Data Encryption Standard

Ir a la navegaciónIr a la búsqueda

Data Encryption Standard (**DES**) es un algoritmo de cifrado, es decir, un método para cifrar información, escogido como un estándar FIPS en los Estados Unidos en 1976, y cuyo uso se ha propagado ampliamente por todo el mundo. El algoritmo fue controvertido al principio, con algunos elementos de diseño clasificados, una longitud de clave relativamente corta, y las continuas sospechas sobre la existencia de alguna puerta trasera para la National Security Agency (NSA). Posteriormente DES fue sometido a un intenso análisis académico y motivó el concepto moderno del cifrado por bloques y su criptoanálisis.

Hoy en día, DES se considera inseguro para muchas aplicaciones. Esto se debe principalmente a que el tamaño de clave de 56 bits es corto; las claves de DES se han roto en menos de 24 horas. Existen también resultados analíticos que demuestran debilidades teóricas en su cifrado, aunque son inviables en la práctica. Se cree que el algoritmo es seguro en la práctica en su variante de Triple DES, aunque existan ataques teóricos.

Desde hace algunos años, el algoritmo ha sido sustituido por el nuevo AES (Advanced Encryption Standard).

En algunas ocasiones, DES es denominado también **DEA** (**Data Encryption Algorithm**).

La historia de DES[editar]

Los orígenes de DES se remontan a principios de los 70. En 1972, tras terminar un estudio sobre las necesidades del gobierno en materia de seguridad informática, la autoridad de estándares estadounidense NBS (National Bureau of Standards), ahora rebautizado NIST (National Institute of Standards and Technology), concluyó en la necesidad de un estándar a nivel gubernamental para cifrar información confidencial. En consecuencia, el 15 de mayo de 1973, tras consultar con la NSA, el NBS solicitó propuestas para un algoritmo que cumpliera rigurosos criterios de diseño. A pesar de todo, ninguna de ellas parecía ser adecuada. Una segunda petición fue realizada el 27 de agosto de 1974. En aquella ocasión, IBM presentó un candidato que fue considerado aceptable, un algoritmo desarrollado durante el periodo 1973–1974 basado en otro anterior, el algoritmo Lucifer de Horst Feistel. El equipo de IBM dedicado al diseño y análisis del algoritmo estaba formado por Feistel, Walter Tuchman, Don Coppersmith, Alan Conheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith, y Bryant Tuckerman.

El papel de la NSA en el diseño[editar]

El 17 de marzo de 1975, la propuesta de DES fue publicada en el Registro Federal. Se solicitaron comentarios por parte del público, y el año siguiente se abrieron dos talleres libres para discutir el estándar propuesto. Hubo algunas críticas desde ciertos sectores, incluyendo a los pioneros de la criptografía asimétrica Martin Hellman y Whitfield Diffie, mencionando la corta longitud de la clave y las misteriosas S-cajas como una evidencia de la inadecuada interferencia de la NSA. La sospecha era que el algoritmo había sido debilitado de manera secreta por la agencia de inteligencia de forma que ellos, y nadie más, pudiesen leer mensajes cifrados fácilmente. Alan Konheim (uno de los diseñadores de DES) comentó en una ocasión "*enviaron las S-cajas a Washington. Cuando volvieron*

eran totalmente diferentes". El Comité de Inteligencia del Senado de los Estados Unidos revisó las acciones de la NSA para determinar si había existido algún comportamiento inadecuado. En el resumen desclasificado sobre sus conclusiones, publicado en 1978, el Comité escribía: "*En el desarrollo de DES, la NSA convenció a IBM de que un tamaño de clave reducido era suficiente; participó de forma indirecta en el desarrollo de las estructuras de las S-cajas; y certificó que, hasta donde ellos conocían, estaban libres de cualquier punto débil matemático o estadístico.*". De todas formas, también concluyó que "*La NSA no ejerció presión en el diseño del algoritmo en modo alguno. IBM inventó y diseñó el algoritmo, tomó todas las decisiones respecto a él, y coincidió en que el tamaño de la clave era más que apropiado para todas las aplicaciones comerciales para las que estaba pensado DES*". Otro miembro del equipo de DES, Walter Tuchman, decía también: "*Desarrollamos todo el algoritmo DES en IBM y con gente de IBM. ¡La NSA no dictó ni un solo paso!*".

Algunas de las sospechas sobre puntos débiles ocultos en las S-cajas fueron descartadas en 1990, con el descubrimiento independiente y la publicación libre por Eli Biham y Adi Shamir del criptoanálisis diferencial, un método general para romper cifrados de bloque. Las S-cajas de DES eran mucho más resistentes al ataque que si hubiesen sido escogidas al azar, lo que sugería que IBM conocía la técnica allá en los 70. Este era de hecho, el caso, en 1994, Don Coppersmith publicó los criterios de diseño originales para las S-cajas. IBM había descubierto el criptoanálisis diferencial en los 70 y, tras asegurar DES, la NSA les ordenó mantener en secreto la técnica. Coppersmith explica: *"Esto era así porque el criptoanálisis diferencial puede ser una herramienta muy potente, contra muchos esquemas diferentes, y había la preocupación de que aquella información en dominio público podía afectar negativamente a la seguridad nacional"*. Shamir también comentó "*Yo diría, al contrario de lo que algunos creen, que no hay evidencias de influencia alguna en el diseño de DES para que su estructura básica esté debilitada.*"

Las otras críticas, sobre que la longitud de clave era demasiado corta, se fundaban en el hecho de que la razón dada por la NSA para reducir la longitud de la clave de 64 bits a 56 era que los 8 bits restantes podían servir como bits de paridad, lo que en cierto modo resultaba sospechoso. Es ampliamente aceptado que la decisión de la NSA estaba motivada por la posibilidad de que ellos podrían llevar a cabo un ataque por fuerza bruta contra una clave de 56 bits varios años antes que el resto del mundo.

El algoritmo como estándar[editar]

A pesar de la polémica, DES fue aprobado como estándar federal en noviembre de 1976, y publicado el 15 de enero de 1977 como **FIPS PUB 46**, autorizado para el uso no clasificado de datos. Fue posteriormente confirmado como estándar en 1983, 1988 (revisado como **FIPS-46-1**), 1993 (**FIPS-46-2**), y de nuevo en 1998 (**FIPS-46-3**), este último definiendo "TripleDES" (véase más abajo). El 26 de mayo de 2002, DES fue finalmente reemplazado por AES (Advanced Encryption Standard), tras una competición pública (véase Proceso de Advanced Encryption Standard). Hasta hoy día (2006), DES continúa siendo ampliamente utilizado.

Otro ataque teórico, el criptoanálisis lineal, fue publicado en 1994, pero fue un ataque por fuerza bruta en 1998 el que demostró que DES podría ser atacado en la práctica, y se destacó la necesidad de un algoritmo de repuesto. Estos y otros métodos de criptoanálisis se comentan con más detalle posteriormente en este artículo.