concordancia con ello obtuvo un trabajo en la Universidad de California del Sur, en Los Angeles, siendo presentado por el profesor de Informática y Biología Molecular Henri Salvatore, en 1980. Tres años después conoció a su futura esposa, Lori Bruce, en un baile. Surgió el amor a primera vista y se casaron a las seis semanas.

Ese mismo año, Adleman junto con R S Rumely y C Pomerance, publica un trabajo describiendo un algoritmo de determinación de factores primos de un número compuesto en un "tiempo cuasi polinomico". Fue el primer resultado de Informática Teórica que se publicaba en Annals of Mathematics (ver artículo de referencia en [4]).

También el mismo año tuvo lugar un descubrimiento que marcaría un hito en la Informática. Fred Cohen, estudiante graduado de la universidad de California del Sur, propuso una nueva idea consistente en un programa que pudiera "infectar" otros programas, modificándolos de forma que aparecieran versiones modificadas de los mismos. Adleman, que era el supervisor de Cohen, se convenció rápidamente de la importancia de la idea, trabajando sobre el tema. Él propuso el nombre ' el virus ' para el programa de Cohen, el cual publicó su primer trabajo en 1984, obteniendo el doctorado con el mismo tema en 1986.

LA MATEMÁTICA DE LA INMUNOLOGIA:

Un hecho importante en la vida de Adleman ocurrió en los primeros años de la década de los 90, cuando dirigió su entusiasmo hacia el campo de la inmunología. Una de las razones de su creciente interés era un tipo de problemas no resuelto en inmunología "que presentaban una inusual belleza a los ojos de los matemáticos" (ver artículo relacionado en [5]). Se preocupó rápidamente por el estudio de los

linfocitos o células blancas de la sangre, también llamadas células T, cuya pérdida en los pacientes de SIDA les dejaba vulnerables a infecciones letales. Las células T son principalmente de dos tipos, CD4 y CD8, y hay aproximadamente 800 células CD4 en cada milímetro cúbico de plasma de sangre de una persona sana o con muy poco tiempo de infección. Este número disminuye gradualmente durante una larga década de latencia, periodo asociado habitualmente al desarrollo del SIDA. Típicamente, cuando el nivel de estas células llega a ser 200 por milímetro cúbico, las infecciones características del SIDA se han manifestado ya. Sin embargo, "perder una célula T no es lo mismo que perder un brazo o una pierna" (ver artículo relacionado en [5]), el cuerpo humano, incluso el de una persona infectada con el VIH, puede regenerar la célula T perdida creando otra nueva. Resultaba, por consiguiente, bastante misterioso que la población de las células CD4 disminuía gradualmente en los pacientes infectados con el VIH.

Adleman y otros sugirieron que el problema se encontraba en el mecanismo homeostático, encargado de supervisar los niveles de células T, sin distinguir entre los tipos CD4 y CD8, sino que regenera el número total de células T. Sin embargo, la creación de células CD8 impide la regeneración total de las células CD4 perdidas, por lo que el VIH continua atacando a las células CD4 y hace bajar su número. Adleman lo indicó con estas palabras: *"el mecanismo homeostático es... ciego".*

Adleman y David Wofsy, de la Universidad de California en S. Francisco, describieron la prueba de esta hipótesis en el número de febrero de 1993 del Journal of Acquired Immune Deficiency Syndromes (JAIDS) (ver artículo relacionado en [6]). Desgraciadamente, las investigaciones sobre el SIDA y la respuesta de la comunidad científica a las ideas de Adleman eran muy desanimadoras. Preocupado por el tema, Adleman decidió adquirir un conocimiento más profundo de la biología del VIH para poder convencer mejor a los demás. Entró en el laboratorio de biología molecular de la Universidad del Sur de California (USC), y comenzó a aprender los métodos de la biología moderna bajo la guía de Nicolás Chelyapov (que en la actualidad es el principal científico en el propio laboratorio de Adleman).

LA COMPUTADORA UNIVERSAL DE ADN:

Fue para Adleman un periodo de aprendizaje muy intenso, cuyos conocimientos previos en biología sufrieron paulatinamente una transformación significativa. El mismo explica el porqué (ver artículo relacionado en [7]): *"La Biología era ahora el estudio de la información que se guardaba en las bases del ADN –los cordones de cuatro letras: A, T, G y C, para la adenina, tiamina, guanina y citosina- y de las transformaciones que la información provoca en las células. ¡Hay mucha matemática aquí!."*

Comenzó leyendo el clásico texto The Molecular Biology of the Gene, uno de cuyos autores es James D. Watson (ver articulo de referencia [13]), famoso como Watson-Crick. Adleman hace una narración del tiempo en el que estudió una enzima muy especial:

Al final del día, mientras leia en la cama el texto de Watson, conocí una descripción de los polímeros del ADN. Es el rey de la enzimas, el fabricante de la vida. Bajo las condiciones apropiadas, desde una cuerda de ADN, el polímero reproduce una segunda cuerda complementaria, la que llamamos Watson-Crick, en la que cada C es reemplazado por un G, cada G por un C, cada A por un T y cada T por un A. Por ejemplo, dada una molécula con la sucesión CATGTC, los polímeros del ADN

producen una nueva molécula con la sucesión GTACAG. Los polímeros permiten al ADN que se reproduzca, con lo cual se reproducen las células y también el mismo polímero se reproduce. Mediante una estricta simplificación puede decirse que la replicación del ADN por los polímeros de ADN establece el proceso por el que se lleva a cabo la vida.

Continúa:

Los polímeros del ADN son pequeñas y asombrosas nanomáquinas. Una sola molécula salta a lo largo de una cuerda de ADN haciendo copias y escribiéndolas en otra cuerda de ADN.

Mientras estudiaba estas enzimas de ADN reparé en su similitud con algo que había sido descrito por el famoso matemático inglés Alan Turing.

De hecho, Adleman pensaba en la Máquina de Turing: *Una versión de la maquina consistía en un par de cintas y un mecanismo finito que leía datos en una de las cintas y escribía en la otra los resultados correspondientes a los datos leídos. El mecanismo era programable con instrucciones muy simples y se podría construir un programa que leyera fácilmente un cordón de ADN, A, T, C, G en la entrada y escribieran un cordón Watson-Crick como rendimiento de salida. La similitud con los polímeros eran obvias.*

Adleman apenas podía contener su excitación:

Esto me hizo sentarme en la cama y comentar a mi esposa Lori: "jo, estas cosas podrían realizar computaciones". Ya no dormí el resto de la noche e intenté deducir una manera de conseguir que el ADN pudiera resolver problemas computacionales.

Decidió construir una computadora de ADN, similar a la máquina de Turing con una enzima reemplazadora del mando de control finito. Una década antes, los investigadores de IBM Charles H. Bennet y Rolf Landauer, habían expuesto ideas esencialmente similares (ver articulo de referencia [8]), pero había serias dudas de que pudieran existir enzimas que no solo produjeran las réplicas Watson-Crick, sino que realizaran también otras funciones matemáticas. Adleman pretendía que su computadora de ADN realizara al menos algo tan interesante como jugar al ajedrez. Con este fin comenzó a aprender las herramientas necesarias de la química del ADN, como polimeros, electrofóresis, síntesis de ADN, etc. El hecho de existir comercialmente el ADN prontamente disponible, con los requisitos específicos le vino perfectamente para sus propósitos.

Es ahora mismo factible escribir en un trozo de papel una sucesión de ADN y enviarlo a una empresa de distribución comercial, recibiendo en unos pocos días un tubo que contiene moléculas de ADN, todas (o la mayoría) con la sucesión descrita. Las moléculas se entregan en un pequeño tubo, apareciendo como un trozo de materia, seco, blanco, amorfo.

Teóricamente se necesitaría solamente dos cosas para construir una computadora capaz de calcular cualquier cosa calculable: un método para almacenar la información y funciones sencillas que actúen operativamente sobre ella. El propio ADN es un almacén de información (pues contiene el genotipo de la vida), y se utilizan enzimas

para operar sobre esta información. Adleman comprendió que esto era suficiente para poder construir una computadora universal.

Leonard Adleman

El siguiente paso en el trabajo que se había impuesto fue elegir algún problema que su computadora pudiese resolver. Eligió el llamado Problema de la Ruta Hamiltoniana:

... dado un gráfico constituido por líneas que conectan a un conjunto de puntos, se dice que hay una ruta hamiltoniana desde el punto A hasta el punto B, si existe un único conjunto de líneas del gráfico que une al punto A con el punto B pasando una sola vez por cada uno de los diferentes puntos del conjunto. El Problema de la Ruta Hamiltoniana consiste en decidir si para un gráfico dado existe o no una ruta hamiltoniana.

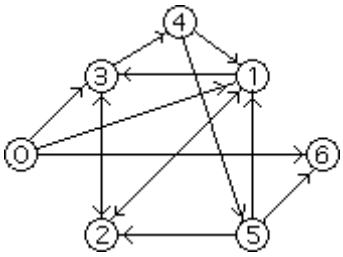
Aunque el Problema de la Ruta Hamiltoniana ha sido estudiado intensamente, todavía está por descubrirse un algoritmo capaz de resolverlo. Durante los primeros años de la década de los 70 no fue posible encontrar ningún algoritmo eficaz, lo que nos demuestra que se trata de un problema aún abierto (de hecho, pertenece a un conjunto más general de problemas llamados "Problemas NP_completos"). Existen, sin embargo, algoritmos que intentan trabajar sobre el problema:

Dado un gráfico G con n vértices, considerando como vértice de salida el u y vértice de llegada el v:

1. *Generar al azar un juego de caminos entre los vértices del gráfico.*
2. *Eliminar cualquier camino que no empieza en u, o bien, no acaba en v.*

3. *Eliminar cualquier camino que no pase por los n vértices.*
4. *Eliminar cualquier camino que no pase por todos los vértices una sola vez.*
5. *Si el gráfico no está vacío, dirá "si". Caso contrario, dirá "no".*

Aunque este algoritmo nos proporciona resultados bastante correctos, se generan al azar gran número de rutas entre los n puntos del problema, y el número de posibilidades de juego son también bastante grandes. Precisamente fue este el algoritmo que Adleman usó en su primer cómputo de ADN. Para el planteamiento de su Problema de la Ruta Hamiltoniana eligió el siguiente gráfico dirigido:



En este gráfico, los puntos de salida y llegada son, respectivamente, los vértices 0 y 6. Adleman asignó primeramente al azar una secuencia de ADN al conjunto de los vértices del gráfico y a los caminos dirigidos (las sucesiones se llaman oligonucleótidos). Puesto que cada sucesión tiene su Watson-C rick complementaria, cada vértices queda asociado con una sucesión complementaria. Una vez fijado un conjunto de codificaciones fijas, se sintetizan automáticamente sucesiones complementarias de ADN tanto para los vértices como para las líneas que les unen. El propio Adleman describe los pasos restantes:

Tomé un puñado (aproximadamente 1014 moléculas) de cada una de las sucesiones diferentes y lo coloqué en el tubo de prueba común. Para comenzar el cómputo simplemente agregué agua –mas la ligasa, sal y otros ingredientes necesarios para obtener las adecuadas condiciones dentro de la célula. En total usé solamente la quinta parte de una cucharilla de solución. En cosa de un segundo tenía en mi mano la respuesta al Problema de la Ruta Hamiltoniana.

Adleman tuvo que realizar un tedioso experimento que consistió en analizar un sistema de más de 100 millones de moléculas que dotaban a los caminos de conexión de código no hamiltoniano. Llevó a cabo el algoritmo descrito antes sobre el significado de que el ADN que permanece en el tubo de prueba después de los pasos precedentes llega necesariamente a obtener el código de la ruta hamiltoniana buscada. Llevó a Adleman siete días en el laboratorio de biología molecular realizar el primer cómputo de ADN del mundo.

Adleman informó de su brillante descubrimiento en el número de noviembre de 1994 de Science (ver articulo de referencia [9]), y se le reconoce ahora como el "padre de la computación ADN". La computación molecular, pues, se establece como uno de los campos más excitantes de la investigación científica contemporánea, dando testimonio otros descubrimientos en los años siguientes al experimento de Adleman. En 1995, Richard J. Lipton en la Universidad de Princeton proponía (ver articulo de referencia [10]), una solución de ADN a otro famoso problema del tipo NP_completo, el llamado SAT (satisfaction). En el año 2002, un equipo de investigación dirigido por Ehud Shapiro del Weizmann Institute de Ciencia en Rehovet, Israel, inventó una máquina de informática molecular compuesta de enzimas y moléculas de ADN que podría realizar

330 millones de funciones por segundo, más de 100000 veces la velocidad del PC más rápido. A los pocos meses, el mismo equipo mejoró el modelo anterior con otro en el que la entrada de ADN es también fuente de combustible para la máquina (ver artículo de referencia [13]). El libro Guinnes reconoció a la computadora como "el dispositivo infirmático" biológico más pequeño construido por el hombre.

Artículos de referencia:

1. G Kolata, 'Hitting the High Spots of Computer Theory: Leonard Adleman', *The New York Times*, December 13, 1994.
2. W Diffie and M Hellman, 'New Directions in Cryptography', *IEEE Transactions on Information Theory*, vol. IT-22, November 1976, pp. 644-654.
3. M Gardner, 'Mathematical Games: A new kind of cipher that would take millions of years to break', *Scientific American*, August 1977, pp. 120-124.
4. L Adleman, R S Rumely, C Pomerance, 'On Distinguishing Prime Numbers from Composite Numbers', *Annals of Mathematics*, **117**, 1983, pp. 173-206.
5. J Rennie, 'Balanced Immunity', *Scientific American*, May 1993, pp. 10-11.
6. L Adleman and David Wofsy, 'T-cell Homeostasis: Implications in HIV', *JAIDS*, 1993, pp. 144-152.
7. L Adleman, 'Computing with DNA', *Scientific American*, August 1998, pp. 34-41.
8. C H Bennet and R Landauer, 'The Fundamental Physical Limits of Computation', *Scientific American*, July 1985, pp. 38-46.
9. L Adleman, 'Molecular Computation of Solutions to Combinatorial Problems', *Science*, **266**, November 11, 1994, pp. 1021-1024.
10. R J Lipton, 'DNA Solution of Hard Computational Problems', *Science*, **268**, April 28 1994, pp. 542-545.
11. S Lovgren, 'Computer Made from DNA and Enzymes', *National Geographic News* (http://news.nationalgeographic.com/news/2003/02), February 24, 2003.
12. E Shapiro, B Gill, R Adar, U Ben-Dor and Y Benenson, 'An Autonomous Molecular Computer for Logical Control of Gene Expression', *Nature*, **429**, pp. 423-429 (Published online on April 28, 2004).
13. J D Watson, N H Hopkins, J W Roberts, J A Steitz, A M Weiner, '*Molecular Biology of the Gene*' (Benjamin/Cummings, Menlo Park, CA, ed. 3, 1987).

El presente artículo es versión traducida de la reseña biográfica de Leonard Adelman que figura en la web de la universidad de St. Andrews, Escocia:

http://www-groups.dcs.st-andrews.ac.uk/~history/Mathematicians/Adleman.html

Carlos S. Chinea

casanchi@teleline.es